UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

ISABELA MONTEIRO MASSANO

ÁLGEBRAS COM IDENTIDADES POLINOMIAIS

SÃO CARLOS

2023

ÁLGEBRAS COM IDENTIDADES POLINOMIAIS

Autora: *Isabela Monteiro Massano*

Orientador: *Prof. Dr. Humberto Luiz Talpo*

Disciplina: Trabalho de Conclusão do Curso B

Curso: Bacharelado em Matemática

Professores Responsáveis: Adriana Ramos Pereira
Luciene Nogueira Bertoncello
Luis Antonio Carvalho dos Santos

Instituição: Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Matemática

São Carlos, 2023.

Massano, Isabela Monteiro

Álgebras com identidades polinomiais / Isabela Monteiro Massano -- 2023.
50f.

TCC (Graduação) - Universidade Federal de São Carlos, campus São Carlos, São Carlos
Orientador (a): Humberto Luiz Talpo
Banca Examinadora: Humberto Luiz Talpo, Dimas José Gonçalves, Fábio Gomes Figueira
Bibliografia

1. Álgebra. 2. Identidades polinomiais. 3. Álgebras graduadas. I. Massano, Isabela Monteiro. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Ronildo Santos Prado - CRB/8 7325

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENAÇÃO DOS CURSOS DE GRADUAÇÃO EM MATEMÁTICA - CCM/CCET
Rod. Washington Luís km 235 - SP-310, s/n - Bairro Monjolinho, São Carlos/SP, CEP 13565-905
Telefone: (16) 33518221 - http://www.ufscar.br

DP-TCC-FA nº 27/2023/CCM/CCET

Graduação: Defesa Pública de Trabalho de Conclusão de Curso

Folha Aprovação (GDP-TCC-FA)

FOLHA DE APROVAÇÃO

ISABELA MONTEIRO MASSANO

IDENTIDADES POLINOMIAIS GRADUADAS

Trabalho de Conclusão de Curso

Universidade Federal de São Carlos – Campus São Carlos

São Carlos, 04 de setembro de 2023

ASSINATURAS E CIÊNCIAS

Cargo/Função	Nome Completo
Orientador	Humberto Luiz Talpo
Membro da Banca 1	Dimas José Gonçalves
Membro da Banca 2	Fábio Gomes Figueira

Documento assinado eletronicamente por **Humberto Luiz Talpo**, **Professor(a) do Ensino Superior**, em 25/09/2023, às 17:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Dimas Jose Goncalves**, **Professor(a) do Ensino Superior**, em 02/10/2023, às 16:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Fabio Gomes Figueira**, **Professor(a) Adjunto(a)**, em 05/10/2023, às 10:33, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufscar.br/autenticacao, informando o código verificador **1189427** e o código CRC **F0DF0E72**.

RESUMO

Neste trabalho são introduzidas denições e resultados básicos sobre Álgebras com Identidades Polinomiais, enunciados e demonstrados alguns resultados clássicos da teoria que as envolvem, como o Teorema de Amitsur-Levitzki, segundo Rosset [4]. Além disso descrevemos uma base para o ideal das identidades $\mathbb{Z}_n$-graduadas da álgebra das matrizes $n \times n$ sobre um corpo de característica zero.

Palavras-chave: álgebras. identidades polinomiais. identidades polinomiais graduadas.

ABSTRACT

In this work, basic definitions and results on Algebras with Polynomial Identities are introduced, some classic results of the theory that involve them are stated and demonstrated, such as the Amitsur-Levitzki Theorem, according to Rosset [4]. Furthermore, we describe a basis for the ideal of the $\mathbb{Z}_n$-graded identities of the matrix algebra $n \times n$ over a field of characteristic zero.

Keywords: algebra. polynomial identities. graded polynomial identities.

SUMÁRIO

1 INTRODUÇÃO

Álgebras são objetos de grande importância na matemática e dentre elas destacamos as álgebras com identidades polinomiais ou PI-álgebras. Tendo em vista que as identidades polinomiais dizem muito sobre a estrutura de uma algebra, seu estudo é algo de grande interesse, sendo um amplo campo de pesquisa atual.

A teoria das álgebras com identidades polinomiais (ou PI-teoria) começou a se desenvolver mais intensamente por volta de 1950, quando foi provado o Teorema de Amitsur-Levitzki [3], o qual garante que a álgebra $M_n(\mathbb{K})$ das matrizes $n \times n$ sobre um corpo $\mathbb{K}$ satisfaz a indentidade "standard" de grau $2n$.

Este trabalho é baseado em argumentos combinatórios e, posteriormente, outras demonstrações foram dadas para este teorema usando-se técnicas diversas, das quais uma delas será abordade nesse texto, a demonstração dada por Rosset [4], que utiliza argumentos algébricos.

Além disso, tomando $\mathbb{K}\langle X\rangle$ a álgebra associativa livre (gerada por um conjunto enumerável X) sobre um corpo $\mathbb{K}$ e A uma álgebra associativa sobre $\mathbb{K}$. O conjunto $T(A)$ das identidades polinomiais de A forma um T-ideal de $\mathbb{K}\langle X\rangle$, isto é, um ideal que tem a propriedade de ser invariante sob todos os endomorfismos de $\mathbb{K}\langle X\rangle$. Como a interseção de uma família qualquer de T-ideais é um T-ideal, dado $S \subset \mathbb{K}\langle X\rangle$ podemos definir o T-ideal gerado por S, denotado por $\langle S\rangle^T$, como a interseção de todos os T-ideais de $\mathbb{K}\langle X\rangle$ que contém S. Se $S \subset T(A)$ é tal que $\langle S\rangle^T = T(A)$, dizemos que S é uma base das identidades de A.

Também em 1950, W. Specht conjecturou que, para corpos de característica zero, todo ideal próprio é finitamente gerado, isto é, possui uma base finita. Esta conjectura ficou conhecida como *Problema de Specht* [9] e a resposta afirmativa foi obtida apenas em 1987 por A. Kemer [6]. No caso particular da álgebra de matrizes $M_n(\mathbb{K})$ a existência de bases finitas para o T-ideal $T(M_n(\mathbb{K}))$ é garantida pelos resultados de Kemer, porém a exibição de tal base é conhecida apenas para $n = 2$ ([11],[12]).

Surge então o interesse por outros tipos de identidades polinomiais, como por exemplo, as identidades graduadas, que possuem, de certo modo, formas mais simples de descrever a base das identidades. O caso de identidades $\mathbb{Z}_n$-graduadas para a álgebra de matrizes $M_n(\mathbb{K})$, o qual será um dos focos deste trabalho, também foi resolvido inicialmente para $n = 2$ por O. M. Di Vicenzo [8] e posteriormente para um n qualquer por S. Yu Vasilovsky em 1999 [10], ainda no caso de corpos de característica zero. O resultado de Vasilovsky foi generalizado para corpos infinitos em 2002 por S. S. Azevedo [7].

2 NOÇÕES BÁSICAS

O objetivo deste capítulo é introduzir o objeto básico deste estudo, uma álgebra sobre um corpo $\mathbb{K}$, e fornecer diversos exemplos clássicos desse objeto. Iremos assumir conhecimento prévio de alguns conceitos e resultados básicos de estruturas algébricas como grupos, anéis, corpos e espaços vetoriais os quais serão fundamentais para a construção do texto.

Definição 2.1. Um conjunto A é uma **álgebra** sobre um corpo $\mathbb{K}$, ou uma $\mathbb{K}$-álgebra, se possui as seguintes operações binárias e se, dados $x, y, z \in A$, $\lambda, \mu \in \mathbb{K}$ essas satisfazem os seguintes axiomas:

(i) Adição $A \times A \to A$, $(x, y) \mapsto x + y$, satisfazendo

  (a) $(x + y) + z = x + (y + z) = x + y + z$ *(Associatividade)*

  (b) Existe $0 \in A$ tal que $x + 0 = x$ *(Elemento neutro)*

  (c) Para cada $x \in A$, existe $x' \in A$ tal que $x + x' = 0$ *(Elemento inverso)*

  (d) $x + y = y + x$ *(Comutatividade)*

(ii) Multiplicação por escalar $\mathbb{K} \times A \to A$, $(\lambda, x) \mapsto \lambda x$, sendo que vale

  (a) $(\lambda + \mu)x = \lambda x + \mu x$ *(Distributividade com relação à adição em* $\mathbb{K}$*)*

  (b) $\lambda(x + y) = \lambda x + \lambda y$ *(Distributividade com relação à adição em A)*

  (c) $\lambda(\mu x) = (\lambda\mu)x$ *(Compatibilidade com a multiplicação em* $\mathbb{K}$*)*

  (d) $1x = x$ *(Elemento identidade)*

(iii) Multiplicação $A \times A \to A$, $(x, y) \mapsto xy$, a qual satisfaz

  (a) $(xy)z = x(yz) = xyz$ *(Associatividade)*

  (b) $(x + y)z = xz + yz$ *(Distributiva à direita)*

  (c) $x(y + z) = xy + xz$ *(Distributiva à esquerda)*

  (d) $(\lambda x)(\mu y) = (\lambda\mu)(xy)$ *(Compatibilidade com os escalares)*

Observe que exigimos que a multiplicação dos elementos da álgebra seja associativa, também poderiamos definir uma álgebra sem essa necessidade, mas como nesse trabalho trataremos apenas de álgebras associativas, já incluímos esse item na definição, assim quando dizemos que A é uma álgebra, entenda como uma álgebra associativa. Agora, dizemos que A é **comutativa** se

$xy = yx$ para quaisquer $x, y \in A$ e ainda que A é **unitária** se existir $1_A \in A$ tal que $1_A x = x1_A = x$ para todo $x \in A$. Além disso, se existe $n \in \mathbb{N}$ tal que $A^n = 0$, isto é, que o produto de quaisquer n elementos de A é igual a zero, A é **nilpotente**, neste caso, o menor n que satisfaz esta condição é dito **índice de nilpotência** de A.

Note que podemos considerar uma $\mathbb{K}$-álgebra A como um espaço vetorial sobre o corpo $\mathbb{K}$ (itens (i) e (ii)) dotado de uma multiplicação associativa entre os vetores (item (iii)), ou então como um anel associativo (itens (i) e (iii)) munido de uma multiplicação por escalares em um corpo $\mathbb{K}$. Assim, uma álgebra possui ambas as propriedades de um espaço vetorial e de um anel associativo.

Dessa maneira, podemos dizer que um subconjunto β é uma **base** da álgebra A se é base de A como espaço vetorial, bem como a **dimensão** de A é sua dimensão como espaço vetorial sobre $\mathbb{K}$ e essa será denotada por $[A : \mathbb{K}]$. Além disso, uma **subálgebra** é um subanel que também é um subespaço e um **ideal** de uma álgebra é um ideal no sentido da teoria de anéis e também é um subespaço. Se I é um ideal da $\mathbb{K}$-álgebra A, então o anel quociente A/I se torna uma $\mathbb{K}$-álgebra, chamada **álgebra quociente**, se definirmos a multiplicação por escalar como

$$\lambda(x + I) \coloneqq \lambda x + I.$$

Definição 2.2. Dadas duas $\mathbb{K}$-álgebras A e B, um **homomorfismo** $\varphi : A \to B$ é uma função tal que dados $x, y \in A$ e $\lambda \in \mathbb{K}$ tem-se

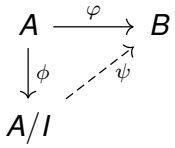
(i) $\varphi(x + y) = \varphi(x) + \varphi(y)$

(ii) $\varphi(xy) = \varphi(x)\varphi(y)$

(iii) $\varphi(\lambda x) = \lambda\varphi(x)$

Um homomorfismo é dito **isomorfismo** se é bijetor e, quando existe um isomorfismo $\varphi : A \to B$, dizemos que A e B são isomorfas e denotamos $A \simeq B$. Um **endomorfismo** de uma álgebra A é um homomorfismo de A em A. Observe que um homomorfismo de álgebras é um homomorfismo de anéis que também é uma transformação linear. Logo, os resultados usuais referentes a homomorfismos de espaços vetoriais e anéis continuam válidos para homomorfismos de álgebras, por exemplo os dois teoremas enunciado a seguir, que serão utilizados durante o texto. A demonstração desse resultado é essencialmente a mesma do caso de anéis, basta verficar que, nesse caso, a multiplicação por escalar também é preservada.

Teorema 2.1 (Teorema Fundamental dos Homomorfismos)**.** *Dadas duas álgebras A e B e um homomorfismo de álgebras $\varphi : A \to B$, seja I um ideal de A e ϕ o homomorfismo sobrejetivo canônico $A \to A/I$, onde A/I é a álgebra quociente. Se I é um subconjunto de* $\ker(\varphi)$ *então existe um único homomorfismo $\psi : A/I \to B$ tal que $\varphi = \psi \circ \phi$.*



Teorema 2.2 (Teorema do Isomorfismo)**.** *Seja $\varphi : A \to B$ um homomorfismo de álgebras. Então* $\ker(\varphi) = \{x \in A \mid \varphi(x) = 0\}$*, o núcleo de φ, é um ideal de A e*

$$\frac{A}{\ker(\varphi)} \simeq \mathrm{Im}(\varphi)$$

isto é, a álgebra quociente $A/\ker(\varphi)$ é isomorfa à imagem $\mathrm{Im}(\varphi) = \{\varphi(x) \mid x \in A\}$*. Em particular, se φ é sobrejetor então* $\dfrac{A}{\ker(\varphi)} \simeq B$*.*

Agora vejamos alguns exemplos de álgebras. Não colocaremos a verificação de que tais exemplos são, de fato, álgebras, por essa ser direta e não ser o objetivo desse texto.

Exemplo 2.1. O espaço vetorial dos polinômios em n variáveis comutativas, denotado por $\mathbb{K}[x_1, x_2, \ldots, x_n]$, é uma $\mathbb{K}$-álgebra comutativa e unitária com relação ao produto usual de polinômios.

Exemplo 2.2. O espaço das matrizes $n \times n$ com coeficientes em $\mathbb{K}$, denotado por $M_n(\mathbb{K})$, é uma $\mathbb{K}$-álgebra unitária, com relação ao produto usual de matrizes. Notemos que essa álgebra não é comutativa. Nela, destacamos as matrizes unitárias E_{ij}, para $1 \leq i, j \leq n$, onde E_{ij} é a matriz cuja única entrada não nula é 1 na i-ésima linha e j-ésima coluna. Essas matrizes formam uma base para $M_n(\mathbb{K})$, chamada base canônica, e assim $[M_n(\mathbb{K}) : \mathbb{K}] = n^2$.

Exemplo 2.3. Seja V um espaço vetorial sobre $\mathbb{K}$. Então $End_{\mathbb{K}}(V)$, o conjunto de todos os endomorfismos de V (isto é, operadores lineares de V em V) se torna uma $\mathbb{K}$-álgebra se definirmos a adição, multiplicação por escalar e multiplicação por

$$(A + B)(v) := A(v) + B(v),$$

$$(\lambda A)(v) := \lambda A(v),$$

$$(AB) := A(B(v)).$$

Para o alguns exemplos, incluindo o próximo, precisaremos do seguinte conceito. Dizemos que um corpo $\mathbb{K}$ tem característica p onde p é o menor número natural tal que $1 + 1 + \cdots + 1$ (p vezes) $= 0$. Caso não tenhamos esse número dizemos que $\mathbb{K}$ tem característica 0. Denotaremos por $\mathrm{char}(\mathbb{K})$ a característica do corpo $\mathbb{K}$.

