



Revista Eletrônica
Paulista de Matemática

ISSN 2316-9664

v. 26, 2025.

Iniciação Científica

Isadora Vanzella Picinini

Universidade Tecnológica Federal
do Paraná (UTFPR), Toledo, isado-
ravanzeila@alunos.utfpr.edu.br

Jahina Fagundes de Assis Hattori

Universidade Tecnológica Federal
do Paraná (UTFPR), Toledo

Wilian Francisco de Araújo

Universidade Tecnológica Federal
do Paraná (UTFPR), Toledo

Um estudo sobre a forma canônica de Jordan em espaços vetoriais sobre corpos finitos

A study on the Jordan canonical form in vector spaces over
finite fields

Resumo

Neste trabalho, será apresentada a construção do teorema que fundamenta a existência e unicidade da Forma Canônica de Jordan para uma dada transformação em um espaço vetorial sobre um corpo algebricamente fechado partindo do fato de que, se T é uma transformação linear em um espaço vetorial V de dimensão finita sobre um corpo $\mathbb{K}$ e λ é um autovalor de T , então a restrição de $T - \lambda I_d$ à $\ker(T - \lambda I_d)^j$ (onde j é o menor inteiro tal que $\ker(T - \lambda I_d)^j = \ker(T - \lambda I_d)^{j+1}$) é nilpotente, o que possibilita encontrar conjuntos de vetores $\beta = \{v, (T - \lambda I_d)(v), \dots, (T - \lambda I_d)^{m-1}(v)\}$ de modo que a restrição de $T - \lambda I_d$ ao conjunto gerado por β pode ser representada por uma matriz do tipo $J_m(0)$, e portanto, a restrição de T a $[\beta]$ pode ser representada por $J_m(\lambda_i)$.

Em seguida, será utilizada a Teoria de Corpos para estender tal construção possibilitando sua utilização em espaços vetoriais sobre corpos finitos, uma vez que se $p(x)$ é um polinômio irredutível sobre um corpo $\mathbb{K}$, então $\mathbb{K}[x]/\langle p(x) \rangle$ é um corpo onde $p(x)$ possui raízes.

Palavras-chave: Álgebra linear. Corpos finitos. Formas canônicas.

Abstract

In this work, we will present the construction of the theorem that substantiates the existence of the Jordan Canonical Form for a given linear transformation on a vector space over and algebraically closed field using the fact that, if T is a linear transformation in a finite dimensional vector space V over a field $\mathbb{K}$ and λ is an eigenvalue of T , then the restriction of $T - \lambda I_d$ to $\ker(T - \lambda I_d)^j$ (where j is the smallest integer such that $\ker(T - \lambda I_d)^j = \ker(T - \lambda I_d)^{j+1}$) is nilpotent, which allows us to find a set of vectors $\beta = \{v, (T - \lambda I_d)(v), \dots, (T - \lambda I_d)^{m-1}(v)\}$ such that the restriction of $T - \lambda I_d$ to the set generated by β can be represented by a matrix of the type $J_m(0)$, therefore, the restriction of T to $[\beta]$ can be represented by $J_m(\lambda)$.

Following that, we will use Field Theory to extend such construction in order to allow it to be used in vector spaces over finite fields, since if $p(x)$ is an irreducible polynomial over a field $\mathbb{K}$, then $\mathbb{K}[x]/\langle p(x) \rangle$ is a field where $p(x)$ has roots.

Keywords: Canonical forms. Finite fields. Linear algebra.



1 Introdução

Um dos conteúdos estudados nas disciplinas de Álgebra Linear dos cursos de licenciatura em matemática é a forma diagonal de uma dada transformação linear em um espaço vetorial. No entanto, nem toda matriz é diagonalizável, e, apesar da Forma Canônica de Jordan generalizar a diagonalização de matrizes, é comum que tal conteúdo não seja apresentado. Além disso, é comum trabalhar formas canônicas apenas sobre corpos infinitos e de característica 0, apesar da possibilidade de construir espaços vetoriais sobre corpos finitos.

A utilização de corpos finitos permite uma visão aprofundada da Álgebra Linear, não somente devido ao fato de possibilitar espaços vetoriais finitos, mas devido ao comportamento de tais corpos e suas extensões, dado que certas propriedades dos corpos de característica 0 naturalizadas no estudo da Álgebra Linear não se mantêm ao trabalhar com corpos finitos. Um exemplo disso é que corpos finitos não são algebricamente fechados, o que leva à necessidade de trabalhar com corpos de extensão para garantir autovalores de uma dada transformação, o que não acontece ao se utilizar o corpo dos complexos.

O objetivo deste trabalho é, portanto, estudar a teoria que fundamenta a existência da Forma Canônica de Jordan para transformações em espaços vetoriais sobre corpos algebricamente fechados de característica 0 e, utilizando ferramentas da teoria de corpos, estender este processo para corpos finitos.

2 Forma Canônica de Jordan

Ao longo desta seção, a obra utilizada como fonte principal foi o livro **Um Curso de Álgebra Linear**, de Coelho e Lourenço (1).

2.1 Operadores diagonalizáveis

Seja V um espaço vetorial de dimensão finita sobre um corpo $\mathbb{K}$, $\mathcal{B}$ uma base de V , $T \in \mathcal{L}(V, V)$ um operador linear e $[T]_{\mathcal{B}}$ a matriz de T na base $\mathcal{B}$.

Definição 1 Um *autovalor* de T é um elemento $\lambda \in \mathbb{K}$ tal que existe um vetor não nulo $v \in V$ com $T(v) = \lambda v$.

Proposição 2 λ é um autovalor de T se, e somente se, λ é uma raiz de $\det([xI_d - T]_{\mathcal{B}})$.

Demonstração: Seja $\mathcal{B}$ uma base qualquer de V . Se λ é autovalor de T , então a transformação $\lambda I_d - T$ tem núcleo não trivial, uma vez que existe $v \neq 0$ tal que $T(v) = \lambda v$. Assim, $\lambda I_d - T$ é não injetora e portanto não invertível, de modo que $\det([\lambda I_d - T]_{\mathcal{B}}) = 0$, e, portanto, λ é raiz de $\det([xI_d - T]_{\mathcal{B}})$. A volta é recíproca. □

Definição 3 Se λ é um autovalor de T , então todo vetor não nulo $v \in V$ tal que $T(v) = \lambda v$ é chamado de *autovetor* de T associado a λ . Denotaremos por $\text{Aut}(\lambda)$ o subespaço de V gerado por todos os autovetores associados a λ .

Suponha que $\dim V = n < \infty$. Dizemos que T é **diagonalizável** se existir uma base $\mathcal{B}$ tal que $[T]_{\mathcal{B}}$ é diagonal, o que é equivalente a dizer que existe uma base formada por autovetores de T .

Teorema 4 *Seja $T : V \rightarrow V$ um operador linear onde V é um espaço vetorial sobre $\mathbb{K}$ de dimensão finita e sejam $\lambda_1, \dots, \lambda_t, t > 1$, autovalores de T , dois a dois distintos.*

- i. *Se $v_1 + \dots + v_t = 0$ com $v_i \in \text{Aut}(\lambda_i), i = 1, \dots, t$, então $v_i = 0$ para cada i .*
- ii. *Para cada $i = 1, \dots, t$, seja $\mathcal{B}_i$ um conjunto linearmente independente contido em $\text{Aut}(\lambda_i)$. Então $\mathcal{B}_1 \cup \mathcal{B}_2 \cup \dots \cup \mathcal{B}_t$ é linearmente independente.*

Demonstração:

- i. Demonstraremos por indução em t . Se $t = 1$, o resultado é imediato. Se $t > 1$, suponha que para $j < t$, o resultado vale. Aplicando T na igualdade

$$v_1 + \dots + v_t = 0 \quad (*)$$

temos

$$T(v_1 + \dots + v_t) = \lambda_1 v_1 + \dots + \lambda_t v_t = T(0) = 0. \quad (**)$$

Multiplicando (*) por λ_1 e subtraindo (**), temos

$$(\lambda_1 - \lambda_2)v_2 + \dots + (\lambda_1 - \lambda_t)v_t = 0.$$

Como cada $(\lambda_1 - \lambda_i)v_i \in \text{Aut}(\lambda_i)$, por hipótese de indução, $(\lambda_1 - \lambda_i)v_i = 0$. Como $\lambda_i \neq \lambda_1$ para $i \neq 1$, $v_i = 0$ para $i > 1$. Substituindo em (*), conclui-se que $v_1 = 0$.

- ii. Para cada i , denote por $\mathcal{B}_i$ o conjunto $\{v_{i,1}, \dots, v_{i,n_i}\}$. Assuma que

$$a_{11}v_{11} + \dots + a_{1n_1}v_{1n_1} + \dots + a_{t1}v_{t1} + \dots + a_{tn_t}v_{tn_t} = 0.$$

Como $\sum_{j=1}^{n_i} a_{ij}v_{ij} \in \text{Aut}(\lambda_i)$, pelo item (i), $\sum_{j=1}^{n_i} a_{ij}v_{ij} = 0$ para $i = 1, \dots, t$. Como $\mathcal{B}_i$ é linearmente independente (L.I.), segue que cada $a_{ij} = 0$, portanto, $\mathcal{B}_1 \cup \dots \cup \mathcal{B}_t$ é L.I.

□

Corolário 5 *Se $\lambda_1, \dots, \lambda_t$ são todos os autovalores de T , então T é diagonalizável se, e somente se*

$$\dim V = \sum_{i=1}^t \dim \text{Aut}(\lambda_i).$$

Definição 6 *Sejam V um $\mathbb{K}$ -espaço vetorial de dimensão finita, $T \in \mathcal{L}(V, V)$ um operador linear e $\mathcal{B}$ uma base de V . Chamamos o polinômio $\det([xI_d - T]_{\mathcal{B}})$ de polinômio característico de T e o denotamos por $p_T(x)$.*

Se $\mathcal{B}'$ é uma base qualquer de V e $I_{\mathcal{B}'}^{\mathcal{B}}$, a matriz de mudança de base de $\mathcal{B}$ para $\mathcal{B}'$, tem-se que

$$\begin{aligned} \det([xI_d - T]_{\mathcal{B}'}) &= \det(I_{\mathcal{B}'}^{\mathcal{B}}[xI_d - T]_{\mathcal{B}}(I_{\mathcal{B}'}^{\mathcal{B}})^{-1}) \\ &= \det(I_{\mathcal{B}'}^{\mathcal{B}})\det([xI_d - T]_{\mathcal{B}})\det((I_{\mathcal{B}'}^{\mathcal{B}})^{-1}) \\ &= \det(I_{\mathcal{B}'}^{\mathcal{B}})\det([xI_d - T]_{\mathcal{B}})\det(I_{\mathcal{B}'}^{\mathcal{B}})^{-1} \\ &= \det([xI_d - T]_{\mathcal{B}}), \end{aligned}$$

isto é, a definição do polinômio característico não depende da escolha da base.

Seja λ um autovalor de um operador linear $T : V \rightarrow V$, onde V é um $\mathbb{K}$ -espaço vetorial de dimensão finita e suponhamos que $p_T(x) = (x - \lambda)^m q(x)$, com $q(\lambda) \neq 0$, seja o polinômio característico de T . O número m é chamado de multiplicidade algébrica de λ e o denotamos por $ma(\lambda)$. Chamamos de multiplicidade geométrica de λ a dimensão do subespaço $Aut(\lambda)$ e indicamos tal número por $mg(\lambda)$.

