UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

T-Ideal das matrizes de ordem 2 sobre um corpo finito

Luis Felipe dos Santos Luccas

São Carlos-SP
Agosto de 2025

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

T-Ideal das matrizes de ordem 2 sobre um corpo finito

Luis Felipe dos Santos Luccas

Orientador: Prof. Dr. Dimas José Gonçalves

Tese/Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de São Carlos como parte dos requisitos para a obtenção do Título de Mestre em Matemática.

São Carlos-SP
Agosto de 2025

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Matemática

Folha de Aprovação

Defesa de Dissertação de Mestrado do candidato Luis Felipe dos Santos Luccas, realizada em 22/08/2025.

Comissão Julgadora:

Prof. Dr. Dimas José Gonçalves (UFSCar)

Prof. Dr. Claudemir Fidelis Bezerra Júnior (UFCG)

Prof. Dr. Pedro Souza Fagundes (UFSCar)

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Matemática.

Dedico este trabalho
a Deus e a minha família.

Agradecimentos

Agradeço à minha família que sempre esteve por perto e me apoiando e aos meus amigos que me inspiraram. Agradeço, em especial, ao meu grande amigo Rafael por me encorajar e me cobrar para que eu sempre esteja dando o meu melhor todo dia.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) – Código de Financiamento 001

Resumo

O objetivo desta dissertação é estudar os conceitos necessários de álgebras e PI-álgebras com foco na álgebra das matrizes e em álgebras sobre corpos finitos. Como resultado principal, apresentaremos a base descrita por Mal'tsev e Kuz'min para as identidades polinomiais da álgebra das matrizes 2×2 sobre corpos finitos.

Palavras-chave: PI-álgebras. Identidades polinomiais. T-ideais. Matrizes sobre um corpo finito. Matrizes 2×2 sobre corpos finitos.

Abstract

The goal of this dissertation is to study the necessary concepts of algebras and PI-algebras, with a focus on matrix algebras and algebras over finite fields. As the main result, we present the basis described by Mal'tsev and Kuz'min for the polynomial identities of the algebra of 2×2 matrices over finite fields.

Keywords: PI-algebras. Polynomial identities. T-ideals. Matrices over a finite field. 2×2 matrices over finite fields.

Sumário

Introdução

O assunto tratado nesta dissertação está inserido dentro da Teoria das PI-álgebras, ou seja, álgebras que satisfazem identidades polinomiais.

Um polinômio $f(x_1,\ldots,x_n)$ nas variáveis não comutativas $x_1,\ldots,x_n$ e com coeficientes num corpo F é dito ser uma identidade polinomial de uma F-álgebra R se ele se anula sempre que trocamos suas variáveis por elementos de R. Quando isso ocorrer para um polinômio não nulo diremos que R é uma PI-álgebra. São exemplos de PI-álgebras as álgebras comutativas, as de dimensão finita e, em particular, a álgebra $M_n(F)$ das matrizes quadradas de ordem n com entradas em F. Chamaremos o conjunto de todas as identidades polinomiais de uma álgebra R de T-ideal de R.

A Teoria de PI-Álgebras existe desde os anos 30. Em 1937, Wagner [31] mostrou que a álgebra $M_2(F)$ satisfaz a identidade

$$[[x_1,x_2]^2,x_3],$$

onde $[x_1,x_2] = x_1x_2 - x_2x_1$. Mais tarde, em 1943, tal resultado foi estendido por Hall [14] para as álgebras de divisão não comutativas e, depois, para os quatérnions. Ainda na década de 40, surgiram os trabalhos de Kaplansky [18], Levitzki [21] e Jacobson [17] para provar o famoso Problema de Kurosh, impulsionando assim a teoria em questão.

Na década de 50 surgiram dois estudos importantes: O Teorema de Amitsur-Levitzki e o Problema de Specht. O Teorema de Amitsur-Levitzki foi apresentado em [1] e nos dá uma identidade para as álgebras das matrizes quadradas, chamada de polinômio standard. Com ele começamos a estudar melhor tal álgebra podendo estudar seus T-ideais.

O Problema de Specht foi apresentado em [30] e nos levanta uma questão importante sobre os T-ideais das álgebras associativas:

Problema. Toda álgebra associativa possui uma base finita para suas identidades polinomiais?

Tal problema foi estudado por vários matemáticos e, em 1987, Kemer [19] conseguiu provar que para o caso de álgebras sobre um corpo de característica 0 a resposta é sim. Porém, em 1999, Belov ([3] e [4]) provou que existem T-ideais sem base finita para álgebras sobre um corpo de característica positiva. Em 1999 Grishin [11] [12] e em 2002 Gupta e Krasilnikov [13] explicitaram, em estudos paralelos, contraexemplos para o caso de corpos de característica 2.

Seguindo a questão de Specht, um dos principais problemas sobre identidades é achar uma base das identidades para alguma álgebra, por exemplo, a álgebra de matrizes $M_n(F)$. Em 1973, Razmyslov [25] explicitou uma base finita com 9 polinômios para as identidades da álgebra $M_2(F)$ com $char(F) = 0$, base esta que foi otimizada em 1981 por Drensky [7] para dois polinômios, sendo eles

$$st_4(x_1, x_2, x_3, x_4) \text{ e } [[x_1, x_2]^2, x_1].$$

Em 2001, Koshlukov [20] exibiu uma base finita para as identidades da álgebra $M_2(F)$ quando F é um corpo infinito de característica diferente de 2. Vale chamar a atenção para o fato que o caso de F infinito com característica 2 ainda permanece em aberto.

Voltando-nos para as álgebras $M_n(F_q)$, onde F_q é um corpo finito com q elementos, podemos encontrar mais alguns resultados. Em [9], Genov explicitou uma base para as identidades da álgebra $M_3(F_q)$ e em [10] Genov e Siderov apresentaram uma base para as identidades da álgebra $M_4(F_q)$.

Nesta dissertação veremos o resultado de Mal'tsev e Kuz'min, apresentado em [23], explicitando uma base de dois elementos para as identidades polinomiais da álgebra $M_2(F_q)$. Para tal, apresentaremos nos dois primeiros capítulos desta dissertação os conceitos e resultados necessários para chegarmos em tal resultado. Esta dissertação está estruturada conforme os parágrafos seguintes.

No primeiro capítulo apresentaremos algumas definições básicas e resultados a respeito das estruturas das álgebras associativas. Em destaque encontram-se os teoremas de Wedderburn.

No segundo capítulo entraremos na área das PI-álgebras com definições importantes como T-ideais e variedades, apresentando as ferramentas necessárias para chegarmos no nosso resultado principal.

No terceiro capítulo apresentaremos o resultado principal desta dissertação que consiste em descrever uma base para as identidades polinomiais de $M_2(F_q)$.

CAPÍTULO 1

Álgebras

Neste capítulo introduziremos o conceito de álgebra, veremos algumas propriedades e exemplos que foram retirados de [2], [6], [8], [15], [22], [24] e [27]. Além disto, estudaremos alguns resultados importantes como os Teoremas de Wedderburn sobre as estruturas das álgebras de dimensão finita bem como alguns teoremas sobre módulos, somas subdiretas e álgebras algébricas.

1.1 Definições básicas

Começaremos nossos estudos apresentando algumas definições básicas que podem ser encontradas em [22], em [8] e em [6]. Nesta dissertação estudaremos a álgebra associativa das matrizes quadradas de ordem 2 sobre o corpo finito F_q de característica p e com $q = p^r$ elementos. Durante este estudo usaremos objetos importantes da área de álgebra, como os ideais e os homomorfismos, mas para definirmos eles, primeiro precisamos definir o que é uma álgebra associativa.

De agora em diante, F denotará um corpo qualquer.

Definição 1.1. Um F-espaço vetorial R é chamado de F-álgebra (ou álgebra) se existe uma operação binária $*$ em R, chamada de multiplicação, tal que para cada $a,\ b,\ c \in R$ e $\alpha \in F$ valem as seguintes igualdades:

i) $a*(b+c) = a*b+a*c$,

ii) $(a+b)*c = a*c+b*c$,

iii) $\alpha(a*b) = (\alpha a)*b = a*(\alpha b)$.

Além disso, uma álgebra R é dita ser associativa se para todos $a,b,c \in R$ vale

$$(a*b)*c = a*(b*c).$$

Exemplo 1.2. Alguns exemplos de F-álgebras são:

i) Qualquer corpo que é uma extensão do corpo F.

ii) O F-espaço vetorial $M_n(F)$ das matrizes quadradas $n \times n$, cujas entradas estão em F, com a multiplicação usual de matrizes.

iii) O F-espaço vetorial $End_F(V)$ de todas as transformações lineares de um F-espaço vetorial V nele mesmo com a multiplicação $\circ$ (composição de funções).

iv) O F-espaço vetorial dos polinômios nas variáveis comutativas $x_1,\ x_2,\ \ldots,\ x_n$ com coeficientes em F e produto usual de polinômios. Denotaremos tal álgebra por $F[x_1, x_2, \ldots, x_n]$.

v) O subespaço vetorial $sl_n(F)$ de $M_n(F)$ formado pelas matrizes com traço 0 (zero) e multiplicação $[\ ,\ ]$ dada por:

$$[r_1, r_2] = r_1 \cdot r_2 - r_2 \cdot r_1,\ r_1, r_2 \in sl_n(F),$$

onde $\cdot$ é a multiplicação usual de matrizes.

Note que as álgebras dos itens i), ii), iii) e iv) são álgebras associativas, porém a álgebra do item v) não é uma álgebra associativa se $n \geq 2$, pois nem sempre vale a igualdade $[[r_1, r_2], r_3] = [r_1, [r_2, r_3]]$ para todos $r_1, r_2, r_3 \in sl_n(F)$. Apenas para curiosidade do leitor, a álgebra $sl_n(F)$ é um exemplo do que chamamos de álgebra de Lie, assunto este a ser omitido nesta dissertação.

Um ponto interessante das álgebras é que quando vamos definir sua multiplicação, basta definirmos para os elementos de sua base como espaço vetorial. O exemplo a seguir explica o porque disso.

Exemplo 1.3. Seja R um F-espaço vetorial com base $\{e_k \mid k \in I\}$. Para cada par e_i, e_j defina a multiplicação $e_i \cdot e_j$ como

$$e_i \cdot e_j = \sum_{k \in I} \alpha_{ij}^k e_k,$$

onde os $\alpha_{ij}^k \in F$ são nulos, a menos de uma quantidade finita de índices k. A partir disso, defina a multiplicação de dois elementos quaisquer de R como

$$\left(\sum_{i \in I} \xi_i e_i\right) \cdot \left(\sum_{j \in I} \eta_j e_j\right) = \sum_{i,j \in I} \xi_i \eta_j (e_i \cdot e_j).$$

Desta forma, temos que o F-espaço vetorial R munido da multiplicação $\cdot$ é uma F-álgebra.

De agora em diante, todas as álgebras e espaços vetoriais serão sobre F a menos que se diga algo contrário. Um último exemplo importante de álgebra é o produto direto.

Definição 1.4. O produto direto das álgebras R_i, com i em algum conjunto de índices I, é o conjunto

$$\prod_{i\in I} R_i = \left\{ f : I \to \bigcup_{i\in I} R_i \mid f(i) \in R_i \text{ para todo } i \in I \right\}$$

munido das operações $f+g$, fg e αf como segue:

$$(f+g)(i) = f(i)+g(i), \qquad (fg)(i) = f(i)g(i), \qquad (\alpha f)(i) = \alpha f(i)$$

para todo $i \in I$.

Quando estamos falando de um produto direto finito normalmente denotamos os seus elementos usando o sistema de coordenadas, isto é, se $I = \{1,\ldots,n\}$ e $\tilde{r} \in \prod_{i\in I} R_i$, então escrevemos $\tilde{r} = (r_1, r_2, \ldots, r_n)$ com $r_i \in R_i$.

Definido o que vem a ser uma álgebra, podemos prosseguir com a definição de subálgebra.

Definição 1.5. Um subespaço vetorial S da álgebra R é chamado de subálgebra de R se é fechado com respeito a multiplicação $\cdot$ de R, isto é, se para todos $s_1, s_2 \in S$ vale que $s_1 \cdot s_2 \in S$.

Exemplo 1.6. O espaço vetorial $U_n(F)$ das matrizes triangulares superiores $n \times n$ é uma subálgebra de $M_n(F)$.

Note que nem todo subespaço que é uma álgebra será uma subálgebra. Por exemplo, a álgebra de Lie $sl_n(F)$, apesar de ser um subespaço, não é uma subálgebra da álgebra associativa $M_n(F)$, pois não é fechada com respeito a multiplicação usual de matrizes.

Observação 1.7. De agora em diante, todas as álgebras consideradas serão associativas a menos que se diga algo contrário. Neste caso, omitiremos o termo "associativa", ou seja, diremos simplesmente "álgebra" ao invés de "álgebra associativa".

Uma das principais subálgebras que teremos é o ideal de uma álgebra.

Definição 1.8. Dada uma álgebra R com multiplicação $\cdot$, um subespaço vetorial I de R é chamado de ideal à esquerda de R se $R \cdot I \subseteq I$ isto é, $r \cdot i \in I$ para todo $r \in R$ e $i \in I$. De forma análoga definimos ideal à direita de R. Um ideal bilateral (ou simplesmente ideal) de R é um subespaço vetorial I de R que é ao mesmo tempo um ideal à esquerda e à direita.

Exemplo 1.9. Alguns exemplos de ideais são:

i) Para toda álgebra R temos que 0 e R são ideais chamados de triviais.

ii) As matrizes estritamente triangulares superiores formam um ideal das matrizes triangulares superiores.

iii) Seja R uma álgebra qualquer e $u \in R$, então Ru é um ideal à esquerda de R, uR é um ideal à direita de R e RuR é um ideal bilateral de R.

Ideais são estruturas muito importantes que possuem várias aplicações, como por exemplo, a álgebra quociente.

Definição 1.10. Dada uma F-álgebra R com multiplicação $\cdot$, seja I um ideal bilateral de R. Denote por R/I o conjunto dos elementos $\overline{r} = r + I$ (classes laterais), onde $r \in R$. Relembramos que

$$\overline{r_1} = \overline{r_2} \iff r_1 - r_2 \in I.$$

Defina a soma e multiplicação em R/I, respectivamente, por

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I \text{ e } (r_1 + I)(r_2 + I) = (r_1 \cdot r_2) + I$$

e o produto por escalar

$$\alpha(r + I) = \alpha r + I,$$

onde $r_1, r_2, r \in R$ e $\alpha \in F$. Com tais operações, dizemos que R/I é a álgebra quociente de R por I.

Na definição acima, note que $\overline{r} = \overline{0}$ se, e somente se, $r \in I$. Além disso, quando dois elementos $r_1, r_2 \in R$ estão em uma mesma classe $\overline{r}$ de R/I, dizemos que r_1 e r_2 são côngruos módulo I.

Quando estudamos álgebras distintas, muitas vezes encontramos álgebras que são muito similares em seus comportamentos. Por exemplo, a álgebra das matrizes triangulares superiores e a álgebra das matrizes triangulares inferiores têm as mesmas propriedades, com a única diferença sendo a forma em que elas aparecem. Para melhor estudarmos as álgebras sem nos preocuparmos com estas "repetições" nós distinguimos as álgebras via o conceito de isomorfismo.

Definição 1.11. Uma transformação linear $\phi : R_1 \to R_2$, onde R_1 e R_2 são F-álgebras, é chamada de homomorfismo de álgebras se para todos $x, y \in R_1$ temos

$$\phi(x \cdot y) = \phi(x) \times \phi(y)$$

onde $\cdot$ é o produto em R_1 e $\times$ é o produto em R_2.

Um isomorfismo de álgebras é um homomorfismo de álgebras que é bijetor, e duas álgebras são ditas isomorfas se existe um isomorfismo entre elas. Se R_1 e R_2 são álgebras isomorfas, denotaremos $R_1 \cong R_2$.

Exemplo 1.12. Um exemplo bem importante de isomorfismo de álgebras que será usado nesta dissertação é a função $\psi : End_F(V) \to M_n(F)$, onde V é um F-espaço vetorial com dimensão finita n. Para construí-la, fixe uma base ordenada $B = \{v_1, \ldots, v_n\}$ de V. Para cada $f \in End_F(V)$ e para cada $1 \leq j \leq n$, existem únicos $t_{ij} \in F$ tais que

$$f(v_j) = t_{1j}v_1 + t_{2j}v_2 + \cdots + t_{nj}v_n.$$

Com isso, podemos definir $\psi(f)$ da seguinte forma:

$$\psi(f) = \begin{pmatrix} t_{11} & t_{12} & \cdots & t_{1n} \\ t_{21} & t_{22} & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \cdots & t_{nn} \end{pmatrix}.$$

Da Álgebra Linear, note que $\psi(f)$ é a matriz de f com relação à base B.

Um exemplo de homomorfismo que usaremos neste artigo é a representação regular de uma álgebra. A ideia de representação regular pode ser encontrada com mais detalhes no livro [6]. Porém, antes de definirmos este homomorfismo, primeiro veremos uma técnica bem útil para mergulharmos uma álgebra qualquer R em uma álgebra unitária. Aqui, uma álgebra A é chamada de unitária (ou com unidade) se existe um elemento em A, denotado por 1, tal que

$$a1 = a = 1a$$

para todo $a \in A$. Tal elemento 1 é chamado de unidade de A. Quando uma F-álgebra A for unitária, identificaremos o elemento $\alpha \in F$ com o elemento $\alpha 1 \in A$ e assim teremos $F \subseteq A$.

Definição 1.13 (Unitarização)**.** Seja R uma F-álgebra não unitária. Denote $R^{\#} = F \times R$ e defina as operações de adição, multiplicação por escalar e produto, respectivamente, por

$$\begin{aligned} (\alpha, r) + (\beta, s) &= (\alpha + \beta, r + s), \\ \beta(\alpha, r) &= (\beta\alpha, \beta r), \\ (\alpha, r) \cdot (\beta, s) &= (\alpha\beta, \beta r + \alpha s + rs), \end{aligned}$$

onde $\alpha, \beta \in F$ e $r, s \in R$. Temos que $R^{\#}$ é uma F-álgebra e $(1,0)$ é a sua unidade. Chamamos a álgebra $R^{\#}$ de unitarização de R.