Exemplo 2.4. Seja $\mathbb{K}$ um corpo tal que char($\mathbb{K}$) = 0. Defina $D, L \in End_{\mathbb{K}}(\mathbb{K}[\omega])$ por

$$D(f(\omega)) = f'(\omega), \quad L(f(\omega)) = \omega f(\omega).$$

Aqui, $f'(\omega)$ é a derivada de $f(\omega)$. A subálgebra de $End_{\mathbb{K}}(\mathbb{K}[\omega])$ gerada por D e L é chamada **álgebra de Weyl**, ou então **a primeira álgebra de Weyl**, e é denotada por $\mathscr{A}_1$.

Exemplo 2.5. Agora iremos definir a chama **álgebra de grupo**, denotada por $\mathbb{K}[G]$. Assuma temporariamente que G é um conjunto arbitrário e $\mathbb{K}$ um corpo. Assim podemos construir o espaço vetorial sobre $\mathbb{K}$ cuja base é G e seus elementos são as somas formais $\sum_{g \in G} \lambda_g g$ onde $\lambda_g \in \mathbb{K}$ e somente uma quantidade finita dos λ_g é não nula. Dado isso, as definições de adição e multiplicação por escalar são intuitivas. Agora, assuma que G é grupo, então tal espaço vetorial se torna uma álgebra, basta definir a multiplicação simplismente estendendo a multiplicação de G para o espaço todo fazendo

$$\left(\sum_{g \in G} \lambda_g g\right)\left(\sum_{h \in G} \mu_h h\right) = \sum_{k \in G}\left(\sum_{gh=k} \lambda_g \mu_h\right) k$$

Note que é suficiente assumir que G é simplesmente um semigrupo para construir $\mathbb{K}[G]$. Nesse caso chamamos $\mathbb{K}[G]$ de **álgebra de semigrupo**. Analogamente podemos falar sobre uma **álgebra de monóide** se G é um monóide.

3 IDENTIDADES POLINOMIAIS

Neste capítulo iremos definir o principal objeto de estudo desse trabalho, as identidades polinomiais, essas são polinômios não comutativos que são iguais a zero quando subtituímos as indeterminadas por elementos arbitrários de uma dada álgebra, mas antes de falarmos sobre isso iremos definir precisamente os polinômios não comutativos e a álgebra livre, que é a álgebra formada por tais polinômios. Por fim, trataremos sobre os polnômios alternados, uma classe de polinômios não comutativos multilineares que são de grande importância dentro das identidades polinomiais.

3.1 ÁLGEBRA LIVRE E POLINÔMIOS NÃO COMUTATIVOS

Tome um conjunto não vazio X, é convenitente considerá-lo um conjunto indexado, então iremos fixar a notação $X = \{x_i \mid i \in I\}$. Uma sequência finita de elementos de X será denotada por $x_{i_1}x_{i_2}...x_{i_m}$ e chamada de **palavra**. A sequência vazia é denotada por 1 e chamada de **palavra vazia**. Definindo a multiplicação por justaposição, isto é,

$$(x_{i_1}x_{i_2}\cdots x_{i_m})\cdot(x_{j_1}x_{j_2}\cdots x_{j_n}) := x_{i_1}x_{i_2}\cdots x_{i_m}x_{j_1}x_{j_2}\cdots x_{j_n}$$

o conjunto de todas as palavras se torna um monóide (com unidade 1), o qual é denotado por X^* e é chamado de **monóide livre** em X.

Olhando $x_i \in X$ como um elemento de X^* podemos escrever x_i^2 para x_ix_i, x_i^3 para $x_ix_ix_i$ e assim em diante. Dessa maneira, todo $w \neq 1$ em X^* pode ser escrito como $w = x_{i_1}^{k_1}x_{i_2}^{k_2}...x_{i_r}^{k_r}$ onde $i_j \in I$ e $k_j \in \mathbb{N}$. É claro que i_j pode ser igual a i_k se $j \neq k$, mas podemos garantir que $i_j \neq i_{j+1}$.

Agora, lembre-se que, conforme o Exemplo 2.5, dado um monóide e um corpo podemos formar uma álgebra de monóide.

Definição 3.1. Seja $\mathbb{K}$ um corpo de X um conjunto. A **$\mathbb{K}$-álgebra livre** sobre X é a álgebra de monóide de X^* sobre $\mathbb{K}$, a qual será denotada por $\mathbb{K}\langle X\rangle$ ou, se X for finito (resp. infinito contável) por $\mathbb{K}\langle x_1, ..., x_n\rangle$ (resp. $\mathbb{K}\langle x_1, x_2, ...\rangle$).

Os elementos em X são chamadas **indeterminadas** e os elementos da álgebra livre são os **polinômios não comutativos**. As noções de **coeficiente**, **termo constante** e **polinômio constante** são definidas para polinômios não comutativos da mesma maneira que para polinômios comutativos.

Um polinômio é dito um **monômio** se é um múltiplo escalar não-nulo de uma palavra. Todo polinômio não-nulo $f \in \mathbb{K}\langle X\rangle$ é soma de monômios. Mais precisamente, f pode ser escrito de forma única como $f = \lambda_1 w_1 + \cdots + \lambda_m w_m$ onde $w_1, ..., w_m$ são palavras diferentes duas a duas e

os coeficienter $\lambda_1, \dots, \lambda_m$ são escalares não-nulos. Assim, f é a soma dos monõmios $\lambda_i w_i$.

Exemplo 3.1. Por exemplo, se $X = \{x, y\}$, então $\langle x, y\rangle = \{e, x, y, xx, xy, yx, yy, \dots\}$ onde e é a palavra vazia (que será o elemento neutro de $\mathbb{K}\langle x, y\rangle$). Em $\mathbb{Q}\langle x, y\rangle$ temos, por exemplo, que

$$\left(\frac{2}{3}e + 5xx\right)\left(1yxy - \frac{12}{7}y\right) = \frac{2}{3}yxy - \frac{8}{7}y + 5xxyxy - \frac{60}{7}xxy$$

A álgebra livre $\mathbb{K}\langle X\rangle$ possui a seguinte *propriedade universal*: Dadas A uma $\mathbb{K}$-álgebra associativa e unitária e uma função $\varphi : X \to A$ arbitrárias, podemos construir um único homomorfismo de álgebras $\tilde{\varphi} : \mathbb{K}\langle X\rangle \to A$, tal que

$$\varphi(f(x_1, \dots, x_n)) = f(\tilde{\varphi}(x_1), \dots, \tilde{\varphi}(x_n)).$$

Isso significa que podemos substituir os elementos da álgebra no polinômio. Isto é, digamos que $f = x_1x_3^2x_2 + 3x_3x_1^2 - 7x_2 + 1$, então $f(a_1, a_2, a_3) = a_1a_3^2a_2 + 3a_3a_1^2 - 7a_2 + 1 \in A$, ou seja, apenas substituímos x_i por a_i.

Por fim iremos falar sobre algumas outras definições que também são utilizadas para polinômios não comutativos.

Definimos o **comprimento** de uma palavra não-vazia $w = x_{i_1 \, i_m}$ por $l(w) := m$ e o comprimento da palavra vazia é $l(1) := 0$. O **grau** de um polinômio não nulo $f = \lambda_1 w_1 + \cdots + \lambda_m w_m$ é dado por $\mathrm{gr}(f) := \max\{l(w_1), \dots, l(w_m)\}$. Se $l(w_1) = \cdots = l(w_m)$, isto é, se todos os monômios de f possuem o mesmo grau, então f é dito **polinômio homogêneo**. Por exemplo, $x^2\eta - x + \eta^3$ é homogêneo de grau 3. Daqui para frente, estaremos interessados em polinõmios homogêneos do seguinte tipo: $f = f(x_1, \dots, x_n)$ no qual cada indeterminada x_i aparece em todo monômio exatamente uma vez, os chamados **polinômios multilineares**. Ou seja, f é da forma

$$f = \sum_{\sigma \in S_n} \lambda_\sigma x_{\sigma(1)\sigma(n)}$$

onde $\lambda_\sigma \in \mathbb{K}$ e S_n é o grupo simétrico em $\{1, \dots, n\}$. Em especial, algumas propriedades de tais polinômios serão essenciais para a demonstração do Teorema de Amitsur-Levitzki.

Tome polinômios não nulos $f = \lambda_1 w_1 + \cdots + \lambda_m w_m$ e $g = \mu_1 z_1 + \cdots + \mu_n z_n$ e, para simplificar a notação, assuma, sem perda de generalidade (pois a soma é comutativa), que $\mathrm{gr}(f) = l(w_1)$ e $\mathrm{gr}(g) = l(z_1)$. Note qur $w_1 z_1 = w_k z_l$ ocorre apenas quando $k = l = 1$ pois $w_i \neq w_j$ para $i \neq j$, assim como $z_i \neq z_j$ com $i \neq j$, e a multiplicação não é comutativa. Logo, $\mathrm{gr}(fg) = l(w_1 z_1) = l(w_1) + l(z_1)$ e então

$$\mathrm{gr}(fg) = \mathrm{gr}(f) + \mathrm{gr}(g)$$

vale para todo $f, g \in \mathbb{K}\langle X\rangle$ não nulos. Uma consequência imediata disso é que $\mathbb{K}\langle X\rangle$ é um domínio pois se $f \neq 0$ e $g \neq 0$ então $\text{gr}(f) \geq 0$ e $\text{gr}(g) \geq 0$, portanto $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g) \geq 0$ e assim devemos ter $fg \neq 0$.

3.2 DEFINIÇÃO E EXEMPLOS DE PI-ÁLGEBRAS

Definição 3.2. Um polinômio $f = f(x_1, \ldots, x_n) \in \mathbb{K}\langle X\rangle$ é dito uma **identidade polinomial** (ou simplesmente **identidade**) de uma $\mathbb{K}$-álgebra A se $f(a_1, \ldots, a_n) = 0$ para todo $a_1, \ldots, a_n \in A$. Nesse caso também dizemos que A **satisfaz** f, e se f for não nulo então A é chamada de **PI-álgebra**.

É interessante observar que se $f = f(x_1, \ldots, x_n) \in \mathbb{K}\langle X\rangle$ é uma identidade polinomial, então f tem termo constante nulo. Além disso, f é uma identidade polinomial de A se, e somente se, f pertence ao núcleo de todos os homomorfismos de $\mathbb{K}\langle X\rangle$ em A.

Agora vejamos alguns exemplos de identidades polinomiais e PI-álgebras.

Exemplo 3.2. Toda álgebra nilpotente é uma PI-álgebra. De fato, seja n tal que $A^n = 0$, então o polinômio $f(x_1, \cdots, x_n) = x_1 \cdots x_n$ é uma identidade de A. Um exemplo concreto é a álgebra das matrizes triangulares estritamente superiores (isto é, matrizes triangulares superiores com diagonal nula).

Definição 3.3. O **comutador de tamanho** n, $n > 1$, é definido indutivamente por

$$[x_1, x_2] := x_1x_2 - x_2x_1,$$

$$[x_1, \ldots, x_{n-1}, x_n] := [[x_1, \ldots, x_{n-1}], x_n], \ n > 2.$$

Exemplo 3.3. É claro que dados x e y em uma álgebra A temos $[x, y] = 0$ se, e somente se, x e y comutam. Logo, toda álgebra comutativa é uma PI-álgebra pois satisfaz tal identidade.

Exemplo 3.4. Seja $U_n(\mathbb{K})$ a álgebra das matrizes triangulares superiores $n \times n$. Como o comutador de quaisquer duas matrizes de $U_n(\mathbb{K})$ é uma matriz triangular estritamente superior então $U_n(\mathbb{K})$ satisfaz a identidade $[x_1, y_1] \cdots [x_n, y_n] = 0$ e assim é uma PI-álgebra.

Exemplo 3.5. A álgebra $M_2(\mathbb{K})$ das matrizes 2×2 satisfaz a chamada **identidade de Hall** $[[x_1, x_2]^2, x_3] = 0$. De fato, note que se $x \in M_2(\mathbb{K})$ seu polinômio característico é $p(\lambda) = \lambda^2 - \text{tr}(x)\lambda + \det(x)$, onde $\text{tr}(x)$ é o traço de x e $\det(x)$ seu determinante. Pelo Teorema de Cayley-Hamilton temos que $x^2 - \text{tr}(x)x + \det(x) \cdot I_2 = 0$. Assim, se $x = [x_1, x_2]$, com $x_1, x_2 \in M_2(\mathbb{K})$,

digamos

$$x_1 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{e} \quad x_2 = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

então teremos

$$x = \begin{pmatrix} a_{12}b_{21} - a_{21}b_{12} & a_{11}b_{12} + a_{12}b_{22} - a_{12}b_{11} - a_{22}b_{12} \\ a_{21}b_{11} + a_{22}b_{21} - a_{11}b_{21} - a_{21}b_{22} & a_{21}b_{12} - a_{12}b_{21} \end{pmatrix}$$

logo $\mathrm{tr}(x) = 0$ e então $x^2 = -\det(x) \cdot I_2$, ou seja, x^2 é uma matriz escalar, isto é uma matriz múltipla da matriz identidade, e portanto comuta com qualquer outra matriz, daí $[[x_1, x_2]^2, x_3] = 0$.

Exemplo 3.6. Suponha que x^2 é uma identidade de uma $\mathbb{K}$-álgebra arbitrária A. Isso não necessariamente significa que $A^2 = 0$, isto é, que $xy = 0$ para quaisquer $x, y \in A$, mas podemos afirmar que $A^3 = 0$ desde que $\mathrm{char}(\mathbb{K}) \neq 2$. Com efeito, sabemos que $x^2 = 0$ para todo $x \in A$, assim, substituindo x por $x + y$ e usando que $x^2 = y^2 = 0$ obtemos $xy + yx = 0 \Rightarrow xy = -yx$ para quaisquer $x, y \in A$ (repare que isso mostra que $x\eta+$ é uma identidade de A). Consequentemente, para todo $x, y, z \in A$ temos

$$xyz = (xy)z = -z(xy) = -(zx)y = y(zx) = (yz)x = -x(yz) = -xyz$$

logo $xyz = 0$.

Exemplo 3.7. Seja $\{A_i \mid i \in I\}$ uma família de álgebras. Se cada A_i satisfaz a mesma identidade f então o mesmo vale para o produto direto $\prod_{i \in I} A_i$. Por outro lado, se cada A_i é uma PI-álgebra, não podemos afirmar que $\prod_{i \in I} A_i$ também é uma PI-álgebra. No entanto, se o conjunto I é finito, digamos $I = \{1, \ldots, n\}$, então isso é verdade. De fato, se f_i é uma identidade de A_i então $f_1 \ldots f_n$ é identidade de $A_1 \times \cdots \times A_n$.

Dados os exemplos acima poderíamos pensar que a maioria das álgebras são PI-álgebras, por isso colocamos o próximo exemplo, um tanto óbvio, de uma álgebra que não possui identidades.

Exemplo 3.8. A álgebra livre $\mathbb{K}\langle x_1, x_2, \ldots \rangle$ não é uma PI-álgebra.

3.3 POLINÔMIOS ALTERNADOS

Nessa seção consideraremos polinômios especiais que possuem um papel importante na teoria das identidades polinomiais, os polinômios alternados. Dois polinômios famosos que são desse tipo são os chamados polinômio standard e polinômio de Capelli. Este primeiro é justamente o polinômio tratado no Teorema de Amitsur-Levitzki, demonstrado no Capítulo 5, este afirma que o polinômio standard de grau $2n$ é uma identidade para as matrizes $n \times n$.

Vamos começar com um exemplo. Considere o polinômio

$$h(x_1, x_2, x_3, \eta) = x_{12}x_3 - x_{13}x_2 + x_{23}x_1 - x_{21}x_3 + x_{31}x_2 - x_{32}x_1.$$

Substituindo x_1 em x_2 obtemos 0, isto é, $h(x_1, x_1, x_3, \eta) = 0$. Analogamente, $h(x_1, x_2, x_1, \eta) = 0$ e $h(x_1, x_2, x_2, \eta) = 0$.