Proposição 7 *Seja λ um autovalor de $T : V \rightarrow V$ onde V é um $\mathbb{K}$ -espaço vetorial de dimensão finita. Então $mg(\lambda) \leq ma(\lambda)$.*

Demonstração: Seja $W = Aut(\lambda)$ e suponha que a dimensão de W seja s . Sejam $\mathcal{B}' = \{w_1, \dots, w_s\}$ uma base para W e $\mathcal{B}$ uma base de V contendo $\mathcal{B}'$. Então a matriz de T na base $\mathcal{B}$ é do tipo

$$\begin{bmatrix} \lambda & 0 & \dots & 0 & & \\ 0 & \lambda & \dots & 0 & & \\ \vdots & \vdots & \ddots & \vdots & & \\ 0 & 0 & \dots & \lambda & & \\ & & & & A_1 & \\ 0 & 0 & \dots & 0 & & \\ & & & & & A_2 \\ 0 & 0 & \dots & 0 & & \end{bmatrix},$$

de modo que

$$p_T(x) = \det(xI_d - [T]_{\mathcal{B}}) = (x - \lambda)^s \det(xI_d - A_2),$$

logo, $s \leq ma(\lambda)$. □

O *polinômio minimal* de um operador linear T em $\mathcal{L}(V, V)$ é o polinômio mônico $m_T(x)$ de menor grau tal que $m_T(T)(v) = 0$ para todo $v \in V$.

Um operador linear $T \in \mathcal{L}(V, V)$ é um zero de seu polinômio característico $p_T(x)$, isto é, $p_T(T) = 0$.

Os polinômios característico e minimal de T tem as mesmas raízes a menos de multiplicidade.

2.2 Subespaços invariantes

Definição 8 *Seja $T : V \rightarrow V$ um operador linear onde V é um $\mathbb{K}$ -espaço vetorial e seja $W \subset V$ um subespaço de V . Dizemos que W é um subespaço T -invariante de V se $T(w) \in W$ para todo $w \in W$.*

Definição 9 *Seja V um espaço vetorial de dimensão finita e $T : V \rightarrow V$ um operador linear. Se $V = W_1 \oplus \dots \oplus W_n$ e cada W_i é T -invariante, então as restrições $T_i = T|_{W_i}$ são operadores lineares de $\mathcal{L}(W_i, W_i)$, e dizemos que T é a soma direta dos operadores T_i , isto é, $T = T_1 \oplus \dots \oplus T_n$.*

Proposição 10 *Se $T = T_1 \oplus T_2$, então $p_T(x) = p_{T_1}(x) \cdot p_{T_2}(x)$.*

Demonstração: Se $T = T_1 \oplus T_2$, então existem $W_1, W_2 \subset V$ invariantes por T tais que $V = W_1 \oplus W_2$. Seja $\mathcal{B}_1$ uma base para W_1 , $\mathcal{B}_2$ uma base para W_2 e $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$. Então

$$[T]_{\mathcal{B}} = \begin{bmatrix} [T_1]_{\mathcal{B}_1} & 0 \\ 0 & [T_2]_{\mathcal{B}_2} \end{bmatrix},$$

onde os zeros indicam matrizes nulas de tamanho apropriado. Logo,

$$p_T(x) = \det(xI_d - [T]_{\mathcal{B}}) = \det(xI_d - [T_1]_{\mathcal{B}_1}) \det(xI_d - [T_2]_{\mathcal{B}_2}) = p_{T_1}(x) \cdot p_{T_2}(x).$$

□

Proposição 11 *W é $(\lambda I_d - T)$ -invariante se, e somente se, W for T -invariante.*

Demonstração: ($\Rightarrow$) Suponha que W é $(\lambda I_d - T)$ -invariante. Então dado $w \in W$, $(\lambda I_d - T)w = w_1$ para algum $w_1 \in W$, de modo que $T(w) = \lambda w - w_1$, que pertence a W . Logo, W é T invariante.

($\Leftarrow$) Suponha que W é T -invariante. Então dado $w \in W$, $T(w) = w_1$ para algum $w_1 \in W$, de modo que $(\lambda I_d - T)(w) = \lambda w - w_1$, que pertence a W . Logo, W é $(\lambda I_d - T)$ -invariante.

□

2.3 Operadores nilpotentes

Definição 12 *Um operador linear $T \in \mathcal{L}(V, V)$ é chamado de nilpotente se existir um $m > 0$ tal que $T^m = 0$. O índice de nilpotência de um tal operador será o menor índice com esta propriedade.*

Proposição 13 *Seja $T : V \rightarrow V$ um operador linear, onde V é um $\mathbb{K}$ -espaço vetorial de dimensão finita. Então, T é a soma direta de um operador nilpotente e um operador invertível.*

Demonstração: Considere a seguinte sequência de subespaços de V :

$$\ker(T) \subseteq \ker(T^2) \subseteq \dots \subseteq \ker(T^k) \subseteq \dots$$

Como V tem dimensão finita, a sequência acima deve estacionar, isto é, existe $m \in \mathbb{N}$ minimal tal que $\ker(T^m) = \ker(T^{m+i})$ para todo $i \geq 1$. Afirmamos que $W_1 = \ker(T^m)$ e $W_2 = \text{Im}(T^m)$ induzem a soma desejada.

De fato, $W_1 \cap W_2 = \{0\}$, uma vez que se houvesse $v \in W_1 \cap W_2$, então $T^m(v) = 0$ e $T^m(v_1) = v$ para algum $v_1 \in V$, de modo que $T^{2m}(v_1) = T^m(v) = 0$, e como $\ker(T^{2m}) = \ker(T^m)$ por hipótese, $v_1 \in \ker(T^m)$, portanto, $v = T^m(v_1) = 0$.

Como T^m é linear e $W_1 \cap W_2 = \{0\}$, pelo teorema da dimensão do núcleo e da imagem,

$$\dim(V) = \dim(W_1 + W_2),$$

logo, $V = W_1 \oplus W_2$.

Considere, então, as restrições $T_1 = T|_{W_1}$ e $T_2 = T|_{W_2}$. Como $T = T_1 \oplus T_2$, resta mostrar que T_1 é nilpotente e T_2 é invertível.

A nilpotência de T_1 é imediata, uma vez que $T_1^m(w) = 0$ para todo $w \in W_1$.

Seja $v \in W_2$. Então $v = T^m(v_1)$, para algum $v_1 \in V$. Se $T_2(v) = 0$, então $T_2(v) = T(v) = T^{m+1}(v_1) = 0$, de modo que $v_1 \in W_1$, e portanto, $v = T^m(v_1) = 0$, ou seja, o núcleo de T_2 contém somente o vetor nulo. Assim, T_2 é injetora e portanto, invertível.

□

Proposição 14 *Seja $T : V \rightarrow V$ um operador linear nilpotente de índice de nilpotência $m \geq 1$, onde V é um $\mathbb{K}$ -espaço vetorial de dimensão finita. Se $v \in V$ é tal que $T^{m-1}(v) \neq 0$, então:*

i. *O conjunto $\{v, T(v), \dots, T^{m-1}(v)\}$ é linearmente independente.*

ii. Existe um subespaço T -invariante W de V tal que $V = U \oplus W$, onde $U = [v, T(v), \dots, T^{m-1}(v)]$

Demonstração:

i. Suponha que o conjunto é linearmente dependente. Então existem $a_0, \dots, a_{m-1}$ não todos nulos tais que

$$a_0 v + \dots + a_{m-1} T^{m-1}(v) = 0.$$

Seja k o menor índice tal que a_k é não nulo. Então

$$T^k(v) = \sum_{i=k+1}^{m-1} \frac{-a_i}{a_k} T^i(v),$$

de modo que

$$T^{m-1}(v) = T^{m-(k+1)}(T^k(v)) = T^{m-(k+1)} \left(\sum_{i=k+1}^{m-1} \frac{-a_i}{a_k} T^i(v) \right) = \sum_{i=k+1}^{m-1} \frac{-a_i}{a_k} T^{m+i-(k+1)}(v) = 0,$$

o que contradiz a hipótese de que $T^{m-1}(v) \neq 0$.

ii. A demonstração será feita por indução no índice de nilpotência de T . Para $m = 1$ é imediato, uma vez que T seria o operador nulo. Suponha que $m > 1$ e que a afirmação seja verdadeira para todo $1 \leq k < m$. Como $Im(T)$ é T -invariante, a restrição de T a $Im(T)$ é nilpotente de índice $m-1$. Considere então o subespaço $U' = U \cap Im(T)$. Então $U' = [T(v), \dots, T^{m-1}(v)]$. Por hipótese de indução, existe um subespaço T -invariante W' de V tal que $Im(T) = U' \oplus W'$.

Construiremos o subespaço W desejado a partir de $W'' = \{w \in V : T(w) \in W'\}$.

Afirmação 1: $V = U + W''$.

De fato, dado $u \in V$, $T(u) \in Im(T) = U' \oplus W'$, de modo que $T(u) = u' + w'$ para algum $u' \in U'$, $w' \in W'$. Como $u \in U'$, devem existir $a_1, \dots, a_{m-1}$ tais que

$$u' = \sum_{i=1}^{m-1} a_i T^i(v) = T \left(\sum_{i=1}^{m-1} a_i T^{i-1}(v) \right).$$

Para $u'' = \sum_{i=1}^{m-1} a_i T^{i-1}(v)$ em U , temos que $T(u'') = u'$ e portanto $T(u) = T(u'') + w'$, de modo que $T(u - u'') = w' \in W'$, logo, $u - u''$ pertence a W'' . Assim, $u = u'' + (u - u'') \in U + W''$, como desejado.

Afirmação 2: $U \cap W' = \{0\}$.

Dado $u \in U \cap W'$, é fácil ver que $T(u)$ pertence a $U' = U \cap Im(T)$ e a W' , uma vez que ambos U e W' são T -invariantes. Como $Im(T) = U' \oplus W'$, $T(u) = 0$.

Por outro lado, como $u \in U$, existem escalares $a_0, \dots, a_{m-1}$ tais que $u = \sum_{i=0}^{m-1} a_i T^i(v)$, logo,

$$0 = T(u) = T \left(\sum_{i=0}^{m-1} a_i T^i(v) \right) = \sum_{i=0}^{m-1} a_i T^{i+1}(v) = \sum_{i=0}^{m-2} a_i T^{i+1}(v).$$

Como $\{T(v), \dots, T^{m-1}(v)\}$ é linearmente independente, $a_0 = \dots = a_{m-2} = 0$, de modo que $u = a_{m-1}T^{m-1}(v) \in U'$. Logo, $u \in U' \cap W' = \{0\}$, portanto, $U \cap W' = \{0\}$, como queríamos.

Desta afirmação 2, segue imediatamente que a intersecção entre $U \cap W''$ e W' é $\{0\}$, e como ambos estão contidos em W'' , segue que existe $\overline{W}$ tal que

$$W'' = \overline{W} \oplus W' \oplus (U \cap W'').$$

Afirmação 3: $W = \overline{W} \oplus W'$ é o subespaço desejado.

De fato, como $W \subseteq W''$ e $W \cap (U \cap W'') = \{0\}$, segue que $U \cap W = \{0\}$. Por outro lado, da afirmação 1, segue que

$$\dim(V) = \dim(U) + \dim(W'') - \dim(U \cap W''),$$

mas,

$$\dim(W'') - \dim(U \cap W'') = \dim(W)$$

e portanto,

$$\dim(V) = \dim(U) + \dim(W),$$

de modo que $V = U \oplus W$.

Resta mostrar que W é T -invariante. De fato, como $W \subseteq W''$, tem-se que $T(W) \subseteq W' \subseteq W$.