Note que é possível mergulhar R em $R^{\#}$ através do homomorfismo injetor $\psi : R \to R^{\#}$ dado por

$$\psi(r) = (0, r).$$

Identificando R com $\psi(R)$, note que R é um ideal de $R^{\#}$.

Podemos, agora, seguir com a construção da representação regular. Seja R uma F-álgebra e L_a a multiplicação à esquerda por $a \in R$. Aqui, $L_a : R \to R$ é a transformação linear definida por

$$L_a(x) = ax$$

para todo $x \in R$. Note que a função $\phi : R \to End_F(R)$ definida por $\phi(a) = L_a$ é um homomorfismo de álgebras, pois

$$L_{\gamma a + \lambda b} = \gamma L_a + \lambda L_b \text{ e } L_{ab} = L_a \circ L_b$$

para todos $a, b \in A$ e $\gamma, \lambda \in F$. Com isso em mente, temos a seguinte definição.

Definição 1.14. O homomorfismo ϕ definido acima é chamado de representação regular de R.

O interessante da representação regular é que, quando ela for injetora, podemos mergulhar R em uma álgebra já muito estudada na Álgebra Linear. Para que a representação regular ϕ seja injetora basta mostrarmos que $\ker\phi = 0$, ou seja, mostrarmos que se $rR = 0$ então $r = 0$. Uma das formas de garantirmos isso é mostrando que R é unitária, pois desta forma teríamos

$$rR = 0 \Rightarrow r1 = r = 0.$$

Porém, mesmo quando a ϕ definida acima não for injetora, ainda podemos mergulhar R em um ambiente melhor.

Proposição 1.15. *Toda F-álgebra R pode ser mergulhada na álgebra $End_F(V)$ para algum F-espaço vetorial V. Se R tiver dimensão finita, então podemos tomar V com dimensão finita.*

Demonstração. Se R for unitária, então podemos tomar $V = R$ e aplicar a representação regular. Se R não for unitária, então podemos mergulhar R na sua unitarização $R^{\#}$ e, então, tomar $V = R^{\#}$. Em ambos os casos, se R tiver dimensão finita então V também terá. □

Aqui ainda vale um comentário referente a proposição: pelo Exemplo 1.12, se R tem dimensão finita n, então podemos mergulhar R em $M_n(F)$ (se R tem unidade) ou podemos mergulhar R em $M_{n+1}(F)$ (se R não tem unidade).

1.2 Produto tensorial

Uma definição importante que precisaremos nesta dissertação é o produto tensorial entra duas álgebras. Tal definição vem da definição do mesmo para espaços vetoriais. As demonstrações dos resultados apresentados nesta seção podem ser encontradas no Capítulo 4 do livro [6].

Definição 1.16. Sejam U e V dois espaços vetoriais sobre F. Seja P o espaço vetorial com base $U \times V$. Seja N o subespaço de P gerado por todos os elementos da forma

$$(\lambda u + \lambda' u', v) - \lambda(u, v) - \lambda'(u', v),$$
$$(u, \lambda v + \lambda' v') - \lambda(u, v) - \lambda'(u, v'),$$

onde $u, u' \in U,\ v, v' \in V$ e $\lambda, \lambda' \in F$. O produto tensorial de U e V é o espaço vetorial quociente P/N. Denotamos tal espaço por $U \otimes V$ (ou por $U \otimes_F V$).

Para trabalharmos melhor com tal definição podemos ver alguns resultados e características dos produtos tensoriais.

Teorema 1.17. *Sejam U e V espaços vetoriais sobre F. Então existe uma aplicação bilinear $\alpha : U \times V \to U \otimes V, \alpha(u, v) = u \otimes v$, tal que*

(a) Todo elemento em $U \otimes V$ é uma soma de elementos da forma $u \otimes v$ com $u \in U, v \in V$.

(b) Dada uma aplicação bilinear $\beta : U \times V \to W$, onde W é um espaço vetorial sobre F, existe uma aplicação linear $\overline{\beta} : U \otimes V \to W$ tal que $\overline{\beta}(u \otimes v) = \beta(u,v)$ para todo $u \in U$ e $v \in V$.

As propriedades (a) e (b) , a menos de isomorfismo, definem o produto tensorial $U \otimes V$.

Demonstração. A demonstração pode ser encontrada no Teorema 4.2 do livro [6]. □

Segue do item (a) que a transformação linear $\overline{\beta}$ é única.

Uma propriedade importante no teorema anterior é que a aplicação α é bilinear, isto é, para todo $\lambda, \lambda' \in F,\ u, u' \in U,\ v, v' \in V$ temos que:

$$(\lambda u + \lambda' u') \otimes v = \lambda(u \otimes v) + \lambda'(u' \otimes v),$$
$$u \otimes (\lambda v + \lambda' v') = \lambda(u \otimes v) + \lambda'(u \otimes v').$$

Segue direto destas fórmulas que $u \otimes 0 = 0 \otimes v = 0$ para todos $u \in U$ e $v \in V$.

Outra propriedade bem útil que temos sobre o produto tensorial é que é possível formar uma base do produto usando as bases dos espaços vetoriais.

Teorema 1.18. *Se $\{e_i \mid i \in I\}$ e $\{f_j \mid j \in J\}$ são bases de U e V, respectivamente, então*

$$\{e_i \otimes f_j \mid i \in I,\ j \in J\}$$

é uma base de $U \otimes V$.

Demonstração. A demonstração pode ser encontrada no Teorema 4.12 do livro [6]. □

Corolário 1.19. *Sejam U e V espaços vetoriais sobre F ambos de dimensão finita. Se* $\dim_F U = n$ *e* $\dim_F V = m$*, então* $\dim_F U \otimes V = nm$.

Demonstração. Consequência direta do teorema anterior. □

Agora que já mostramos algumas características do produto tensorial de dois espaços vetoriais podemos seguir com a definição do produto tensorial de duas álgebras. Para isso, precisamos do seguinte lema

Lema 1.20. *Se R e S são duas F-álgebras, então $R \otimes S$ será uma F-álgebra com a multiplicação definida por*

$$(r \otimes s)(r' \otimes s') = rr' \otimes ss'$$

para todos $r, r' \in R$ e $s, s' \in S$.

Demonstração. A demonstração pode ser encontrada no Lema 4.19 do livro [6]. □

Dados $u, v \in R \otimes S$, podemos escrevê-los como

$$u = \sum_i r_i \otimes s_i \text{ e } v = \sum_j r'_j \otimes s'_j$$

Pelo lema anterior, o produto entre quaisquer dois elementos $u, v \in R \otimes S$ é

$$uv = \sum_i \sum_j r_i r'_j \otimes s_i s'_j.$$

O espaço vetorial $R \otimes S$ com o produto definido acima é uma álgebra, chamada de produto tensorial das álgebras R e S.

Algumas propriedades importantes que temos do produto tensorial, tanto de espaços vetoriais quanto de álgebras, são as seguintes: para todas F-álgebras (ou F-espaços vetoriais) R, R', S, S', T vale:

1. $R \otimes S \cong S \otimes R$,
2. $(R \otimes S) \otimes T \cong R \otimes (S \otimes T)$,
3. $R \otimes F \cong R$ e $F \otimes S \cong S$,
4. Se $R \cong R'$ e $S \cong S'$, então $R \otimes S \cong R' \otimes S'$.

Um último resultado que nos será bem útil é o seguinte.

Proposição 1.21. *Para toda F-álgebra R e todo $n \geq 1$ temos que*

$$M_n(F) \otimes R \cong M_n(R).$$

Demonstração. Seja $f : M_n(F) \times R \to M_n(R)$ definida por $f(m, r) = mr$. Aqui, mr é a matriz obtida a partir de m por multiplicando cada uma de suas entradas por r. Temos que f será uma aplicação bilinear. Logo, pelo item (b) do Teorema 1.17, existe uma transformação linear $\overline{f} : M_n(F) \otimes R \to M_n(R)$ tal que $\overline{f}(m \otimes r) = mr$. Note que $\overline{f}$ será um homomorfismo de álgebras. De fato, se $m, m' \in M_n(F)$ e $r, r' \in R$, então

$$\begin{aligned} \overline{f}((m \otimes r) \cdot (m' \otimes r')) &= \overline{f}(mm' \otimes rr') \\ &= (mm')(rr') \\ &= (mr)(m'r') \\ &= \overline{f}(m \otimes r)\overline{f}(m' \otimes r'). \end{aligned}$$

Nos resta mostrar que $\overline{f}$ é um isomorfismo. Sabemos que todo elemento de $M_n(R)$ pode ser escrito da forma

$$\sum_{i=1}^{n} \sum_{j=1}^{n} e_{ij} a_{ij},$$

onde $a_{ij} \in R$. Portanto,

$$\overline{f}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} e_{ij} \otimes a_{ij}\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} e_{ij}a_{ij},$$

e todo elemento de $M_n(R)$ está na imagem de $\overline{f}$, ou seja, $\overline{f}$ é sobrejetora. É fácil ver que o núcleo (kernel) de $\overline{f}$ é o espaço nulo e, portanto, $\overline{f}$ é injetora. Logo, $\overline{f}$ é bijetora e, portanto, um isomorfismo de álgebras. □

1.3 Módulos e bimódulos

Estudaremos agora um pouco da teoria dos módulos. A Teoria dos módulos é uma área que estuda módulos e bimódulos. Ela possui muitas ligações com a teoria dos anéis e, portanto, com a de álgebras. Veremos um breve resumo com algumas definições e resultados que podem ser encontrados em [27] e [6]. No final da seção veremos o Teorema 1.37, um resultado de extrema importância para o nosso resultado principal.

Para começar, precisamos definir o que é um módulo.

Definição 1.22. Seja R uma F-álgebra. Um R-módulo à esquerda é um F-espaço vetorial M junto com uma aplicação $(r,m) \mapsto rm$ saindo de $R \times M$ e chegando em M de forma que, para todos $r,s \in R$ e $m,n \in M$, valem as seguintes propriedades:

1. $(r+s)m = rm + sm$;
2. $r(m+n) = rm + rn$;
3. $r(sm) = (rs)m$.

Se R for uma álgebra com unidade e $1m = m$ para todo $m \in M$, então M é chamado R-módulo unitário à esquerda.

De forma análoga, definimos R-módulo e R-módulo unitário à direita invertendo as posições dos elementos de R e M.

Note que se R for comutativa, então todo R-módulo à esquerda será um R-módulo à direita se definirmos

$$mr = rm,\ m \in M,\ r \in R.$$

Portanto, só faz sentido separarmos os módulos em à esquerda e à direita quando R não for comutativa. A partir daqui, quando não especificado, chamaremos os R-módulos à esquerda de R-módulos.

Exemplo 1.23. Um espaço vetorial sobre um corpo F é um F-módulo unitário.

Exemplo 1.24. Seja $R = End_F(M)$, onde M é F-espaço vetorial. Temos que M é um R-módulo unitário com a aplicação $(f,m) \mapsto fm = f(m),\ f \in R,\ m \in M$.

Exemplo 1.25. Seja M um F-espaço vetorial de dimensão finita. Fixe $T \in End_F(M)$. Então M é um $F[x]$-módulo com a aplicação $(f(x), m) \mapsto f(x)m = (f(T))(m),\ f(x) \in F[x],\ m \in M$.

Exemplo 1.26. Um ideal à esquerda L de R é um R-módulo à esquerda, onde a aplicação $(r, l) \mapsto rl$ é o produto da álgebra R. Em particular, R é um R-módulo à esquerda.

De forma semelhante, um ideal à direita D de R é um R-módulo à direita. Em particular, R é um R-módulo à direita.

Note que pelo exemplo anterior, um ideal (bilateral) I de R é um R-módulo à esquerda e à direita. Portanto, como veremos em breve, I é um exemplo de R-bimódulo.

Definição 1.27. Sejam R uma álgebra e M um R-módulo. Um subconjunto L de M é chamado de submódulo de M se é um subespaço de M e se, para todos $r \in R$ e $l \in L$, tem-se $rl \in L$.

Exemplo 1.28. Se M é um R-módulo e $m \in M$, então $Rm = \{rm \mid r \in R\}$ é um submódulo de M.

Um conceito importante envolvendo submódulos é o de módulo simples.

Definição 1.29. Seja R uma álgebra. Um R-módulo M é chamado de simples se $RM \neq 0$ e se seus únicos submódulos são 0 e M.

Exemplo 1.30. O R-módulo M do Exemplo 1.24 é simples se $M \neq 0$. De fato:

(a) $RM \neq 0$, pois $Id \in R$.

(b) Se $W \neq 0$ é um submódulo de M, fixe um elemento não nulo $w \in W$. Da Álgebra Linear, M admite uma base B tal que $w \in B$. Ainda da Álgebra Linear, dado $m \in M$ existe $T \in End_F(M)$ tal que $T(w) = m$ e $T(b) = 0$ para os demais elementos b em B. Logo, $Tw = T(w) = m \in W$ e temos $W = M$.

Definição 1.31. O anulador de um R-módulo M é o conjunto definido por

$$ann_R(M) := \{r \in R \mid rM = 0\},$$

onde $rM = \{rm \mid m \in M\}$.

Note que o anulador é um ideal bilateral de R.

Exemplo 1.32. No Exemplo 1.25, temos que $f(x) \in ann_{F[x]}(M)$ se, e somente se, $f(x)m = 0$ para todo $m \in M$. Como $f(x)m = (f(T))(m)$, temos que

$$ann_{F[x]}(M) = \{f(x) \in F[x] \mid f(T) = 0 \text{ (função nula)}\}.$$

Da Álgebra Linear, sabemos que tal ideal é gerado pelo polinômio minimal do operador T.

Definição 1.33. Seja R uma álgebra. Um ideal I de R é dito primitivo se I é o anulador de um R-módulo simples.

Com isso, podemos definir o Radical de Jacobson que será de suma importância nesta dissertação.

Definição 1.34. O Radical de Jacobson de uma álgebra R, denotado por $Jac(R)$ (ou $rad(R)$ dependendo do autor), é a intersecção de todos os ideais primitivos de R. Se R não possuir ideais primitivos, dizemos que $Jac(R) = R$.

Em breve daremos uma outra caracterização para o radical de Jacobson de uma álgebra de dimensão finita.

Definição 1.35. Sejam R e S duas álgebras. Se M é um R-módulo à esquerda e, ao mesmo tempo, um S-módulo à direita tal que

$$(rm)s = r(ms) \text{ para todos } r \in R,\ m \in M,\ s \in S,$$

então M é um (R,S)-bimódulo. Neste caso, se $R = S$ então dizemos que M é um R-bimódulo.

Seguiremos, agora, com a definição de elemento distinguível e com o principal resultado da seção.

Definição 1.36. Seja F um corpo e M um F-bimódulo unitário.

1. Dizemos que $x \in M$ é um elemento distinguível de M sobre F se existe um automorfismo σ do corpo F tal que $xa = \sigma(a) \cdot x$ para todo a em F.

2. Dizemos que uma base $\{x_i\}_{i \in I}$ de M como um F-espaço vetorial à esquerda é uma base distinguível se cada elemento dela é distinguível.

Na definição acima, $\sigma(a) \cdot x$ representa o produto $\sigma(a)x$, mas optamos por destacar o produto $\cdot$.

Teorema 1.37. *Seja M um F_q-bimódulo unitário de dimensão finita, onde F_q é um corpo finito com q elementos. Então M possui ao menos uma base distinguível sobre F_q.*

Demonstração. Podemos encontrar a demonstração deste teorema em [27, Teorema 1]. □

1.4 Teoremas de Wedderburn sobre as estruturas das álgebras de dimensão finita

Vimos algumas definições e propriedades básicas das álgebras associativas. Veremos agora os Teoremas de Wedderburn que são resultados interessantes sobre a estrutura de tais álgebras quando sua dimensão for finita. As referências utilizadas aqui foram [6], [2] e [29].

Definição 1.38. Uma álgebra unitária R é chamada de álgebra de divisão se para todo $r \in R$ existe $s \in R$ tal que

$$rs = sr = 1.$$

Neste caso, denotamos $s = r^{-1}$ e o chamamos de inverso de r.

Todo corpo F é uma F-álgebra de divisão. Os quatérnions $\mathbb{H}$ é uma $\mathbb{R}$-álgebra de divisão "infinita" que não é um corpo. Podemos nos perguntar: existem álgebras de divisão "finitas" que não são corpos? O primeiro teorema de Wedderburn abaixo, que pode ser encontrado na Seção 1.8 do livro do [6], responde esta pergunta.

Teorema 1.39 (Wedderburn)**.** *Toda álgebra de divisão finita é um corpo.*

Para o nosso próximo resultado precisaremos de algumas definições.

Definição 1.40. Uma álgebra R é dita simples se $R^2 \neq 0$ e seus únicos ideais são 0 e R.

Um exemplo comum de álgebra simples é o seguinte.

Exemplo 1.41. A álgebra $M_n(D)$ das matrizes de ordem $n \geq 1$ com entradas numa álgebra de divisão D é simples. De fato, sejam e_{ij} as usuais matrizes canônicas. Como D possui unidade 1, então $M_n(D)$ também possui unidade e, portanto, $M_n(D)^2 \neq 0$.

Suponha que $I \neq 0$ é um ideal de $M_n(D)$. Como $I \neq 0$, existe $A = (a_{ij})_{ij} \in I$ não nulo. Neste caso, existem t, l tais que $a_{tl} \neq 0$. Note que

$$e_{it} A e_{lj} = a_{tl} e_{ij}$$

para todos i, j. Logo, como I é um ideal, temos $a_{tl} e_{ij} \in I$ e também $e_{ij} = (a_{tl}^{-1} Id_n)(a_{tl} e_{ij}) \in I$. Assim, $Id_n = e_{11} + \cdots + e_{nn} \in I$ e $I = M_n(D)$.

Definição 1.42. Uma álgebra é dita prima se o produto de quaisquer dois ideais não nulos dela é não nulo.