Definição 3.4. Um polinômio multilinear $f = f(x_1, \dots, x_n, \eta_1, \dots, \eta_r) \in \mathbb{K}\langle X\rangle$ é dito **alternado** em $x_1, \dots, x_n$ se f se torna zero sempre que x_j é substituído por x_i com $1 \leq i < j \leq n$, isto é, $f(x_1, \dots, x_i, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_n, \eta_1, \dots, \eta_r) = 0$.

Substituindo x_1 por $x_1 + x_2$ em $f(x_1, x_1, x_3, \dots, x_n, \eta_1, \dots, \eta_r) = 0$ obtemos

$$f(x_1, x_1, x_3, \dots, x_n, \eta_1, \dots, \eta_r) = -f(x_2, x_1, x_3, \dots, x_n, \eta_1, \dots, \eta_r).$$

Do mesmo modo, f muda de sinal se trocarmos qualquer par de indeterminadas x_i e x_j. O nome alternado decorre dessa condição, a qual é equivalente à definição se $\text{char}(\mathbb{K}) \neq 2$.

Agora falaremos da conexão dos polinômios alternados com a noção de dependência linear, sendo que essa para álgebras é a mesma que para espaços vetoriais.

Proposição 3.1. *Sejam A uma $\mathbb{K}$-álgebra e $a_1, \dots, a_n \in A$ elementos linearmente dependentes. Se um polinômio multilinear $f = f(x_1, \dots, x_n, \eta_1, \dots, \eta_r) \in \mathbb{K}\langle X\rangle$ é alternado em $x_1, \dots, x_n$ então $f(a_1, \dots, a_n, x_1, \dots, x_r) = 0$ para todo $x_1, \dots, x_r \in A$.*

Demonstração. Como $a_1, \dots, a_n$ são linearmente dependentes podemos assumir que $a_n = \sum_{i=1}^{n-1} \lambda_i a_i$ para certos $\lambda_i \in \mathbb{K}$. Consequentemente, como f é multilinear,

$$f(a_1, \dots, a_n, x_1, \dots, x_r) = \sum_{i=1}^{n-1} \lambda_i f(a_1, \dots, a_{n-1}, a_i, x_1, \dots, x_r) = 0$$

pois, sendo f alternado, $f(x_1, \dots, x_i, \dots, x_{n-1}, x_i, \eta_1, \dots, \eta_r) = 0$ para $i = 1, \dots, n-1$. □

Exemplo 3.9. Toda álgebra de dimensão finita é uma PI-álgebra. Se $[A : \mathbb{K}] = d$ então todo polinômio multilinear alternado em $n > d$ indeterminadas é uma identidade de A pela proposição anterior, já que qualquer coleção com mais elementos de d elementos de A é linearmente dependente.

Agora, os polinômios alternados que comentamos. O primeiro que iremos apresentar consiste nos polinômios que são alternados em todas as indeterminadas, isto é, não há $\eta_j's$.

Definição 3.5. Seja $n \geq 2$. O polinômio

$$s_n = s_n(x_1, \dots, x_n); = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) x_{\sigma(1)\sigma(n)}$$

é chamado **polinômio standard** de grau n.

Fixando índices i, j e uma permutação σ, escreva $x_{\sigma(1)\sigma(n)}$ como $mx_i m' x_j m''$ onde m, m' e m'' são monômios nas indeterminadas restantes. Então o termo $mx_j m' x_i m''$ corresponde à permutação cujo sinal é oposto ao de σ. Isso mostra que s_n é alternado. Assim, pela proposição anterior, já sabemos que a álgebra $M_n(\mathbb{K})$ das matrizes $n \times n$, que possui dimensão n^2, satisfaz s_{n^2+1}. O Teorema de Amitsur-Levitski, que será abordado com maiores detalhes adiante, afirma que isso também é verdade para s_{2n}.

Exemplo 3.10. A álgebra $M_2(\mathbb{K})$ das matrizes 2×2 satisfaz a identidade $s_4(x_1, x_2, x_3, x_4) = 0$. Com efeito, fixando a base $\{E = E_{11} + E_{22}, E_{11}, E_{12}, E_{21}\}$ de $M_2(\mathbb{K})$, como s_n é multilinear, basta mostrar que $s_4(E, E_{11}, E_{12}, E_{21}) = 0$. Podemos reescrever o polinômio standard s_4 na forma

$$s_4 = [x_1, x_2][x_3, x_4] + [x_1, x_3][x_4, x_2] + [x_1, x_4][x_2, x_3]$$

Então, como E é a matriz identidade, comuta com qualquer outra matriz, assim teremos $s_4(E, E_{11}, E_{12}, E_{21}) = 0$.

O próximo polinômio é similar, mas envolve os $\eta_j's$.

Definição 3.6. Seja $n \geq 2$. O polinômio

$$c_n = c_n(x_1, \dots, x_n, \eta_1, \dots, \eta_{n-1}) \coloneqq \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) x_{\sigma(1)} \eta_1 x_{\sigma(2)} \eta_2 \dots \eta_{n-1} x_{\sigma(n)}$$

é chamado **n-ésimo polinômio de Capelli**.

Pelo mesmo raciocínio utilizado para s_n podemos ver que c_n é de fato alternado. Também é interessante observar que que $s_n(x_1, \dots, x_n) = c_n(x_1, \dots, x_n, 1, \dots, 1)$.

Exemplo 3.11. A álgebra das matrizes $M_n(\mathbb{K})$ satisfaz a identidade

$$c_{n+1}(1, x, x^2, \dots, x^n, 1, \eta_1, \dots, \eta_n, 1) = \sum_{\sigma \in S_{n+1}} \operatorname{sgn}(\sigma) x^{\sigma(0)} \eta_1 x^{\sigma(1)} \eta_2 \dots \eta_n x^{\sigma(n)} = 0$$

onde o grupo simétrico S_{n+1} age em $\{0, 1, \dots, n+1\}$. De fato, basta observar que, pelo Teorema de Cayley-Hamilton, $1, x, x^2, \dots, x^n$ são linearmente dependentes para qualquer matriz $x \in M_n(\mathbb{K})$, pois este afirma que dado p o polinômio característico da matriz x, o qual tem grau n, temos que $p(x) = 0$, ou seja, existem escalares não nulos em $\mathbb{K}$ cuja combinação linear com $1, x, x^2, \dots, x^n$

é nula.

4 PRODUTO TENSORIAL

O objetivo dessa seção é definir o produto tensorial, que é um mecanismo para transformar funções bilineares - ou até multilineares, mas aqui iremos nos restringir apenas às primeiras, que são suficientes para prosseguirmos - em funções lineares, e demonstrar algumas de suas propriedades que serão utilizadas posteriormente na seção 5.3. Primeiro consideramos o produto tensorial de espaços vetoriais e para depois proceder com o produto tensorial de álgebras.

4.1 DEFINIÇÃO E PROPRIEDADES BÁSICAS

Considere dois espaços vetoriais U e V sobre um corpo $\mathbb{K}$ com $\dim_{\mathbb{K}} U = m$ e $\dim_{\mathbb{K}} V = n$. Tome $\{u_1, \dots, u_m\}$ e $\{v_1, \dots, v_n\}$ bases de U e V respectivamente. Observe que uma função bilinear β de $U \times V$ em um outro $\mathbb{K}$- espaço vetorial W é unicamente determinada pelos seus mn valores $\beta(u_i, v_j)$, $1 \leq i \leq m$, $1 \leq j \leq n$. Agora, tome qualquer espaço vetorial de dimensão mn, escolha sua base e defina uma função linear $\overline{\beta}$ desse espaço em W tal que os elementos da base escolhida são levados nos elementos $\beta(u_i, v_j)$. É claro que $\overline{\beta}$ junto das bases tomadas contêm toda a informação sobre β. Desse modo, ao invés de considerar uma função bilinear em $U \times V$ podemos considerar uma função linear em um espaço de dimensão $\dim_{\mathbb{K}} U \cdot \dim_{\mathbb{K}} V$.

Agora generalizaremos esse conceito com a definição formal do produto tensorial, o qual independe da base. Para isso, iremos considerar, conforme o Exemplo 2.5, o espaço vetorial sobre $\mathbb{K}$ tendo $U \times V$ como base. Enfatizemos que aqui consideramos $U \times V$ apenas como um conjunto e não como espaço vetorial, consequentemente, dados $u, u' \in U$, $v \in V$, $\lambda \in \mathbb{K}$, $(u + u', v)$ é um elemento da base e, portanto, é diferente de $(u, v) + (u', v)$, o qual é a soma de dois elementos da base, do mesmo modo, $\lambda(u, v)$ coincide com $(\lambda u, v)$ apenas quando $\lambda = 1$.

Definição 4.1. Sejam U e V espaços vetoriais sobre $\mathbb{K}$. Denote por $\mathscr{Y}$ o espaço vetorial com base $U \times V$. Seja $\mathscr{N}$ o subespaço de $\mathscr{Y}$ gerado por todos os elementos da forma

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

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

com $\lambda, \lambda' \in \mathbb{K}$, $u, u' \in U$ e $v, v' \in V$. O **produto tensorial** de U e V é o espaço vetorial quociente $\mathscr{Y}/\mathscr{N}$ e é denotado por $U \otimes V$ (ou $U \otimes_{\mathbb{K}} V$ quando se deseja enfatizar que consideramos espaços sobre $\mathbb{K}$).

Tal definição possui pouca utilidade prática, a propriedade característica de $U \otimes V$ descrita no próximo teorema é a que realmente importa.

Teorema 4.1. *Sejam U e V espaços vetoriais sobre $\mathbb{K}$. Então existe uma função bilinear*

$U \times V \to U \otimes V$, $(u, v) \mapsto u \otimes v$ *tal que*

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

(ii) Dada uma função bilinear $\beta : U \times V \to W$, *onde* W *é um espaço vetorial sobre* $\mathbb{K}$, *existe uma única função linear* $\overline{\beta} : U \otimes V \to W$ *tal que* $\overline{\beta}(u \otimes v) = \beta(u, v)$ *para todo* $u \in U$, $v \in V$.

Mais ainda, as propriedades (i) e (ii) caracterizam $U \otimes V$ *a menos de isomorfismo.*

Demonstração. Defina $u \otimes v$ como a classe lateral $(u, v) + \mathscr{N}$. Para mostrar que tal função é de fato bilinear precisamos mostrar que, dados $\lambda, \lambda' \in \mathbb{K}$, $u, u' \in U$ e $v, v' \in V$ os elementos $(\lambda u + \lambda' u', v)$ e $\lambda(u, v) + \lambda'(u', v)$ estão na mesma classe lateral, assim como $(u, \lambda v + \lambda' v')$ e $\lambda(u, v) + \lambda'(u, v')$. Ou seja, que $(\lambda u + \lambda' u', v) - \lambda(u, v) - \lambda'(u', v)$ e $(u, \lambda v + \lambda' v') - \lambda(u, v) - \lambda'(u, v')$ pertencem a $\mathscr{N}$, mas isso é óbvio pois esses são justamente os elementos que geram $\mathscr{N}$. Além disso, pela maneira como definimos $u \otimes v$ também é claro que todo elemento em $U \otimes V$ pode ser escrito como uma combinação linear de elementos da forma $u \otimes v$. E então, como $(\lambda u, v) - \lambda(u, v) \in \mathscr{N}$, isto é, $(\lambda u, v)$ e $\lambda(u, v)$ estão na mesma classe lateral, segue que $\lambda(u \otimes v) = (\lambda u) \otimes v$, logo (i) está provado.

Agora, para provar (ii), considere $\beta : U \times V \to W$ uma função bilinear. Já que $U \times V$ é base de $\mathscr{Y}$ podemos construir uma função linear $B : \mathscr{Y} \to W$ tal que $B((u, v)) = \beta(u, v)$ para todo $u \in U$, $v \in V$. A bilinearidade de β implica que $\mathscr{N} \subseteq \ker B$, portanto, pelo Teorema 2.1, existe uma função linear $\overline{\beta}$ de $\mathscr{Y}/\mathscr{N} = U \otimes V$ em W tal que $\overline{\beta}(x + \mathscr{N}) = B(x)$, ou seja, $\overline{\beta}(u \otimes v) = \beta(u, v)$. Note que como por (i) os elementos $u \otimes v$ geram o espaço $U \otimes V$ segue que $\overline{\beta}$ é a única função linear de $U \otimes V$ em W levando $u \otimes v$ em $\beta(u, v)$ pois uma transformação linear é unicamente determinada por seus valores em um conjunto de geradores.

Por fim, para provar a última afirmação, assuma que T é outro espaço o qual existe uma função bilinear $U \times V \to T$, $(u, v) \mapsto u \odot v$, com as propriedades (i) e (ii). Já que $(u, v) \mapsto u \otimes v$ é uma função bilinear então existe uma função linear $\varphi : T \to U \otimes V$ satisfazendo $\varphi(u \odot v) = u \otimes v$. Analogamente, existe uma função linear $\psi : U \otimes V \to T$ tal que $\psi(u \otimes v) = u \odot v$. Consequentemente, φ e ψ são inversas e então T e $U \otimes V$ são espaços isomorfos. □

A propriedade (ii) do Teorema anterior é chamada **propriedade universal**, podemos interpretá-la através do seguinte diagrama

$$\begin{array}{ccc} U \times V & \xrightarrow{\otimes} & U \otimes V \\ & {\scriptstyle\beta}\searrow \quad \swarrow{\scriptstyle\overline{\beta}} & \\ & W & \end{array}$$

Aqui $\otimes$ denota a função $(u, v) \mapsto u \otimes v$. Vale enfatizar que $\otimes$ e β são bilineares enquanto $\overline{\beta}$ é linear.

Dessa forma, o produto tensorial de espaços vetoriais U e V é o espaço vetorial $U \otimes V$ cujos elementos podem ser escritos como

$$u_1 \otimes v_1 + u_2 \otimes v_2 + \cdots + u_n \otimes v_n, \quad u_i \in U, v_i \in V$$

Tal expressão não é única, afinal, $u \otimes v$ é a classe lateral de (u, v) em $\mathscr{Y}/\mathscr{N} = U \otimes V$, assim, podemos representar $u \otimes v$ com qualquer outro $u' \otimes v'$ onde (u', v') está na mesma classe de (u, v). Além disso, também podemos observar que como a função $(u, v) \mapsto u \otimes v$ é bilinear então

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

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

E tais fórmulas implicam que para todo $u \in U$, $v \in V$

$$u \otimes 0 = 0, \quad 0 \otimes v = 0.$$

Os elementos da forma $u \otimes v$ são chamados **tensores simples**. Devemos sempre lembrar que esses são os geradores do espaço $U \otimes V$ e não seus elementos típicos, no entanto algumas considerações básicas podem ser tratadas apenas em tensores simples, por exemplo, o Teorema 4.1 descreve $\overline{\beta}$ em $U \otimes V$ usando tensores simples, mas isso é válido pois tal função é linear.

Aqui temos um simples exemplo de onde o produto tensorial pode ser aplicado.

Exemplo 4.1. Seja A uma $\mathbb{K}$-álgebra, a multiplicação em A é, por definição, uma função bilinear $(x, y) \mapsto xy$ de $A \times A$ em A. As vezes é mais apropriado considerar a multiplicação como uma função linear de $A \odot A$ em A determinada por $x \otimes y \mapsto xy$.

A próxima proposição introduz o **produto tensorial de funções lineares**. Ela basicamente afirma que a função dada por

$$\sum_i u_i \otimes v_i \mapsto \sum_i \phi(u_i) \otimes \psi(v_i)$$

está bem definida.

Proposição 4.1. *Sejam $\varphi : U \to U'$ e $\psi : V \to V'$ funções lineares entre espaçoes vetoriais. Então existe uma única função linear $\varphi \otimes \psi : U \otimes V \to U' \otimes V'$ tal que,*

$$(\varphi \otimes \psi)(u \otimes v) = \varphi(u) \otimes \psi(v)$$

para todo $u \in U$, $v \in V$.