□

Proposição 15 *Seja $T : V \rightarrow V$ um operador linear nilpotente com índice de nilpotência $m \geq 1$, onde V é um $\mathbb{K}$ -espaço vetorial de dimensão finita. Então existem números positivos $t, m_1, \dots, m_t$ e vetores $v_1, \dots, v_t \in V$ tais que:*

- i. $m = m_1 \geq m_2 \geq \dots \geq m_t$;
- ii. O conjunto $\mathcal{B} = \{v_1, T(v_1), \dots, T^{m_1-1}(v_1), \dots, v_t, T(v_t), \dots, T^{m_t-1}(v_t)\}$ é uma base de V ;
- iii. $T^{m_i}(v_i) = 0$, para cada $i = 1, \dots, t$.

Demonstração: Como T é nilpotente de índice m , existe $v \in V$ tal que $T^{m-1}(v) \neq 0$, e portanto, $\mathcal{B}_1 = \{v, T(v), \dots, T^{m-1}(v)\}$ é linearmente independente e $V = W_1 \oplus W'_2$, onde W_1 é o subespaço gerado por $\mathcal{B}_1$ e W'_2 é T -invariante. Tome $m_1 = m$. A restrição T_2 de T a W'_2 também deve ser nilpotente, com índice $m_2 \leq m_1$. De maneira análoga, existe $v_2 \in W'_2$ tal que $\mathcal{B}_2 = \{v_2, T(v_2), \dots, T^{m_2-1}(v_2)\}$ é linearmente independente e $W'_2 = W_2 \oplus W'_3$, com W_2 gerado por $\mathcal{B}_2$ e W'_3 T -invariante. Repetindo-se o argumento, obtêm-se os valores $m_1, \dots, m_t$ desejados, com

$$\mathcal{B} = \bigcup_{i=1}^t \mathcal{B}_i.$$

□

Note que, para uma transformação linear T como descrita acima terá como matriz associada

$$[T]_{\mathcal{B}} = \begin{bmatrix} J_{m_1}(0) & 0 & \dots & 0 \\ 0 & J_{m_2}(0) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_{m_t}(0) \end{bmatrix},$$

onde $J_{m_i}(0)$ é um bloco de Jordan de tamanho $m_i \times m_i$ e diagonal nula, isto é,

$$J_{m_i}(0) = \begin{bmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix}$$

Teorema 16 (Forma Canônica de Jordan) *Seja $T : V \rightarrow V$ um operador linear, onde V é um espaço vetorial de dimensão finita sobre $\mathbb{K}$ tal que $p_T(x) = (x - \lambda_1)^{m_1} \dots (x - \lambda_r)^{m_r}$, $m_i \geq 1$ e $\lambda_i \neq \lambda_j$, se $i \neq j$. Então $V = U_1 \oplus \dots \oplus U_r$, onde, para cada $i = 1, \dots, r$, temos:*

- i. $\dim U_i = m_i$;
- ii. O subespaço U_i é T -invariante;
- iii. A restrição do operador $\lambda_i I_d - T$ a U_i é nilpotente.

Demonstração: Para cada $i = 1, \dots, r$, considere $T_i : V \rightarrow V$ definida por $T_i = \lambda_i I_d - T$. Tomando U_i como $\ker(T_i^k)$, onde k é o menor inteiro positivo tal que $\ker(T_i^{k+1}) = \ker(T_i^k)$, tem-se que a restrição de T_i a U_i é nilpotente. Pela proposição 14, existe W'_i T -invariante tal que $V = U_i \oplus W'_i$. Como U_i e W'_i são T -invariantes, então são T_i -invariantes.

Sejam T' e T'' as restrições de T a U_i e W'_i , respectivamente. Então $p_T(x) = p_{T'}(x)p_{T''}(x)$. Como λ_i é o único autovalor de T' e não é autovalor de T'' , conclui-se que $p_{T'}(x) = (x - \lambda_i)^{m_i}$, de modo que $\dim(U_i) = m_i$ e a intersecção de U_i com $(U_1 + \dots + U_{i-1} + U_{i+1} + \dots + U_r)$ é $\{0\}$.

Como $\dim(V) = \sum_{i=1}^r \dim(U_i)$, conclui-se que $V = U_1 \oplus \dots \oplus U_r$, como queríamos.

□

Note que, utilizando o teorema antes, para cada $T - \lambda_i I_d$, como a restrição ao autoespaço gerado por λ_i é nilpotente, é possível encontrar conjuntos $\mathcal{B}_j$ como na proposição 15 de modo que a matriz de $T - \lambda_i I_d$, restrita ao conjunto gerado por $\mathcal{B}_j$, é

$$\begin{bmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix},$$

e portanto, a restrição de T ao mesmo conjunto tem como matriz associada,

$$\begin{bmatrix} \lambda_i & 0 & \dots & 0 & 0 \\ 1 & \lambda_i & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & \lambda_i \end{bmatrix},$$

de modo que é possível encontrar uma base $\mathcal{B}$ de V onde $[T]_{\mathcal{B}}$ é uma matriz diagonal em blocos onde cada bloco é como descrito acima.

3 Espaços vetoriais sobre corpos finitos

Na seção anterior, para construir a Forma Canônica de Jordan, foram feitas suposições de forma implícita, como, por exemplo, a de que o corpo em que se trabalha é algebricamente fechado, uma vez que supõe-se que o polinômio característico de uma dada transformação pode ser fatorado em termos lineares. No entanto, é possível construir espaços vetoriais sobre corpos finitos, que não são algebricamente fechados (o que será demonstrado posteriormente). Neste caso, uma transformação linear pode não ter autovalores no corpo sobre o qual se define o espaço vetorial.

Um exemplo (não finito) é o caso do espaço $\mathbb{R}^2$ sobre o corpo $\mathbb{R}$ e transformações associadas a rotações, cujos autovalores não estão no corpo dos reais. Para resolver este problema, normalmente consideram-se as raízes complexas da transformação e encontra-se uma forma diagonal sobre o espaço $\mathbb{C}^2$ sobre o corpo $\mathbb{C}$. Para um dado espaço vetorial sobre um corpo finito, é possível resolver este problema de maneira análoga.

Ao longo desta seção, as obras utilizadas como fonte principal foram os livros **Contemporary abstract algebra**, de Gallian (3) e **Exemplos de álgebra linear sobre corpos**, de Shokranian (5).

3.1 Corpos finitos

Alguns dos corpos mais conhecidos e estudados são os racionais, os reais e os complexos, que são corpos infinitos. No entanto, existem corpos que tem uma quantidade finita de elementos, como $\mathbb{Z}_p$ (onde p é um inteiro primo). Nesta seção, será discutida a existência de corpos finitos com um dado número de elementos.

Teorema 17 *Todo corpo finito possui p^k elementos, onde p é um número primo e k um inteiro natural.*

Demonstração: Seja $\mathbb{F}_q$ um corpo finito com q elementos e característica p (isto é, p é o menor inteiro positivo que satisfaz $p \cdot 1_{\mathbb{F}_q} = 0_{\mathbb{F}_q}$) e considere a função $f : \mathbb{Z} \rightarrow \mathbb{F}_q$ dada por $f(x) = x \cdot 1_{\mathbb{F}_q}$. É fácil ver que f é um homomorfismo. Note que, como o núcleo de f é o ideal gerado por p , pelo Teorema do Homomorfismo, $\mathbb{Z}/p\mathbb{Z}$ é isomorfo à imagem de f , que é um subconjunto de $\mathbb{F}_q$. Portanto, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ é um subcorpo de $\mathbb{F}_q$, e assim, $\mathbb{F}_q$ pode ser visto como um espaço vetorial sobre $\mathbb{F}_p$.

Como $\mathbb{F}_q$ é finito, sua dimensão também deve ser finita. Portanto, seja $\dim_{\mathbb{F}_p} \mathbb{F}_q = k$ para algum inteiro k . Então existem $\{a_1, \dots, a_k\} \in \mathbb{F}_q$ tais que todo elemento de $\mathbb{F}_q$ pode ser escrito de forma única como uma combinação linear de $a_1, \dots, a_k$ com coeficientes em $\mathbb{F}_p$, e portanto, existem p^k elementos em $\mathbb{F}_q$. □

Um resultado importante é que $\mathbb{F}_q^*$ é um grupo cíclico. Para demonstrar tal proposição, faz-se necessário o seguinte lema:

Lema 18 *Seja G um grupo finito de ordem m com elemento neutro 1 . Suponhamos que para todo divisor d de m , o subconjunto*

$$E_d = \{x \in G : x^d = 1\}$$

possui d elementos. Então G é cíclico.

Demonstração: Seja O_d o subconjunto de elementos de ordem d de E_d . Se O_m é não vazio, então existe um elemento de ordem m em G e portanto, G é cíclico. Assim, basta mostrar que $|O_m| \geq 1$.

Para cada d divisor de m , se $|O_d| \neq 0$ e $x \in O_d$, então $x \in E_d$, de modo que o subgrupo gerado por x (denotado $\langle x \rangle$) é um subgrupo de E_d , uma vez que, para todo $0 \leq i \leq d-1$, $(x^i)^d = (x^d)^i = 1$. No entanto, $|E_d| = d = |\langle x \rangle|$, de modo que $\langle x \rangle = E_d$. Logo, E_d é cíclico de ordem d e tem $\varphi(d)$ geradores (onde φ é a função totiente de Euler) e assim, $|O_d| = \varphi(d)$.

Por outro lado, como consequência do Teorema de Lagrange (ver (2), pg. 195), temos que G é a união disjunta de cada O_d , de modo que $m = \sum_{d|m} |O_d|$. Pela fórmula de Gauss (ver (5), pg. 26),

$m = \sum_{d|m} \varphi(d)$, de modo que $|O_d|$ deve necessariamente ser $\varphi(d)$. Em particular, $|O_m| = \varphi(m) \geq 1$, logo, G é cíclico. □

Teorema 19 $\mathbb{F}_q^*$ é um grupo cíclico com $q-1$ elementos. Ele possui $\varphi(q-1)$ geradores.

Demonstração: Como $\mathbb{F}_q$ é um corpo, $\mathbb{F}_q^*$ é um grupo multiplicativo. Considere, portanto, um subgrupo G de ordem m de $\mathbb{F}_q^*$. Como o polinômio $x^m - 1$ possui exatamente m raízes no corpo, nenhuma repetida (pois sua derivada não se anula em $\mathbb{F}_q^*$), pelo lema anterior, $\mathbb{F}_q^*$ é cíclico e tem $\varphi(q-1)$ geradores. □

Definição 20 Seja $\mathbb{K}$ um corpo com característica p (primo). A função $\mathcal{F} : \mathbb{K} \rightarrow \mathbb{K}$, definida por

$$\mathcal{F}(x) = x^p,$$

é chamada de **homomorfismo de Frobenius**.

Proposição 21 A função $\mathcal{F}$ é um homomorfismo entre corpos.

Demonstração: Decorre do fato de que se p é um inteiro primo e $1 \leq n \leq p-1$, então p divide $\binom{p}{n}$.

$$\mathcal{F}(xy) = (xy)^p = x^p y^p = \mathcal{F}(x)\mathcal{F}(y)$$

$$\mathcal{F}(x+y) = (x+y)^p = \sum_{n=0}^p \binom{p}{n} x^{p-n} y^n = x^p + y^p = \mathcal{F}(x) + \mathcal{F}(y).$$

□

Definição 22 (Corpo perfeito) Um corpo $\mathbb{F}$ é dito perfeito se $\mathbb{F}$ tem característica 0 ou se $\mathbb{F}$ tem característica p e $\mathbb{F}^p = \{a^p : a \in \mathbb{F}\} = \mathbb{F}$.

Teorema 23 Todo corpo finito é perfeito.