Note que toda álgebra R simples será prima, pois $RR = R^2 \neq 0$ é o único produto de ideais não nulos possível em uma álgebra simples. Porém, nem toda álgebra prima é simples como nos mostra o seguinte exemplo.

Exemplo 1.43. A álgebra $F[t]$ é prima mas não é simples. De fato, como $F[t]$ é um domínio de integridade, se I e J são dois ideais não nulos de $F[t]$, então existem $0 \neq f \in I$ e $0 \neq g \in J$ tais que $0 \neq fg \in IJ$, provando assim que $F[t]$ é prima. Por outro lado, o subconjunto de $F[t]$ formado pelos polinômios $f(t)$ com termo constante nulo ($f(0) = 0$) é um ideal de $F[t]$ diferente dos triviais.

Na verdade é possível se dizer mais do que apenas isso sobre as álgebras primas, o lema a seguir nos traz quatro condições equivalentes para uma álgebra ser prima.

Lema 1.44. *Seja R uma álgebra. As seguintes condições são equivalentes:*

1. *Para todos $a, b \in R$, $aRb = 0$ implica que $a = 0$ ou $b = 0$;*
2. *Para todos ideais à esquerda I e J de R, $IJ = 0$ implica que $I = 0$ ou $J = 0$;*
3. *Para todos ideais à direita I e J de R, $IJ = 0$ implica que $I = 0$ ou $J = 0$;*

4. *R é prima.*

Demonstração. A demonstração pode ser encontrada no Lema 2.17 do livro [6]. □

Com estas definições, já podemos seguir com o segundo Teorema de Wedderburn.

Teorema 1.45 (Wedderburn)**.** *Seja R uma F-álgebra de dimensão finita não nula. As seguintes sentenças são equivalentes:*

- *R é prima;*
- *R é simples;*
- *Existe um $n \in \mathbb{N}$ e uma F-álgebra de divisão D tal que $R \cong M_n(D)$.*

Demonstração. A prova pode ser encontrada no Lema 2.61 do livro [6]. □

Corolário 1.46. *Seja R uma álgebra de dimensão finita não nula sobre um corpo finito F. Então, R é simples se, e somente se, existe $n \in \mathbb{N}$ e um corpo finito D tal que $F \subseteq D$ e $R \cong M_n(D)$.*

Demonstração. Suponha que R é simples. Pelo Teorema 1.45, existe $n \in \mathbb{N}$ e uma F-álgebra de divisão D tal que $R \cong M_n(D)$. Como D é finita, pelo Teorema 1.39 temos que D é um corpo. A recíproca já é conhecida. □

Aqui cabe um comentário: no teorema acima, a hipótese "R uma álgebra de dimensão finita não nula sobre um corpo finito F" pode ser trocada por "R uma F-álgebra finita não nula" pois são informações equivalentes.

Para os próximos resultados serão necessárias mais algumas definições.

Definição 1.47. Um ideal I de uma álgebra R é dito nilpotente se existe um $n \in \mathbb{N}$ tal que $I^n = 0$.

Exemplo 1.48. O ideal R das matrizes estritamente triangulares superiores de ordem n é um ideal nilpotente de $U_n(F)$ pois $R^n = 0$.

Lema 1.49. *A soma de dois ideais nilpotentes de uma álgebra é um ideal nilpotente.*

Demonstração. Sejam I e J ideais tais que $I^n = J^m = 0$. Provaremos que $(I+J)^{n+m-1} = 0$. Se u é um produto de $n+m-1$ elementos da forma $a+b$, onde $a \in I$ e $b \in J$, então u pode ser escrito como uma soma de elementos da forma

$$w = w_1 w_2 \cdots w_{n+m-1},$$

onde $w_i \in I \cup J$ para todo $1 \leq i \leq n+m-1$. Note que se n dos $n+m-1$ fatores w_i pertencem a I, então $w = 0$, pois $I^n = 0$. Porém, se menos de n elementos pertencem a I, então pelo menos m fatores pertencem a J, o que implica que $w = 0$, pois $J^m = 0$.

Desta forma temos que, independente do caso, $w = 0$ e portanto $u = 0$, o que prova o resultado. □

Definição 1.50. Dada uma álgebra R, dizemos que o ideal nilpotente maximal de R é o radical de R, se ele existir.

Proposição 1.51. *Se o radical de uma álgebra R existe, então ele contém todos os ideais nilpotentes de R. Em particular, o radical de R é único.*

Demonstração. Seja N o radical de R e I um ideal nilpotente. Pelo Lema 1.49 temos que $I+N$ é um ideal nilpotente. Porém, como $N \subseteq I+N$ e N é maximal, temos que $N = I+N$, logo $I \subseteq N$. □

Teorema 1.52. *Se R é uma álgebra de dimensão finita, então o seu radical existe e coincide com o radical de Jacobson de R.*

Demonstração. Como R é de dimensão finita, ele admite um ideal nilpotente de maior dimensão. Tal ideal é o radical de R. Agora, a demonstração de que o radical e o radical de Jacobson coincidem pode ser encontrada no Teorema 5.46 do livro [6]. □

Definição 1.53. Uma álgebra R é dita semiprima se ela não possui ideais nilpotentes não nulos.

Assim como no caso das álgebras primas, podemos criar outras maneiras equivalentes de se definir uma álgebra semiprima, veja o próximo lema.

Lema 1.54. *Seja R uma álgebra. As seguintes condições são equivalentes:*

1. *Para todo $a \in R$, $aRa = 0$ implica que $a = 0$;*
2. *Para todo ideal à esquerda I de R, $I^2 = 0$ implica que $I = 0$;*
3. *Para todo ideal à direita I de R, $I^2 = 0$ implica que $I = 0$;*
4. *Para todo ideal I de R, $I^2 = 0$ implica que $I = 0$;*
5. *R é semiprima.*

Demonstração. A prova pode ser encontrada no Lema 2.21 do livro [6]. □

Corolário 1.55. *Toda álgebra prima é semiprima.*

Demonstração. Seja R uma álgebra prima. Pelo Lema 1.44 temos que para todos $a, b \in R$, $aRb = 0$ implica que $a = 0$ ou $b = 0$; em particular, $aRa = 0$ implica que $a = 0$. Portanto, pelo lema anterior, temos que R é semiprima. □

Dada uma álgebra R e um ideal nilpotente I de R, seja $n \in \mathbb{N}$ tal que

$$I^n = 0 \text{ mas } I^{n-1} \neq 0.$$

Dizemos que n é o índice de nilpotência de I.

Lema 1.56. *Se N é o radical de uma álgebra R de dimensão finita, então a álgebra quociente R/N é semiprima.*

Demonstração. Sejam n o índice de nilpotência de N e J um ideal nilpotente de R/N. Temos que $J = I/N$ para algum ideal I de R que contém N. Como J é nilpotente, então $J^k = 0$ para algum $k \in \mathbb{N}$. Logo, $I^k \subseteq N$. Como $N^n = 0$, segue que $I^{kn} = 0$, ou seja, I é ideal nilpotente de R. Pelo fato de N ser o radical de R, então $I \subseteq N$ e $J = I/N = 0$.

Provamos que todo ideal nilpotente de R/N é nulo. Logo, R/N é semiprima. □

Com isso, seguem os próximos teoremas.

Teorema 1.57 (Wedderburn)**.** *Seja R uma F-álgebra não nula de dimensão finita. Então R é semiprima se, e somente se, existem $n_1, \ldots, n_s \in \mathbb{N}$ e F-álgebras de divisão $D_1, \ldots, D_s$ tais que*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s).$$

Demonstração. Provaremos apenas a volta deste teorema. Primeiro note que se D é uma álgebra de divisão, então $R \cong M_n(D)$ é semiprima. De fato, pelo Teorema 1.45 temos que R é prima e, pelo Corolário 1.55, R é semiprima.

Suponha agora que $R \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s)$, onde $D_1, \ldots, D_s$ são álgebras de divisão. Se $a \in R$, então $a = (a_1, \ldots, a_s)$, onde $a_i \in M_{n_i}(D_i)$. Como

$$aRa = a_1 M_{n_1}(D_1) a_1 \times \cdots \times a_s M_{n_s}(D_s) a_s,$$

temos que se $aRa = 0$, então $a_i M_{n_i}(D_i) a_i = 0$ para todo $1 \leq i \leq s$. Porém, como cada $M_{n_i}(D_i)$ é, pelo primeiro caso, semiprima, então $a_i M_{n_i}(D_i) a_i = 0$ implica que $a_i = 0$. Ou seja, $aRa = 0$ implica que $a = 0$ e, portanto, R é semiprima.

A implicação $(\Rightarrow)$ deste teorema pode ser encontrada no Teorema 2.64 do livro [6]. □

Observação 1.58. É interessante destacar que decorre deste teorema que, como as álgebras $M_{n_i}(D_i)$ possuem unidade, toda álgebra semiprima tem unidade.

Corolário 1.59. *Seja R uma álgebra de dimensão finita não nula sobre um corpo finito F. Então, R é semiprima se, e somente se, existem $n_1, \ldots, n_s \in \mathbb{N}$ e corpos finitos $D_1, \ldots, D_s$ tais que*

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_s}(D_s).$$

Demonstração. É resultado direto dos Teoremas 1.39 e 1.57. □

Relembramos do Teorema 1.52 que toda álgebra de dimensão finita tem radical. Ainda pelo Teorema 1.52, cabe observar que no enunciado do próximo teorema podemos trocar a hipótese "radical" por "radical de Jacobson".

Teorema 1.60 (Teorema Principal de Wedderburn)**.** *Seja R uma F-álgebra de dimensão finita sobre um corpo perfeito F e seja N o seu radical. Então existe uma subálgebra S de R isomorfa a R/N tal que R, considerado como F-espaço vetorial, é a soma direta dos subespaços S e N.*

Demonstração. No que diz respeito ao enunciado do teorema, a definição de corpo perfeito pode ser encontrada no apêndice desta dissertação.

A demonstração do caso em que a álgebra tem unidade pode ser encontrada no Teorema 2.5.37 da página 163 do livro [29].

Agora, suponha que a álgebra R não tem unidade. Seja $R^{\#} = F \times R$ a unitarização de R. Como o teorema é válido para $R^{\#}$, pois ele é unitário e de dimensão finita, podemos decompô-lo na soma direta de "subespaços vetoriais"

$$R^{\#} = \tilde{S} \oplus \tilde{N},$$

onde $\tilde{N}$ é o radical de $R^{\#}$, e $\tilde{S}$ é uma subálgebra de $R^{\#}$ isomorfa a $R^{\#}/\tilde{N}$.

Denote por S o conjunto

$$S = \{s \in R \mid (0,s) \in \tilde{S}\}$$

e denote por N o radical de R. Mostraremos que S é uma subálgebra de R isomorfa a R/N e que $R = S \oplus N$.

É fácil notar que S é uma subálgebra de R e que $0 \times N$ é um ideal nilpotente de $R^{\#}$. Pela Proposição 1.51, temos que $0 \times N \subseteq \tilde{N}$. Por outro lado, seja $n \geq 1$ tal que $\tilde{N}^n = 0$. Se $(\alpha, r) \in \tilde{N}$, então

$$0 = (0,0) = (\alpha, r)^n = (\alpha^n, r')$$

para algum $r' \in R$ e, portanto, $\alpha = 0$. Ou seja, $\tilde{N} = 0 \times N'$ para algum ideal nilpotente N' de R. Logo, $N' \subseteq N$ e $\tilde{N} = 0 \times N$.

Como $\tilde{S} \cap \tilde{N} = 0$, $0 \times S \subseteq \tilde{S}$ e $0 \times N = \tilde{N}$, segue que $(0 \times S) \cap (0 \times N) = 0$ e, portanto, $S \cap N = 0$. Nos resta provar que $R = S \oplus N$. Seja $r \in R$. Como $(0,r) \in R^{\#}$, existem $(\alpha, s) \in \tilde{S}$ e $(0,t) \in \tilde{N} = 0 \times N$ tais que

$$(0,r) = (\alpha, s) + (0,t) = (\alpha, s+t).$$

Logo, $\alpha = 0$ e, portanto, $s \in S$. Com isso, provamos que se $r \in R$, então $r = s + t$ onde $s \in S$ e $t \in N$, isto é, $R = S \oplus N$.

□

Pelo Teorema A.7 do apêndice desta dissertação, temos que todo corpo finito é perfeito. Logo, o resultado abaixo é uma consequência direta do anterior e do Lema 1.56.

Teorema 1.61. *Seja R uma álgebra de dimensão finita sobre um corpo finito F, e seja N o radical de R. Então existe uma subálgebra semiprima S de R isomorfa a R/N tal que R, considerado como F-espaço vetorial, é a soma direta dos subespaços S e N.*

1.5 Soma subdireta

Nesta seção vamos estudar o conceito de soma subdireta e álgebras subdiretamente irredutíveis. Tais conceitos serão extremamente importantes para a demonstração do nosso resultado principal pois, usando o Teorema 1.66, poderemos reduzir nossos estudos de álgebras finitas a somente o caso de álgebras subdiretamente irredutíveis finitas. Podemos encontrar mais detalhes em [15].

Começamos esta seção vendo a definição de soma subdireta.

Definição 1.62. Seja π_i a projeção de $\prod_{i\in I} R_i$ em R_i. Dizemos que uma álgebra R é uma soma subdireta das álgebras R_i se existir um homomorfismo injetor $\phi : R \to \prod_{i\in I} R_i$ tal que $(\pi_i \circ \phi)(R) = R_i$ para todo $i \in I$.

A ideia principal da soma subdireta é mergulhar a álgebra R em um produto direto de R_i de forma que a projeção de R cubra todas as R_i sem que R precise cobrir o produto inteiro. Os seguintes lemas nos ajudarão a trabalhar com esta definição.

Lema 1.63. *R é uma soma subdireta das álgebras R_i, $i \in I$, se, e somente se, existem homomorfismos sobrejetores $\varphi_i : R \to R_i$ tais que $\bigcap_{i\in I} \ker \varphi_i = 0$.*

Demonstração. Suponha que R é uma soma subdireta das álgebras R_i, $i \in I$. Pela definição, existe um homomorfismo injetor $\varphi : R \to \prod_{i\in I} R_i$ tal que $(\pi_i \circ \varphi)(R) = R_i$ para todo $i \in I$. Para cada i podemos definir

$$\begin{aligned} \varphi_i &: R \to R_i \\ &\varphi_i(r) = (\pi_i \circ \varphi)(r). \end{aligned}$$

Note que φ_i é sobrejetor, pois $\varphi_i(R) = (\pi_i \circ \varphi)(R) = R_i$. Além disso, temos que

$$\begin{aligned} \bigcap_{i\in I} \ker \pi_i &= \bigcap_{i\in I} \left\{ f \in \prod_{j\in I} R_j \mid f(i) = 0 \right\} \\ &= \left\{ f \in \prod_{j\in I} R_j \mid f(i) = 0 \text{ para todo } i \in I \right\} = 0. \end{aligned}$$

Portanto, como φ é injetora,

$$\begin{aligned} \bigcap_{i\in I} \ker \varphi_i &= \bigcap_{i\in I} \ker(\pi_i \circ \varphi) \\ &= \bigcap_{i\in I} \{ r \in R \mid \varphi(r) \in \ker \pi_i \} \\ &= \{ r \in R \mid \varphi(r) \in \ker \pi_i \text{ para todo } i \in I \} \\ &= \{ r \in R \mid \varphi(r) = 0 \} \\ &= \ker \varphi = 0. \end{aligned}$$

Por outro lado, suponha que existam homomorfismos sobrejetores $\varphi_i : R \to R_i$ tais que $\cap_{i\in I} \ker \varphi_i = 0$. Dado $r \in R$ definimos a função $f_r : I \to \cup_{i\in I} R_i$ como $f_r(i) = \varphi_i(r)$. Pela construção temos que $f_r \in \prod_{i\in I} R_i$. Além disso, a aplicação φ definida por

$$\begin{aligned} \varphi \quad : \quad & R \to \prod_{i\in I} R_i \\ & \varphi(r) = f_r \end{aligned}$$

é um homomorfismo tal que $(\pi_i \circ \varphi)(R) = \varphi_i(R) = R_i$ e

$$\begin{aligned} \ker \varphi &= \{r \in R \mid f_r = 0\} \\ &= \{r \in R \mid f_r(i) = 0 \text{ para todo } i \in I\} \\ &= \{r \in R \mid \varphi_i(r) = 0 \text{ para todo } i \in I\} \\ &= \cap_{i\in I} \ker \varphi_i = 0. \end{aligned}$$

Logo, φ é injetora. □

O próximo lema é consequência direta deste último.

Lema 1.64. *R é uma soma subdireta das álgebras R_i, $i \in I$, se, e somente se, existem ideais r_i de R tais que $R/r_i \cong R_i$ e $\bigcap_{i\in I} r_i = 0$.*

Demonstração. Se R é soma subdireta dos R_i, então pelo lema anterior, temos que existem homomorfismos sobrejetores $\varphi_i : R \to R_i$ tais que $\bigcap_{i\in I} \ker \varphi_i = 0$. Como $\ker \varphi_i$ é um ideal de R e $R/\ker \varphi_i \cong R_i$ temos que existem os ideais $r_i = \ker \varphi_i$ tais que $\bigcap_{i\in I} r_i = 0$.

Agora, suponha que existem ideais r_i de R tais que $R/r_i \cong R_i$ e $\bigcap_{i\in I} r_i = 0$. Denote por $\eta_i : R/r_i \to R_i$ tal isomorfismo. Definindo $\varphi_i : R \to R_i$ por

$$\varphi_i(x) = \eta_i(x + r_i)$$

teremos que tais funções satisfazem as condições do último lema. Logo, R é a uma soma subdireta das álgebras R_i, $i \in I$. □

Seja $\{r_i \mid i \in I\}$ uma família de ideais de R. Pelo lema acima, se algum r_j é o ideal nulo, então R é uma soma subdireta das álgebras R/r_i, $i \in I$. Mas tal decomposição não é interessante, ou seja, estamos interessados nas somas subdiretas cujos ideais envolvidos são todos não nulos. Diante disso, podemos pensar nas álgebras que não admitem tal decomposição (ambientes mais "simples"), o que nos leva a seguinte definição.