Demonstração. A linearidade de φ e ψ, juntas da bilinearidade de $\otimes$, implicam que a função $(u, v) \mapsto \varphi(u) \otimes \psi(v)$ é bilinear. Assim, pelo Teorema 4.1, considerando W como $U' \otimes V'$, de fato existe uma única função linear levando $u \otimes v$ em $\varphi(u) \otimes \psi(v)$. □

A demonstração dada utiliza um método muito comum quando se trata de estabelecer algo sobre o produto tensorial, começamos introduzindo uma função bilinear e então, pela propriedade universal, transformamos-na em linear.

Já comentamos que os tensores simples podem ser escritos de diversas maneiras, assim, a mesma coisa ocorre com os elementos de $U \otimes V$. Mas agora veremos que essa não-unicidade tem algumas limitações.

Lema 4.1. *Seja $e_1, \dots, e_n \in U$ linearmente independetes. Se $v_1, \dots, v_n \in V$ são tais que*

$$e_1 \otimes v_1 + \cdots + e_n \otimes v_n = 0$$

então cada $v_i = 0$.

Demonstração. Seja $f_i : U \to \mathbb{K}$ um funcional linear tal que $f_i(e_j) = \delta_{ij}$ para $j = 1, \dots, n$, isto é

$$f_i(e_j) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

Então a função de $U \times V$ em V dada por $(u, v) \mapsto f_i(u)v$ é bilinear, assim, usando a propriedade universal (Teorema 4.1 (ii)), existe uma função linear $\alpha_i : U \otimes V \to V$ satisfazendo $\alpha_i(u \otimes v) = f_i(u)v$. Consequentemente podemos escrever

$$v_i = \sum_{j=1}^{n} f_i(e_j)v_j = \sum_{j=1}^{n} \alpha_i(e_j \otimes v_j) = \alpha_i \left(\sum_{j=1}^{n} e_j \otimes v_j \right) = \alpha_i(0) = 0$$

□

Em particular isso mostra que para todo $u \in U$, $v \in V$

$$u \otimes v = 0 \Rightarrow u = 0 \quad \text{ou} \quad v = 0$$

O próximo teorema afirma que com bases de U e V podemos construir uma base para $U \otimes V$

Teorema 4.2. *Se $\{e_i \mid i \in I\}$ é base de U e $\{f_j \mid j \in J\}$ é base de V então $\{e_i \otimes f_j \mid i \in I, j \in J\}$ é base de $U \otimes V$.*

Demonstração. Escrevendo $u \in U$ e $v \in V$ como combinação linear dos $e_i's$ e dos $f_j's$, respectivamente, segue, pela bilinearidade de $\otimes$, que $u \otimes v$ é combinação linear dos $e_i \otimes f_j's$. Assim, o conjunto $\{e_i \otimes f_j \mid i \in I, j \in J\}$ gera $U \otimes V$. Falta mostrar que é linearmente independente. Por definição, um subconjunto infinito de um espaço vetorial é linearmente independete se cada um de seus subconjuntos finitos são linearmente independentes. Agora, todo subconjunto finito de $\{e_i \otimes f_j \mid i \in I, j \in J\}$ está contido em um conjunto da forma $\{e_{i_k} \otimes f_{j_l} \mid k = 1, \dots, m,\ l = 1, \dots, n\}$. Assim, é suficiente mostrar que tais conjuntos são linearmente independentes. Assuma, então, que

$$\sum_{k=1}^{m} \sum_{l=1}^{n} \lambda_{kl}(e_{i_k} \otimes f_{j_l}) = 0$$

para certos $\lambda_{kl} \in \mathbb{K}$. Pela bilinearidade de $\otimes$ podemos escrever isso como

$$\sum_{k=1}^{m} \left(e_{i_k} \otimes \left(\sum_{l=1}^{n} \lambda_{kl} f_{jl} \right) \right) = 0$$

Já que $e_{i_1}, \dots, e_{i_m}$ são linearmente independentes, pelo Lema 4.1, $\sum_{i=1}^{n} \lambda_{kl} f_{j_l} = 0$ para todo k. Por fim, a independência linear de $f_{j_1}, \dots, f_{j_n}$ implica em $\lambda_{kl} = 0$ para todos k e l.

Logo $\{e_i \otimes f_j \mid i \in I, j \in J\}$ é linearmente independente e, portanto, é base de $U \otimes V$. □

Corolário 4.1. *Se $\{e_i \mid i \in I\}$ é base de U, então todo elemento em $U \otimes V$ pode ser escrito na forma $\sum_{i \in I} e_i \otimes v_i$.*

4.2 PRODUTO TENSORIAL DE ÁLGEBRAS

Dados A e B sobre um corpo $\mathbb{K}$, o espaço vetorial $A \otimes B$ pode ser transformado em uma álgebra defininfo a multiplicação de maneira simples e natural.

Proposição 4.2. *Se A e B são $\mathbb{K}$-álgebras então $A \otimes B$ é uma $\mathbb{K}$-álgebra com multiplicação determinada por*

$$(x \otimes y)(z \otimes w) = xz \otimes yw)$$

para todo $x, z \in A$, $y, w \in B$.

Demonstração. Tome $z \in A$ e $w \in B$. Sejam R_z e R_w as funções multiplicação à direita, isto é

$$\begin{aligned} R_z : A &\to A & \qquad R_w : B &\to B \\ x &\mapsto xz & \qquad y &\mapsto yw \end{aligned}$$

É claro que tais funções são lineares, assim, pela Proposição 4.1, existe um endomorfismo em $A \otimes B$, denotado por $R_z \otimes R_w$, tal que

$$(R_z \otimes R_w)(x \otimes y) = xz \otimes yw$$

Agora, pela linearidade de $R_z \otimes R_w$, a função

$$A \times B \to \mathrm{End}_{\mathbb{K}}(A \otimes B), \quad (z, w) \mapsto R_z \otimes R_w$$

é bilinear. Logo, existe uma função linear

$$\begin{aligned} \varphi : A \otimes B &\to \mathrm{End}_{\mathbb{K}}(A \otimes B) \\ z \otimes w &\mapsto R_z \otimes R_w \end{aligned}$$

Então definimos o produto de $r, s \in A \otimes B$ por

$$rs := (\varphi(s))(r)$$

Tal multiplicação é bilinear devido à linearidade de φ e $R_z \otimes R_w$ e temos, para todo $x, z \in A$, $y, w \in B$,

$$(x \otimes y)(z \otimes w) = \varphi(z \otimes w) = (x \otimes y) = (R_z \otimes R_w)(x \otimes y) = xz \otimes yw.$$

Por fim, a associatividade em A e B implica na associatividade da multiplicação em $A \otimes B$. □

Essa proposição basicamente afirma que a operação

$$\left(\sum_i x_i \otimes y_i\right)\left(\sum_j z_j \otimes w_j\right) := \sum_{i,j} x_i z_j \otimes y_i w_j$$

está bem definida em $A \otimes B$.

Assim, agora podemos considerar $A \otimes B$, o **produto tensorial de álgebras** A e B, como uma álgebra cuja multiplicação está definida pela proposição acima. Note que as propriedades provadas para o produto tensorial de espaços vetoriais continuam válidas nesse caso.

Agora daremos um exemplo de onde o produto tensorial de álgebras pode ser utilizado.

Exemplo 4.2. Para toda $\mathbb{K}$-álgebra A e todo $n \in \mathbb{N}^+$ temos

$$M_n(\mathbb{K}) \cong M_n(A) \tag{4.1}$$

De fato, pelo Corolário 4.1 todo elemento de $M_n(\mathbb{K}) \otimes A$ pode ser escrito como soma de tensores simples do tipo $E_{ij} \otimes a_{ij}$, onde E_{ij} são as matrizes da base canônica, então segue que a função

$$M_n(\mathbb{K}) \otimes A \to M_n(A)$$
$$\sum_{i=1}^{n}\sum_{j=1}^{n} E_{ij} \otimes a_{ij} \mapsto \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{ij}$$

é um isomorfismo de álgebras. Um caso importante de ((4.1)) é

$$M_n(\mathbb{K}) \otimes M_m(\mathbb{K}) \cong M_{nm}(\mathbb{K})$$

4.3 EXTENSÃO ESCALAR

Agora falaremos da exetensão escalar. A ideia básica aqui é: dadas uma $\mathbb{K}$-álgebra A e uma extensão F do corpo $\mathbb{K}$, construir uma F-álgebra A_F que possua a mesma multiplicação que A. Para isso, faremos uso do produto tensorial para que tal propriedade independa de escolher uma base.

Uma extensão F do corpo $\mathbb{K}$ pode ser considerada uma $\mathbb{K}$-álgebra, assim $F \otimes_{\mathbb{K}} A$ é uma $\mathbb{K}$-álgebra, nosso objetivo é convertê-la em uma F-álgebra.

Proposição 4.3. *Sejam A uma $\mathbb{K}$-álgebra e F uma extensão de $\mathbb{K}$. Então $F \otimes_{\mathbb{K}} A$ é uma F-álgebra com a multiplicação por escalar dada por*

$$\lambda(\mu \otimes x) = (\lambda\mu) \otimes x, \quad \lambda, \mu \in F, x \in A$$

Demonstração. Tomando $\lambda \in F$, a função

$$F \times A \to F \otimes A, \quad (\mu, x) \mapsto (\lambda\mu) \otimes x$$

é bilinear, pela bilinearidade da multiplicação em $\mathbb{K}$ e do produto tensorial. Assim, pela propriedade universal (Teorema 4.1 (ii)), esxite uma única função $\mathbb{K}$-linear

$$F \otimes_{\mathbb{K}} A \to F \otimes_{\mathbb{K}} A$$
$$\mu \otimes x \mapsto (\lambda\mu) \otimes x$$

Desse modo, de fato podemos definir

$$F \times (F \otimes A) \to F \otimes_{\mathbb{K}} A(\lambda, \mu \otimes x) \quad \mapsto (\lambda\mu) \otimes x$$

E como tal multiplicação é bilinear podemos defini-la nos tensores simples e extender para os demais elementos de $F \otimes_{\mathbb{K}} A$. Assim, para $\lambda, \mu \in F$, $r, s \in F \otimes_{\mathbb{K}} A$, temos

$$\lambda(r+s) = \lambda r + \lambda s \quad (\lambda+\mu)r = \lambda r + \mu r \quad (\lambda\mu)r = \lambda(\mu r) \quad \lambda(rs) = (\lambda r)s = r(\lambda s)$$

Além disso, note que essa multiplicação é associativa devido a associatividade da multiplicação em F. □

Definição 4.2. Sejam A uma $\mathbb{K}$-álgebra e F uma extensão de $\mathbb{K}$. A F-álgebra $F \otimes_{\mathbb{K}} A$ (definida na Proposição 4.3) é chamada **extensão escalar** de A em F. Será denotada por A_F.

Não desenvolveremos nenhuma propriedade a mais dessa definição pois só isso já é suficiente para nosso objetivo da Seção 5.3

5 O TEOREMA DE AMITSUR-LEVITZKI

A álgebras das matrizes é um objeto muito importante dentro da teoria das álgebras com identidades polinomiais, por isso nesse capítulo nosso objetivo é provar o Teorema de Amitsur-Levitzki, o qual afirma que a álgebra das matrizes $n \times n$ satisfaz a identidade standard de grau $2n$. Todas as seções desse capítulo são dedicadas a conceitos que serão necessárias para a demonstração de tal teorema.

5.1 ÁLGEBRA DE GRASSMANN

Nessa seção nosso objetivo é definir a álgebra de Grassmann, que é uma das álgebras mais importantes dentro da PI-teoria, e comentar algumas de suas propriedades. Para isso começaremos falando sobre uma álgebra definida por geradores e relações.

Dados um corpo $\mathbb{K}$ e um conjunto $X = \{x_i \mid i \in I\}$ construa a álgebra quociente $\frac{\mathbb{K}\langle X\rangle}{(R)}$ onde $\mathbb{K}\langle X\rangle$ é a álgebra livre e (R) é o ideal de $\mathbb{K}\langle X\rangle$ gerado por $R = \{f_j = f_j(x_{i_1}, \dots, x_{i_{n(j)}} \mid j \in J\}$. Denote a classe lateral $x_i + (R)$ por x_i. Note que $f(x_{i_1}, \dots, x_{i_{n(j)}}) = 0$ para todo $j \in J$. Então iremos trocar a notação e escrever $\frac{\mathbb{K}\langle X\rangle}{(R)}$ como

$$\mathbb{K}\langle x_i, i \in I \mid f_j(x_{i_1}, \dots, x_{i_{n(j)}}) = 0, j \in J\rangle$$

Dizemos que essa álgebra é definida pelos **geradores** x_i e **relações** f_j.

De fato, os elementos x_i, $i \in I$, juntos com 1 geram a álgebra e, ao contrário dos geradores x_i da álgebra livre $\mathbb{K}\langle X\rangle$, eles não são independentes, estão relacionados através dos polinômios f_j.

Várias álgebras famosas são isomorfas a álgebras desse tipo, por exemplo a álgebra $M_2(\mathbb{K})$ das matrizes 2×2 sobre um corpo $\mathbb{K}$ é isomorfa a $A = \mathbb{K}\langle x, y \mid x^2 = 0, y^2 = 0, xy + yx = 1\rangle$ e a álgebra de Weyl $\mathscr{A}_1$ é isomorfa a $A = \mathbb{K}\langle x, y \mid [x, y] = 1\rangle$. Agora iremos definir a álgebra de Grassmann, que também é uma álgebra definida por geradores e relações.

Definição 5.1. A **álgebra de Grassmann** (ou **álgebra exterior**) sobre um corpo $\mathbb{K}$ com $\text{char}(\mathbb{K}) \neq 2$ é definida por

$$G := \mathbb{K}\langle x_i, i \in \mathbb{N} \mid x_i^2 = 0, x_i x_j + x_j x_i = 0, i, j \in \mathbb{N}\rangle$$

Assim, temos, por exemplo $x_1 x_2 x_1 = x_1(-x_1 x_2) = -x_1^2 x_2 = 0$, e em geral $x_i G x_i = 0$. Note também que todo produto de diferentes $x_i's$ pode ser escrito como

$$\pm x_{i_1} x_{i_2} \dots x_{i_n}, \quad i_1 < i_2 < \cdots < i_n \tag{5.1}$$

sendo que o sinal depende da quantidade de permutações que foi feita. Portanto, tais elementos, junto de 1, geram G.

Além disso, observe que x_1x_2 comuta com todo x_i, logo pertence a $Z(G)$, o centro de G. Da mesma maneira, todo elemento de ((5.1)) com n par pertence a $Z(G)$. Mais ainda, podemos ver que $Z(G)$ é linearmente gerado por tais elementos junto de 1. Escreveremos G_0 para $Z(G)$ e G_1 para o espaço linearmente gerado pelo elementos da forma ((5.1)) com n ímpar. Logo $G = G_0 \oplus G_1$.

5.2 LINEARIZAÇÃO

O propósito dessa seção é se familiarizar com o **processo de linearização**. Tal conceito é aplicável em diversas situações na matemática, aqui será utilizado para reformular uma identidade polinomial qualquer em uma identidade multilinear. No Exemplo 3.6 temos um simples exemplo de uma linearização: se A satisfaz x^2 então também satisfaz a identidade $x\eta+$. Essa simples ideia, que é a essência da linearização, pode ser levada adiante.