Demonstração: Decorre do Teorema 3.1, uma vez que, como todo homomorfismo de corpos não trivial é injetor e $\mathcal{F}(1) = 1$, $\mathcal{F}$ é injetor. Se $\mathbb{K}$ é um corpo finito, $\mathcal{F}$ também será sobrejetor. Assim, $\mathcal{F}$ é um automorfismo de $\mathbb{K}$, de modo que $\mathbb{K}^p = \mathbb{K}$ e $\mathbb{K}$ é um corpo perfeito. □

3.2 Adjunção de Raízes em corpos finitos

Como discutido anteriormente, o problema dos corpos finitos no que diz respeito à Forma Canônica de Jordan é o fato de não ser possível garantir a existência de autovalores de uma dada transformação, uma vez que nem todo polinômio com coeficientes em um corpo finito terá raízes no corpo.

Teorema 24 *Nenhum corpo finito é algebricamente fechado.*

Demonstração: Seja $\mathbb{K}$ um corpo finito tal que $\mathbb{K} = \{\alpha_1, \dots, \alpha_n\}$. Considere o polinômio $p(x) = (x - \alpha_1) \dots (x - \alpha_n) + 1 \in \mathbb{K}[x]$. É fácil ver que $p(x)$ não possui raízes em $\mathbb{K}$, portanto, $\mathbb{K}$ não é algebricamente fechado. □

No entanto, dado um corpo $\mathbb{F}$, é possível estender $\mathbb{F}$ de modo a obter um corpo que contenha $\mathbb{F}$ e as raízes de um dado polinômio irreduzível. Nesta seção, será discutida tal construção.

Definição 25 (Corpo de extensão) *Um corpo $\mathbb{E}$ é dito corpo de extensão de um corpo $\mathbb{F}$ se $\mathbb{F} \subset \mathbb{E}$ e as operações de $\mathbb{F}$ são as operações de $\mathbb{E}$ restritas a $\mathbb{F}$.*

Teorema 26 (Kronecker) *Seja $\mathbb{F}$ um corpo e $f(x)$ um polinômio não-constante de $\mathbb{F}[x]$. Então existe um corpo de extensão de $\mathbb{F}$ onde $f(x)$ possui uma raiz.*

Demonstração: Como $\mathbb{F}[x]$ é um domínio de fatoração única, então existe $p(x) \in \mathbb{F}[x]$ irreduzível sem raízes em $\mathbb{F}$ tal que $f(x) = q(x)p(x)$, para algum $q(x) \in \mathbb{F}[x]$, de forma que é suficiente encontrar um corpo de extensão onde $p(x)$ tenha raiz.

Afirmamos que $\mathbb{E} = \mathbb{F}[x]/\langle p(x) \rangle$ satisfaz a condição indicada. Como $p(x)$ é irreduzível, $\langle p(x) \rangle$ é maximal e $\mathbb{E}$ é um corpo. Além disso, como $\phi : \mathbb{F} \rightarrow \mathbb{E}$, onde $\phi(a) = a + \langle p(x) \rangle$ é um homomorfismo injetor, $\mathbb{E}$ possui um subcorpo isomorfo a $\mathbb{F}$.

Para mostrar que $p(x)$ possui raiz em $\mathbb{E}$, escreva $p(x) = a_0 + a_1x + \dots + a_nx^n$, com $a_i \in \mathbb{F}$, e note que

$$\begin{aligned} p(x + \langle p(x) \rangle) &= a_0 + a_1(x + \langle p(x) \rangle) + \dots + a_n(x + \langle p(x) \rangle)^n \\ &= a_0 + a_1x + \dots + a_nx^n + \langle p(x) \rangle \\ &= p(x) + \langle p(x) \rangle \\ &= 0 + \langle p(x) \rangle \end{aligned}$$

Assim, $\mathbb{E}$ é um corpo de extensão de $\mathbb{F}$, e $x + \langle p(x) \rangle \in \mathbb{E} = \mathbb{F}[x]/\langle p(x) \rangle$ é uma raiz de $p(x)$ e, portanto, de $f(x)$. □

Um exemplo da aplicação deste teorema é a construção dos números complexos como corpo de extensão dos reais. Considere, portanto, $\mathbb{F} = \mathbb{R}$ e $f(x) = x^2 + 1$. Em $\mathbb{R}[x]/\langle x^2 + 1 \rangle$, $x + \langle x^2 + 1 \rangle$ é raiz de $f(x)$, uma vez que,

$$\begin{aligned} f(x + \langle x^2 + 1 \rangle) &= (x + \langle x^2 + 1 \rangle)^2 + 1 \\ &= x^2 + \langle x^2 + 1 \rangle + 1 \\ &= 0 + \langle x^2 + 1 \rangle \end{aligned}$$

Para mostrar que $\mathbb{E} = \mathbb{R}/\langle x^2 + 1 \rangle$ é isomorfo ao corpo dos complexos, nota-se, inicialmente, que todo elemento de $\mathbb{E}$ é do tipo $p(x) + \langle x^2 + 1 \rangle$, onde $p(x) = 0$ ou o grau de p , denotado $\text{gr}(p)$ (aqui gr denota o grau do polinômio p), é tal que $\text{gr}(p) \leq 1$. De fato, seja $a(x) \in \mathbb{R}[x]$. Realizando a divisão por $x^2 + 1$, encontram-se polinômios $q(x), r(x)$, com $r(x) = 0$ ou $\text{gr}(r) < \text{gr}(x^2 + 1) = 2$, tal que $a(x) = q(x)(x^2 + 1) + r(x)$, de forma que $a(x) - r(x) \in \langle x^2 + 1 \rangle$ implica que $a(x) + \langle x^2 + 1 \rangle = r(x) + \langle x^2 + 1 \rangle$.

Desta forma, considere a aplicação $\phi : \mathbb{E} \rightarrow \mathbb{C}$ definida por $\phi(a + bx + \langle x^2 + 1 \rangle) = a + bi$ e sejam $r = a + bx + \langle x^2 + 1 \rangle, s = c + dx + \langle x^2 + 1 \rangle$.

$$\begin{aligned}\phi(r + s) &= \phi((a + bx + \langle x^2 + 1 \rangle) + (c + dx + \langle x^2 + 1 \rangle)) \\ &= \phi((a + c) + (b + d)x + \langle x^2 + 1 \rangle) \\ &= (a + c) + (b + d)i \\ &= a + bi + c + di \\ &= \phi(a + bx + \langle x^2 + 1 \rangle) + \phi(c + dx + \langle x^2 + 1 \rangle) \\ &= \phi(r) + \phi(s)\end{aligned}$$

$$\begin{aligned}\phi(rs) &= \phi((a + bx + \langle x^2 + 1 \rangle)(c + dx + \langle x^2 + 1 \rangle)) \\ &= \phi((a + bx)(c + dx) + \langle x^2 + 1 \rangle) \\ &= \phi(ac + (ad + bc)x + bdx^2 + \langle x^2 + 1 \rangle) \\ &= \phi(ac - bd + (ad + bc)x + bd(x^2 + 1) + \langle x^2 + 1 \rangle) \\ &= \phi((ac - bd) + (ad + bc)x + \langle x^2 + 1 \rangle) \\ &= ac - bd + (ad + bc)i \\ &= (a + bi)(c + di) \\ &= \phi(r)\phi(s)\end{aligned}$$

Como $\ker(\phi) = \{a + bx + \langle x^2 + 1 \rangle \in \mathbb{E} : a + bi = 0\} = \{0\}$, ϕ é injetora e, dado um complexo $a + bi$, existe $a + bx + \langle x^2 + 1 \rangle \in \mathbb{E}$ tal que $\phi(a + bx + \langle x^2 + 1 \rangle) = a + bi$, logo ϕ é sobrejetora, e portanto, um isomorfismo.

Anteriormente, construiu-se o corpo dos complexos a partir do corpo dos reais e um polinômio irreduzível em $\mathbb{R}$. No entanto, apesar de $f(x) = x^2 + 1$ também ser irreduzível em $\mathbb{Q}$, existe um corpo, menor que os complexos, que contém $\mathbb{Q}$ e uma raiz de $f(x)$. Tal corpo, $\mathbb{Q}[x]/\langle f(x) \rangle$, é isomorfo ao conjunto $\{a + bi : a, b \in \mathbb{Q}\} \subset \mathbb{C}$. Para generalizar esta afirmação, considere, portanto, a seguinte definição.

Definição 27 *Seja $\mathbb{F}$ um corpo e $a_1, a_2, \dots, a_n$ elementos de uma extensão $\mathbb{E}$ de $\mathbb{F}$. Denota-se por $\mathbb{F}(a_1, a_2, \dots, a_n)$ o menor subcorpo de $\mathbb{E}$ que contém $\mathbb{F}$ e o conjunto $\{a_1, a_2, \dots, a_n\}$.*

É possível perceber que $\mathbb{F}(a_1, a_2, \dots, a_n)$ é a interseção de todos os subcorpos de $\mathbb{E}$ que contém $\mathbb{F}$ e o conjunto $\{a_1, a_2, \dots, a_n\}$.

Definição 28 (Corpo de decomposição) *Seja $\mathbb{E}$ um corpo de extensão de $\mathbb{F}$ e seja $f(x) \in \mathbb{F}[x]$ tal que $\text{gr}(f) \geq 1$. Dizemos que f se decompõe em $\mathbb{E}$ se existem $a \in \mathbb{F}$ e $a_1, a_2, \dots, a_n \in \mathbb{E}$ tal que*

$$f(x) = a(x - a_1)(x - a_2) \dots (x - a_n).$$

Dizemos que $\mathbb{E}$ é um corpo de decomposição de $f(x)$ sobre $\mathbb{F}$ se

$$\mathbb{E} = \mathbb{F}(a_1, a_2, \dots, a_n).$$

Teorema 29 *Seja $\mathbb{F}$ um corpo e $f(x) \in \mathbb{F}[x]$ um polinômio não constante. Então existe um corpo de decomposição $\mathbb{E}$ de $f(x)$ sobre $\mathbb{F}$.*

Demonstração: Procedemos por indução no grau de f . Se $\text{gr}(f) = 1$, então f é linear e pode ser escrito como $a(x - b)$ para dados $a, b \in \mathbb{F}$. Seja $k \in \mathbb{Z}$ tal que $k > 1$ e suponha, portanto, que a afirmação seja válida para todo polinômio de grau até k e seja $f(x)$ com grau $k + 1$. Então, pelo Teorema de Kronecker, existe um corpo $\mathbb{E}$ onde $f(x)$ possui uma raiz a_1 . Portanto, existe $g(x) \in \mathbb{E}[x]$ tal que $f(x) = (x - a_1)g(x)$. Como $\text{gr}(g) \geq k$, deve existir um corpo $\mathbb{K}$ que contém $\mathbb{E}$ e as raízes $a_2, \dots, a_n$ de $g(x)$. Então, $\mathbb{F}(a_1, a_2, \dots, a_n)$ é um corpo de decomposição de $f(x)$ sobre $\mathbb{F}$. □

Uma vez definido o que é um corpo de decomposição, é possível mostrar que o corpo obtido por $\mathbb{E} = \mathbb{F}/\langle p(x) \rangle$ é isomorfo ao corpo de decomposição de $p(x)$ e, com isto, encontrar uma maneira simples de representar os elementos de $\mathbb{E}$, como comentado anteriormente. Para isto, é necessário inicialmente demonstrar o seguinte lema:

Lema 30 *Seja $\mathbb{F}$ um corpo e $p(x) \in \mathbb{F}[x]$ um polinômio irreduzível. Se $\mathbb{E}$ é um corpo que contém $\mathbb{F}$ e existe $a \in \mathbb{E}$ tal que $p(a) = 0$, então a aplicação $\phi : \mathbb{F}[x] \rightarrow \mathbb{E}$ dada por $\phi(f(x)) = f(a)$ é um homomorfismo de anéis e $\ker(\phi) = \langle p(x) \rangle$.*

Demonstração: Primeiramente, verificamos que ϕ é um homomorfismo de anéis:

$$\begin{aligned}\phi(f_1(x) + f_2(x)) &= \phi((f_1 + f_2)(x)) \\ &= (f_1 + f_2)(a) \\ &= f_1(a) + f_2(a) \\ &= \phi(f_1(x)) + \phi(f_2(x))\end{aligned}$$

$$\begin{aligned}\phi(f_1(x)f_2(x)) &= \phi((f_1f_2)(x)) \\ &= (f_1f_2)(a) \\ &= f_1(a)f_2(a) \\ &= \phi(f_1(x))\phi(f_2(x))\end{aligned}$$

Resta portanto mostrar que $\ker(\phi) = \langle p(x) \rangle$.