Definição 1.65. Uma álgebra é subdiretamente irredutível se a intersecção de todos os ideais não nulos dela é não nulo.

Teorema 1.66. *Qualquer álgebra finita é isomorfa a uma soma subdireta finita de álgebras subdiretamente irredutíveis finitas.*

Demonstração. Seja R uma álgebra finita. Para cada $0 \neq a \in R$, denote por I_a o conjunto de todos os ideais de R que não contêm a. Note que $\{0\} \in I_a$, ou seja, $I_a \neq \emptyset$. Como R é um conjunto finito, temos que I_a é finito. Logo, I_a admite pelo menos um elemento maximal (com respeito a inclusão), que denotaremos por M_a. Portanto, se J é um ideal de R tal que $a \notin J$ e $M_a \subseteq J$, então $M_a = J$.

Pela construção dos ideais M_a, segue que

$$\bigcap_{a \in R} M_a = 0,$$

pois do contrário, existiria um elemento $0 \neq x \in R$ tal que $x \in M_a$ para todo $a \in R$ e, em particular, $x \in M_x$, o que seria um absurdo. Portanto, pelo Lema 1.64, R é uma soma subdireta das álgebras R/M_a, onde $a \in R - \{0\}$. Como R é finita, segue que R/M_a é finita para todo $a \in R$ e existe uma quantidade finita de tais álgebras. Portanto, resta-nos provar que cada R/M_a é subdiretamente irredutível.

Dado um ideal J_a de R/M_a, temos $J_a = J/M_a$ para algum ideal J de R com $M_a \subseteq J$. Se $J_a \neq 0$, então J contém propriamente M_a; neste caso, pela maximalidade de M_a, temos $a \in J$ e $0 \neq (a + M_a) \in J_a$. Portanto, a interseção de todos os ideais não nulos de R/M_a é não nula, pois contém o elemento $(a + M_a) \neq 0$. Isso prova que R/M_a é subdiretamente irredutível. □

CAPÍTULO 2

PI-Álgebras

Entraremos, agora, na teoria das PI-álgebras, onde veremos as definições iniciais desta área e alguns resultados importantes sobre T-ideais, variedades e álgebras algébricas. Para um maior aprofundamento do assunto, veja as referências [22],[15] e [8]. Ao longo deste capítulo, F é um corpo e todas as álgebras e espaços vetoriais serão sobre F, a menos que se diga algo contrário. Além disso, todas as álgebras consideradas aqui são associativas.

2.1 Álgebra Livre

O nosso principal objetivo nesta dissertação é encontrar o T-ideal das identidades polinomiais da álgebra das matrizes 2×2 com entradas em um corpo finito. Os resultados desta seção vem nos ajudar neste objetivo e podem ser encontrados em [22].

O primeiro passo para entrarmos na teoria das PI-álgebras é entender o que é a álgebra associativa livre, mas para isso primeiro precisamos definir o que é uma subálgebra gerada por um subconjunto.

Definição 2.1. Dado um subconjunto $X \neq \emptyset$ de uma álgebra A, definimos a subálgebra de A gerada por X como sendo a interseção de todas as subálgebras de A que contêm X.

Note que, pela definição, a subálgebra de A gerada por X é a menor subálgebra que contém X. É fácil mostrar que ela é, de fato, uma álgebra e, além disso, é possível descrevê-la de uma forma mais precisa.

Proposição 2.2. *Dado um subconjunto $X \neq \emptyset$ de uma álgebra associativa A, a subálgebra de A gerada por X é a álgebra formada por todos os elementos da forma*

$$\sum_i \alpha_i x_{i_1} x_{i_2} \cdots x_{i_n},$$

onde $\alpha_i \in F$, $i = (i_1, i_2, \ldots, i_n)$, $x_{i_1}, x_{i_2}, \ldots, x_{i_n} \in X$ e $n \geq 1$.

Demonstração. Denote por B o subconjunto de A formado por todos os elementos da forma

$$\sum_i \alpha_i x_{i_1} x_{i_2} \cdots x_{i_n},$$

onde $\alpha_i \in F$, $i = (i_1, i_2, \ldots, i_n)$, $x_{i_1}, x_{i_2}, \ldots, x_{i_n} \in X$ e $n \geq 1$. Note que toda subálgebra de A que contém X necessariamente contém B. Agora basta observar que B por si só também é uma subálgebra de A. □

Definida álgebra gerada, podemos agora seguir com a definição de álgebra livre de uma classe de álgebras.

Definição 2.3. Seja $\mathbb{D}$ uma classe de álgebras e seja $\mathscr{F} \in \mathbb{D}$ uma álgebra gerada por um conjunto X. Dizemos que $\mathscr{F}$ é uma álgebra livre em $\mathbb{D}$, livremente gerada por X, se para toda álgebra $R \in \mathbb{D}$, toda aplicação f de X em R pode ser estendida para um homomorfismo ϕ de $\mathscr{F}$ em R.

A álgebra livre na classe de todas as álgebras associativas é chamada de álgebra associativa livre. Tal nome vem do fato que ela é livre de quaisquer outras propriedades que não sejam a associatividade e aquelas que definem uma álgebra. É possível descrever a álgebra associativa livre da seguinte forma:

Seja X um conjunto infinito enumerável de letras $\{x_1, x_2, \ldots, x_n, \ldots\}$. Definimos uma palavra como uma sequência finita de letras concatenadas, isto é, $x_{n_1} x_{n_2} \cdots x_{n_k}$, em que as letras podem se repetir porém letras diferentes não podem comutar. Definimos a álgebra $F\langle X\rangle$ como a álgebra cuja base são todas as palavras

$$x_{n_1} x_{n_2} \cdots x_{n_k}, x_{n_j} \in X,\ k = 1, 2, \ldots,$$

e com multiplicação definida por justaposição, ou seja,

$$(x_{n_1} x_{n_2} \cdots x_{n_k})(x_{m_1} x_{m_2} \cdots x_{m_l}) = x_{n_1} x_{n_2} \cdots x_{n_k} x_{m_1} x_{m_2} \cdots x_{m_l}.$$

Vale ressaltar que $F\langle X\rangle$ não é unitária. Note que todo elemento de $F\langle X\rangle$ é escrito de maneira única como combinação linear de palavras e o produto entre quaisquer dois elementos de $F\langle X\rangle$ é obtido como no Exemplo 1.3. Vamos chamar os elementos $f \in F\langle X\rangle$ de polinômios. A álgebra $F\langle X\rangle$ é livre na classe de todas as álgebras associativas, livremente gerada por X. Ela é a álgebra associativa livre, livremente gerada por X.

Com isso, podemos finalmente definir o que é uma identidade polinomial e uma PI-álgebra.

Definição 2.4. Sejam $f = f(x_1, x_2, \ldots, x_n) \in F\langle X\rangle$ e R uma álgebra. Dizemos que f é uma identidade polinomial de R se

$$f(r_1, r_2, \ldots, r_n) = 0 \text{ para todos } r_1, r_2, \ldots, r_n \in R.$$

Denotamos por $T(R)$ o conjunto das identidades polinomiais de R. Se $T(R) \neq 0$ dizemos que R é uma PI-álgebra.

Exemplo 2.5. Qualquer álgebra comutativa é uma PI-álgebra, pois o polinômio comutador $f(x,y) = [x,y] = xy - yx$ é uma identidade para tais álgebras.

Exemplo 2.6. Toda álgebra R finita é uma PI-álgebra, pois tem o polinômio

$$f(x) = \prod_{1 \leq m < n \leq |R|+1} (x^m - x^n)$$

como identidade polinomial.

Exemplo 2.7. Se R é uma álgebra com dimensão finita k, então R é uma PI-álgebra, pois R satisfaz a identidade Standard

$$St_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} (-1)^{\sigma} x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$$

para todo $n > k$. Aqui, S_n é o grupo simétrico de $\{1, \ldots, n\}$, e $(-1)^{\sigma}$ é o sinal da permutação σ.

De fato, se $\{e_1, \ldots, e_k\}$ é uma base de R, como $St_n = St_n(x_1, \ldots, x_n)$ é um polinômio multilinear, basta provarmos que St_n se anula quando substituímos as suas variáveis por elementos da base de R, mas como $n > k$, ao menos um elemento e_i se repetirá nas variáveis o que anulará o polinômio. Uma demonstração mais detalhada pode ser encontrada na Proposição 2.1.6 de [22].

A seguir enunciamos o famoso Problema de Kurosh:

Problema. Se R é uma álgebra algébrica sobre F, um número finito de elementos de R sempre vai gerar uma subálgebra de dimensão finita de R?

Para entendermos este problema primeiro precisamos das definições de álgebra algébrica e localmente finita.

Definição 2.8. Seja R uma F-álgebra. Dizemos que um elemento $r \in R$ é algébrico se existe um polinômio $f(x) \in F[x]$ não nulo tal que $f(r) = 0$. Se todos os elementos de R são algébricos, dizemos que R é uma álgebra algébrica.

Toda álgebra de dimensão finita é algébrica. De fato, se R é uma F-álgebra de dimensão finita n e $r \in R$, então os elementos $r, r^2, \ldots, r^{n+1}$ devem ser linearmente dependentes, ou seja, existem $\alpha_1, \ldots, \alpha_{n+1} \in F$ não todos nulos tais que

$$\alpha_1 r + \alpha_2 r^2 + \cdots + \alpha_{n+1} r^{n+1} = 0.$$

Portanto, para todo $r \in R$ existe $f(x) = \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{n+1} x^{n+1} \in F[x]$ tal que $f(r) = 0$.

Definição 2.9. Uma F-álgebra R é dita localmente finita se toda subálgebra de R finitamente gerada tiver dimensão finita.

Observação 2.10. Seja R uma álgebra localmente finita e finitamente gerada. Como R é uma subálgebra de si mesma, então R tem dimensão finita.

Além disso, se F é um corpo finito, então uma álgebra R tem dimensão finita se, e somente se, R é finita.

Voltando para o Problema de Kurosh, já foi comprovado que ele não será verdade para toda álgebra. Porém, foi provado que se a álgebra for uma PI-álgebra então a resposta ao problema será sim.

Teorema 2.11. *Se R é uma álgebra algébrica e R é uma PI-álgebra, então R é localmente finita.*

Demonstração. A demonstração pode ser encontrada no Teorema 6.4.3 do livro [15]. □

2.2 T-ideais e variedades

Dada uma álgebra R, temos que $T(R)$ é um subespaço vetorial de $F\langle X\rangle$. Além disso, se $f = f(x_1,\ldots,x_n) \in T(R)$ e $u_1,u_2,g_1,\ldots,g_n \in F\langle X\rangle$, então

$$f(g_1,\ldots,g_n),\ u_1f(g_1,\ldots,g_n),\ f(g_1,\ldots,g_n)u_2,\ u_1f(g_1,\ldots,g_n)u_2$$

pertencem à $T(R)$. Ou seja, $T(R)$ é um ideal de $F\langle X\rangle$ que é invariante sobre qualquer endomorfismo de $F\langle X\rangle$. Com isso em mente, temos a seguinte definição.

Definição 2.12. Um ideal I de $F\langle X\rangle$ é chamado de T-ideal se ele é invariante por todos os endomorfismos de $F\langle X\rangle$, isto é, se $\psi(I) \subseteq I$ para todo endomorfismo ψ de $F\langle X\rangle$.

Um exemplo de T-ideal importante é o T-ideal gerado por um subconjunto $S \subset F\langle X\rangle$, conforme a próxima definição.

Definição 2.13. Dado $S \subset F\langle X\rangle$, $S \neq \emptyset$, dizemos que a interseção de todos os T-ideais que contêm S é o T-ideal gerado por S. Denotamos ele por $\langle S\rangle^T$.

Ou seja, $\langle S\rangle^T$ é o menor T-ideal que contém S. É possível descrever este T-ideal conforme o próximo teorema.

Teorema 2.14. *Se $S \subseteq F\langle X\rangle$, $S \neq \emptyset$, então $\langle S\rangle^T$ é o subespaço vetorial de $F\langle X\rangle$ gerado por todos os polinômios*

$$f(g_1,\ldots,g_n),\ u_1f(g_1,\ldots,g_n),\ f(g_1,\ldots,g_n)u_2,\ u_1f(g_1,\ldots,g_n)u_2, \tag{2.1}$$

onde $u_1,u_2,g_1,\ldots,g_n \in F\langle X\rangle$ e $f(x_1,\ldots,x_n) \in S$.

Demonstração. Denote por J o subespaço vetorial de $F\langle X\rangle$ gerado pelos polinômios em (2.1). Temos que J é um T-ideal e $S \subseteq J$. Logo, pela definição de T-ideal gerado, temos que $\langle S\rangle^T \subseteq J$. Por outro

lado, como $\langle S\rangle^T$ é um ideal de $F\langle X\rangle$ que contém S, segue que $\langle S\rangle^T$ contém o subespaço vetorial gerado pelos polinômios

$$f(x_1,\ldots,x_n),\ u_1f(x_1,\ldots,x_n),\ f(x_1,\ldots,x_n)u_2,\ u_1f(x_1,\ldots,x_n)u_2, \tag{2.2}$$

onde $u_1,u_2 \in F\langle X\rangle$ e $f(x_1,\ldots,x_n) \in S$. Como $\langle S\rangle^T$ também é invariante por endomorfismos de $F\langle X\rangle$, segue que $\langle S\rangle^T$ contém J. Logo, $J = \langle S\rangle^T$. □

Lema 2.15. *Se I é um T-ideal de $F\langle X\rangle$, então*

$$T\left(\frac{F\langle X\rangle}{I}\right) = I.$$

Demonstração. Para provar $(\supseteq)$, seja $f(x_1,\ldots x_n) \in I$ e sejam $f_1+I,\ldots,f_n+I \in F\langle X\rangle/I$, onde $f_1,\ldots,f_n \in F\langle X\rangle$. Como I é um T-ideal, segue que $f(f_1,\ldots,f_n) \in I$ e, portanto,

$$f(f_1+I,\ldots,f_n+I) = f(f_1,\ldots,f_n)+I = I = 0.$$

Logo, $f(x_1,\ldots,x_n) \in T(F\langle X\rangle/I)$.

Para provar $(\subseteq)$, seja $f(x_1,\ldots,x_n) \in T(F\langle X\rangle/I)$. Em particular, temos

$$I = 0 = f(x_1+I,\ldots,x_n+I) = f(x_1,\ldots,x_n)+I.$$

Logo, $f(x_1,\ldots,x_n) \in I$. □

Como já comentado no início desta seção, se R é uma álgebra, então $T(R)$ é um T-ideal. Agora, se I é um T-ideal, então $R = \frac{F\langle X\rangle}{I}$ será uma álgebra tal que $T(R) = I$. Portanto, o conjunto de identidades de uma álgebra é um T-ideal e todo T-ideal é o conjunto de identidades de alguma álgebra; por isso chamamos o conjunto de identidades polinomiais de uma álgebra de seu T-ideal. Porém, como duas álgebras distintas (ou não isomorfas) podem ter o mesmo T-ideal, classificamos as PI-álgebras por meio das variedades.

Definição 2.16. Dado $S \subseteq F\langle X\rangle$, $S \neq \emptyset$, a classe de todas as álgebras R tais que toda $f \in S$ é uma identidade polinomial de R é chamada de variedade determinada por S, e denotada por $var(S)$. Note que

$$R \in var(S) \Leftrightarrow S \subseteq T(R).$$

A seguir fornecemos um exemplo simples de variedade.

Exemplo 2.17. A classe das álgebras comutativas é a variedade determinada por $\{[x_1,x_2]\}$. Portanto, toda álgebra comutativa está na variedade determinada por $\{[x_1,x_2]\}$.

Definição 2.18. Se $\mathscr{C}$ é uma classe de álgebras, dizemos que

$$T(\mathscr{C}) = \bigcap_{A\in\mathscr{C}} T(A)$$

é o T-ideal de $\mathscr{C}$. Além disso, dizemos que $var(T(\mathscr{C}))$ é a variedade gerada por $\mathscr{C}$, e a denotamos por $var(\mathscr{C})$.

Como vimos anteriormente, se R é uma F-álgebra e $S \subseteq F\langle X\rangle$, então toda $f \in S$ é identidade de R se, e somente se, toda $g \in \langle S\rangle^T$ é identidade de R. Portanto, pela definição de variedade determinada por S, temos que $var(S) = var(\langle S\rangle^T)$. Com isso, toda variedade é determinada a partir de um T-ideal. Na verdade podemos falar mais sobre as relações de T-ideais e variedades.

Proposição 2.19. *Seja $\mathbb{T}$ o conjunto de todos os T-ideais de $F\langle X\rangle$ e seja $\mathbb{V}$ o conjunto de todas as variedades. Denote por $var : \mathbb{T} \to \mathbb{V}$ a função dada por $I \to var(I)$. Então:*

(a) A função $var : \mathbb{T} \to \mathbb{V}$ é bijetora.

(b) Se $I, J \in \mathbb{T}$, então

$$I \subseteq J \iff var(I) \supseteq var(J).$$

(c) A função inversa de var é $T : \mathbb{V} \to \mathbb{T}$ dada por $\mathscr{C} \to T(\mathscr{C})$.

Demonstração. Temos os seguintes itens:

(a) Pelo comentário feito no parágrafo anterior a esta proposição, temos que a função *var* é sobrejetora. A injetividade de *var* é consequência do item (b) que provaremos abaixo.

(b) Suponha que $I \subseteq J$. Seja $R \in var(J)$, isto é, $J \subseteq T(R)$. Como $I \subseteq J$, temos $I \subseteq T(R)$. Logo, $R \in var(I)$ e $var(J) \subseteq var(I)$.

Para a recíproca, suponha que $var(J) \subseteq var(I)$. Se $R = F\langle X\rangle/J$, sabemos que $T(R) = J$. Logo, de $R \in var(J) \subseteq var(I)$ temos $R \in var(I)$. Agora, pela definição de variedade, $I \subseteq T(R)$, ou seja, $I \subseteq J$.