Exemplo 5.1. Vamos considerar uma situação um pouco mais complicada na qual A satisfaz $f(x) = x^3$. Defina dois novos polinômios $g = g(x_1, x_2)$ e $h = h(x_1, x_2, x_3)$ do seguinte modo

$$g := f(x_1 + x_2) - f(x_1) - f(x_2)$$
$$h := g(x_1, x_2 + x_3) - g(x_1, x_2) - g(x_1, x_3)$$

Assim, podemos calcular h primeiro calculando g da seguinte maneira

$$g(x_1, x_2) = (x_1 + x_2)^3 - x_1^3 - x_2^3 = x_1^2x_2 + x_1x_2x_1 + x_1x_2^2 + x_2x_1^2 + x_2x_1x_2 + x_2^2x_1$$

e então

$$\begin{aligned} g(x_1, x_2 + x_3) =& x_1^2(x_2 + x_3) + x_1(x_2 + x + 3)x_1 + x_1(x_2 + x_3)^2 + (x_2 + x_3)x_1^2 \\ &+ (x_2 + x_3)x_1(x_2 + x_3) + (x_2 + x_3)^2x_1 \\ =& \sum_{\sigma\in S_3} x_{\sigma(1)}x_{\sigma(2)}x_{\sigma(3)} + g(x_1, x_2) + g(x_1, x_3) \end{aligned}$$

se abrimos as multiplicações e agruparmos de modo conveniente. Logo

$$h = \sum_{\sigma\in S_3} x_{\sigma(1)}x_{\sigma(2)}x_{\sigma(3)}$$

No entanto também podemos escrever h em função de f

$$h = f(x_1 + x_2 + x_3) - f(x_1, x_2) - f(x_1, x_3) - f(x_2, x_3) + f(x_1) + f(x_2) + f(x_3)$$

Portanto, como A satisfaz f, também satisfaz h, e este, como visto antes, é um polinômio multilinear, mas com mais indeterminadas.

Agora, para considerar polinômios arbitrários, definimos o **grau do polinômio** f **em** x_i pelo maior número de ocorrências de x_i em cada um dos monômios de f.

Teorema 5.1. *Se uma álgebra A satisfaz uma identidade polinomial não nula então A também satisfaz uma identidade polinomial multilinear não nula de grau igual ou menor. Em outras palavras, toda PI-álgebra satisfaz alguma identidade multilinear não trivial.*

Demonstração. Seja $f = f(x_1, \dots, x_n)$ uma identidade polinomial não nula de A. Denote por d_i o grau de f em x_i. A demonstração do teorema será feita por indução em $d := \max\{d_1, \dots, d_n\} > 0$.

Se $d = 1$ então cada x_i aparece em todo monômio de f no máximo uma vez - no máximo e não exatamente, portanto f não é necessariamente multilinear, mas se esse for o caso nada precisa ser feito. Assim, digamos que $_{i_1 i_m}$, $\lambda \in \mathbb{K}\{0\}$ e $i_1, \dots, i_n \in \{1, \dots, n\}$, seja um monômio de f de menor grau, então, substituindo 0 nas outras indeterminadas obtemos uma identidade multilinear em $x_{i_1}, \dots, x_{i_m}$ com grau menor ou igual a $\mathrm{gr}(f)$.

Agora, seja $d > 1$. Sem perda de generalidade, pois a soma é comutativa, podemos assumir que exite $k \leq n$ tal que $d_k = \cdots = d_n = d$ e $d_i < d$ para todo $i < k$. Então, defina um novo polinômio que envolve uma indeterminada adicional $g = g(x_1, \dots, x_n, x_{n+1})$ por

$$g := f(x_1, \dots, x_{n-1}, x_n + xn + 1) - f(x_1, \dots, x_{n-1}, x_n) - f(x_1, \dots, x_{n-1}, x_{n+1})$$

Note que g também é uma identidade de A. Denotemos $f = \sum \lambda_i w_i$ onde os $w_i's$ são as palavras diferentes duas a duas e os $\lambda_i's$ são escalares não nulos. Então g pode ser escrito como $g = \sum \lambda_i g_i$ onde g_i é obtido de w_i do mesmo modo que g é obtido de f. Por isso, se x_n não ocorre em w_i então $g_i = -w_i$. Já se x_n ocorre apenas uma vez em w_i então $g_i = 0$. Por fim, se x_n ocorre ao menos duas vezes em w_i então g_i é a soma de todas as possíveis palavras obtidas quando substituímos ao menos um mas não todos os $x_n's$ em w_i por x_{n+1}, pois os $w_i's$ com somente x_n e somente x_{n+1} no lugar de x_n desaparecerão por causa da parte $-f(x_1, \dots, x_{n-1}, x_n) - f(x_1, \dots, x_{n-1}, x_{n+1})$ de g. Assim, nesse caso, se em qualquer uma dessas palavras de g_i substituirmos x_n em x_{n+1} voltamos a ter a palavra w_i.. Assim, como os $w_i's$ são diferentes dois a dois, também temos que as palavras de g_i são diferentes das palavras que aparecendo em $g_{i'}$ sempre que $i \neq i'$. Como $d > 1$, os índices em i tal que x_n ocorre ao menos duas vezes em w_i realmente existem. Isso mostra que $g \neq 0$.

Dessa forma podemos concluir que g é uma identidade não nula de A e $\mathrm{gr}(g) \leq \mathrm{gr}(f)$, já que $\mathrm{gr}(f) = d = d_n$, o grau de f em x_n, e com esse processo diminuímos a quantidade de vezes que x_n aparece em cada palavra de g_i, mas ainda podemos ter $\mathrm{gr}(g) = \mathrm{gr}(f) = d$ pois podem existir

outros x_j com $d_j = d_n$. Além disso, podemos afirmar precisamente que o grau de g em x_n e x_{n+1} é $d-1$ e para $j = 1, \ldots, n-1$ o grau de g em x_j é menor ou igual que d_j.

Assim, repita esse processo, primeiro com g no lugar de f e x_{n-1} no lugar de x_n, e então com outras indeterminadas diminuindo até x_k. No final, chegamos a uma situação na qual uma identidade não nula possui grau no máximo $d-1$ em todas as indeterminadas. Assim, se $d-1=1$ realizamos o que foi feito no primeiro caso mas se $d-1>1$ retomamos esse processo criando novas identidades de grau menor até que esse chegue em 1 e assim possa ser transformada em uma identidade multilinear. □

5.3 IDENTIDADES ESTÁVEIS

Dadas uma $\mathbb{K}$-álgebra A, $f \in \mathbb{K}\langle X\rangle$ uma identidade de A e uma extensão F do corpo $\mathbb{K}$, nosso objetivo é analisar quando f também é indentidade de $A_F = F \otimes A$, a extensão escalar de A em F.

Seria intuitivo, considerando que A_F possui a mesma tabela de multiplicação de A, afirmar que isso ocorre sempre, no entanto, o próximo exemplo mostra que isso pode não ser verdade mesmo quando $A = \mathbb{K}$.

Exemplo 5.2. Seja $\mathbb{K}$ um corpo finito com n elementos. Então $f = x^n - x$ é uma identidade de $\mathbb{K}$. De fato, temos que $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ é um grupo multiplicativo com $n-1$ elementos. Assim, pelo Teorema de Lagrange, a ordem $m < \infty$ de qualquer elemento $x \in \mathbb{K}^*$ deve ser um divisor de $n-1$, isto é, existe $q \in \mathbb{Z}$ com $qm = (n-1)$. Desse modo, como a ordem de um elemento, quando finita, é o menor inteiro positivo tal que $x^m = 1$, segue que

$$x^{n-1} = x^{mq} = (x^m)^q = 1^q = 1$$

Consequentemente $x^n = x$ para todo $x \in \mathbb{K}$, ou seja, todo elemento em $\mathbb{K}$ é raiz do polinômio $f = x^n - x$. Assim, como f não pode ter mais que n raízes em qualquer corpo, f não é identidade de nenhuma extensão prórpia L do corpo $\mathbb{K}$.

Por outro lado, mostraremos que quando $\mathbb{K}$ é infinito então isso ocorre. Para generalizarmos ainda mais esse conceito podemos substituir o corpo L por uma álgebra comutativa arbitrária C.

Definição 5.2. Uma identidade f de uma $\mathbb{K}$-álgebra A é dita **estável** (para A) se f é identidade de $C \otimes A$ para qualquer $\mathbb{K}$-álgebra comutativa C.

O exemplo anterior nos mostra que $x^n - x$ não é uma identidade estável para $A = \mathbb{K}$ se $|\mathbb{K}| = n$. Vamos agora a resultados positivos.

Lema 5.1. *Toda identidade multilinear é estável.*

Demonstração. Seja $f = f(x_1, \dots, x_n)$ uma identidade multilinear da $\mathbb{K}$-álgebra A. Agora considere $f(\overline{x}_1, \dots, \overline{x}_n)$ com $\overline{x}_i \in C \otimes A$, onde C é uma $\mathbb{K}$-álgebra comutativa arbitrária. Cada $\overline{x}_i$ é soma de tensores simples, então, pela multilinearidade de f, $f(\overline{x}_1, \dots, \overline{x}_n)$ pode ser escrito como soma de elementos da forma $f(c_1 \otimes x_1, \dots, c_n \otimes x_n)$ com $c_i \in C$ e $x_i \in A$. Por fim, como f é multilinear e C é comutativo podemos reagrupar os $c_i's$ em qualquer ordem e escrever

$$f(c_1 \otimes x_1, \dots, c_n \otimes x_n) = c_1 \dots c_n \otimes f(x_1, \dots, x_n) = c_1 \dots c_n \otimes 0 = 0$$

pois f é identidade de A □

Lema 5.2. *Seja $f = f(x_1, \dots, x_n)$ uma identidade da $\mathbb{K}$-álgebra A. Se f é identidade de $\mathbb{K}[\omega_1, \dots, \omega_s] \otimes A$ para todo $s \in \mathbb{N}$ então f é estável para A.*

Demonstração. Seja C uma $\mathbb{K}$-álgebra comutativa unitária. Já que toda álgebra comutativa é subálgebra de uma álgebra comutativa unitária, é suficiente mostrar que f é uma identidade de $C \otimes A$. Tome elementos arbitrários $\overline{x}_i = \sum_{j=1}^{m_i} c_{ij} \otimes x_{ij}$, $i = 1, \dots, n$, em $C \otimes A$. Defina

$$\tilde{x}_i = \sum_{j=1}^{m_i} \omega_{ij} \otimes x_{ij} \in \mathbb{K}[\Omega] \otimes A$$

onde $\Omega = \{\omega_{ij} \mid i = 1, \dots, n; j = 1, \dots, m_i\}$. Pela hipótese, $f(\tilde{x}_1, \dots, \tilde{x}_n) = 0$, assim, se φ é o homomorfismo de $\mathbb{K}[\Omega]$ em C levando ω_{ij} em c_{ij} então, usando a Proposição 4.1, temos $f(\overline{x}_1, \dots, \overline{x}_n) = (\varphi \otimes \mathrm{id}_A)(f(\tilde{x}_1, \dots, \tilde{x}_n)) = 0$. □

Na demonstração do próximo teorema utilizaremos o mesmo tipo de homomorfismo φ usado na demonstração do lema anterior, mas, afim de evitar muito formalismo, falaremos apenas em substituir as indeterminadas por elementos da álgebra ou do corpo.

Teorema 5.2. *Seja $\mathbb{K}$ um corpo infinito. Então toda identidade polinomial de uma $\mathbb{K}$-álgebra arbitrária A é estável.*

Demonstração. Seja $f = f(x_1, \dots, x_n)$ uma identidade de A. Tome $s \in \mathbb{N}$ e elementos arbitrários $\hat{x}_i = \sum_j p_{ij} \otimes x_{ij}$ em $\mathbb{K}[\omega_1, \dots, \omega_s] \otimes A$, $i = 1, \dots, n$. Pelo Lema 5.2 é suficiente mostrar que $f(\hat{x}_1, \dots, \hat{x}_n) = 0$. Suponha que isso não é verdade. Então podemos escrever

$$f(\hat{x}_1, \dots, \hat{x}_n) = \sum_k q_k \otimes a_k \tag{5.2}$$

onde $q_1 \neq 0$ e os $a_k's$ são linearmente independentes. Já que $\mathbb{K}$ é infinito existem $\lambda_1, \dots, \lambda_s \in \mathbb{K}$ com $q_1(\lambda_1, \dots, \lambda_s) \neq 0$, isso é claro por uma simples indução pois se s=1 usamos o fato de que o número de raízes de um polinômio não pode ultrapassar seu grau, agora se isso é válido para um $s \in \mathbb{N}$ qualquer então também vale para $s+1$, basta fazer $\lambda_{s+1} = 1$. Agora defina $\alpha_{ij} := p_{ij}(\lambda_1, \dots, \lambda_s)$ e $\beta_k := q_k(\lambda_1, \dots, \lambda_s)$, assim $\beta_1 \neq 0$. Substituindo ω_i por λ_i em ((5.2)) obtemos

$$f\left(\sum_j \alpha_{1j} \otimes x_{1j}, \dots, \sum_j \alpha_{nj} \otimes x_{nj}\right) = \sum_k \beta_k \otimes a_k.$$

Agora, como $\alpha_{ij}, \beta_k \in \mathbb{K}$, temos $\sum_j \alpha_{ij} \otimes x_{ij} = 1 \otimes (\sum_j \alpha_{ij} x_{ij})$ e $\sum_k \beta_k \otimes a_k = 1 \otimes (\sum_k \beta_k a_k)$. E então podemos escrever a igualdade acima como

$$1 \otimes f\left(\sum_j \alpha_{1j} x_{1j}, \dots, \sum_j \alpha_{nj} x_{nj}\right) = 1 \otimes \left(\sum_k \beta_k a_k\right),$$

o que é uma contradição, visto que o lado esquerdo é 0 pois f é identidade de A, enquanto o lado direito não é 0 já que $\beta_1 \neq 0$ e os $a_k's$ são linearmente independentes. □

5.4 POLINÔMIO CARACTERÍSTICO

Esse tópico é muito abordado em cursos de Álgebra Linear, no entanto nesses casos é comum considerar matrizes com entradas sobre um corpo, aqui iremos substituir o corpo por um anel qualquer, mas veremos que muitos conceitos ainda se aplicam.