Como $p(a) = 0$, $\langle p(x) \rangle \subseteq \ker(\phi)$. Como $p(x)$ é irreduzível, sabe-se que $\langle p(x) \rangle$ é um ideal maximal em $\mathbb{F}[x]$, e como $\ker(\phi) \neq \mathbb{F}[x]$ (pois existe $1 \in \mathbb{F}[x]$ tal que $1 \notin \ker(\phi)$), então, $\langle p(x) \rangle \subseteq \ker(\phi) \subset \mathbb{F}[x]$, o que implica que $\ker(\phi) = \langle p(x) \rangle$. □

Teorema 31 *Seja $\mathbb{F}$ um corpo e $p(x) \in \mathbb{F}[x]$ um polinômio irreduzível. Se a é uma raiz de $p(x)$ em uma extensão $\mathbb{E}$ de $\mathbb{F}$, então $\mathbb{F}[x]/\langle p(x) \rangle$ é isomorfo a $\mathbb{F}(a)$. Além disso, se $\text{gr}(p) = n$, então todo elemento de $\mathbb{F}(a)$ pode ser expresso de maneira única como*

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1a + c_0,$$

com $c_i \in \mathbb{F}$.

Demonstração: Seja ϕ o homomorfismo dado no lema anterior. Como $\ker(\phi) = \langle p(x) \rangle$, pelo Teorema do Homomorfismo, $\mathbb{F}[x]/\langle p(x) \rangle$ é isomorfo a $\phi(\mathbb{F}[x]) \subset \mathbb{F}(a)$, portanto, $\phi(\mathbb{F}[x])$ é um subcorpo de $\mathbb{F}(a)$. No entanto, como $\mathbb{F}(a)$ é o menor corpo contendo $\mathbb{F}$ e a , e $\phi(\mathbb{F}[x])$ contém ambos $\mathbb{F}$ e a , então temos que $\phi(\mathbb{F}[x]) = \mathbb{F}(a)$. Resta mostrar a segunda parte do teorema.

Para isto, note, inicialmente, que dado um polinômio $t(x) \in \mathbb{F}[x]$, pelo algoritmo da divisão, existe um resto $r(x)$ com grau menor que n tal que $t(x) + \langle p(x) \rangle = r(x) + \langle p(x) \rangle$, de modo que cada elemento de $\mathbb{F}[x]/\langle p(x) \rangle$ pode ser representado por um polinômio de grau menor que n .

Assim, como ϕ é um isomorfismo, cada $c_kx^k + \langle p(x) \rangle$ é levado a c_ka^k por ϕ , de modo que cada elemento de $\mathbb{F}(a)$ corresponde a um único polinômio $c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0$ que é levado para $\mathbb{F}(a)$ como $c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1a + c_0$. □

Tem-se, portanto, uma maneira mais prática de encontrar a menor extensão de um corpo finito contendo uma raiz de um dado polinômio. Considere, por exemplo, o corpo $\mathbb{Z}_2$ e o polinômio $f(x) = x^2 + x + 1$. Obviamente, f é irreduzível em $\mathbb{Z}_2$. O Teorema de Kronecker garante que $\mathbb{E} = \mathbb{Z}_2[x]/\langle f(x) \rangle$ é um corpo de extensão de $\mathbb{Z}_2$ onde $f(x)$ possui uma raiz.

Pelo teorema anterior, tal corpo pode ser construído de tomando uma raiz α de f em um corpo de extensão de $\mathbb{Z}_2$ e realizando combinações lineares $a_1\alpha + a_0$ com $a_0, a_1 \in \mathbb{Z}_2$, de modo que obtemos o corpo $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$. Sabendo que α é uma raiz de f e, portanto $\alpha^2 = -(\alpha + 1) = \alpha + 1$, tem-se as seguintes tábuas:

+	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

·	1	α	$\alpha + 1$
1	1	α	$\alpha + 1$
α	α	$\alpha + 1$	1
$\alpha + 1$	$\alpha + 1$	1	α

Note que $\alpha + 1$ também é raiz de $f(x)$ em $\mathbb{F}_4$, e, além disso,

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

como esperado.

Como discutido anteriormente, se um dado polinômio que não possui raízes no corpo em questão não é irreduzível, basta fatorá-lo e adjuntar as raízes dos polinômios irreduzíveis obtidos.

Considerando que uma transformação cuja matriz é não diagonalizável terá um polinômio característico com raízes repetidas, surge o interesse em estudar a possibilidade de um dado polinômio ter raízes múltiplas em um corpo de extensão.

Teorema 32 *Um polinômio $f(x)$ sobre um corpo $\mathbb{F}$ tem uma raiz múltipla em um corpo de extensão $\mathbb{E}$ se, e somente se, $f(x)$ e $f'(x)$ têm um fator em comum em $\mathbb{F}[x]$.*

Demonstração: ($\implies$) Se $f(x)$ tem uma raiz múltipla a em um corpo de extensão $\mathbb{E}$, então deve existir $g(x) \in \mathbb{E}[x]$ tal que $f(x) = (x - a)^2 g(x)$, de modo que $f'(x) = 2(x - a)g(x) + (x - a)^2 g'(x)$ e, portanto, $f'(a) = 0$. Portanto, $x - a$ é um fator de ambos $f(x)$ e $f'(x)$ em $\mathbb{E}[x]$.

Se $f(x)$ e $f'(x)$ não possuem um fator comum de grau positivo em $\mathbb{F}[x]$, então existem $h(x), k(x) \in \mathbb{F}[x]$ tal que $f(x)h(x) + f'(x)k(x) = 1$, de modo que, como $h(x), k(x)$ são elementos de $\mathbb{E}[x]$, conclui-se que $x - a$ é um fator de 1, o que é um absurdo.

($\impliedby$) Se $f(x)$ e $f'(x)$ possuem um fator comum em $\mathbb{F}[x]$, seja a uma raiz de tal fator. Então a é raiz de $f(x)$ e $f'(x)$. Como a é raiz de $f(x)$, existe $q(x) \in \mathbb{F}[x]$ tal que $f(x) = (x - a)q(x)$ e portanto, $f'(x) = (x - a)q'(x) + q(x)$, de modo que $0 = f'(a) = q(a)$, e portanto, $x - a$ é um fator de $q(x)$ e a será raiz múltipla de $f(x)$.

□

Teorema 33 *Seja $f(x)$ um polinômio irredutível sobre um corpo $\mathbb{F}$. Se $\mathbb{F}$ tem característica 0, então $f(x)$ não possui raízes múltiplas. Se $\mathbb{F}$ tem característica $p \neq 0$, então $f(x)$ tem raízes múltiplas se, e somente se, $f(x) = g(x^p)$ para algum $g(x) \in \mathbb{F}[x]$.*

Demonstração: Se $f(x)$ possui raízes múltiplas, então, pelo teorema anterior, $f(x)$ e $f'(x)$ tem fator comum em $\mathbb{F}[x]$. No entanto, como $f(x)$ é irredutível, o único fator de $f(x)$, a menos de elementos inversíveis, é o próprio $f(x)$, de modo que $f(x)$ divide $f'(x)$. Como um polinômio não pode dividir outro polinômio de menor grau, tem-se que $f'(x) = 0$.

Assim, se $f(x) = a_n x^n + \dots + a_1 x + a_0$, então $f'(x) = n a_n x^{n-1} + \dots + a_1$. Então, se $f'(x) = 0$, $k a_k = 0$ para $k = 1, \dots, n$.

Se a característica de $\mathbb{F}$ for 0, então $f(x) = a_0$ e $f(x)$ não é irredutível, o que contraria a hipótese, portanto, $f(x)$ não tem raízes múltiplas.

Se a característica de $\mathbb{F}$ for $p \neq 0$, então $a_k = 0$ sempre que k não divide p , de modo que os termos de $f(x)$ serão da forma $x^{pj} = (x^p)^j$ e, portanto, $f(x) = g(x^p)$ para algum $g(x) \in \mathbb{F}[x]$.

□

Teorema 34 *Se $f(x)$ é um polinômio irredutível sobre um corpo perfeito, então $f(x)$ não possui raízes múltiplas.*

Demonstração: Se a característica de $\mathbb{F}$ é 0, então o resultado decorre do teorema anterior.

Se a característica de $\mathbb{F}$ é $p \neq 0$ e $f(x)$ tem raízes múltiplas, então $f(x) = g(x^p)$ para algum $g(x) \in \mathbb{F}[x]$. Escrevendo $g(x) = a_n x^n + \dots + a_1 x + a_0$, como $\mathbb{F}$ é perfeito e $\mathbb{F}^p = \mathbb{F}$, cada $a_i \in \mathbb{F}$ pode ser escrito como b_i^p para algum $b_i \in \mathbb{F}$, de modo que

$$f(x) = g(x^p) = b_n^p x^{pn} + \dots + b_1^p x^p + b_0^p = (b_n x^n + \dots + b_1 x + b_0)^p = (h(x))^p,$$

logo, $f(x)$ não é irredutível, o que contraria a hipótese.

□

Corolário 35 *Se $f(x)$ é um polinômio irredutível sobre um corpo finito, então $f(x)$ não possui raízes múltiplas.*

Demonstração: Decorre do fato de todo corpo finito ser perfeito.

□

3.3 Forma de Jordan em espaços sobre corpos finitos

Apesar dos corpos finitos não serem fechados algebricamente, a construção anterior nos permite encontrar uma forma canônica de Jordan para qualquer transformação linear, uma vez que, caso o polinômio associado à transformação não possua raízes, basta adjuntar a raiz trabalhando com um corpo de extensão.

Para exemplificar esta construção, relembramos as operações elementares sobre as linhas de uma matriz que levam à sua forma reduzida (ver (1) e (4)).

- Permutação de duas linhas. ($L_i \leftrightarrow L_j$)
- Multiplicação de linha por um escalar diferente de zero. ($L_i \rightarrow cL_i$)
- Substituição de uma linha por sua soma com outra linha previamente multiplicada por um escalar diferente de zero. ($L_i \rightarrow L_i + cL_j$).

Considere, portanto, os seguintes exemplos.

Exemplo 36 Considere o espaço vetorial $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ sobre o corpo $\mathbb{Z}_2$ e a transformação linear dada pela seguinte matriz:

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

O polinômio característico de A é dado por

$$p_A(\lambda) = \begin{vmatrix} 1 - \lambda & 0 & 0 & 1 \\ 0 & -\lambda & 1 & 0 \\ 1 & 1 & 1 - \lambda & 1 \\ 1 & 0 & 0 & -\lambda \end{vmatrix} = \lambda^4 + \lambda^2 + 1.$$

Note que $p_A(x)$ não é irredutível em $\mathbb{Z}_2$, no entanto, $p_A(x) = (x^2 + x + 1)^2$, e $q(x) = x^2 + x + 1$ é irredutível em $\mathbb{Z}_2[x]$ com grau 2, de modo que o corpo de decomposição de $p_A(x)$ é o corpo finito

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}.$$

Além disso, como $\alpha^4 + \alpha^2 + 1 = 0$, percebe-se que

$$\begin{aligned} (x - \alpha)^2(x - (\alpha + 1))^2 &= (x^2 - \alpha^2)(x^2 - (\alpha + 1)^2) = x^4 - (\alpha^2 + \alpha^2 + 1)x^2 + \alpha^2(\alpha^2 + 1) \\ &= x^4 - x^2 + \alpha^4 + \alpha^2 = x^4 + x^2 + \alpha^2 + 1 + \alpha^2 = x^4 + x^2 + 1 = p_A(x), \end{aligned}$$

como esperado. A fatoração de $p_A(x)$ indica que os autovalores de A são α e $\alpha + 1$.