(c) Precisamos provar que $T(var(I)) = I$ para todo $I \in \mathbb{T}$. Pela definição de variedade, se $A \in var(I)$, então $I \subseteq T(A)$. Logo, $I \subseteq T(var(I))$. Agora, como $F\langle X\rangle/I \in var(I)$ e $T(F\langle X\rangle/I) = I$, segue que $T(var(I)) \subseteq I$. Logo, $T(var(I)) = I$.

Finalizamos a demonstração da proposição. □

Aqui cabe uma observação: não existe um conjunto que contém todas as variedades e, portanto, não existe uma função *var* como no enunciado. O que existe na verdade é uma classe de variedades e uma correspondência *var*. Porém, preferimos usar a linguagem de conjunto e função para facilitar o entendimento e escrita.

Um resultado importante que temos sobre as variedades é o seguinte.

Proposição 2.20. *Se $\mathscr{C}$ é uma variedade de álgebras, então $\mathscr{C}$ é gerada por suas álgebras finitamente geradas.*

Demonstração. Seja $I \subseteq F\langle X\rangle$ definido por

$$I = T(\mathscr{C}) = \bigcap_{A\in\mathscr{C}} T(A).$$

Pela última proposição, $var(I) = var(T(\mathscr{C})) = \mathscr{C}$.

Seja $W = \{F_n(I) \mid n \in \mathbb{N}\}$, onde

$$F_n(I) = \frac{F\langle x_1,\ldots,x_n\rangle}{I \cap F\langle x_1,\ldots,x_n\rangle}.$$

Aqui, $F\langle x_1,\ldots,x_n\rangle$ é a subálgebra de $F\langle X\rangle$ gerada por $x_1,\ldots,x_n$. Note que cada álgebra $F_n(I)$ é finitamente gerada pelos $\overline{x_1},\ldots,\overline{x_n}$, onde por $\overline{f}$ entende-se o elemento $\overline{f} = f + (I \cap F\langle x_1,\ldots,x_n\rangle)$. Provaremos que a variedade gerada por W coincide com $\mathscr{C}$. Pela última proposição, devemos provar que

$$I = T(W), \text{ onde } T(W) = \bigcap_{n\in\mathbb{N}} T(F_n(I)).$$

($\subseteq$) Seja $f(x_1,\ldots,x_m) \in I$. Se $\overline{f_1},\ldots,\overline{f_m} \in F_n(I)$, onde $f_i = f_i(x_1,\ldots,x_n) \in F\langle x_1,\ldots,x_n\rangle$, então

$$f(\overline{f_1},\ldots,\overline{f_m}) = \overline{f(f_1,\ldots,f_m)}.$$

Como $f(x_1,\ldots,x_m) \in I$, temos que $f(f_1,\ldots,f_m) \in I$. Note que $f(f_1,\ldots,f_m) \in F\langle x_1,\ldots,x_n\rangle$, pois $f_i(x_1,\ldots,x_n) \in F\langle x_1,\ldots,x_n\rangle$. Logo,

$$f(\overline{f_1},\ldots,\overline{f_m}) = \overline{0}$$

e $f(x_1,\ldots,x_m) \in T(F_n(I))$. Como tal fato vale para todo n, segue que $I \subseteq T(W)$.

($\supseteq$) Seja $f(x_1,\ldots,x_m) \in T(W)$ e suponha que $f \notin I$. Neste caso, em $F_m(I)$, temos

$$\overline{0} \neq \overline{f} = \overline{f(x_1,\ldots,x_m)} = f(\overline{x_1},\ldots,\overline{x_m}).$$

Como $\overline{x_1},\ldots,\overline{x_m} \in F_m(I)$, temos que $f(x_1,\ldots,x_m) \notin T(F_m(I))$. Mas isso é um absurdo, pois $F_m(I) \in W$ e $f(x_1,\ldots,x_m) \in T(W)$. Logo, $T(W) \subseteq I$.

Portanto, $var(W) = \mathscr{C}$. □

Definição 2.21. Seja R uma PI-álgebra e seja $S \subseteq F\langle X\rangle$. Se $T(R) = \langle S\rangle^T$, dizemos que S é uma base para as identidades polinomiais de R.

No próximo capítulo apresentaremos uma base com dois elementos para as identidades polinomiais da álgebra de matrizes de ordem 2 com entradas num corpo finito.

Para isso, usaremos a seguinte técnica para descrever as identidades polinomiais de uma PI-álgebra R:

(a) Primeiro encontramos um "bom" conjunto S de identidades polinomiais para R. Ou seja, um conjunto em que acreditamos ser uma base para $T(R)$. Daqui obtemos

$$T(R) \supseteq \langle S \rangle^T.$$

(b) Da Proposição 2.19 temos $var(T(R)) \subseteq var(\langle S \rangle^T)$. Além disso,

$$T(R) = \langle S \rangle^T \Leftrightarrow var(T(R)) = var(\langle S \rangle^T).$$

(c) Como $var(S) = var(\langle S \rangle^T)$, para provar a igualdade $T(R) = \langle S \rangle^T$ precisamos provar que

$$var(T(R)) \supseteq var(S).$$

Usaremos a "receita" acima no próximo capítulo.

CAPÍTULO 3

T-ideal da álgebra das matrizes 2×2 com entradas num corpo finito

Quando vamos estudar as identidades das álgebras das matrizes 2×2 nos deparamos com alguns resultados bem interessantes. Razmyslov, em [26], foi o primeiro a mostrar que, se F é um corpo de característica 0, existirá uma base finita para as identidades de $M_2(F)$. Ele provou isso explicitando uma base com 9 elementos. Mais tarde, Drensky, em [7], melhorou esse resultado para uma base com somente duas identidades. Koshlukov provou em [20] que as identidades de $M_2(F)$ possuem uma base finita para todo corpo infinito F de característica positiva diferente de 2. O caso em que F é infinito de característica 2 permanece em aberto.

Saindo dos corpos infinitos, Mal'tsev e Kuz'min exibiram em [23] uma base com duas identidades para a álgebra $M_2(F_q)$ sobre qualquer corpo finito F_q. Neste capítulo estudaremos os resultados apresentados por eles.

Ao longo deste capítulo, F_q será um corpo finito de característica p e com $q = p^r$ elementos.

3.1 Algumas identidades polinomiais para $M_2(F_q)$

O nosso foco neste capítulo será a álgebra de matrizes $M_2(F_q)$. Veremos, então, alguns exemplos de identidades polinomiais para tal álgebra.

Como $M_2(F_q)$ é uma álgebra de dimensão 4 sobre o corpo F_q, vimos no Exemplo 2.7 que o polinômio Standard $St_5(x_1,\ldots,x_5)$ é uma identidade polinomial para $M_2(F_q)$ e, por meio do Exemplo 2.6, pudemos construir outra identidade polinomial. Além delas, existem outras identidades polinomiais interessantes. Veremos nesta seção duas identidades importantes. Para isso, será necessário um resultado que vem da teoria dos grupos. Como $F_q \setminus \{0\}$ é um grupo multiplicativo com $q-1$ elementos, segue do Teorema de Lagrange que $\alpha^{q-1} = 1$ para todo $\alpha \in F_q \setminus \{0\}$. Logo,

$$\alpha^q = \alpha \text{ para todo } \alpha \in F_q.$$

3.1.1 Identidade polinomial f_1

A primeira identidade que veremos usará o comutador $[x,y] = xy - yx$. De agora em diante, denotaremos por $f_1 = f_1(x,y)$ o seguinte polinômio:

$$f_1(x,y) = (x - x^q)(y - y^{q^2})(1 - [x,y]^{q-1}).$$

Para provarmos que f_1 é uma identidade polinomial para $M_2(F_q)$ relembraremos um resultado já conhecido da teoria de Álgebra Linear.

Fixada uma matriz $A \in M_2(F_q)$, denote por $p(x)$ seu polinômio característico. O grau de $p(x)$ é dois, portanto $p(x)$ admite duas raízes (iguais ou distintas) λ_1 e λ_2. Note que $\lambda_1, \lambda_2 \in F_q$ ou $p(x)$ é um polinômio irredutível de $F_q[x]$. No segundo caso, se $(p(x))$ é o ideal de $F_q[x]$ gerado por $p(x)$, então

$$K = \frac{F_q[x]}{(p(x))}$$

é um corpo que satisfaz as seguintes propriedades:

(a) $F_q \subset K$ (extensão de corpos),

(b) $\lambda_1, \lambda_2 \in K$,

(c) $[K : F_q] = 2$ e, em particular, $|K| = |F_q|^2 = q^2$.

Pela teoria de Galois, K é o único corpo, a menos de isomorfismo, com q^2 elementos, o qual denotaremos por $K = F_{q^2}$. Portanto, pelo Teorema de Jordan, temos o seguinte resultado.

Teorema 3.1 (Jordan)**.** *Se $A \in M_2(F_q)$, então existe uma matriz invertível $B \in M_2(F_{q^2})$ tal que*

$$BAB^{-1} = \begin{pmatrix} \lambda_1 & \varepsilon \\ 0 & \lambda_2 \end{pmatrix},$$

onde $\lambda_1, \lambda_2 \in F_{q^2}$ e ε satisfaz:

1. *$\varepsilon = 0$ se $\lambda_1 \neq \lambda_2$;*
2. *$\varepsilon = 0$ ou $\varepsilon = 1$ se $\lambda_1 = \lambda_2$.*

O teorema fala da existência da Forma de Jordan de uma matriz e pode ser encontrado na Seção 5.6 do livro [5], mais especificamente no Teorema 5.174.

Usando o Teorema de Jordan, podemos seguir com o seguinte resultado.

Proposição 3.2. *O polinômio*

$$f_1(x,y) = (x - x^q)(y - y^{q^2})(1 - [x,y]^{q-1})$$

é uma identidade polinomial para $M_2(F_q)$.

Demonstração. Sejam $X,Y \in M_2(F_q)$. Provaremos que $f_1(X,Y) = 0$. Para isso, considere o polinômio característico $p(x)$ de Y, e denote por λ_1, λ_2 suas raízes. Aqui teremos dois casos, o primeiro referente a $\lambda_1 \neq \lambda_2$ e o segundo referente a $\lambda_1 = \lambda_2 = \lambda$.

Caso 1: $\lambda_1 \neq \lambda_2$.

Neste caso, pelo Teorema de Jordan, existe uma matriz invertível B com entradas em F_{q^2} tal que

$$BYB^{-1} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

Como $\lambda_1, \lambda_2 \in F_{q^2}$, temos que $\lambda_1 = \lambda_1^{q^2}$ e $\lambda_2 = \lambda_2^{q^2}$. Logo,

$$BY^{q^2}B^{-1} = (BYB^{-1})^{q^2} = \begin{pmatrix} (\lambda_1)^{q^2} & 0 \\ 0 & (\lambda_2)^{q^2} \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} = BYB^{-1}.$$

Portanto, $Y^{q^2} = Y$. Ou seja, $(Y - Y^{q^2}) = 0$ e $f_1(X,Y) = 0$ para todos $X,Y \in M_2(F_q)$.

Caso 2: $\lambda_1 = \lambda_2 = \lambda$.

Neste caso, o Teorema de Jordan nos diz que existe uma matriz invertível B com entradas em F_{q^2} tal que

$$BYB^{-1} = \begin{pmatrix} \lambda & \varepsilon \\ 0 & \lambda \end{pmatrix},$$

onde $\varepsilon = 0$ ou 1. Como o traço $tr(CD) = tr(DC)$, temos

$$tr(Y) = tr(BYB^{-1}) = 2\lambda.$$

Se $\mathrm{char}(F_q) = p \neq 2$, então $\lambda \in F_q$, pois $tr(Y) \in F_q$. Se $p = 2$, então $F_q = F_{2^r}$ é um corpo perfeito, ou seja, pela Proposição A.9, os polinômios irredutíveis com coeficientes em F_q devem ter raízes simples. Como o λ não é uma raiz simples do polinômio característico $p(x)$ de Y, então tal polinômio pode ser fatorado em $F_q[x]$ como $p(x) = (x-\lambda)(x-\lambda)$, ou seja, $\lambda \in F_q$. Desta forma, temos que $B \in M_2(F_q)$. Provamos que independente da característica de F_q, sempre teremos $\lambda \in F_q$.

Note que, se $f_1(X,Y) = 0$, então

$$\begin{aligned}
0 &= B0B^{-1} \\
&= Bf_1(X,Y)B^{-1} \\
&= B(X - X^q)(Y - Y^{q^2})(1 - [X,Y]^{q-1})B^{-1} \\
&= B(X - X^q)B^{-1}B(Y - Y^{q^2})B^{-1}B(1 - [X,Y]^{q-1})B^{-1} \\
&= (BXB^{-1} - (BXB^{-1})^q)(BYB^{-1} - (BYB^{-1})^{q^2})(1 - [BXB^{-1}, BYB^{-1}]^{q-1}) \\
&= f_1(BXB^{-1}, BYB^{-1}),
\end{aligned}$$

e, de forma semelhante, se $f_1(BXB^{-1},BYB^{-1})=0$ então $f_1(X,Y)=0$. Portanto,

$$f_1(X,Y)=0 \iff f_1(BXB^{-1},BYB^{-1})=0.$$

Com isso, como $BXB^{-1}\in M_2(F_q)$, para provarmos que $f_1(X,Y)=0$, podemos supor, sem perda de generalidade, que $Y=\lambda 1+E$, onde

$$E=\begin{pmatrix} 0 & \varepsilon \\ 0 & 0 \end{pmatrix}.$$

De forma semelhante à Proposição A.4, como $\lambda 1$ e E comutam, segue que

$$(\lambda 1+E)^{q^2}=\lambda^{q^2}1+E^{q^2}=\lambda^{q^2}1=\lambda 1.$$

Por outro lado, como $\lambda 1$ comuta com qualquer outra matriz em $M_2(F_{q^2})$, temos que

$$[X,\lambda 1+E]=[X,\lambda 1]+[X,E]=[X,E],$$

ou seja,

$$\begin{aligned} f_1(X,\lambda 1+E) &= (X-X^q)(\lambda 1+E-(\lambda 1+E)^{q^2})(1-[X,\lambda 1+E]^{q-1}) \\ &= (X-X^q)(\lambda 1+E-\lambda 1)(1-[X,E]^{q-1}) \\ &= (X-X^q)(E)(1-[X,E]^{q-1}). \end{aligned} \tag{3.1}$$

Se $\varepsilon=0$, então $E=0$ e (3.1) torna-se 0. Suponha

$$X=\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \quad \text{e} \quad E=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Então

$$[X,E]=\begin{pmatrix} 0 & x_{11} \\ 0 & x_{21} \end{pmatrix}-\begin{pmatrix} x_{21} & x_{22} \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} -x_{21} & x_{11}-x_{22} \\ 0 & x_{21} \end{pmatrix}.$$

(a) Se $x_{21}\neq 0$, então de $z^{q-1}=1$ para todo $z\in F_q\setminus\{0\}$, obtemos

$$1-[X,E]^{q-1}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}-\begin{pmatrix} (-x_{21})^{q-1} & c \\ 0 & x_{21}^{q-1} \end{pmatrix}=\begin{pmatrix} 0 & -c \\ 0 & 0 \end{pmatrix}.$$

Neste caso, $E(1-[X,E]^{q-1})=0$ e (3.1) torna-se 0.

(b) Se $x_{21}=0$, então de $z^q=z$ para todo $z\in F_q$, obtemos

$$X-X^q=\begin{pmatrix} x_{11} & x_{12} \\ 0 & x_{22} \end{pmatrix}-\begin{pmatrix} x_{11}^q & c' \\ 0 & x_{22}^q \end{pmatrix}=\begin{pmatrix} 0 & x_{12}-c' \\ 0 & 0 \end{pmatrix}.$$

Neste caso, $(X-X^q)E=0$ e (3.1) torna-se 0.

Pelos dois casos, provamos que $f_1(X,Y)=0$ para todos $X,Y\in M_2(F_q)$. □

3.1.2 Identidade polinomial f_2

A segunda identidade que veremos usará o produto de Jordan $x \circ y = xy + yx$. De agora em diante, denotaremos por $f_2 = f_2(x,y)$ o seguinte polinômio:

$$f_2(x,y) = (x - x^q) \circ (y - y^q) - ((x - x^q) \circ (y - y^q))^q .$$

Para provarmos que f_2 é uma identidade polinomial para $M_2(F_q)$, enunciaremos alguns lemas na sequência.