O **determinante** de uma matriz $A \in M_n(C)$, denotado por $\det(A)$, pode ser definido da mesma maneira desde que C seja um anel comutativo. Assim podemos definir o **polinômio característico** de A como

$$p_A(\omega) := \det(A - \omega I) \in C[\omega]$$

Para qualquer polinômio $q \in C[\omega]$ definimoa $q(A)$ do mesmo modo quando C é um corpo. Assim, o **Teorema de Cayley-Hamilton**, cuja demonstração no caso em que C é um anel comutativo é análoga a muitas que usam um corpo, afirma que

$$p_A(A) = 0$$

Para qualquer matriz $A \in M_n(C)$ definimos o **traço** de A $\mathrm{tr}(A)$ da maneira usual. Nosso objetivo nessa seção é expressar os coeficientes de p_A em função do traço das potências de A. Para isso precisaremos de algumas fórmulas, as quais foram descobertas por Isaac Newton, de polinômios simétricos em indeterminadas comutativas com coeficientes inteiros. Um polinômio f

é dito **simétrico** se permanece o mesmo após uma permutação de indeterminadas, isto é, se $f(\omega_1, \dots, \omega_n) = f(\omega_{\sigma(1)}, \dots, \omega_{\sigma(n)})$. Os **polinômios simétricos elementares** são definidos por

$$e_0 := 1$$
$$e_k = e_k(\omega_1, \dots, \omega_n) := \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} \omega_{i_1}\omega_{i_2} \dots \omega_{i_k}$$

sendo que a segunda expressão está definida para $k \in \{1, \dots, n\}$. Se $k > n$ colocamos $e_k(\omega_1, \dots, \omega_n) := 0$. Em particular, e_1 é a soma de todos os $\omega_i's$ e e_n é seu produto. Seja ω outra indeterminada, usando as chamadas Fórmulas de Vieta podemos provar que

$$(-1)^n(\omega - \omega_1)(\omega - \omega_2) \dots (\omega - \omega_n) = \sum_{j=0}^{n}(-1)^j e_{n-j}\omega^j \tag{5.3}$$

Assim, os polinômios simétricos elementares estão relacionados com as raízes de polinômios. Usaremos isso para relacioná-los com os polinômios simétricos

$$p_j = p_j(\omega_1, \dots, \omega_n) := \sum_{i=1}^{n} \omega_i^j, \ j \ge 1$$

Lema 5.3 (Fórmulas de Newton)**.** *Para $k = 1, \dots, n$ temos*

$$ke_k = \sum_{j=1}^{k}(-1)^{j-1} e_{k-j}p_j \tag{5.4}$$

Demonstração. De ((5.3)) segue que

$$\sum_{j=0}^{n}(-1)^j e_{n-j}\omega_i^j = 0, \ i = 1, \dots, n$$

Somando sobre i obtemos ((5.4)) para $k = n$. De fato,

$$\sum_{i=1}^{n}\sum_{j=0}^{n}(-1)^j e_{n-j}\omega_i^j = 0 \Rightarrow \sum_{i=1}^{n}\left(e_n + \sum_{j=1}^{n}(-1)^j e_{n-j}w_i^j\right) = 0$$
$$\Rightarrow \sum_{i=1}^{n} e_n + \sum_{i=1}^{n}\sum_{j=1}^{n}(-1)^j e_{n-j}\omega_i^j = 0 \Rightarrow ne_n = -\sum_{i=1}^{n}\sum_{j=1}^{n}(-1)^j e_{n-j}\omega_i^j$$
$$\Rightarrow ne_n = \sum_{i=1}^{n}\sum_{j=1}^{n}(-1)^{j-1} e_{n-j}\omega_i^j = \sum_{j=1}^{n}(-1)^{j-1} e_{n-j}\left(\sum_{i=1}^{n}\omega_i^j\right)$$
$$\Rightarrow ne_n = \sum_{j=1}^{n}(-1)^{j-1} e_{n-j}p_j$$

O caso $k < n$ deriva facilmente desse, basicamente o problema é a notação, a que estamos usando sugere que n está fixo e k varia e, por mais que isso seja mais natural pensando em aplicações, para a demonstração é conveniente considerar n variável. Assim, iremos escrever $e_{k,n}$ para e_k e $p_{j,n}$ para p_j. Então nosso objeitvo é mostrar que o polinômio

$$P := ke_{k,n} - \sum_{j=1}^{k}(-1)^{j-1}e_{k-j,n}p_{j,n}$$

é 0. Note que para quaisquer $i, j \leq k$ temos

$$e_{i,n}(\omega_1, \dots, \omega_k, 0, \dots, 0) = e_{i,k}(\omega_1, \dots, \omega_k)$$
$$p_{j,n}(\omega_1, \dots, \omega_k, 0, \dots, 0) = p_{j,k}(\omega_1, \dots, \omega_k)$$

Já que ((5.4)) vale para $n = k$ segue que $P(\omega_1, \dots, \omega_k, 0, \dots, 0) = 0$. Isso significa que P só contém monômios nulos nas indeterminadas $\omega_1, \dots, \omega_k$. Analogamente, colocando zero em outros lugares vemos que P só contém monômios nulos em qualquer conjunto de k indeterminadas. No entanto, pela definição de P, seus monômios só podem ter grau k, assim, não pode involver mais do que k indeterminadas. Logo $P = 0$. □

Assim, em geral para $k = 1, \dots, n$, existe um polinômio $q_k = q_k(\omega_1, \dots, \omega_k) \in \mathbb{Q}[\omega_1, \omega_2, \dots]$ tal que

$$e_k = q_k(p_1, \dots, p_k) \tag{5.5}$$

Para o próximo teorema é intererssante notar que q_k possui termo constante igual a zero e também que se $\lambda\omega_1^{m_1} \dots \omega_k^{m_k}$, $\lambda \in \mathbb{Q}$ é um monômio de q_k então $m_1 + 2m_2 + \cdots + km_k = k$. Além disso, definimos $q_0 := 1$ para que ((5.5)) seja válido para $k = 0, 1, \dots, n$.

Teorema 5.3. *Se C é uma $\mathbb{Q}$-álgebra comutativa, então para todo $A \in M_n(C)$ temos*

$$p_A(\omega) = \sum_{j=0}^{n}(-1)^j q_{n-j}(\mathrm{tr}(A), \mathrm{tr}(A^2), \dots, \mathrm{tr}(A^{n-j}))\omega^j$$

Demonstração. Seja A uma matriz genérica de $M_n(C)$. Aqui o que importa é essa matriz e suas entradas, então, como C é uma $\mathbb{Q}$-álgebra, podemos reduzir $C = \mathbb{Q}[\omega_{11}, \omega_{12}, \dots, \omega nn]$. Assim, em particular, C é um domínio comutativo, então pode ser imerso em um corpo, seu corpo de frações, o qual pode ser imerso em um corpo algebricamente fechado, seu fecho algébrico. Mas assim podemos assumir sem perda de generalidade que C é um corpó algébricamente fechado. Assim, temos $p_A(\omega) = (-1)^n(\omega - \lambda_1) \dots (\omega - \lambda_n)$, onde os $\lambda_i's$ são os autovalores de A. Usando a forma canônica de Jordan segue que $\mathrm{tr}(A^i) = p_i(\lambda_1, \dots, \lambda_n)$, $i = 1, \dots, n$. Por ((5.3)) obtemos

$$
\begin{aligned}
p_A(\omega) &= \sum_{j=0}^{n} (-1)^j e_{n-j}(\lambda_1, \dots, \lambda_n)\omega^j \\
&= \sum_{j=0}^{n} (-1)^j q_{n-j}(p_1(\lambda_1, \dots, \lambda_n), \dots, p_{n-j}(\lambda_1, \dots, \lambda_n))\omega^j \\
&= \sum_{j=0}^{n} (-1)^j q_{n-j}(\mathrm{tr}(A), \dots, \mathrm{tr}(A^{n-j}))\omega^j
\end{aligned}
$$

□

Corolário 5.1. *Seja C uma $\mathbb{Q}$-álgebra comutativa. Se $A \in M_n(C)$ é tal que* $\mathrm{tr}(A) = \mathrm{tr}(A^2) = \cdots = \mathrm{tr}(A^n) = 0$ *então* $A^n = 0$*,*

Demonstração. Já que os polinômios q_k, $k = 1, \dots, n$, possuem termo constante nulo segue que $p_A(\omega) = (-1)^n \omega^n$, então, pelo Teorema de Cayley-Hamilton,temos que $p_A(A) = 0$ e assim $A^n = 0$. □

5.5 DEMONSTRAÇÃO DO TEOREMA DE AMITSUR-LEVITZKI

Por fim chegamos ao nosso maior objetivo: o Teorema de Amitsur-Levitzki. Já vimos que como a álgebra das matrizes $M_n(\mathbb{K})$ tem dimensão n^2 ela satisfaz o polinômio standard s_{n^2+k} para todo $k \in \mathbb{Z}^+$. Agora, antes de demonstrar que tal álgebra satisfaz s_{2n}, veremos qual é o menor grau de um polinômio que pode ser identidade de $M_n(\mathbb{K})$.

Lema 5.4. *Um polinômio não-nulo de grau menor que* $2n$ *não é identidade de* $M_n(\mathbb{K})$*.*

Demonstração. Pelo Teorema 5.1 é suficiente tratar apenas de polinômios multilineares. Assim, tome um polinômio multilinear f de grau $2n-1$, ou seja, $f = \sum_{\sigma \in S_{2n-1}} \lambda_\sigma x_{\sigma(1)} \dots x_{\sigma(2n-1)}$ com digamos $\lambda_1 \neq 0$. Considere sequência das matrizes $E_{11}, E_{12}, E_{22}, \dots, E_{n-1,n}, E_{nn}$, isto é, as matrizes E_{ij} da base canônica tais que $i = j$ ou $i = j - 1$. Como o produto de matrizes elementares satisfaz

$$
E_{ij}E_{hk} = \begin{cases} 0, & \text{se} \quad j \neq h \\ E_{ik}, & \text{se} \quad j = h \end{cases} \tag{5.6}
$$

então tal sequência de matrizes possui a propriedade de que seu produto nessa ordem dada é E_{1n} enquanto que o produto em qualquer outra ordem é zero. Assim $f(E_{11}, E_{12}, \dots, E_{nn}) = \lambda_1 E_{1n} \neq 0$. Analogamente, tomando subsequências apropriadas vemos que um polinômio multilinear não-nulo de grau menor que $2n - 1$ também não é identidade de $M_n(\mathbb{K})$. □

Agora enfim temos todas as ferramentas necessárias para demonstrar o Teorema de Amitsur-Levitzki.

Teorema 5.4 (Teorema de Amitsur-Levitzki)**.** *O polinômio standard s_{2n} é uma identidade de $M_n(C)$ para toda álgebra comutativa C.*

Demonstração. Por hipótese C é uma álgebra sobre um corpo $\mathbb{K}$. Seja $\mathbb{K}_0$ o subcorpo primo de $\mathbb{K}$ e considere C como uma álgebra sobre $\mathbb{K}_0$. Já que, pelo Exemplo 4.2, $M_n(C) \cong C \otimes_{\mathbb{K}_0} M_n(\mathbb{K}_0)$ e como, pelo Lema 5.1, identidades multilineares são estáveis, é suficiente provar que s_{2n} é uma identidade de $M_n(\mathbb{K}_0)$. Suponha que isso é verdade para $\mathbb{K}_0 = \mathbb{Q}$. Então s_{2n} também é identidade de $M_n(\mathbb{Z})$, pois $\mathbb{Z} \subset \mathbb{Q}$. Mas como podemos construir um homomorfismo de $M_n(\mathbb{Z})$ em $M_n(\mathbb{Z}_p)$ a partir do homomorfismo canônico de $\mathbb{Z}$ em $\mathbb{Z}_p$ que leva cada número inteiro em sua classe de equivalência em $\mathbb{Z}_p$, então s_{2n} também é identidade de $M_n(\mathbb{Z}_p)$. Assim, como todo subcorpo primo é isomorfo a Q ou a algum $\mathbb{Z}_p$, basta provar que s_{2n} é identidade de $M_n(\mathbb{Q})$.

Tome $A_1, \dots, A_{2n} \in M_n(\mathbb{Q})$. Devemos mostrar que $s_{2n}(A_1, \dots, A_{2n}) = 0$. Faremos isso utilizando a álgebra de Grassmann $G = G_0 \otimes G_1$ sobre $\mathbb{Q}$ com geradores $x_1, x_2, \dots$, assim, para $B = (b_{ij}) \in M_n(\mathbb{Q})$ e $x \in G$ defina Bx como a matriz $(b_{ij}x) \in M_n(G)$. Note que o produto $(Bx)(B'x')$ é igual a $(BB')(xx')$. Seja

$$A; = A_1x_1 + A_2x_2 + \cdots + A_{2n}x_{2n} \in M_n(G)$$

Como $x_iGx_i = 0$ temos que

$$A^{2n} = \sum_{\sigma \in S_{2n}} A_{\sigma(1)}A_{\sigma(2)} \dots A_{\sigma(2n)}x_{\sigma(1)}x_{\sigma(2)} \dots x_{\sigma(2n)}$$

Observe que $x_{\sigma(1)} \dots x_{\sigma(r)} = \operatorname{sgn}(\sigma)x_1 \dots x_r$. De fato, escrevendo σ como produto de transposições, vemos que é suficiente mostrar isso para quando σ é uma transposição, mas nesse caso a fórmula é evidente devido a definição da álgebra de Grassmann. Consequentemente,

$$A^{2n} = s_{2n}(A_1, A_2, \dots, A_{2n})x_1x_2 \dots x_{2n}$$

Logo devemos provar que $A^{2n} = 0$, isto é, $(A^2)^n = 0$. Note que A^2 pertence a $M_n(G_0)$ pois quando fazemos essa multiplicação obtemos uma soma de $(A_iA_j)(x_ix_j)$ e como x_ix_j tem tamanho par então pertence a G_0. Agora, como G_0 é uma álgebra comutativa, o Corolário 5.1 diz que para isso é suficiente mostrar que $(A^2)^k = A^{2k}$ tem traço zero para $k = 1, \dots, n$. Assim, note que $A^{2k-1} = \sum_j B_jy_j$ para algum $B_j \in M_n(\mathbb{Q})$ e $y_j \in G_1$. Consequentemente,

$$\operatorname{tr}(A^{2k}) = \operatorname{tr}(AA^{2k-1}) = \operatorname{tr}\left(\sum_{i,j} A_iB_jx_iy_j\right) = \sum_{i,j} \operatorname{tr}(A_iB_j)x_iy_j$$

Por outro lado,

$$\mathrm{tr}(A^{2k}) = \mathrm{tr}(A^{2k-1}A) = \sum_{i,j} \mathrm{tr}(B_j A_i) y_j x_i$$

Comparando as duas expressões e usando a propriedade do traço $\mathrm{tr}(A_i B_j) = \mathrm{tr}(B_j A_i)$ e que $x_i y_j = -y_j x_i$, já que $y_j \in G_1$, obtemos $\mathrm{tr}(A^{2k}) = 0$. □

6 IDENTIDADES POLINOMIAIS GRADUADAS

6.1 DEFINIÇÃO E EXEMPLOS

Tomando $\mathbb{K}\langle X\rangle$ a álgebra associativa livre sobre um corpo $\mathbb{K}$ e A uma álgebra associativa sobre $\mathbb{K}$. O conjunto $T(A)$ das identidades polinomiais de A forma um T-ideal de $\mathbb{K}\langle X\rangle$, isto é, um ideal que tem a propriedade de ser invariante sob todos os endomorfismos de $\mathbb{K}\langle X\rangle$. Como a interseção de uma família qualquer de T-ideais é um T-ideal, dado $S \subset \mathbb{K}\langle X\rangle$ podemos definir o T-ideal gerado por S, denotado por $\langle S\rangle^T$, como a interseção de todos os T-ideais de $\mathbb{K}\langle X\rangle$ que contém S. Se $S \subset T(A)$ é tal que $\langle S\rangle^T = T(A)$, dizemos que S é uma base das identidades de A.

Em 1950, W. Specht conjecturou que, para corpos de característica zero, todo ideal próprio é finitamente gerado, isto é, possui uma base finita. Esta conjectura ficou conhecida como *Problema de Specht* [9] e a resposta afirmativa foi obtida apenas em 1987 por A. Kemer [6]. No caso particular da álgebra de matrizes $M_n(\mathbb{K})$ a existência de bases finitas para o T-ideal $T(M_n(\mathbb{K}))$ é garantida pelos resultados de Kemer, porém a exibição de tal base é conhecida apenas para $n = 2$ ([11],[12]).

Surge então o interesse por outros tipos de identidades polinomiais, como por exemplo, as identidades graduadas, que possuem, de certo modo, formas mais simples de descrever a base das identidades.

Assim, agora vamos definir a álgebra graduada e apresentar alguns exemplos.

Definição 6.1. Seja G um grupo. Uma álgebra A é dita **G-graduada** se $A = \oplus_{g\in G} A_g$ onde A_g é subespaço de A e $A_g A_h \subseteq A_{gh}$ para todos $g, h \in G$.

Exemplo 6.1. Seja A uma álgebra e G um grupo. Então, fixado $\epsilon \in G$, a decomposição

$$\oplus_{g\in G} A_g$$

onde $A_g = \{0\}$ se $g \neq \epsilon$ e $A_\epsilon = A$ é uma G-graduação em A. Esta graduação é chamada de graduação trivial.