Para $\lambda_1 = \alpha$:

$$A - \alpha I_d = \begin{bmatrix} \alpha + 1 & 0 & 0 & 1 \\ 0 & \alpha & 1 & 0 \\ 1 & 1 & \alpha + 1 & 1 \\ 1 & 0 & 0 & \alpha \end{bmatrix}$$

$$\begin{array}{ccc}
 \left[\begin{array}{cccc|c} \alpha+1 & 0 & 0 & 1 & 0 \\ 0 & \alpha & 1 & 0 & 0 \\ 1 & 1 & \alpha+1 & 1 & 0 \\ 1 & 0 & 0 & \alpha & 0 \end{array} \right] & \begin{array}{l} L_1 \leftrightarrow L_4 \\ L_2 \rightarrow (\alpha+1)L_2 \\ L_3 \rightarrow L_3 \end{array} & \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & 1 & \alpha+1 & 0 & 0 \\ 1 & 1 & \alpha+1 & 1 & 0 \\ \alpha+1 & 0 & 0 & 1 & 0 \end{array} \right] \\
 \\
 \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & 1 & \alpha+1 & 0 & 0 \\ 1 & 1 & \alpha+1 & 1 & 0 \\ \alpha+1 & 0 & 0 & 1 & 0 \end{array} \right] & \begin{array}{l} L_3 \rightarrow L_3 + L_1 \\ L_4 \rightarrow L_4 + (\alpha+1)L_1 \end{array} & \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & 1 & \alpha+1 & 0 & 0 \\ 0 & 1 & \alpha+1 & \alpha+1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \\
 \\
 \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & 1 & \alpha+1 & 0 & 0 \\ 0 & 1 & \alpha+1 & \alpha+1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] & L_3 \rightarrow L_3 + L_2 & \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & 1 & \alpha+1 & 0 & 0 \\ 0 & 0 & 0 & \alpha+1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \\
 \\
 \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & 1 & \alpha+1 & 0 & 0 \\ 0 & 0 & 0 & \alpha+1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] & L_3 \rightarrow \alpha L_3 & \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & 1 & \alpha+1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \\
 \\
 \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & 1 & \alpha+1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] & L_1 \rightarrow L_1 + \alpha L_3 & \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & \alpha+1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]
 \end{array}$$

Portanto, uma base para $\ker(A - \alpha I_d)$ é $\left\{ \begin{bmatrix} 0 \\ \alpha+1 \\ 1 \\ 0 \end{bmatrix} \right\}$.

$$\begin{array}{ccc}
 (A - \alpha I_d)^2 = \begin{bmatrix} \alpha+1 & 0 & 0 & 1 \\ 0 & \alpha & 1 & 0 \\ 1 & 1 & \alpha+1 & 1 \\ 1 & 0 & 0 & \alpha \end{bmatrix}^2 & = & \begin{bmatrix} \alpha+1 & 0 & 0 & 1 \\ 1 & \alpha & 1 & 1 \\ 1 & 1 & \alpha+1 & 0 \\ 1 & 0 & 0 & \alpha \end{bmatrix} \\
 \\
 \left[\begin{array}{cccc|c} \alpha+1 & 0 & 0 & 1 & 0 \\ 1 & \alpha & 1 & 1 & 0 \\ 1 & 1 & \alpha+1 & 0 & 0 \\ 1 & 0 & 0 & \alpha & 0 \end{array} \right] & L_1 \leftrightarrow L_4 & \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 1 & \alpha & 1 & 1 & 0 \\ 1 & 1 & \alpha+1 & 0 & 0 \\ \alpha+1 & 0 & 0 & 1 & 0 \end{array} \right] \\
 \\
 \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 1 & \alpha & 1 & 1 & 0 \\ 1 & 1 & \alpha+1 & 0 & 0 \\ \alpha+1 & 0 & 0 & 1 & 0 \end{array} \right] & \begin{array}{l} L_2 \rightarrow L_2 + L_1 \\ L_3 \rightarrow L_3 + L_1 \\ L_4 \rightarrow L_4 + (\alpha+1)L_1 \end{array} & \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & \alpha & 1 & \alpha+1 & 0 \\ 0 & 1 & \alpha+1 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \\
 \\
 \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & \alpha & 1 & \alpha+1 & 0 \\ 0 & 1 & \alpha+1 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] & \begin{array}{l} L_2 \rightarrow (\alpha+1)L_2 \\ L_3 \rightarrow L_3 + (\alpha+1)L_2 \\ L_4 \rightarrow L_4 \end{array} & \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha & 0 \\ 0 & 1 & \alpha+1 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]
 \end{array}$$

Portanto, uma base para $\ker(A - \alpha I_d)^2$ é $\left\{ \begin{bmatrix} 0 \\ \alpha + 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} \alpha \\ \alpha \\ 0 \\ 1 \end{bmatrix} \right\}$.

Assim, $v_1 = \begin{bmatrix} \alpha \\ \alpha \\ 0 \\ 1 \end{bmatrix}$ é um vetor tal que $(A - \alpha I_d)(v_1) \neq 0$, $(A - \alpha I_d)^2(v_1) = 0$, portanto, v_1 é uma opção válida para a primeira cadeia de vetores da forma de Jordan.

$$v_2 = (A - \alpha I_d)(v_1) = \begin{bmatrix} \alpha + 1 & 0 & 0 & 1 \\ 0 & \alpha & 1 & 0 \\ 1 & 1 & \alpha + 1 & 1 \\ 1 & 0 & 0 & \alpha \end{bmatrix} \begin{bmatrix} \alpha \\ \alpha \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \alpha + 1 \\ 1 \\ 0 \end{bmatrix}$$

Para $\lambda_2 = \alpha + 1$:

$$A - (\alpha + 1)I_d = \begin{bmatrix} \alpha & 0 & 0 & 1 \\ 0 & \alpha + 1 & 1 & 0 \\ 1 & 1 & \alpha & 1 \\ 1 & 0 & 0 & \alpha + 1 \end{bmatrix}$$

$$\begin{array}{c} \left[\begin{array}{cccc|c} \alpha & 0 & 0 & 1 & 0 \\ 0 & \alpha + 1 & 1 & 0 & 0 \\ 1 & 1 & \alpha & 1 & 0 \\ 1 & 0 & 0 & \alpha + 1 & 0 \end{array} \right] \quad \begin{array}{l} L_1 \leftrightarrow L_4 \\ L_2 \rightarrow \alpha L_2 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & 1 & \alpha & 0 & 0 \\ 1 & 1 & \alpha & 1 & 0 \\ \alpha & 0 & 0 & 1 & 0 \end{array} \right] \\ \\ \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & 1 & \alpha & 0 & 0 \\ 1 & 1 & \alpha & 1 & 0 \\ \alpha & 0 & 0 & 1 & 0 \end{array} \right] \quad \begin{array}{l} L_3 \rightarrow L_3 + L_1 \\ L_4 \rightarrow L_4 + \alpha L_1 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & \alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \\ \\ \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & \alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad L_3 \rightarrow L_3 + L_2 \quad \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & 1 & \alpha & 0 & 0 \\ 0 & 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \\ \\ \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & 1 & \alpha & 0 & 0 \\ 0 & 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad L_3 \rightarrow (\alpha + 1)L_3 \quad \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & 1 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \\ \\ \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & 1 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad L_1 \rightarrow L_1 + (\alpha + 1)L_3 \quad \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \end{array}$$

Portanto, uma base para $\ker(A - (\alpha + 1)I_d)$ é $\left\{ \begin{bmatrix} 0 \\ \alpha \\ 1 \\ 0 \end{bmatrix} \right\}$.

$$\begin{aligned}
 (A - (\alpha + 1)I_d)^2 &= \begin{bmatrix} \alpha & 0 & 0 & 1 \\ 0 & \alpha + 1 & 1 & 0 \\ 1 & 1 & \alpha & 1 \\ 1 & 0 & 0 & \alpha + 1 \end{bmatrix}^2 = \begin{bmatrix} \alpha & 0 & 0 & 1 \\ 1 & \alpha + 1 & 1 & 1 \\ 1 & 1 & \alpha & 0 \\ 1 & 0 & 0 & \alpha + 1 \end{bmatrix} \\
 \left[\begin{array}{cccc|c} \alpha & 0 & 0 & 1 & 0 \\ 1 & \alpha + 1 & 1 & 1 & 0 \\ 1 & 1 & \alpha & 0 & 0 \\ 1 & 0 & 0 & \alpha + 1 & 0 \end{array} \right] & \xleftrightarrow{L_1 \leftrightarrow L_4} \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 1 & \alpha + 1 & 1 & 1 & 0 \\ 1 & 1 & \alpha & 0 & 0 \\ \alpha & 0 & 0 & 1 & 0 \end{array} \right] \\
 \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 1 & \alpha + 1 & 1 & 1 & 0 \\ 1 & 1 & \alpha & 0 & 0 \\ \alpha & 0 & 0 & 1 & 0 \end{array} \right] & \begin{array}{l} L_2 \rightarrow L_2 + L_1 \\ L_3 \rightarrow L_3 + L_1 \\ L_4 \rightarrow L_4 + \alpha L_1 \end{array} \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & \alpha + 1 & 1 & \alpha & 0 \\ 0 & 1 & \alpha & \alpha + 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \\
 \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & \alpha + 1 & 1 & \alpha & 0 \\ 0 & 1 & \alpha & \alpha + 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] & \begin{array}{l} L_2 \rightarrow \alpha L_2 \\ L_3 \rightarrow L_3 + \alpha L_2 \end{array} \left[\begin{array}{cccc|c} 1 & 0 & 0 & \alpha + 1 & 0 \\ 0 & 1 & \alpha & \alpha + 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]
 \end{aligned}$$

Portanto, uma base para $\ker(A - (\alpha + 1)I_d)^2$ é $\left\{ \begin{bmatrix} 0 \\ \alpha \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} \alpha + 1 \\ \alpha + 1 \\ 0 \\ 1 \end{bmatrix} \right\}$.