Lema 3.3. *Se $X, Y \in M_2(F_q)$ são matrizes com traço nulo, então $X \circ Y$ é uma matriz escalar.*

Demonstração. Sejam

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \text{ e } Y = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}.$$

Como X e Y têm traço nulo, então $x_{11} + x_{22} = y_{11} + y_{22} = 0$. Fazendo as multiplicações obtemos

$$XY = \begin{pmatrix} x_{11}y_{11} + x_{12}y_{21} & x_{11}y_{12} + x_{12}y_{22} \\ x_{21}y_{11} + x_{22}y_{21} & x_{21}y_{12} + x_{22}y_{22} \end{pmatrix} \text{ e } YX = \begin{pmatrix} y_{11}x_{11} + y_{12}x_{21} & y_{11}x_{12} + y_{12}x_{22} \\ y_{21}x_{11} + y_{22}x_{21} & y_{21}x_{12} + y_{22}x_{22} \end{pmatrix},$$

e, portanto,

$$\begin{aligned}
X \circ Y &= XY + YX \\
&= \begin{pmatrix} x_{11}y_{11} + x_{12}y_{21} & x_{11}y_{12} + x_{12}y_{22} \\ x_{21}y_{11} + x_{22}y_{21} & x_{21}y_{12} + x_{22}y_{22} \end{pmatrix} + \begin{pmatrix} y_{11}x_{11} + y_{12}x_{21} & y_{11}x_{12} + y_{12}x_{22} \\ y_{21}x_{11} + y_{22}x_{21} & y_{21}x_{12} + y_{22}x_{22} \end{pmatrix} \\
&= \begin{pmatrix} x_{11}y_{11} + x_{12}y_{21} + y_{11}x_{11} + y_{12}x_{21} & x_{11}y_{12} + x_{12}y_{22} + y_{11}x_{12} + y_{12}x_{22} \\ x_{21}y_{11} + x_{22}y_{21} + y_{21}x_{11} + y_{22}x_{21} & x_{21}y_{12} + x_{22}y_{22} + y_{21}x_{12} + y_{22}x_{22} \end{pmatrix} \\
&= \begin{pmatrix} 2x_{11}y_{11} + x_{12}y_{21} + y_{12}x_{21} & y_{12}(x_{11} + x_{22}) + x_{12}(y_{11} + y_{22}) \\ x_{21}(y_{11} + y_{22}) + y_{21}(x_{11} + x_{22}) & 2x_{22}y_{22} + x_{12}y_{21} + y_{12}x_{21} \end{pmatrix} \\
&= \begin{pmatrix} 2x_{11}y_{11} + x_{12}y_{21} + y_{12}x_{21} & y_{12}0 + x_{12}0 \\ x_{21}0 + y_{21}0 & 2(-x_{11})(-y_{11}) + x_{12}y_{21} + y_{12}x_{21} \end{pmatrix} \\
&= \begin{pmatrix} 2x_{11}y_{11} + x_{12}y_{21} + y_{12}x_{21} & 0 \\ 0 & 2x_{11}y_{11} + x_{12}y_{21} + y_{12}x_{21} \end{pmatrix} \\
&= (2x_{11}y_{11} + x_{12}y_{21} + y_{12}x_{21}) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},
\end{aligned}$$

como era o desejado. □

Lema 3.4. *Se $X \in M_2(F_q)$, então $X - X^q$ é uma matriz com traço nulo.*

Demonstração. Sejam λ_1 e λ_2 raízes do polinômio característico de $X \in M_2(F_q)$. Sabemos, pelo Teorema de Jordan, que existe uma matriz invertível B com entradas no corpo F_{q^2} tal que

$$BXB^{-1} = \begin{pmatrix} \lambda_1 & \varepsilon \\ 0 & \lambda_2 \end{pmatrix}$$

para alguns $\lambda_1, \lambda_2 \in F_{q^2}$ e $\varepsilon = 0$ ou 1. Como $tr(CD) = tr(DC)$, temos que $tr(X) = tr(BXB^{-1})$, logo

$$tr(X^q) = tr(BX^qB^{-1}) = tr((BXB^{-1})^q).$$

Note que

$$(BXB^{-1})^q = \begin{pmatrix} \lambda_1 & \varepsilon \\ 0 & \lambda_2 \end{pmatrix}^q = \begin{pmatrix} \lambda_1^q & k \\ 0 & \lambda_2^q \end{pmatrix}$$

para algum $k \in F_{q^2}$. Portanto, $tr((BXB^{-1})^q) = \lambda_1^q + \lambda_2^q$. Como $q = p^r$, para algum $r \geq 1$, e $\lambda_1, \lambda_2 \in F_{q^2}$, segue da Proposição A.4 que $\lambda_1^q + \lambda_2^q = (\lambda_1 + \lambda_2)^q$ e, portanto,

$$tr(X^q) = tr((BXB^{-1})^q) = \lambda_1^q + \lambda_2^q = (\lambda_1 + \lambda_2)^q = (tr(BXB^{-1}))^q = tr(X)^q.$$

Como $tr(X) \in F_q$ temos que $tr(X^q) = tr(X)^q = tr(X)$. Logo,

$$tr(X - X^q) = tr(X) - tr(X^q) = 0$$

e a demonstração está finalizada. □

Proposição 3.5. *O polinômio*

$$f_2(x,y) = (x - x^q) \circ (y - y^q) - ((x - x^q) \circ (y - y^q))^q$$

é uma identidade polinomial para $M_2(F_q)$.

Demonstração. Sabemos pelo Lema 3.4 que se $X, Y \in M_2(F_q)$ então $X - X^q$ e $Y - Y^q$ são matrizes com traço nulo. Com isso, pelo Lema 3.3, existe um $\lambda \in F_q$ tal que

$$(X - X^q) \circ (Y - Y^q) = \lambda 1.$$

Logo,

$$((X - X^q) \circ (Y - Y^q))^q = \lambda^q 1 = \lambda 1,$$

ou seja,

$$(X - X^q) \circ (Y - Y^q) - ((X - X^q) \circ (Y - Y^q))^q = 0$$

para todos $X, Y \in M_2(F_q)$. Provamos que $f_2(x,y)$ é uma identidade polinomial para $M_2(F_q)$. □

3.2 Descrição das identidades polinomiais para $M_2(F_q)$

Nesta seção, assim como antes, F_q denotará um corpo finito com q elementos e com característica p. Neste caso, $|F_q| = p^d$ para algum $d \geq 1$.

Dado um subcorpo $F_{q'}$ de F_q, podemos olhar para $M_2(F_q)$ como uma álgebra sobre $F_{q'}$. Além disso, os polinômios f_1 e f_2, definidos na seção anterior, estão em $F_{q'}\langle X \rangle$. Denote por $J_{q'}$ o T-ideal de $F_{q'}\langle X \rangle$ gerado pelos polinômios f_1 e f_2. Nesta seção, provaremos que o subconjunto de $F_{q'}\langle X \rangle$ formado pelas identidades polinomiais de $M_2(F_q)$ coincide com $J_{q'}$.

De agora em diante, escreveremos $F = F_{q'}$, M denotará a variedade de F-álgebras gerada pelo conjunto $\{f_1, f_2\}$ e $var(M_2(F_q))$ denotará a variedade de F-álgebras gerada pelo subconjunto de $F\langle X \rangle$ consistindo das identidades polinomiais de $M_2(F_q)$.

Usaremos a técnica do final da Seção 2.2 desta dissertação. Note que o subconjunto de $F\langle X\rangle$ formado pelas identidades polinomiais de $M_2(F_q)$ coincide com $J_{q'}$ se, e somente se, $M = var(M_2(F_q))$. A inclusão $var(M_2(F_q)) \subseteq M$ segue da seção anterior, então resta-nos provar a outra inclusão. Para isso, precisamos de uma definição e de alguns resultados sobre a variedade M.

Definição 3.6. Dada uma variedade de álgebras $\mathscr{V}$, denote por $In(\mathscr{V})$ o conjunto dos índices de nilpotência das álgebras nilpotentes de $\mathscr{V}$. Se $In(\mathscr{V})$ é finito, dizemos que seu maior elemento é o índice de nilpotência de $\mathscr{V}$.

Lema 3.7. *A variedade M possui índice de nilpotência finito igual a* 2*.*

Demonstração. Seja $N \in M$ uma álgebra nilpotente com índice de nilpotência n. Se $n > 2$, então existem elementos $a_1, a_2, \ldots, a_{n-1} \in N$ tais que

$$a_1 a_2 \cdots a_{n-1} \neq 0.$$

Sejam $X = a_1 a_2 \cdots a_{n-2}$ e $Y = a_{n-1}$. De $f_1(X,Y) = 0$ obtemos

$$\begin{aligned} 0 &= (X - X^q)(Y - Y^{q^2})(1 - [X,Y]^{q-1}) \\ &= XY - XY[X,Y]^{q-1} - XY^{q^2} + XY^{q^2}[X,Y]^{q-1} \\ &\quad - X^qY + X^qY[X,Y]^{q-1} + X^qY^{q^2} - X^qY^{q^2}[X,Y]^{q-1} \\ &= XY. \end{aligned}$$

Como $XY \neq 0$ temos um absurdo. Note que a última igualdade se deve ao fato de que $f_1(X,Y)$ é uma soma de oito elementos, dos quais sete serão compostos por produtos de no mínimo n elementos de N, ou seja, são nulos, e o oitavo é XY. Portanto, $n = 2$ para toda álgebra nilpotente de M não nula. O F-subespaço vetorial de $M_2(F_q)$ gerado pela matriz e_{12} é uma álgebra nilpotente da variedade M com índice de nilpotência 2. Logo, o índice de nilpotência de M é exatamente 2. □

Proposição 3.8. *A variedade M é gerada por suas álgebras finitas.*

Demonstração. Seja I o T-ideal gerado por f_1 e f_2, isto é,

$$I = \langle f_1, f_2 \rangle^T.$$

Como $f_1 \in I$ temos que

$$g(x) = f_1(x,x) = (x - x^q)(x - x^{q^2}) \in I.$$

Logo, $g(x)$ é uma identidade polinomial para toda álgebra em M, ou seja, toda álgebra em M é uma PI-álgebra e é uma álgebra algébrica. Então, pelo Teorema 2.11, temos que toda álgebra em M é localmente finita.

Aplicando a Proposição 2.20, temos que a variedade M é gerada por suas álgebras finitamente geradas $F_n(I)$, $n \in \mathbb{N}$. Como $F_n(I)$ é localmente finita, segue que $F_n(I)$ é de dimensão finita. Como o corpo F é finito, segue que $F_n(I)$ é finita. Ou seja, M é gerada por suas álgebras finitas. □

Proposição 3.9. *A inclusão $M \subseteq var(M_2(F_q))$ é verdadeira.*

Demonstração. Usando a Proposição 3.8 temos que M é gerada por suas álgebras finitas $\overline{R}$. Portanto, para provarmos que $M \subseteq var(M_2(F_q))$ basta provarmos que $\overline{R} \in var(M_2(F_q))$ para toda álgebra finita $\overline{R}$ de M.

Pelo Teorema 1.66, existem álgebras subdiretamente irredutíveis finitas $R_1, \ldots, R_n$ tais que $\overline{R}$ é isomorfa a uma soma subdireta delas.

Afirmação 1. Vale a igualdade

$$T(\overline{R}) = \bigcap_{i=1}^{n} T(R_i).$$

Demonstração da Afirmação 1. Como $\overline{R}$ é uma soma subdireta das álgebras $R_1, \ldots, R_n$, então existe um monomorfismo de álgebras $\phi : \overline{R} \to \prod_{i=1}^{n} R_i$ tal que $(\pi_i \circ \phi)(\overline{R}) = R_i$. Relembrando que π_i é o homomorfismo projeção que leva $(y_1, \ldots, y_n)$ em y_i.

Seja $f(x_1, \ldots, x_s) \in T(\overline{R})$. Por definição, $f(r_1, \ldots, r_s) = 0$ para todos $r_1, \ldots, r_s \in \overline{R}$. Como $(\pi_i \circ \phi)(\overline{R}) = R_i$, para todo $r_k^i \in R_i$ existe um $r_k' \in \overline{R}$ tal que $(\pi_i \circ \phi)(r_k') = r_k^i$. Com isso, temos que para todos $r_1^i, \ldots, r_s^i \in R_i$ vale

$$f(r_1^i, \ldots, r_s^i) = f((\pi_i \circ \phi)(r_1'), \ldots, (\pi_i \circ \phi)(r_s')) = (\pi_i \circ \phi)(f(r_1', \ldots, r_s')) = (\pi_i \circ \phi)(0) = 0.$$

Ou seja, $f(x_1, \ldots, x_s) \in T(R_i)$ para todo $1 \leq i \leq n$, o que implica que $f(x_1, \ldots, x_s) \in \bigcap_{i=1}^{n} T(R_i)$.

Por outro lado, seja $f(x_1, \ldots, x_s) \in \bigcap_{i=1}^{n} T(R_i)$. Note que $f(x_1, \ldots, x_s) \in T\left(\prod_{i=1}^{n} R_i\right)$, pois

$$f((r_1^1, \ldots, r_1^n), \ldots, (r_s^1, \ldots, r_s^n)) = (f(r_1^1, \ldots, r_s^1), \ldots, f(r_1^n, \ldots, r_s^n)) = (0, \ldots, 0)$$

para todos $r_l^i \in R_i$ com $1 \leq l \leq s$ e $1 \leq i \leq n$. Portanto, como $\phi(\overline{R}) \subseteq \prod_{i=1}^{n} R_i$, segue que $f(x_1, \ldots, x_s) \in T(\phi(\overline{R}))$, o que implica que $f(x_1, \ldots, x_s) \in T(\overline{R})$ pois ϕ é injetora.

Portanto, pelos dois últimos parágrafos, temos que $T(\overline{R}) = \bigcap_{i=1}^{n} T(R_i)$ como queríamos demonstrar.

Segue da Afirmação 1 que para provarmos a proposição basta provarmos que cada álgebra R_i está em $var(M_2(F_q))$. Para isso, provaremos que cada uma destas álgebras R_i pode ser mergulhada em $M_2(F_q)$, e isso é o suficiente para a conclusão da demonstração da proposição. Por comodidade, fixe i e denote $R = R_i$. Portanto, de agora em diante, R será uma álgebra subdiretamente irredutível finita em M e, nos próximos quatro casos, mostraremos que R pode ser mergulhada em $M_2(F_q)$.

(a) Caso R nilpotente.

Suponha que R é uma álgebra nilpotente em M. Neste caso, segue do Lema 3.7 que $R^2 = 0$. Suponha que $\dim_F R \geq 2$ e fixe dois elementos distintos a, b de uma base de R. Como $R^2 = 0$, segue

que

$$I_a = Fa \text{ e } I_b = Fb$$

são dois ideais de R. Por outro lado, do fato que R é uma álgebra subdiretamente irredutível, temos $I_a \cap I_b \neq 0$, o que é um absurdo. Portanto, $\dim_F R = 1$ e podemos mergulhar R em $M_2(F_q)$ por meio da função $\alpha a \mapsto \alpha e_{12}$, onde $\alpha \in F$ e $\{a\}$ é base de R.

(b) Caso R simples.

Suponha que R é uma álgebra simples em M. Pelo Corolário 1.46, R é isomorfo a $M_k(F_{p^t})$ para alguns $k,t \geq 1$. Portanto, $M_k(F_{p^t})$ também está na variedade M e podemos supor, sem perda de generalidade, que $R = M_k(F_{p^t})$.

Se $k \geq 3$, então

$$\begin{aligned} f_1(e_{12}, e_{23}) &= (e_{12} - e_{12}^q)(e_{23} - e_{23}^{q^2})(1 - [e_{12}, e_{23}]^{q-1}) \\ &= (e_{12})(e_{23})(1 - e_{13}^{q-1}) \\ &= e_{13} - e_{13}^q = e_{13} \neq 0. \end{aligned}$$

Neste caso, temos um absurdo, pois $R \in M$. Logo, obrigatoriamente devemos ter $k \leq 2$.

Suponha agora que $k = 2$, isto é, suponha que $R = M_2(F_{p^t})$. Para todo $\alpha \in F_{p^t}$ temos

$$\begin{aligned} f_1(\alpha e_{11}, e_{12}) &= (\alpha e_{11} - (\alpha e_{11})^q)(e_{12} - e_{12}^{q^2})(1 - [\alpha e_{11}, e_{12}]^{q-1}) \\ &= ((\alpha - \alpha^q)e_{11})(e_{12})(1 - (\alpha e_{12})^{q-1}) \\ &= ((\alpha - \alpha^q)e_{12})(1 - \alpha^{q-1} e_{12}^{q-1}) \\ &= (\alpha - \alpha^q)e_{12} - ((\alpha - \alpha^q)\alpha^{q-1} e_{12}^q) \\ &= (\alpha - \alpha^q)e_{12}. \end{aligned}$$

Como $f_1(x,y)$ é uma identidade polinomial de R, segue que $\alpha - \alpha^q = 0$ para todo $\alpha \in F_{p^t}$. Portanto, pelo Teorema A.2, podemos mergulhar F_{p^t} em F_q e, consequentemente, mergulhar $R = M_2(F_{p^t})$ em $M_2(F_q)$. Note que tal mergulho é um monomorfismo de "F-álgebras", pois no mergulho entre os corpos, os elementos de F ficam fixados.

Suponha que $k = 1$, isto é, $R = M_1(F_{p^t}) = F_{p^t}$. Se $\alpha \in F_{p^t}$, então

$$0 = f_1(\alpha, \alpha) = (\alpha - \alpha^q)(\alpha - \alpha^{q^2})(1 - [\alpha, \alpha]^{q-1}) = (\alpha - \alpha^q)(\alpha - \alpha^{q^2}),$$

ou seja, como F_{p^t} é um corpo,

$$\alpha - \alpha^q = 0 \quad \text{ou} \quad \alpha - \alpha^{q^2} = 0.$$

No primeiro caso,

$$\alpha = \alpha^q = (\alpha^q)^q = \alpha^{q^2}.$$

Assim, em ambos os casos teremos $\alpha - \alpha^{q^2} = 0$ para todo $\alpha \in F_{p^t}$. Portanto, podemos mergulhar $R = F_{p^t}$ em F_{q^2}. Como $\dim_{F_q} F_{q^2} = 2$, segue da Proposição 1.15 que a F_q-álgebra F_{q^2} é mergulhada na álgebra $M_2(F_q)$. Em particular, R é mergulhado em $M_2(F_q)$.

(c) Caso R semiprima.

Suponha que R é uma álgebra semiprima em M. Pelo Teorema 1.57 de Wedderburn, existem subálgebras simples $B_1, \ldots, B_n$ de R tais que $R = B_1 \oplus \cdots \oplus B_n$. Se $n = 1$, então R é simples e este caso já foi estudado anteriormente. Suponha $n \geq 2$. Neste caso, $B_1, \ldots, B_n$ são ideais bilaterais de R cuja interseção é 0, que é um absurdo pois R é uma álgebra subdiretamente irredutível.

(d) Caso R diferente dos anteriores.