Exemplo 6.2. A álgebra de Grassmann E possui uma $\mathbb{Z}_2$-graduação natural $E = E_0 \oplus E_1$, onde E_0 e E_1 são, respectivamente, os subespaços gerados pelos conjuntos $\{e_{i_1} e_{i_2} \cdots e_{i_m} | m \text{ é par}\}$ e $\{e_{i_1} e_{i_2} \cdots e_{i_k} | k \text{ é ímpar}\}$. Aqui, a operação usada em $\mathbb{Z}_2$ deve ser a adição.

Exemplo 6.3. Seja $R = A[x, y]$ a álgebra polinomial nas indeterminadas x e y. Seja R_n, $n \geq 0$, o conjunto dos polinômios de grau n. Por exemplo,

$$R_0 = A, \quad R_1 = Ax + Ay, \quad R_2 = Ax^2 + Axy + Ay^2.$$

Definindo também $R_n = \{0\}$ para $n < 0$, temos que $R = \sum_{n=0}^{\infty} R_n$ e $R_n R_m = R_{n+m}$. Assim R é uma álgebra graduada, sendo essa a graduação natural de R. Em geral, a graduação natural da álgebra polinomial $R = A[x_1, \dots, x_m]$ é definida por $R = \sum_{n=0}^{\infty} R_n$, onde R_n é o conjunto dos polinômios de grau n.

Agora precisamos do conceito de álgebra associativa livre G-graduada, a qual será o "ambiente" das identidades polinomiais graduadas. Para isso, considere uma família $\{X_g \mid g \in G\}$ de conjuntos enumeráveis e dois a dois disjuntos. Tomemos então $X = \cup_{g\in G} X_g$ e considere a álgebra associativa livre unitária $\mathbb{K}\langle X\rangle$. Definimos agora

$$\alpha(1) = 0 \quad \text{e} \quad \alpha(x_1 x_2 \dots x_m) = \alpha(x_1)\alpha(x_2)\dots\alpha(x_m)$$

onde $\alpha(x_i) = g$ se $x_i \in X_g$. Sendo então m um monômio de $\mathbb{K}\langle X\rangle$, dizemos que $\alpha(m)$ é o G-grau de m. Tomando, para cada $g \in G$,

$$\mathbb{K}\langle X\rangle_g = \langle m \mid m \text{ é monômio de } \mathbb{K}\langle X\rangle \text{ e } \alpha(m) = g\rangle$$

temos

$$\mathbb{K}\langle X\rangle = \sum_{g\in G} \mathbb{K}\langle X\rangle_g \quad \text{e} \quad \mathbb{K}\langle X\rangle_g \mathbb{K}\langle X\rangle_h \subseteq \mathbb{K}\langle X\rangle_{gh}$$

para quaisquer $g, h \in G$. Assim $\mathbb{K}\langle X\rangle$ é uma álgebra G-graduada denominada a álgebra associativa livre G-graduada.

Analogamente, tal álgebra também possui a propriedade universal. Assim, podemos definir as identidades polinomiais graduadas.

Definição 6.2. Seja $A = \sum_{g\in G} A_g$ uma álgebra G-graduada. Dizemos que um polinômio $f(x_1, \dots, x_n) \in \mathbb{K}\langle X\rangle$ é uma **identidade G-graduada** de A se $f(a_1, \dots, a_n) = 0$ para quaisquer $a_i \in A_{\alpha(x_i)}$ com $i = 1, \dots, n$.

Por fim, daremos alguns exemplos de identidades graduadas e nos aprofundaremos no próximo capítulo nas identidades $\mathbb{Z}_n$-graduadas da álgebra de matrizes de ordem n.

Exemplo 6.4. Consideremos a álgebra de Grassmann E com sua $\mathbb{Z}_2$-graduação natural conforme definimos anteriormente. Como $ab = -ba$ para quaisquer elementos $a, b \in E_1$, temos que $f(x_1, x_2) = x_1x_2 + x_2x_1 \in \mathbb{K}\langle X\rangle$, onde $\mathbb{K}\langle X\rangle$ é a álgebra livre $\mathbb{Z}_2$-graduada, com $\alpha(x_1) = \alpha(x_2) = 1$, é identidade $\mathbb{Z}_2$-graduada de E.

Exemplo 6.5. Seja $M_2(E)$ a álgebra de matrizes de ordem 2 com entradas na álgebra de

Grassmann. A $\mathbb{Z}_2$-graduação em $M_2(E)$ é dada pela composição

$$M_2(E) = (M_2(E))_0 \oplus (M_2(E))_1,$$

onde

$$(M_2(E))_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in E_0 \right\}, \ (M_2(E))_1 = \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \mid b, c \in E_1 \right\}.$$

Temos que os polinômios $x_1x_2 - x_2x_1$ e $y_1y_2y_3 + y_3y_2y_1$ são identidades polinomiais graduadas de tal álgebra graduada. De fato, se

$$x_1 = \begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix} \in (M_2(E))_0 \quad \text{e} \quad x_2 = \begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix} \in (M_2(E))_0,$$

então $a_1, a_2, d_1, d_2 \in E_0$ e

$$x_1x_2 = \begin{pmatrix} a_1a_2 & 0 \\ 0 & d_1d_2 \end{pmatrix} = \begin{pmatrix} a_2a_1 & 0 \\ 0 & d_2d_1 \end{pmatrix} = x_2x_1$$

ou seja, $x_1x_2 - x_2x_1 = 0$. Além disso, se

$$y_i = \begin{pmatrix} 0 & b_i \\ d_i & 0 \end{pmatrix} \in (M_2(E))_1, \ i = 1, 2, 3,$$

então

$$y_1y_2y_3 + y_3y_2y_1 = \begin{pmatrix} 0 & b_1c_2b_3 + b_3c_2b_1 \\ c_1b_2c_3 + c_3b_2c_1 & 0 \end{pmatrix} = 0.$$

Tais identidades inclusive formam uma base para todas as identidades de $M_2(E)$.

6.2 IDENTIDADES $\mathbb{Z}_n$-GRADUADAS DA ÁLGEBRA DE MATRIZES DE ORDEM n

Agora iremos definir uma $\mathbb{Z}_n$-graduação na álgebras das matrizes de ordem n. Para isso denote por $E_{i,j}$, $1 \leq i, j \leq n$, a matriz $n \times n$ cuja única entrada não nula é 1 na i-ésima fileira e j-ésima coluna. As matrizes $E_{i,j}$, conhecidas como matrizes unitárias, formam uma base de $M_n(\mathbb{K})$ como espaço vetorial. Para $t \in \mathbb{Z}$, denote por $\bar{t}$ a classe de equivalência em $\mathbb{Z}_n$ que contém t. Para $\alpha \in \mathbb{Z}_n$, seja $\mathcal{M}_n^{(\alpha)}$ o subespaço de $M_n(\mathbb{K})$ gerado por todas as matrizes unitárias $E_{i,j}$ tais que $\overline{j-i} = \alpha$.

Assim, $\mathcal{M}_n^{(\bar{0})}$ consiste nas matrizes da forma

$$\begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ 0 & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n,n} \end{pmatrix}, \quad a_{1,1}, a_{2,2}, a_{n,n} \in \mathbb{K}$$

e, para $0 < t \leq n-1$, $\mathcal{M}_n^{(\bar{t})}$ consiste nas matrizes da forma

$$\begin{pmatrix} 0 & \cdots & 0 & a_{1,t+1} & \cdots & \cdots & 0 \\ \vdots & & \vdots & \vdots & a_{2,t+2} & & \vdots \\ \vdots & & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \cdots & a_{n-t,n} \\ a_{n-t+1,1} & \cdots & 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & & & \vdots \\ 0 & \cdots & a_{n,t} & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

onde $a_{1,t+1}, a_{2,t+2}, \ldots, a_{n-t,n}, a_{n-t+1,1}, a_{n-t+2,2}, \ldots, a_{n,t} \in \mathbb{K}$.

Então $M_n(\mathbb{K})$ é a soma direta dos subespaços $\mathcal{M}_n^{(\alpha)}$:

$$M_n(\mathbb{K}) = \sum_{\alpha \in \mathbb{Z}_n} \mathcal{M}_n^{(\alpha)} \tag{6.1}$$

Note que, de fato, a soma é direta pois classes distintas em $\mathbb{Z}_n$ não possuem interseção.

Agora, observe que

$$E_{i,j} \cdot E_{r,s} = \begin{cases} E_{i,s}, & \text{se } j = r \\ 0, & \text{se } j \neq r \end{cases}.$$

De fato, dadas matrizes $A \cdot B = C$, temos pela definição do produto de matrizes $c_{k,l} = \sum_{m=1}^{n} a_{k,m} b_{m,l}$. Assim, o único elemento não nulo possível de $E_{i,j} \cdot E_{r,s}$ é $1 = 1_{i,j} \cdot 1_{r,s}$ e isso só acontece se $j = r$ e acontecerá na posição i, s.

Segue que $\mathcal{M}^{(\overline{p})}\mathcal{M}^{(\overline{q})} \subseteq \mathcal{M}^{(\overline{p+q})}$ para $p, q \in \{0, 1, \ldots, n-1\}$. Pois se $\mathcal{M}^{(\overline{p})}$ e $\mathcal{M}^{(\overline{q})}$ são gerados, respectivamente, pelas matrizes $E_{i,j}$ e $E_{r,s}$ tais que $\overline{j-i} = \overline{p}$ e $\overline{s-r} = \overline{q}$, então, pelo que observamos do produto das matrizes $E_{i,j}$ e $E_{r,s}$, temos que $\mathcal{M}^{(\overline{p})}\mathcal{M}^{(\overline{q})} \subseteq \mathcal{M}^{(\overline{p+q})}$ é claro no caso $j \neq r$ e, para $j = r$ temos que $\overline{p+q} = \overline{j-i+s-r} = \overline{s-i}$, ou seja, $\mathcal{M}^{(\overline{p+q})}$ é gerado pelas matrizes $E_{i,s}$ e assim o resultado também vale.

Assim, a decomposição (6.1) define uma $\mathbb{Z}_n$ graduação da álgebra $M_n(\mathbb{K})$, a qual será denotada por $\mathcal{M}_n(\mathbb{K})$.

No caso das matrizes 4x4, por exemplo, temos

$$\begin{pmatrix} a_{11} & 0 & 0 & 0 \\ 0 & a_{22} & 0 & 0 \\ 0 & 0 & a_{33} & 0 \\ 0 & 0 & 0 & a_{44} \end{pmatrix} \in \mathcal{M}_4^{(\bar{0})}, \qquad \begin{pmatrix} 0 & a_{12} & 0 & 0 \\ a_{21} & 0 & a_{23} & 0 \\ 0 & a_{32} & 0 & a_{34} \\ 0 & 0 & a_{43} & 0 \end{pmatrix} \in \mathcal{M}_4^{(\bar{1})},$$

$$\begin{pmatrix} 0 & 0 & a_{13} & 0 \\ 0 & 0 & 0 & a_{24} \\ a_{31} & 0 & 0 & 0 \\ 0 & a_{42} & 0 & 0 \end{pmatrix} \in \mathcal{M}_4^{(\bar{2})}, \quad \text{e} \quad \begin{pmatrix} 0 & 0 & 0 & a_{14} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ a_{41} & 0 & 0 & 0 \end{pmatrix} \in \mathcal{M}_4^{(\bar{3})}.$$

Agora, seja $\{X^{(\alpha)}, \alpha \in \mathbb{Z}_n\}$ uma família de conjuntos $X^{(\alpha)}$ contáveis distintos. Coloque $X = \cup_{\alpha\in\mathbb{Z}_n} X^{(\alpha)}$ e denote por $A[X]$ a álgebra associativa livre gerada pelo conjunto X. Os monômios

$$\{x_{i_1} x_{i_2} \cdots x_{i_k} : k = 1, 2, \ldots ; x_{i_1}, x_{i_2}, \ldots, x_{i_k} \in X\}$$

formam uma base de $A[X]$ como espaço vetorial. A indeterminada $x \in X$ é dita de *grau homogêneo* α, denotado por $\alpha(x) = \alpha$, se $x \in X^{(\alpha)}$. O grau homogêneo de um monômio $n = x_{i_1} x_{i_2} \ldots x_{i_k}$ é definido por $\alpha(n) = \alpha(x_{i_1}) + \alpha(x_{i_2}) + \cdots + \alpha(x_{i_k})$.

Para $\alpha \in \mathbb{Z}_n$, denote por $A[X]^{(\alpha)}$ o subespaço de $A[X]$ gerado por todos os monômios de grau homogêneo α. Note que $A[X]^{(\alpha)} \cdot A[X]^{(\beta)} \subseteq A[X]^{(\alpha+\beta)}$ para todo $\alpha, \beta \in \mathbb{Z}_n$. E como

$$A[X] = \sum_{\alpha\in\mathbb{Z}_n} A[X]^{(\alpha)},$$

pois é claro que todo monômio possui um grau e ele pertence a uma única classe de equivalência de $\mathbb{Z}_n$, isso mostra que $A[X]$ é uma álgebra $\mathbb{Z}_n$-graduada. Seus elementos são chamados *$\mathbb{Z}_n$-polinômios graduados* ou simplesmente *polinômios graduados*.

Um ideal I de $A[X]$ é dito um *T_n-ideal* se é invariante sob todo $\mathbb{K}$-endomorfismo $\gamma : A[X] \to A[X]$ tal que $\gamma(A[X]^{(\alpha)}) \subseteq A[X]^{(\alpha)}$ para todo $\alpha \in \mathbb{Z}_n$.

Seja $\mathcal{A} = \sum_{\alpha\in\mathbb{Z}_n} \mathcal{A}^{(\alpha)}$ uma álgebra associativa $\mathbb{Z}_n$ graduada. Um polinômio $\mathbb{Z}_n$-graduado $f(x_1, x_2, \ldots, x_k)$ é dito uma *identidade polinomial graduada* da álgebra $\mathbb{Z}_n$-graduada $\mathcal{A}$ se $f(a_1, a_2, \ldots, a_k) = 0$ para todo $a_1, a_2, \ldots, a_k \in \cup_{\alpha\in\mathbb{Z}_n} \mathcal{A}^{(\alpha)}$ tal que $a_s \in \mathcal{A}^{(\alpha(x_s))}$, $s = 1, 2, \ldots, k$. O conjunto $T_n(\mathcal{A})$ de todas as identidades graduadas de uma álgebra $\mathbb{Z}_n$-graduada $\mathcal{A}$ é um T_n-ideal de $A[X]$.

Agora queremos mostrar que as identidades polinomiais $\mathbb{Z}_n$-graduadas das matrizes $M_n(\mathbb{K})$

seguem de

$$x_1x_2 - x_2x_1, \quad \alpha(x_1) = \alpha(x_2) = \overline{0} \tag{6.2}$$

e

$$x_1xx_2 - x_2xx_1, \quad \alpha(x_1) = \alpha(x_2) = -\alpha(x) \tag{6.3}$$

Lema 6.1. *A álgebra graduada $\mathcal{M}_n$ satisfaz (6.2) e (6.3).*

Demonstração. Já que duas matrizes diagonais comutam, segue que $\mathcal{M}_n$ satisfaz a identidade graduada (6.2).