Assim, $v_3 = \begin{bmatrix} \alpha + 1 \\ \alpha + 1 \\ 0 \\ 1 \end{bmatrix}$ é um vetor tal que $(A - (\alpha + 1)I_d)(v_3) \neq 0$, $(A - (\alpha + 1)I_d)^2(v_3) = 0$,

portanto, v_3 é uma opção válida para a segunda cadeia de vetores da forma de Jordan.

$$v_4 = (A - (\alpha + 1)I_d)(v_3) = \begin{bmatrix} \alpha & 0 & 0 & 1 \\ 0 & \alpha + 1 & 1 & 0 \\ 1 & 1 & \alpha & 1 \\ 1 & 0 & 0 & \alpha + 1 \end{bmatrix} \begin{bmatrix} \alpha + 1 \\ \alpha + 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \alpha \\ 1 \\ 0 \end{bmatrix}$$

De fato, seja $\mathcal{B} = \{v_1, v_2, v_3, v_4\}$ uma base de $\mathbb{Z}_2^4$, então

$$\begin{aligned}
 Av_1 &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \alpha \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha + 1 \\ 0 \\ 1 \\ \alpha \end{bmatrix} = \alpha \begin{bmatrix} \alpha \\ \alpha \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ \alpha + 1 \\ 1 \\ 0 \end{bmatrix} = \alpha v_1 + v_2 \\
 Av_2 &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ \alpha + 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ \alpha \\ 0 \end{bmatrix} = \alpha v_2
 \end{aligned}$$

$$Av_3 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha + 1 \\ \alpha + 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ 0 \\ 1 \\ \alpha + 1 \end{bmatrix} = (\alpha + 1) \begin{bmatrix} \alpha + 1 \\ \alpha + 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ \alpha \\ 1 \\ 0 \end{bmatrix} = (\alpha + 1)v_3 + v_4$$

$$Av_4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ \alpha \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ \alpha + 1 \\ 0 \end{bmatrix} = (\alpha + 1)v_4$$

Portanto,

$$[A]_{\mathcal{B}} = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 \\ 0 & 0 & \alpha + 1 & 0 \\ 0 & 0 & 1 & \alpha + 1 \end{bmatrix}$$

3.3.1 Exemplo 2

Exemplo 37 Considere o espaço vetorial $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ sobre o corpo $\mathbb{Z}_2$ e a transformação linear dada pela seguinte matriz:

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

O polinômio característico de A é dado por:

$$p_A(x) = \begin{vmatrix} 1 - \lambda & 0 & 1 \\ 1 & 1 - \lambda & 0 \\ 0 & 1 & -\lambda \end{vmatrix} = (1 - \lambda)^2(-\lambda) + 1 = (\lambda^2 + 1)\lambda + 1 = \lambda^3 + \lambda + 1$$

Como $p_A(x)$ é irredutível em $\mathbb{Z}_2$, considere α uma raiz de $p(x)$ em algum corpo de extensão de $\mathbb{Z}_2$. Pelo Teorema 31, como $\text{gr}(p) = 3$, todo elemento de $\mathbb{Z}_2 \setminus \langle p(x) \rangle$ pode ser escrito de maneira única como $c_0 + c_1\alpha + c_2\alpha^2$, de modo que o corpo de decomposição de $p_A(x)$ é

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}.$$

A fatoração de $p_A(x)$ em $\mathbb{F}_8$ é dada por

$$p_A(x) = (x - \alpha)(x - \alpha^2)(x - (\alpha^2 + \alpha)),$$

de modo que A possui 3 autovalores distintos, e portanto, é diagonalizável. Assim, seja $\mathcal{B} = \{v_1, v_2, v_3\}$ uma base de autovetores de A . Então a forma de Jordan da matriz A é dada por

$$[A]_{\mathcal{B}} = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \alpha^2 & 0 \\ 0 & 0 & \alpha^2 + \alpha \end{bmatrix}$$

3.3.2 Exemplo 3

Considere o espaço vetorial $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ sobre o corpo $\mathbb{Z}_3$ e a transformação linear dada pela seguinte matriz:

$$A = \begin{bmatrix} 1 & 1 & 2 & 0 \\ 2 & 1 & 2 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix},$$

cujo polinômio característico é dado por

$$p_A(\lambda) = \begin{vmatrix} 1-\lambda & 1 & 2 & 0 \\ 2 & 1-\lambda & 2 & 1 \\ 0 & 2 & 1-\lambda & 0 \\ 0 & 1 & 1 & -\lambda \end{vmatrix} = \lambda^4 + 2\lambda^2 + 1$$

Note que $p_A(x)$ não é irredutível em $\mathbb{Z}_3$, no entanto, $p_A(x) = (x^2 + 1)^2$, e $q(x) = x^2 + 1$ é irredutível em $\mathbb{Z}_3[x]$ com grau 2, de modo que o corpo de decomposição de $p_A(x)$ é o corpo finito

$$\mathbb{F}_9 = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\},$$

e $p_A(x)$ é fatorado como

$$p_A(x) = (x - \alpha)^2(x - 2\alpha)^2,$$

o que indica que os autovalores de A são α e 2α .

Para $\lambda_1 = \alpha$:

$$A - \alpha I_d = \begin{bmatrix} 1-\alpha & 1 & 2 & 0 \\ 2 & 1-\alpha & 2 & 1 \\ 0 & 2 & 1-\alpha & 0 \\ 0 & 1 & 1 & -\alpha \end{bmatrix} = \begin{bmatrix} 2\alpha+1 & 1 & 2 & 0 \\ 2 & 2\alpha+1 & 2 & 1 \\ 0 & 2 & 2\alpha+1 & 0 \\ 0 & 1 & 1 & 2\alpha \end{bmatrix}$$

$$\left[\begin{array}{cccc|c} 2\alpha+1 & 1 & 2 & 0 & 0 \\ 2 & 2\alpha+1 & 2 & 1 & 0 \\ 0 & 2 & 2\alpha+1 & 0 & 0 \\ 0 & 1 & 1 & 2\alpha & 0 \end{array} \right] \quad \begin{array}{l} L_1 \rightarrow (2\alpha+2)L_1 \\ L_2 \rightarrow L_2 + (2\alpha+2)L_1 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 2\alpha+2 & \alpha+1 & 0 & 0 \\ 0 & \alpha & \alpha & 1 & 0 \\ 0 & 2 & 2\alpha+1 & 0 & 0 \\ 0 & 1 & 1 & 2\alpha & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & 2\alpha+2 & \alpha+1 & 0 & 0 \\ 0 & \alpha & \alpha & 1 & 0 \\ 0 & 2 & 2\alpha+1 & 0 & 0 \\ 0 & 1 & 1 & 2\alpha & 0 \end{array} \right] \quad L_2 \leftrightarrow L_4 \quad \left[\begin{array}{cccc|c} 1 & 2\alpha+2 & \alpha+1 & 0 & 0 \\ 0 & 1 & 1 & 2\alpha & 0 \\ 0 & 2 & 2\alpha+1 & 0 & 0 \\ 0 & \alpha & \alpha & 1 & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & 2\alpha+2 & \alpha+1 & 0 & 0 \\ 0 & 1 & 1 & 2\alpha & 0 \\ 0 & 2 & 2\alpha+1 & 0 & 0 \\ 0 & \alpha & \alpha & 1 & 0 \end{array} \right] \quad \begin{array}{l} L_1 \rightarrow L_1 + (\alpha+1)L_2 \\ L_3 \rightarrow L_3 + L_2 \\ L_4 \rightarrow L_4 + 2\alpha L_2 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 0 & 2\alpha+2 & 2\alpha+1 & 0 \\ 0 & 1 & 1 & 2\alpha & 0 \\ 0 & 0 & 2\alpha+2 & 2\alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 2\alpha + 2 & 2\alpha + 1 & 0 \\ 0 & 1 & 1 & 2\alpha & 0 \\ 0 & 0 & 2\alpha + 2 & 2\alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad \begin{array}{l} L_1 \rightarrow L_1 + 2L_3 \\ L_2 \rightarrow L_2 + (\alpha + 2)L_3 \\ L_3 \rightarrow (2\alpha + 1)L_3 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2\alpha + 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

Portanto, uma base para $\ker(A - \alpha I_d)$ é $\left\{ \begin{bmatrix} 2 \\ 2 \\ \alpha + 1 \\ 1 \end{bmatrix} \right\}$.

$$(A - \alpha I_d)^2 = \begin{bmatrix} 2\alpha + 1 & 1 & 2 & 0 \\ 2 & 2\alpha + 1 & 2 & 1 \\ 0 & 2 & 2\alpha + 1 & 0 \\ 0 & 1 & 1 & 2\alpha \end{bmatrix}^2 = \begin{bmatrix} \alpha + 2 & \alpha & 2\alpha & 1 \\ 2\alpha + 1 & \alpha + 1 & 2\alpha & \alpha + 1 \\ 1 & 2\alpha + 1 & \alpha + 1 & 2 \\ 2 & \alpha & \alpha & 0 \end{bmatrix}$$

$$\left[\begin{array}{cccc|c} \alpha + 2 & \alpha & 2\alpha & 1 & 0 \\ 2\alpha + 1 & \alpha + 1 & 2\alpha & \alpha + 1 & 0 \\ 1 & 2\alpha + 1 & \alpha + 1 & 2 & 0 \\ 2 & \alpha & \alpha & 0 & 0 \end{array} \right] \quad L_1 \leftrightarrow L_3 \quad \left[\begin{array}{cccc|c} 1 & 2\alpha + 1 & \alpha + 1 & 2 & 0 \\ 2\alpha + 1 & \alpha + 1 & 2\alpha & \alpha + 1 & 0 \\ \alpha + 2 & \alpha & 2\alpha & 1 & 0 \\ 2 & \alpha & \alpha & 0 & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & 2\alpha + 1 & \alpha + 1 & 2 & 0 \\ 2\alpha + 1 & \alpha + 1 & 2\alpha & \alpha + 1 & 0 \\ \alpha + 2 & \alpha & 2\alpha & 1 & 0 \\ 2 & \alpha & \alpha & 0 & 0 \end{array} \right] \quad \begin{array}{l} L_2 \rightarrow L_2 + (\alpha + 2)L_1 \\ L_3 \rightarrow L_3 + (2\alpha + 1)L_1 \\ L_4 \rightarrow L_4 + L_1 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 2\alpha + 1 & \alpha + 1 & 2 & 0 \\ 0 & 1 & 2\alpha + 1 & 2 & 0 \\ 0 & 2\alpha & 2\alpha + 2 & \alpha & 0 \\ 0 & 1 & 2\alpha + 1 & 2 & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & 2\alpha + 1 & \alpha + 1 & 2 & 0 \\ 0 & 1 & 2\alpha + 1 & 2 & 0 \\ 0 & 2\alpha & 2\alpha + 2 & \alpha & 0 \\ 0 & 1 & 2\alpha + 1 & 2 & 0 \end{array} \right] \quad \begin{array}{l} L_1 \rightarrow L_1 + (\alpha + 2)L_2 \\ L_3 \rightarrow L_3 + \alpha L_2 \\ L_4 \rightarrow L_4 + 2L_2 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 0 & 1 & 2\alpha & 0 \\ 0 & 1 & 2\alpha + 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

Portanto, os vetores do núcleo de $(A - \alpha I_d)^2$ são do tipo $x_3 \begin{bmatrix} 2 \\ \alpha + 2 \\ 1 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} \alpha \\ 1 \\ 0 \\ 1 \end{bmatrix}$.

Para facilitar a construção da base, considere a seguinte combinação linear dos vetores acima:

$$(c_1 + (\alpha + 1)c_2) \begin{bmatrix} 2 \\ \alpha + 2 \\ 1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} \alpha \\ 1 \\ 0 \\ 1 \end{bmatrix} = c_1 \begin{bmatrix} 2 \\ \alpha + 2 \\ 1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 2 \\ 2 \\ \alpha + 1 \\ 1 \end{bmatrix}$$

Assim, uma base para $\ker(A - \alpha I_d)^2$ é $\left\{ \begin{bmatrix} 2 \\ \alpha + 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ \alpha + 1 \\ 1 \end{bmatrix} \right\}$.