Suponha que R é uma álgebra em M não nilpotente, não simples e não semiprima. Como R é uma álgebra sobre um corpo finito, pelo Teorema 1.61 de Wedderburn podemos decompor R como

$$R = B \oplus N,$$

onde B é uma subálgebra semiprima de R, e $N \neq 0$ é o radical de Jacobson de R. Vale lembrar que a soma direta acima é a soma direta de espaços vetoriais. Como N é uma álgebra nilpotente da variedade M, segue do Lema 3.7 que $N^2 = 0$. Além disso, pelo Teorema 1.57, existem $s, k_1, \ldots, k_s, t_1, \ldots, t_s \in \mathbb{N}$ tais que

$$B = B_1 \oplus \cdots \oplus B_s \text{ com } B_i \cong M_{k_i}(F_{p^{t_i}}).$$

Relembramos que $B_1, \ldots, B_s$ são ideais bilaterais de B e, pelo estudo do caso (b) desta demonstração, segue que $1 \leq k_1, \ldots, k_s \leq 2$. Provaremos que $k_1 = \cdots = k_s = 1$. Suponha, por exemplo, que $k_1 = 2$. Por um abuso de notação, escreveremos simplesmente $B_1 = M_2(F_{p^{t_1}})$ e, neste caso, o elemento (matriz canônica) $e_{12} \in B_1$ existe. Se u é um elemento qualquer de N, então

$$\begin{aligned} 0 = f_1(e_{12}, u) &= (e_{12} - e_{12}^q)(u - u^{q^2})(1 - [e_{12}, u]^{q-1}) \\ &= e_{12}u(1 - (e_{12}u - ue_{12})^{q-1}) \\ &= e_{12}u - e_{12}u(e_{12}u - ue_{12})^{q-1}. \end{aligned}$$

Como N é um ideal de R, segue que $e_{12}u, ue_{12} \in N$ e, portanto, $(e_{12}u - ue_{12}) \in N$. De $N^2 = 0$ obtemos

$$e_{12}u(e_{12}u - ue_{12})^{q-1} = 0,$$

ou seja,

$$\begin{aligned} 0 = f_1(e_{12}, u) &= e_{12}u - e_{12}u(e_{12}u - ue_{12})^{q-1} \\ &= e_{12}u. \end{aligned}$$

Portanto, $e_{12}u = 0$ para todo $u \in N$. Por meio da igualdade $0 = f_1(u, e_{12})$ obtemos, com raciocínio análogo, $ue_{12} = 0$ para todo $u \in N$. E o mesmo vale para e_{21}, ou seja, $e_{21}u = ue_{21} = 0$ para todo

$u \in N$. Note que $e_{11} = e_{12}e_{21}$, logo $e_{11}u = e_{12}e_{21}u = e_{12}0 = 0$ para todo $u \in N$ e, com mesmo raciocínio, $ue_{11} = e_{22}u = ue_{22} = 0$. Provamos que $B_1N = NB_1 = 0$ e, desta forma, temos que B_1 é um ideal de R. De fato, se $b+n \in R$, com $b \in B$ e $n \in N$, então $B_1(b+n) = B_1b + B_1n = B_1b \subseteq B_1$ e $(b+n)B_1 = bB_1 + nB_1 = bB_1 \subseteq B_1$.

Como B_1 e N são ideais de R e $B_1 \cap N = 0$ temos um absurdo, pois R é subdiretamente irredutível.

Em resumo, provamos acima que

$$B = B_1 \oplus \cdots \oplus B_s \text{ com } B_i \cong F_{p^{t_i}} \text{ para todo } i.$$

Temos que pelo menos um dos conjuntos RN, NR é não nulo. De fato, se $RN = NR = 0$, então $B_1N = NB_1 = 0$ o que, como vimos acima, é um absurdo. De agora em diante, sem perda de generalidade, assumiremos que

$$RN \neq 0.$$

Como $B_1, \ldots, B_s$ são ideais de B cuja interseção dois a dois é nula, segue que $B_iB_j = 0$ para todos $i \neq j$. Denotando por e_i o elemento identidade de B_i, temos que

$$1_B = e_1 + \cdots + e_s$$

é o elemento identidade de B.

Afirmação 2. e_iN é um ideal de R para todo i.

Demonstração da Afirmação 2. É fácil ver que e_iN é um subespaço vetorial de R. Agora,

$$(e_iN)R = e_i(NR) \subseteq e_iN,$$

pois N é ideal de R. Por outro lado,

$$R(e_iN) = (B+N)(e_iN) = B(e_iN) + N(e_iN) \subseteq B_i(e_iN) + N^2 = e_i(B_iN) + \{0\} \subseteq e_iN.$$

Finalizamos aqui a demonstração da afirmação.

Se $i \neq j$ e $u = e_in = e_jn'$ para certos $n, n' \in N$, então, como e_i é a unidade de B_i,

$$u = e_in = e_ie_in = e_ie_jn' = 0,$$

ou seja, e_iN e e_jN são ideais de R com interseção nula. Como R é álgebra subdiretamente irredutível, segue que apenas um e_iN é não nulo. De agora em diante, sem perda de generalidade, assumiremos que

$$e_1N \neq 0 \text{ e } e_2N = \cdots = e_sN = 0. \tag{3.2}$$

Afirmação 3. $e_1N = N$.

Demonstração da Afirmação 3. Seja $J=\{n-e_1n \mid n\in N\}$. Com raciocínio análogo aos até aqui apresentados, pode ser mostrado que J é um ideal de R. Se $u=n-e_1n=e_1n'$ para certos $n,n'\in N$, então

$$u=e_1n'=e_1e_1n'=e_1(n-e_1n)=0.$$

Ou seja, e_1N e J são ideais de R com interseção nula e, pela irredutibilidade subdireta de R, segue que $J=0$. Portanto, $e_1n=n$ para todo $n\in N$. Finalizamos a demonstração da afirmação.

Fizemos um estudo dos ideais bilaterais e_iN. Agora faremos um estudo dos ideais bilaterais Ne_i. Temos duas situações: $NR=0$ ou $NR\neq 0$. Com raciocínios análogos aos que decorreram ao longo das Afirmações 2 e 3, se $NR\neq 0$ então existe i tal que $Ne_i\neq 0$, $Ne_j=0$ se $j\neq i$, $Ne_i=N$. Então existem 3 casos a serem analisados:

(a) Caso 1. $NR=0$.

(b) Caso 2. $Ne_1\neq 0$, $Ne_j=0$ para todo $j\neq 1$, $Ne_1=N$.

(c) Caso 3. Sem perda de generalidade, $Ne_2\neq 0$, $Ne_j=0$ para todo $j\neq 2$, $Ne_2=N$.

Faremos um estudo caso a caso.

Caso 1. $NR=0$.

Neste caso, a quantidade s de conjuntos B_i's na decomposição de R é 1. De fato, se $s\geq 2$, então de $e_2N=Ne_2=0$ obtemos que B_2 é um ideal de R não nulo tal que $B_2\cap N=0$, o que é um absurdo, pois R é subdiretamente irredutível. Portanto, neste caso, temos $s=1$, ou seja,

$$R=B_1\oplus N.$$

Relembramos que B_1 é um corpo isomorfo a $F_{p^{t_1}}$. Fazendo $f_1(\alpha,u)$ num fixado $0\neq u\in N$ e num elemento qualquer $\alpha\in B_1$, teremos

$$\begin{aligned} 0 &= (\alpha-\alpha^q)(u-u^{q^2})(1-[\alpha,u]^{q-1}) \\ &= (\alpha-\alpha^q)u(1-[\alpha,u]^{q-1}) \\ &= (\alpha-\alpha^q)u. \end{aligned}$$

Nas duas últimas igualdades usamos o fato que N é um ideal de R e $N^2=0$. Como $(\alpha-\alpha^q)u=0$, segue que $\alpha-\alpha^q=0$ para todo $\alpha\in B_1$. Pelo Teorema A.2, podemos mergulhar B_1 em F_q. Sem perda de generalidade, escreveremos $B_1=F_{p^{t_1}}\subseteq F_q$.

Além disso, temos que N é um B_1-espaço vetorial (à esquerda) de dimensão 1. De fato, suponha que existam dois elementos u,v distintos em uma base de N. Temos que B_1u é um ideal de R, pois para todos $b_1,b_1'\in B_1$ e $n\in N$, como $N^2=0$, segue que

$$(b_1+n)(b_1'u)=(b_1b_1')u\in B_1u \text{ e } (b_1'u)(b_1+n)=0\in B_1u.$$

Portanto, B_1u e B_1v são ideais de R não nulos com interseção nula, pois $\{u,v\}$ é L.I., contradizendo assim a irredutibilidade subdireta de R.

Fixada uma base $\{u\}$ para o B_1-espaço vetorial (à esquerda) N, para todo $r \in R$ existem únicos $b_1, b_1' \in B_1$ tais que $r = b_1 + b_1'u$. Denote por ψ a função

$$\begin{array}{rcl} \psi : R & \to & M_2(F_q) \\ r = b_1 + b_1'u & \to & \begin{pmatrix} b_1 & b_1' \\ 0 & 0 \end{pmatrix}. \end{array}$$

A função ψ está bem definida, pois $F_{p^{t_1}} \subseteq F_q$. Provaremos que ψ é um homomorfismo de álgebras. Temos que ψ é transformação linear. Agora, dados $r,s \in R$ tais que $r = b_1 + b_1'u$ e $s = c_1 + c_1'u$, com $b_1, b_1', c_1, c_1' \in B_1$, temos que

$$rs = (b_1 + b_1'u)(c_1 + c_1'u) = b_1c_1 + b_1c_1'u + b_1'uc_1 + b_1'uc_1'u.$$

Como $NB_1 \subseteq NR = 0 = N^2$, temos que

$$rs = b_1c_1 + b_1c_1'u.$$

Logo,

$$\psi(rs) = \begin{pmatrix} b_1c_1 & b_1c_1' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b_1 & b_1' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c_1 & c_1' \\ 0 & 0 \end{pmatrix} = \psi(r)\psi(s).$$

Além disto, ψ é injetiva, pois $\psi(r) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ se, e somente se, $r = 0 + 0u = 0$. Com isso, concluímos que R pode ser mergulhado em $M_2(F_q)$, como era o desejado.

Caso 2. $Ne_1 \neq 0$, $Ne_j = 0$ para todo $j \neq 1$, $Ne_1 = N$.

Neste caso, pela Afirmação 3, temos $N = Ne_1 = e_1Ne_1$. De (3.2) e do enunciado deste caso, temos que $e_2N = Ne_2 = 0$. Portanto, assim como no Caso 1, temos que $R = B_1 \oplus N$ com $B = B_1 = F_{p^{t_1}} \subseteq F_q$.

Sabemos que N é um (B_1, B_1)-bimódulo unitário. De fato, como N é ideal bilateral de R, basta verificar a questão da ação da unidade e_1 nos elementos de N. Pois bem, dado $n \in N = e_1Ne_1$, existe $n' \in N$ tal que $n = e_1n'e_1$ e, portanto,

$$ne_1 = e_1n'e_1e_1 = e_1n'e_1 = n.$$

De maneira análoga, $e_1n = n$, como era o desejado. Desta forma, pelo Teorema 1.37, N admite uma base distinguível D sobre o corpo B_1.

Afirmação 4. Se $u \in D$, então B_1u é um ideal de R.

Demonstração da Afirmação 4. Como u é um elemento distinguível, existe um automorfismo σ do corpo B_1 tal que $ub = \sigma(b)u$ para todo $b \in B_1$. Agora, dados $r \in R$ e $x \in B_1u$, existem $b, b' \in B_1$ e $n \in N$ tais que $r = b+n$ e $x = b'u$, e vale:

$$rx = (b+n)x = bx+nx = bx = bb'u \in B_1u,$$

$$xr = x(b+n) = xb+xn = xb = \sigma(b)x = \sigma(b)b'u \in B_1u,$$

como era o desejado.

Se D tem dois elementos u, v distintos, então $B_1u \cap B_1v = 0$, pois $\{u,v\}$ é L.I. Isso é um absurdo pela Afirmação 4 e pelo fato de R ser subdiretamente irredutível. Portanto, $D = \{u\}$ é uma base de N.

Como $R = B_1 \oplus N$, para todo $r \in R$ existem únicos $b_1, b_1' \in B_1$ tais que $r = b_1 + b_1'u$. Seja ψ definida por

$$\begin{array}{rcl} \psi : R & \to & M_2(F_q) \\ r = b_1 + b_1'u & \to & \begin{pmatrix} b_1 & b_1' \\ 0 & \sigma(b_1) \end{pmatrix}. \end{array}$$

A função ψ está bem definida, pois $B_1 = F_{p^{t_1}} \subseteq F_q$. Provaremos que ψ é um homomorfismo de álgebras. Temos que ψ preserva a soma. Agora, se $\alpha \in F$, então

$$\sigma(\alpha)u = u\alpha = (u\alpha)e_1 = u(\alpha e_1) = \alpha(ue_1) = \alpha u$$

e, consequentemente, $\sigma(\alpha) = \alpha$. Logo, ψ é uma transformação linear. Agora, dados $r, s \in R$ tais que $r = b_1 + b_1'u$ e $s = c_1 + c_1'u$ com $b_1, b_1', c_1, c_1' \in B_1$, temos

$$rs = (b_1 + b_1'u)(c_1 + c_1'u) = b_1c_1 + b_1c_1'u + b_1'uc_1 + b_1'uc_1'u.$$

Como u é distinguível e $N^2 = 0$, segue que

$$rs = b_1c_1 + (b_1c_1' + b_1'\sigma(c_1))u.$$

Logo,

$$\begin{array}{rcl} \psi(rs) & = & \begin{pmatrix} b_1c_1 & b_1c_1' + b_1'\sigma(c_1) \\ 0 & \sigma(b_1c_1) \end{pmatrix} \\ & = & \begin{pmatrix} b_1c_1 & b_1c_1' + b_1'\sigma(c_1) \\ 0 & \sigma(b_1)\sigma(c_1) \end{pmatrix} \\ & = & \begin{pmatrix} b_1 & b_1' \\ 0 & \sigma(b_1) \end{pmatrix} \begin{pmatrix} c_1 & c_1' \\ 0 & \sigma(c_1) \end{pmatrix} \\ & = & \psi(r)\psi(s). \end{array}$$

Além disso, ψ é injetora, pois se $\psi(r) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, então $r = 0 + 0u = 0$.

Com isso, provamos que R pode ser mergulhada em $M_2(F_q)$, como era o desejado.

Caso 3. $Ne_2 \neq 0$, $Ne_j = 0$ para todo $j \neq 2$, $Ne_2 = N$.

Neste caso, de forma semelhante aos anteriores, temos que $e_1Ne_2 = N$ e $B = B_1 \oplus B_2$, portanto $R = B_1 \oplus B_2 \oplus N$. Por um abuso de notação, escreveremos $B_1 = F_{p^{t_1}}$ e $B_2 = F_{p^{t_2}}$.

Afirmação 5. $B_1, B_2 \subseteq F_q$.

Demonstração da Afirmação 5. Dados $\alpha \in B_1$ e $u \in N$, temos que

$$\begin{aligned} 0 = f_2(\alpha, u) &= (\alpha - \alpha^q) \circ (u - u^q) - ((\alpha - \alpha^q) \circ (u - u^q))^q \\ &= (\alpha - \alpha^q) \circ u - ((\alpha - \alpha^q) \circ u)^q \\ &= (\alpha - \alpha^q)u + u(\alpha - \alpha^q) - ((\alpha - \alpha^q)u + u(\alpha - \alpha^q))^q \\ &= (\alpha - \alpha^q)u + u(\alpha - \alpha^q). \end{aligned}$$

Como $Ne_1 = 0$, obtemos

$$0 = f_2(\alpha, u) = (\alpha - \alpha^q)u.$$

Disso, segue que $\alpha - \alpha^q = 0$ para todo $\alpha \in B_1$. Logo, podemos mergulhar B_1 em F_q. Sem perda de generalidade, escreveremos $B_1 = F_{p^{t_1}} \subseteq F_q$.

De forma semelhante, dados $\beta \in B_2$ e $u \in N$, usando (3.2), temos que

$$0 = f_2(\beta, u) = u(\beta - \beta^q)$$

e podemos mergulhar B_2 em F_q. Novamente, sem perda de generalidade, escreveremos $B_2 = F_{p^{t_2}} \subseteq F_q$.

Com isso, provamos que $B_1 \subseteq F_q$ e $B_2 \subseteq F_q$, finalizando assim a demonstração da afirmação.

Se B_1 não admite um subcorpo isomorfo B_2, então $\tilde{N} = F_q \otimes_{B_1} N$ é um (F_q, B_2)-bimódulo unitário. Para facilitar a notação, omitiremos este caso, mas gostaríamos de ressaltar que ele segue as mesmas ideias do caso a seguir, fazendo as devidas adequações.

Suponha que B_1 admite um subcorpo B_2' isomorfo a B_2. Denote por $\rho : B_2 \to B_2'$ tal isomorfismo. Por meio da igualdade $e_1Ne_2 = N$ temos que N é um (B_1, B_2)-bimódulo. Portanto, por meio da multiplicação $*$ dada por

$$b_2 * n = \rho(b_2)n,\ b_2 \in B_2,\ n \in N,$$

podemos ver N como um (B_2, B_2)-bimódulo. Pelo Teorema 1.37, N admite uma base distinguível C sobre B_2. Além disto, temos que N é um B_1-espaço vetorial à esquerda.

Afirmação 6. Se $u \in C$, então B_1u é um ideal de R.

Demonstração da Afirmação 6. Como u é um elemento distinguível, existe um automorfismo σ do corpo B_2 tal que $ub_2 = \sigma(b_2)u$ para todo $b_2 \in B_2$. Agora, dado $r \in R$ e $x \in B_1u$, existem $b_1, b_1' \in B_1$, $b_2 \in B_2$ e $n \in N$ tais que $r = b_1 + b_2 + n$ e $x = b_1'u$, e vale:

$$rx = (b_1 + b_2 + n)x = b_1x + b_2x + nx = b_1x = b_1b_1'u \in B_1u,$$

$$xr = x(b_1 + b_2 + n) = xb_1 + xb_2 + xn = xb_2 = \sigma(b_2) * x = \rho(\sigma(b_2))b_1'u \in B_1u,$$

como era o desejado.

De maneira semelhante ao Caso 2, a Afirmação 6 implica que $\dim_{B_1}(N) = 1$. Fixe uma base $\{u\}$ para o B_1-espaço vetorial à esquerda N.