Assim, $v_1 = \begin{bmatrix} 2 \\ \alpha + 2 \\ 1 \\ 0 \end{bmatrix}$ é um vetor tal que $(A - \alpha I_d)(v_1) \neq 0$, $(A - \alpha I_d)^2(v_1) = 0$, portanto, v_1 é

uma opção válida para a segunda cadeia de vetores da forma de Jordan.

$$v_2 = (A - \alpha I_d)(v_1) = \begin{bmatrix} 2\alpha + 1 & 1 & 2 & 0 \\ 2 & 2\alpha + 1 & 2 & 1 \\ 0 & 2 & 2\alpha + 1 & 0 \\ 0 & 1 & 1 & 2\alpha \end{bmatrix} \begin{bmatrix} 2 \\ \alpha + 2 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2\alpha \\ 2\alpha \\ \alpha + 2 \\ \alpha \end{bmatrix}$$

Para $\lambda_2 = 2\alpha$:

$$A - 2\alpha I_d = \begin{bmatrix} 1 - 2\alpha & 1 & 2 & 0 \\ 2 & 1 - 2\alpha & 2 & 1 \\ 0 & 2 & 1 - 2\alpha & 0 \\ 0 & 1 & 1 & -2\alpha \end{bmatrix} = \begin{bmatrix} \alpha + 1 & 1 & 2 & 0 \\ 2 & \alpha + 1 & 2 & 1 \\ 0 & 2 & \alpha + 1 & 0 \\ 0 & 1 & 1 & \alpha \end{bmatrix}$$

$$\left[\begin{array}{cccc|c} \alpha + 1 & 1 & 2 & 0 & 0 \\ 2 & \alpha + 1 & 2 & 1 & 0 \\ 0 & 2 & \alpha + 1 & 0 & 0 \\ 0 & 1 & 1 & \alpha & 0 \end{array} \right] \quad \begin{array}{l} L_1 \rightarrow (\alpha + 2)L_1 \\ L_2 \rightarrow L_2 + (\alpha + 2)L_1 \end{array} \quad \left[\begin{array}{cccc|c} 1 & \alpha + 2 & 2\alpha + 1 & 0 & 0 \\ 0 & 2\alpha & 2\alpha & 1 & 0 \\ 0 & 2 & \alpha + 1 & 0 & 0 \\ 0 & 1 & 1 & \alpha & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & \alpha + 2 & 2\alpha + 1 & 0 & 0 \\ 0 & 2\alpha & 2\alpha & 1 & 0 \\ 0 & 2 & \alpha + 1 & 0 & 0 \\ 0 & 1 & 1 & \alpha & 0 \end{array} \right] \quad L_2 \leftrightarrow L_4 \quad \left[\begin{array}{cccc|c} 1 & \alpha + 2 & 2\alpha + 1 & 0 & 0 \\ 0 & 1 & 1 & \alpha & 0 \\ 0 & 2 & \alpha + 1 & 0 & 0 \\ 0 & 2\alpha & 2\alpha & 1 & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & \alpha + 2 & 2\alpha + 1 & 0 & 0 \\ 0 & 1 & 1 & \alpha & 0 \\ 0 & 2 & \alpha + 1 & 0 & 0 \\ 0 & 2\alpha & 2\alpha & 1 & 0 \end{array} \right] \quad \begin{array}{l} L_1 \rightarrow L_1 + (2\alpha + 1)L_2 \\ L_3 \rightarrow L_3 + L_2 \\ L_4 \rightarrow L_4 + \alpha L_2 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 0 & \alpha + 2 & \alpha + 1 & 0 \\ 0 & 1 & 1 & \alpha & 0 \\ 0 & 0 & \alpha + 2 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & 0 & \alpha + 2 & \alpha + 1 & 0 \\ 0 & 1 & 1 & \alpha & 0 \\ 0 & 0 & \alpha + 2 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad L_3 \rightarrow (\alpha + 1)L_3 \quad \left[\begin{array}{cccc|c} 1 & 0 & \alpha + 2 & \alpha + 1 & 0 \\ 0 & 1 & 1 & \alpha & 0 \\ 0 & 0 & 1 & \alpha + 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & 0 & \alpha + 2 & \alpha + 1 & 0 \\ 0 & 1 & 1 & \alpha & 0 \\ 0 & 0 & 1 & \alpha + 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right] \quad \begin{array}{l} L_1 \rightarrow L_1 + (2\alpha + 1)L_3 \\ L_2 \rightarrow L_2 + 2L_3 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \alpha + 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

Portanto, uma base para $\ker(A - 2\alpha I_d)$ é $\left\{ \begin{bmatrix} 2 \\ 2 \\ 2\alpha + 1 \\ 1 \end{bmatrix} \right\}$.

$$(A - 2\alpha I_d)^2 = \begin{bmatrix} \alpha + 1 & 1 & 2 & 0 \\ 2 & \alpha + 1 & 2 & 1 \\ 0 & 2 & \alpha + 1 & 0 \\ 0 & 1 & 1 & \alpha \end{bmatrix}^2 = \begin{bmatrix} 2\alpha + 2 & 2\alpha & \alpha & 1 \\ \alpha + 1 & 2\alpha + 1 & \alpha & 2\alpha + 1 \\ 1 & \alpha + 1 & 2\alpha + 1 & 2 \\ 2 & 2\alpha & 2\alpha & 0 \end{bmatrix}$$

$$\left[\begin{array}{cccc|c} 2\alpha + 2 & 2\alpha & \alpha & 1 & 0 \\ \alpha + 1 & 2\alpha + 1 & \alpha & 2\alpha + 1 & 0 \\ 1 & \alpha + 1 & 2\alpha + 1 & 2 & 0 \\ 2 & 2\alpha & 2\alpha & 0 & 0 \end{array} \right] \quad L_1 \leftrightarrow L_3 \quad \left[\begin{array}{cccc|c} 1 & \alpha + 1 & 2\alpha + 1 & 2 & 0 \\ \alpha + 1 & 2\alpha + 1 & \alpha & 2\alpha + 1 & 0 \\ 2\alpha + 2 & 2\alpha & \alpha & 1 & 0 \\ 2 & 2\alpha & 2\alpha & 0 & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & \alpha + 1 & 2\alpha + 1 & 2 & 0 \\ \alpha + 1 & 2\alpha + 1 & \alpha & 2\alpha + 1 & 0 \\ 2\alpha + 2 & 2\alpha & \alpha & 1 & 0 \\ 2 & 2\alpha & 2\alpha & 0 & 0 \end{array} \right] \quad \begin{array}{l} L_2 \rightarrow L_2 + (2\alpha + 2)L_1 \\ L_3 \rightarrow L_3 + (\alpha + 1)L_1 \\ L_4 \rightarrow L_4 + L_1 \end{array} \quad \left[\begin{array}{cccc|c} 1 & \alpha + 1 & 2\alpha + 1 & 2 & 0 \\ 0 & 1 & \alpha + 1 & 2 & 0 \\ 0 & \alpha & \alpha + 2 & 2\alpha & 0 \\ 0 & 1 & \alpha + 1 & 2 & 0 \end{array} \right]$$

$$\left[\begin{array}{cccc|c} 1 & \alpha + 1 & 2\alpha + 1 & 2 & 0 \\ 0 & 1 & \alpha + 1 & 2 & 0 \\ 0 & \alpha & \alpha + 2 & 2\alpha & 0 \\ 0 & 1 & \alpha + 1 & 2 & 0 \end{array} \right] \quad \begin{array}{l} L_1 \rightarrow L_1 + (2\alpha + 2)L_2 \\ L_3 \rightarrow L_3 + 2\alpha L_2 \\ L_4 \rightarrow L_4 + 2L_2 \end{array} \quad \left[\begin{array}{cccc|c} 1 & 0 & 1 & \alpha & 0 \\ 0 & 1 & \alpha + 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right]$$

Portanto, os vetores do núcleo de $(A - 2\alpha I_d)^2$ são do tipo $x_3 \begin{bmatrix} 2 \\ 2\alpha + 2 \\ 1 \\ 0 \end{bmatrix} + x_4 \begin{bmatrix} 2\alpha \\ 1 \\ 0 \\ 1 \end{bmatrix}$.

Para facilitar a construção da base, considere a seguinte combinação linear dos vetores acima:

$$(c_1 + (2\alpha + 1)c_2) \begin{bmatrix} 2 \\ 2\alpha + 2 \\ 1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 2\alpha \\ 1 \\ 0 \\ 1 \end{bmatrix} = c_1 \begin{bmatrix} 2 \\ 2\alpha + 2 \\ 1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 2 \\ 2 \\ 2\alpha + 1 \\ 1 \end{bmatrix}$$

Assim, uma base para $\ker(A - 2\alpha I_d)^2$ é $\left\{ \begin{bmatrix} 2 \\ 2\alpha + 2 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 2\alpha + 1 \\ 1 \end{bmatrix} \right\}$.

Assim, $v_3 = \begin{bmatrix} 2 \\ 2\alpha + 2 \\ 1 \\ 0 \end{bmatrix}$ é um vetor tal que $(A - 2\alpha I_d)(v_3) \neq 0$, $(A - 2\alpha I_d)^2(v_3) = 0$, portanto, v_3

é uma opção válida para a segunda cadeia de vetores da forma de Jordan.

$$v_4 = (A - 2\alpha I_d)(v_3) = \begin{bmatrix} \alpha + 1 & 1 & 2 & 0 \\ 2 & \alpha + 1 & 2 & 1 \\ 0 & 2 & \alpha + 1 & 0 \\ 0 & 1 & 1 & \alpha \end{bmatrix} \begin{bmatrix} 2 \\ 2\alpha + 2 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ \alpha \\ 2\alpha + 2 \\ 2\alpha \end{bmatrix}$$

De fato, seja $\mathcal{B} = \{v_1, v_2, v_3, v_4\}$ uma base de $\mathbb{Z}_3^4$, então

$$\begin{aligned}
 Av_1 &= \begin{bmatrix} 1 & 1 & 2 & 0 \\ 2 & 1 & 2 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ \alpha + 2 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ \alpha + 2 \\ 2\alpha + 2 \\ \alpha \end{bmatrix} = \alpha \begin{bmatrix} 2 \\ \alpha + 2 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 2\alpha \\ 2\alpha \\ \alpha + 2 \\ \alpha \end{bmatrix} = \alpha v_1 + v_2 \\
 Av_2 &= \begin{bmatrix} 1 & 1 & 2 & 0 \\ 2 & 1 & 2 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 2\alpha \\ 2\alpha \\ \alpha + 2 \\ \alpha \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 2\alpha + 2 \\ 2 \end{bmatrix} = \alpha v_2 \\
 Av_3 &= \begin{bmatrix} 1 & 1 & 2 & 0 \\ 2 & 1 & 2 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 2\alpha + 2 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2\alpha \\ 2\alpha + 2 \\ \alpha + 2 \\ 2\alpha \end{bmatrix} = 2\alpha \begin{bmatrix} 2 \\ 2\alpha + 2 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} \alpha \\ \alpha \\ 2\alpha + 2 \\ 2\alpha \end{bmatrix} = 2\alpha v_3 + v_4 \\
 Av_4 &= \begin{bmatrix} 1 & 1 & 2 & 0 \\ 2 & 1 & 2 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \alpha \\ 2\alpha + 2 \\ 2\alpha \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ \alpha + 2 \\ 2 \end{bmatrix} = 2\alpha v_4
 \end{aligned}$$

Portanto,

$$[A]_{\mathcal{B}} = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 \\ 0 & 0 & 2\alpha & 0 \\ 0 & 0 & 1 & 2\alpha \end{bmatrix}$$

Referências

- 1 COELHO, F. U.; LOURENÇO, M. L. **Um curso de álgebra linear**. 2. ed. rev. ampl. São Paulo: Edusp, 2005.
- 2 DOMINGUES, H. H.; IEZZI, G. **Álgebra moderna**. 5. ed. São Paulo: Saraiva, 2018.
- 3 GALLIAN, J. A. **Contemporary abstract algebra**. 9th ed. Boston: Cengage Learning, 2015.
- 4 HOFFMAN, K.; KUNZE, R. **Linear algebra**. 2nd ed. Englewood Cliffs: Prentice-Hall, 1971.
- 5 SHOKRANIAN, S. **Exemplos de álgebra linear sobre corpos: corpos finitos**. Rio de Janeiro: Ciência Moderna, 2015. v. 1.