Deste modo, se $n \in N$, então existe um único $b_1' \in B_1$ tal que $n = b_1'u$. Como $R = B_1 \oplus B_2 \oplus N$, para todo $r \in R$ existem únicos $b_1, b_1' \in B_1$ e $b_2 \in B_2$ tais que $r = b_1 + b_2 + b_1'u$. Seja ψ definida por

$$\begin{array}{rcl} \psi & : & R \to M_2(F_q) \\ & & b_1 + b_2 + b_1'u \to \left(\begin{array}{cc} b_1 & b_1' \\ 0 & \rho(\sigma(b_2)) \end{array} \right). \end{array}$$

A função ψ está bem definida, pois $B_1 = F_{p^{t_1}} \subseteq F_q$ e $B_2 = F_{p^{t_2}} \subseteq F_q$. Provaremos que ψ é um homomorfismo de álgebras. Temos que ψ é uma transformação linear. Agora, dados $r, s \in R$ tais que $r = b_1 + b_2 + b_1'u$ e $s = c_1 + c_2 + c_1'u$ com $b_1, b_1', c_1, c_1' \in B_1$ e $b_2, c_2 \in B_2$, temos

$$\begin{array}{rcl} rs & = & (b_1 + b_2 + b_1'u)(c_1 + c_2 + c_1'u) \\ & = & b_1c_1 + b_1c_2 + b_1c_1'u + b_2c_1 + b_2c_2 + b_2c_1'u + b_1'uc_1 + b_1'uc_2 + b_1'uc_1'u. \end{array}$$

Como $B_1B_2 = 0$ e $N^2 = e_2N = Ne_1 = 0$, então

$$b_1c_2 = b_2c_1 = b_2c_1'u = b_1'uc_1'u = b_1'uc_1 = 0.$$

Além disso, como u é um elemento distinguível de N, temos $b_1'uc_2 = b_1'\rho(\sigma(c_2))u$, e portanto

$$rs = b_1c_1 + b_2c_2 + (b_1c_1' + b_1'\rho(\sigma(c_2)))u.$$

Portanto,

$$\begin{array}{rcl} \psi(rs) & = & \left(\begin{array}{cc} b_1c_1 & b_1c_1' + b_1'\rho(\sigma(c_2)) \\ 0 & \rho(\sigma(b_2c_2)) \end{array} \right) \\ & = & \left(\begin{array}{cc} b_1c_1 & b_1c_1' + b_1'\rho(\sigma(c_2)) \\ 0 & \rho(\sigma(b_2))\rho(\sigma(c_2)) \end{array} \right) \\ & = & \left(\begin{array}{cc} b_1 & b_1' \\ 0 & \rho(\sigma(b_2)) \end{array} \right) \left(\begin{array}{cc} c_1 & c_1' \\ 0 & \rho(\sigma(c_2)) \end{array} \right) = \psi(r)\psi(s). \end{array}$$

Por último, ψ será injetora, pois se $\psi(r) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, então $b_1 = b_1' = 0$ e $\rho(\sigma(b_1)) = 0$. Como ρ e σ são injetores temos que $b_2 = 0$, ou seja, $r = 0+0+0u = 0$.

Com isso, provamos que R pode ser mergulhada em $M_2(F_q)$, como queríamos demonstrar.

Finalizamos aqui a demonstração da proposição. □

Com isso, temos o seguinte teorema:

Teorema 3.10. *Seja F um subcorpo de F_q. O T-ideal de $F\langle X\rangle$ formado pelas identidades polinomiais da F-álgebra $M_2(F_q)$ é gerado pelos polinômios*

$$f_1(x,y) = (x-x^q)(y-y^{q^2})(1-[x,y]^{q-1}) \ \ e$$
$$f_2(x,y) = (x-x^q)\circ(y-y^q) - ((x-x^q)\circ(y-y^q))^q,$$

onde $[x,y] = xy-yx$ e $x\circ y = xy+yx$.

Demonstração. É consequência direta da Proposição 3.9 e dos comentários no início desta seção. □

Provamos então que o T-ideal da álgebra $M_2(F_q)$ é gerado por f_1 e f_2. É possível provar que estas duas identidades são independentes, ou seja,

$$f_1 \notin \langle f_2\rangle^T \ \text{ e } \ f_2 \notin \langle f_1\rangle^T.$$

Para isso, explicitaremos duas álgebras onde apenas uma das duas identidades são satisfeitas.

Seja R a álgebra sobre F_{q^2} com base $\{e,u\}$ e multiplicação definida por

$$e^2 = e,\ ue = u,\ eu = u^2 = 0.$$

Note que, pela construção, se $r \in R$ então $r = ae+bu$ para alguns $a,b \in F_{q^2}$ e

$$\begin{aligned} r^2 &= a^2e+bau \\ r^3 &= a^3e+ba^2u \\ &\cdots \\ r^{q^2} &= a^{q^2}e+ba^{q^2-1}u. \end{aligned}$$

Como $a,b \in F_{q^2}$, temos que $a^{q^2} = a$. Logo,

$$r^{q^2} = ae+ba^{q^2-1}u.$$

Portanto, $r-r^{q^2} = b(1-a^{q^2-1})u \in N$, onde $N = span\{u\}$. Além disto, $RN = 0$ pois $ru = 0$ para todo $r \in R$. Com isso, temos que f_1 é uma identidade de R, pois $(x-x^q) \in R$ e $(y-y^{q^2}) \in N$ para todos

$x, y \in R$. Porém, dado $\alpha \in F_{q^2}$ tal que $\alpha^q \neq \alpha$, temos que

$$\begin{aligned} f_2(u, \alpha e) &= (u - u^q) \circ (\alpha e - (\alpha e)^q) - ((u - u^q) \circ (\alpha e - (\alpha e)^q))^q \\ &= u \circ (\alpha e - (\alpha e)^q) - (u \circ (\alpha e - (\alpha e)^q))^q \\ &= u \circ ((\alpha - \alpha^q)e) - (u \circ ((\alpha - \alpha^q)e))^q \\ &= (\alpha - \alpha^q)u \circ e - ((\alpha - \alpha^q)u \circ e)^q \\ &= (\alpha - \alpha^q)u - (\alpha - \alpha^q)^q u^q \\ &= (\alpha - \alpha^q)u \neq 0. \end{aligned}$$

Ou seja, f_2 não é identidade de R e, portanto, $f_2 \notin \langle f_1 \rangle^T$.

Por outro lado, seja A a álgebra sobre F_q com base $\{u, v, uv\}$ e multiplicação definida por $u^2 = v^2 = 0$ e $uv = -vu$, isto é, $u \circ v = 0$. Temos que se $x, y \in A$, então $x = a_x u + b_x v + c_x uv$ e $y = a_y u + b_y v + c_y uv$ para alguns $a_x, a_y, b_x, b_y, c_x, c_y \in F_q$. Assim, $xy = a_x b_y uv + b_x a_y vu = -yx$ e, portanto, $x \circ y = 0$. Disso obtemos que f_2 é uma identidade para A. Porém,

$$\begin{aligned} f_1(u, v) &= (u - u^q)(v - v^{q^2})(1 - [u, v]^{q-1}) \\ &= uv(1 - [u, v]^{q-1}) \\ &= uv - uv[u, v]^{q-1} = uv \neq 0. \end{aligned}$$

Ou seja, f_1 não é identidade de A e, portanto, $f_1 \notin \langle f_2 \rangle^T$. Com isso, provamos que as duas identidades são independentes.

APÊNDICE A

Alguns resultados da teoria de corpos

Muitas vezes durante esta dissertação nos deparamos com conceitos e propriedades importantes de corpos. Sendo assim, relembraremos neste Apêndice alguns resultados da Teoria de Galois. Os resultados aqui apresentados podem ser encontrados no livro [28].

A.1 Corpos finitos

Dado um corpo F, a sua característica será 0 ou um número primo $p \geq 2$. Em particular, se F é finito, então a sua característica é um número primo.

Se F é um corpo finito de característica p, então temos uma "cópia" de $\mathbb{Z}_p$ dentro de F, e podemos deduzir que F tem p^n elementos para algum $n \geq 1$. A respeito da classificação dos corpos finitos, o seguinte resultado pode ser encontrado nos Teoremas 3.127 e 3.132 de [28].

Teorema A.1. *Se p é um número primo e $n \geq 1$, então existe um corpo finito com exatamente p^n elementos. Além disso, quaisquer dois corpos com p^n elementos são isomorfos.*

Denotamos por F_q o corpo finito com $q = p^n$ elementos e o chamamos de corpo de Galois.

Teorema A.2. *Sejam p um número primo, $n \geq 1$ e $q = p^n$. Sejam L e F_q extensões de um corpo F tal que*

$$\alpha^q - \alpha = 0 \text{ para todo } \alpha \in L.$$

Então, existe um homomorfismo de corpos injetivo $\eta : L \to F_q$ que fixa os elementos de F.

Demonstração. Seguindo a mesma demonstração de [28, Teorema 3.127], existe um corpo $\tilde{L}$ com q elementos que estende L. Tal corpo $\tilde{L}$ é o corpo de fatoração do polinômio

$$f(x) = x^q - x$$

sobre L. Em particular, $\tilde{L}$ é o corpo de fatoração de $f(x)$ sobre F. Como F_q também é o corpo de fatoração de $f(x)$ sobre F, segue do [28, Teorema 3.131] que existe um isomorfismo de corpos

$\eta : \tilde{L} \to F_q$ que fixa os elementos de F. Fazendo a restrição de tal homomorfismo a L teremos o desejado. □

Vale ressaltar que o homomorfismo η do enunciado é um monomorfismo de F-álgebras, pois se $\alpha \in F$ e $u \in L$, então

$$\eta(\alpha u) = \eta(\alpha)\eta(u) = \alpha\eta(u).$$

A.2 Corpos perfeitos

Definição A.3. Se F é um corpo de característica p prima, então a aplicação $\mathscr{F} : F \to F$ definida por

$$\mathscr{F}(\alpha) = \alpha^p, \ \alpha \in F,$$

é chamada de aplicação de Frobenius.

Temos que a aplicação de Frobenius é um homomorfismo de corpos. Porém, para provarmos isso, precisamos do seguinte resultado.

Proposição A.4. *Se F é um corpo de característica p prima, então*

$$(a+b)^p = a^p + b^p$$

para todos $a, b \in F$.

Demonstração. O coeficiente binomial $\binom{p}{i}$ é múltiplo de p se $0 < i < p$. Logo, se $a, b \in F$, então pelo binômio de Newton obtemos

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i = a^p + b^p,$$

o que prova a nossa proposição. □

Vale ressaltar o seguinte corolário.

Corolário A.5. *Se F é um corpo de característica p prima, então*

$$(a+b)^{p^r} = a^{p^r} + b^{p^r}$$

para todos $a, b \in F$.

Demonstração. Pela proposição anterior

$$\begin{aligned} (a+b)^{p^r} &= ((a+b)^p)^{p^{r-1}} \\ &= (a^p + b^p)^{p^{r-1}}. \end{aligned}$$

Repetindo o processo acima r vezes teremos o desejado. □

Vamos mostrar agora que a função de Frobenius $\mathscr{F}$ é um homomorfismo de corpos. Temos que se F é um corpo de característica p prima e $\alpha, \beta \in F$ então, pela proposição anterior,

$$\mathscr{F}(\alpha+\beta) = (\alpha+\beta)^p = \alpha^p + \beta^p = \mathscr{F}(\alpha) + \mathscr{F}(\beta).$$

Logo, $\mathscr{F}$ preserva a soma. As outras propriedades são diretas.

Note que $\mathscr{F}$ é injetora pois é um homomorfismo de corpos. Denotamos por F^p o conjunto $\mathscr{F}(F)$, isto é, a imagem de $\mathscr{F}$, ou seja, o subcorpo de todas as p-ésimas potências dos elementos de F. Se F for sobrejetora, então $F = F^p$ o que implica que todos os elementos de F são p-ésimas raízes de outro elemento de F. Pensando nisso temos a seguinte definição.

Definição A.6. Um corpo F é dito perfeito se ele possui característica 0 ou se possui característica $p > 0$ e $F = F^p$.

Um resultado importante sobre corpos perfeitos é o seguinte.

Teorema A.7. *Todo corpo finito é perfeito.*

Demonstração. Seja F um corpo finito de característica p. Como a aplicação de Frobenius $\mathscr{F} : F \to F$ é injetora e F é finito, temos que $\mathscr{F}(F)$ e F possuem a mesma quantidade de elementos, logo $\mathscr{F}$ é sobrejetora e $F = F^p$. □

Outra definição importante que tem relação com corpos perfeitos é o conceito de separabilidade.

Definição A.8. Um polinômio irredutível $p(x) \in F[x]$ é dito separável se ele não possui raízes repetidas em toda extensão de corpos de F. Um polinômio $f(x) \in F[x]$ é dito separável se seus fatores irredutíveis são separáveis.

Proposição A.9. *Um corpo F é perfeito se, e somente se, todo polinômio em $F[x]$ é separável.*

Demonstração. A demonstração pode ser encontrada no item (i) da Proposição 6.79 do livro [28]. □

Referências Bibliográficas

[1] AMITSUR, Shimshon A.; LEVITZKI, Jacob. **Minimal identities for algebras**. Proceedings of the American Mathematical Society, v. 1, n. 4, p. 449–463, 1950.

[2] BEHRENS, Edward A. **Ring theory**. New York: Academic Press, 1972. (Pure and Applied Mathematics).

[3] BELOV, Aleksei Ya. On non-Spechtian varieties. **Fundamentalnaya i Prikladnaya Matematika**, v. 5, n. 1, p. 47–66, 1999.

[4] BELOV, Aleksei Ya. Counterexamples to the Specht problem. **Sbornik: Mathematics**, v. 191, n. 3, p. 329–340, 2000.

[5] BREŠAR, Matej. **Undergraduate algebra: a unified approach**. Cham: Springer, 2019. (Springer Undergraduate Mathematics Series).

[6] BREŠAR, Matej. **Introduction to noncommutative algebra**. Cham: Springer, 2014. 212 p. (Universitext).

[7] DRENSKY, Vesselin S. A minimal basis for identities of a second-order matrix algebra over a field of characteristic 0. **Algebra i Logika**, v. 20, n. 3, p. 282–290, 1981.

[8] DRENSKY, Vesselin S. **Free Algebras and PI-Algebras**. Springer-Verlag, 2000. (Advanced Courses in Mathematics CRM Barcelona).

[9] GENOV, Georgi K. A basis of identities of the algebra of third-order matrices over a finite field. **Algebra and Logic**, v. 20, n. 4, p. 241–257, 1981.

[10] GENOV, Georgi K.; SIDEROV, Petar N. A basis of identities of the algebra of fourth-order matrices over a finite field. **Serdica**, v. 8, p. 313–323, 351–366, 1982.

[11] GRISHIN, Aleksandr V. Examples of T-spaces and T-ideals over a field of characteristic 2 without the finite basis property. **Fundamentalnaya i Prikladnaya Matematika**, v. 5, n. 1, p. 101–118, 1999.

[12] GRISHIN, Aleksandr V. On non-Spechtianness of the variety of associative rings that satisfy the identity x32 = 0. **Electronic Research Announcements**, v. 6, n. 7, p. 50–51, 2000.

[13] GUPTA, Chandan K.; KRASILNIKOV, Andrei N. A simple example of a non-finitely based system of polynomial identities. **Communications in Algebra**, v. 30, n. 10, p. 4851–4866, 2002.

[14] HALL, Marshall. Projective planes. **Transactions of the American Mathematical Society**, v. 54, n. 2, p. 229–277, 1943.

[15] HERSTEIN, Israel N. **Noncommutative rings**. Washington, D.C.: Mathematical Association of America, 1968. (Carus Mathematical Monographs; 15).

[16] HUNGERFORD, Thomas W. **Algebra**. New York: Springer, 1974. (Graduate Texts in Mathematics; 73).

[17] JACOBSON, Nathan. Structure theory for algebraic algebras of bounded degree. **Annals of Mathematics**, v. 46, n. 4, p. 695–707, 1945.

[18] KAPLANSKY, Irving. On a problem of Kurosh and Jacobson. **Bulletin of the American Mathematical Society**, v. 52, n. 5, p. 419–422, 1946.

[19] KEMER, A. R. Finite basis property of identities of associative algebras. **Algebra and Logic**, v. 26, n. 5, p. 362–397, 1987.

[20] KOSHLUKOV, Plamen. Basis of the identities of the matrix algebra of order two over a field of characteristic $p \neq 2$. **Journal of Algebra**, v. 241, n. 1, p. 410–434, 2001.

[21] LEVITZKI, Jacob. On a problem of Kurosh. **Bulletin of the American Mathematical Society**, v. 52, p. 1033–1035, 1946.

[22] LUCCAS, Luis. **Uma breve introdução à teoria das PI-álgebras**. São Carlos: UFSCar, 2023. Trabalho de Conclusão de Curso – Graduação em Matemática, Universidade Federal de São Carlos.

[23] MAL'TSEV, Yu. N.; KUZ'MIN, E. N. A basis for the identities of the algebra of second-order matrices over a finite field. **Algebra and Logic**, v. 17, p. 18–21, 1978.

[24] MCCOY, Neal H. Subdirect sums of rings. **Bulletin of the American Mathematical Society**, v. 53, n. 9, p. 856–877, 1947.

[25] RAZMYSLOV, Yuri P. Trace identities of full matrix algebras over a field of characteristic zero. **Izvestiya Akademii Nauk SSSR, Seriya Matematicheskaya**, v. 38, p. 723–756, 1974.

[26] RAZMYSLOV, Yuri P. The existence of a finite basis for the identities of the matrix algebra of order two over a field of characteristic zero. **Algebra i Logika**, v. 12, n. 1, p. 83–113, 1973.

[27] RAGHAVENDRAN, R. Finite associative rings. **Compositio Mathematica**, v. 21, p. 195–229, 1969.

[28] ROTMAN, Joseph J. **Advanced modern algebra**. Upper Saddle River: Pearson Education, 2002.

[29] ROWEN, Louis H. **Ring theory**. New York: Academic Press, 1988. v. 83. (Pure and Applied Mathematics).

[30] SPECHT, Wilhelm. Gesetze in Ringen. I. **Mathematische Zeitschrift**, v. 52, n. 1, p. 557–589, 1950.

[31] WAGNER, Wolfgang. Über die Grundlagen der projektiven Geometrie und allgemeine Zahlensysteme. **Mathematische Annalen**, v. 113, n. 1, p. 528–567, 1937.