Como a identidade (6.3) é multilinear, então só precisamos mostrar que tal identidade vale quando

$$x_1 = E_{i_1,j_1}, x_2 = E_{i_2,j_2}, x = E_{r,s}$$

para $E_{i_1,j_1}, E_{i_2,j_2} \in \mathcal{M}_n^{(\overline{t})}$, $E_{r,s} \in \mathcal{M}_n^{(\overline{n-t})}$, onde $0 \leq t \leq n-1$, ou seja,

$$j_1 = \begin{cases} i_1 + t, & \text{se } i_1 + t \leq n \\ i_1 + t - n, & \text{se } i_1 + t > n \end{cases}$$

$$i_2 = \begin{cases} j_2 - t, & \text{se } j_2 - t \geq 1 \\ j_2 - t + n, & \text{se } j_2 - t < 1 \end{cases}$$

$$r = \begin{cases} s + t, & \text{se } s + t \leq n \\ s + t - n, & \text{se } s + t > n \end{cases}$$

Note que como

$$E_{i_1,j_1} \cdot E_{r,s} = \begin{cases} E_{i_1,s}, & j_1 = r \\ 0, & j_1 \neq r \end{cases}$$

e

$$E_{i_1,s} \cdot E_{i_2,j_2} = \begin{cases} E_{i_1,j_2}, & s = i_2 \\ 0, & s \neq i_2 \end{cases}$$

temos $E_{i_1,j_1}E_{r,s}E_{i_2,j_2} \neq 0$ somente quando $j_1 = r$ e $s = i_2$. Afirmamos que, nesse caso, $i_1 = s = i_2$ e $j_1 = r = j_2$. De fato, observe que, se $j_1 = i_1 + t$ e $r = s + t - n$, então de $j_1 = r$ segue que $n = s - i_1$, o que é impossível pois $n \geq s$ e $i_1 \geq 1$. Assim, as igualdades $j_1 = i_1 + t$ e $r = s + t - n$ não podem valer simultaneamente. O mesmo ocorre com as igualdades $r = s + t$ e $i_2 = j_2 - t + n$,

pois, usando que $s = i_2$ temos $n = s - j_2$, o que também é um absurdo. Logo, quando $j_1 = i_1 + t$ temos $r = s + t$ e então $i_2 = j_2 - t$, de modo que

$$i_2 = s = r - t = j_1 - t = i_1$$

e

$$r = j_1 = i_1 + t = i_2 + t = j_2.$$

Analogamente, quando $j_1 = i_1 + t - n$, não podemos ter $r = s_t$ pois isso resulta em $n = i_1 - s$, logo devemos ter $r = s + t - n$. E isso nos dá $i_2 = j_2 - t + n$, já que, caso contrário, isto é, se $i_2 = j_2 - t$, chegamos na contradição $n = j_2 - r$. Portanto

$$i_2 = s = r - t + n = j_1 - t + n = i_1$$

e

$$r = j_1 = i_1 + t - n = i_2 + t - n = j_2$$

provando a afirmação.

Isso nos permite concluir que $E_{i_1,j_1}E_{r,s}E_{i_2,j_2} \neq 0$ se, e somente se, $i_1 = s = i_2$ e $j_1 = r = j_2$, e então, se e somente se, $E_{i_2,j_2}E_{r,s}E_{i_1,j_1} \neq 0$. Nesse caso, temos que

$$E_{i_1,j_1}E_{r,s}E_{i_2,j_2} = E_{i_1,j_2} = E_{i_2,j_1} = E_{i_2,j_2}E_{r,s}E_{i_1,j_1}$$

Caso contrário,

$$E_{i_1,j_1}E_{r,s}E_{i_2,j_2} = 0 = E_{i_2,j_2}E_{r,s}E_{i_1,j_1}.$$

Isso prova que (6.3) vale em $\mathcal{M}_n$. □

A partir de agora iremos denotar por I_n o T_n-ideal gerado pelas identidades graduadas (6.2) e (6.3). Para um inteiro positivo k, denote por S_k o conjunto de todas as permutações de $\{1, 2, \ldots, k\}$. Para $x_1, x_2, \ldots, x_k \in X$ e $\sigma \in S_k$, seja

$$m_\sigma = m_\sigma(x_1, x_2, \ldots, x_k) = x_{\sigma(1)}x_{\sigma(2)} \cdots x_{\sigma(k)}.$$

O monômio multilinear em $x_1, x_2, \ldots, x_k$ correspondendo à permutação identidade será denotado por

$$m = m(x_1, x_2, \ldots, x_k) = x_1x_2 \cdots x_k$$

É claro que $\alpha(m) = \alpha(m_\sigma) = \alpha(x_1) + \alpha(x_2) + \cdots + \alpha(x_k)$. Além disso, todo polinômio multilinear graduado $f(x_1, x_2, \ldots, x_k)$ pode ser expresso como

$$f = \sum_{\sigma \in S_k} a_\sigma m_\sigma,$$

onde $a_\sigma \in \mathbb{K}$.

Entendemos por *substituição standard* a substituição $\mathcal{S}$ da forma

$$x_1 = E_{i_1,j_1}, x_2 = E_{i_2,j_2}, \ldots, x_k = E_{i_k,j_k} \tag{6.4}$$

onde

$$\overline{j_s - i_s} = \alpha(x_s) \tag{6.5}$$

de modo que $E_{i_s,j_s} \in \mathcal{M}_n^{(\alpha(x_s))}$, $s = 1, 2, \ldots, k$. Para um polinômio graduado $f(x_1, x_2, \ldots, x_k)$ e uma substituição $\mathcal{S}$, denotamos por $f|_{\mathcal{S}}$ o valor de f correspondendo à substituição $\mathcal{S}$.

Observe que, quando uma substituição do tipo (6.4) é feita, o valor do monômio $m_\sigma(x_1, x_2, \ldots, x_k)$ é diferente de zero somente se

$$j_{\sigma(1)} = i_{\sigma(2)}, \quad j_{\sigma(2)} = i_{\sigma(3)}, \ldots, \ j_{\sigma(k-1)} = i_{\sigma(k)} \tag{6.6}$$

e nesse caso $m_\sigma|_{(6.4)} = E_{i_{\sigma(1)},j_{\sigma(k)}}$. Além disso, podemos ver que se um polinômio graduado multilinear $f(x_1, x_2, \ldots, x_k)$ é tal que $f|_{\mathcal{S}} = 0$ para toda substituição $\mathcal{S}$, então $f = 0$ é uma identidade graduada de $\mathcal{M}_n$.

Para um monômio $m_\sigma(x_1, x_2, \ldots, x_k)$, $\sigma \in S_k$, e dois inteiros $1 \leq p \leq q \leq k$, denote por $m_\sigma^{[p,q]}$ a subpalavra obtida de m_σ descartando os primeiros $p-1$ e os últimos $k-q$ fatores:

$$m_\sigma^{[p,q]} = x_{\sigma(p)} x_{\sigma(p+1)} \ldots x_{\sigma(q)}.$$

Lema 6.2. *Para qualquer $\sigma \in S_k$, existe uma substituição standard $\mathcal{S}$ tal que*

$$m_\sigma(x_1, x_2, \ldots, x_k)|_{\mathcal{S}} \neq 0.$$

Demonstração. Faremos a demonstração por indução em k. O caso $k = 1$ é trivial pois isso sempre vai ocorrer. Tome $k > 1$ e seja $\alpha(x_k) = \bar{t}$ para algum inteiro $0 \leq t < n$. Pela hipótese de indução, existe uma substituição standard com

$$x_{\sigma(1)} = E_{i_1,j_1}, x_{\sigma(2)} = E_{i_2,j_2}, \ldots, x_{\sigma(k-1)} = E_{i_{k-1},j_{k-1}} \tag{6.7}$$

tal que $m_\sigma^{[1,k-1]} = E_{i_1,j_{k-1}} \neq 0$. Assim, basta fazer $x_{\sigma(k)} = E_{j_{k-1},j_k}$, onde, para respeitar $\alpha(x_k) = \bar{t}$, devemos ter

$$j_k = \begin{cases} j_{k-1} + t, & \text{se } j_{k-1} + t \leq n \\ j_{k-1} + t - n, & \text{se } j_{k-1} + t > n \end{cases}$$

e então obtemos

$$m_\sigma(x_1, x_2, \dots, x_k) = E_{i_1,j_{k-1}} E_{j_{k-1},j_k} \neq 0.$$

□

Lema 6.3. *Se $m_\sigma|_{(6.4)} \neq 0$, então, para quaisquer $1 \leq p \leq q \leq k$,*

$$\alpha(m_\sigma^{[p,q]}) = \overline{j_{\sigma(q)} - i_{\sigma(p)}}.$$

Demonstração. Por (6.5) e (6.6), temos que

$$\alpha(m_\sigma^{[p,q]}) = \alpha(x_{\sigma(q)}) + \alpha(x_{\sigma(q-1)}) + \cdots + \alpha(x_{\sigma(p)})$$

$$= \overline{j_{\sigma(q)} - i_{\sigma(q)}} + \overline{j_{\sigma(q-1)} - i_{\sigma(q-1)}} + \cdots + \overline{j_{\sigma(p)} - i_{\sigma(p)}}$$

Agora, como $m_\sigma|_{(6.4)} \neq 0$, temos $i_{\sigma(q)} = j_{\sigma(q-1)}$, $i_{\sigma(q-1)} = j_{\sigma(q-2)}, \dots, i_{\sigma(p-1)} = j_{\sigma(p)}$ e então

$$\alpha(m_\sigma^{[p,q]}) = \overline{j_{\sigma(q)} - i_{\sigma(p)}}.$$

□

Lema 6.4. *Se, dada uma permutação $\sigma \in S_k$, existe uma substituição standard (6.4) tal que*

$$m_\sigma(x_1, x_2, \dots, x_k)|_{(6.4)} = m(x_1, x_2, \dots, x_k)|_{(6.4)} \neq 0$$

então

$$m_\sigma(x_1, x_2, \dots, x_k) \equiv x_1 \cdot n(x_2, x_3, \dots, x_k) \ (mod\ I_n)$$

para algum monômio $n(x_2, x_3, \dots, x_k) = x_{l_2} x_{l_3} \dots x_{l_k}$.

Demonstração. Suponha que $\sigma(1) \neq 1$, pois, caso contrário, o resultado é imediato. Nosso objetivo é escrever

$$m_\sigma = m_\sigma^{[1,q-1]} \cdot m_\sigma^{[q,r]} \cdot m_\sigma^{[r+1,k]},$$

tal que

$$\alpha(m_\sigma^{[1,q-1]}) = \alpha(m_\sigma^{[q,r]}) = \overline{0}$$

e $x_{\sigma(q)} = 1$. Ou então como

$$m_\sigma = m_\sigma^{[1,p-1]} \cdot m_\sigma^{[p,q-1]} \cdot m_\sigma^{[q,r]} \cdot m_\sigma^{[r+1,k]},$$

tal que

$$\alpha(m_\sigma^{[1,p-1]}) = \alpha(m_\sigma^{[q,r]}) = -\alpha(m_\sigma^{[p,q-1]})$$

e $x_{\sigma(q)} = 1$. Pois assim, em ambos os caso, respectivamente por (6.2) e (6.3), temos que

$$\begin{aligned} m_\sigma &= m_\sigma^{[1,q-1]} \cdot m_\sigma^{[q,r]} \cdot m_\sigma^{[r+1,k]} \\ &\equiv m_\sigma^{[q,r]} \cdot m_\sigma^{[1,q-1]} \cdot m_\sigma^{[r+1,k]} = x_{\sigma(q)} x_{l_2} \cdots x_{l_k} = x_1 x_{l_2} \cdots x_{l_k} \pmod{I_n} \end{aligned}$$

e

$$\begin{aligned} m_\sigma &= m_\sigma^{[1,p-1]} \cdot m_\sigma^{[p,q-1]} \cdot m_\sigma^{[q,r]} \cdot m_\sigma^{[r+1,k]} \\ &\equiv m_\sigma^{[q,r]} \cdot m_\sigma^{[p,q-1]} \cdot m_\sigma^{[1,p-1]} \cdot m_\sigma^{[r+1,k]} = x_{\sigma(q)} x_{l_2} \cdots x_{l_k} = x_1 x_{l_2} \cdots x_{l_k} \pmod{I_n}, \end{aligned}$$

provando o resultado. Assim, para isso, observe que como $\sigma(1) \neq 1$, temos que $\sigma^{-1}(\sigma(1)) = 1 < \sigma^{-1}(1)$. Seja t o menor inteiro positivo tal que $\sigma^{-1}(t+1) < \sigma^{-1}(1)$. É claro que

$$1 \leq \sigma^{-1}(t+1) < \sigma^{-1}(1) \leq \sigma^{-1}(t).$$

Como, por hipótese,

$$E_{i_1,j_1} E_{i_2,j_2} \cdots E_{i_k,j_k} = E_{i_{\sigma(1)},j_{\sigma(1)}} E_{i_{\sigma(2)},j_{\sigma(2)}} \cdots E_{i_{\sigma(k)},j_{\sigma(k)}} \neq 0$$

segue que $i_1 = i_{\sigma(1)}$, $j_t = i_{t+1}$ e, para todo $s > 1$, $j_{\sigma(s-1)} = i_{\sigma(s)}$. Assim, colocando $p = \sigma^{-1}(t+1)$, $q = \sigma^{-1}(1)$ e $r = \sigma^{-1}(t)$ temos que $1 \leq p < q \leq r$ com $j_{\sigma(q-1)} = i_{\sigma(q)} = i_{\sigma(1)}$ (pois $q > 1$), $j_{\sigma(r)} = i_{\sigma(p)}$ e, quando $p > 1$, $j_{\sigma(p-1)} = i_{\sigma(p)}$. Primeiro considere o caso $p > 1$, das igualdades

$$j_{\sigma(r)} = i_{\sigma(p)} = j_{\sigma(p-1)} \quad \text{e} \quad j_{\sigma(q-1)} = i_{\sigma(q)} = i_{\sigma(1)},$$

obtemos que

$$j_{\sigma(p-1)} - i_{\sigma(1)} = i_{\sigma(p)} - j_{\sigma(q-1)} = j_{\sigma(r)} - i_{\sigma(q)} = t_0$$

para algum $t_0 \in \mathbb{Z}$. Pelo Lema 6.3, temos que

$$\alpha(m_\sigma^{[1,p-1]}) = \overline{j_{\sigma(p-1)} - i_{\sigma(1)}} = \overline{t_0};$$
$$\alpha(m_\sigma^{[p,q-1]}) = \overline{j_{\sigma(q-1)} - i_{\sigma(p)}} = -\overline{t_0};$$
$$\alpha(m_\sigma^{[q,r]}) = \overline{j_{\sigma(r)} - i_{\sigma(q)}} = \overline{t_0}.$$

E $m_\sigma = m_\sigma^{[1,p-1]} \cdot m_\sigma^{[p,q-1]} \cdot m_\sigma^{[q,r]} \cdot m_\sigma^{[r+1,k]}$, obtendo o resultado desejado através do segundo caso dito no início, isto é, usando (6.3). Agora, se $p = 1$, temos $j_{\sigma(q-1)} = i_{\sigma(q)} = i_{\sigma(1)} = j_{\sigma(r)}$, e, novamente pelo Lema 6.3,

$$\alpha(m_\sigma^{[1,q-1]}) = \overline{j_{\sigma(q-1)} - i_{\sigma(1)}} = \overline{0};$$
$$\alpha(m_\sigma^{[q,r]}) = \overline{j_{\sigma(r)} - i_{\sigma(q)}} = \overline{0}.$$

E então caímos no primeiro caso dito anteriormente, o qual prova o resultado utilizando (6.2). Assim completamos a demonstração. □

Lema 6.5. *Se, dada uma permutação $\sigma \in S_k$, existe uma substituição standard (6.4) tal que*

$$m_\sigma(x_1, x_2, \dots, x_k)\big|_{(6.4)} = m(x_1, x_2, \dots, x_k)\big|_{(6.4)} \neq 0$$

então

$$m_\sigma(x_1, x_2, \dots, x_k) \equiv m(x_1, x_2, \dots, x_k) \ (mod\ I_n).$$

Demonstração. Seja r o maior inteiro positivo tal que

$$m_\sigma(x_1, x_2, \dots, x_k) \equiv x_1 x_2 \cdots x_r \cdot n(x_{r+1}, \dots, x_k) \ (\text{mod } I_n)$$

para algum monômio multilinear $n = n(x_{r+1}, \dots, x_k)$. Iremos mostrar que $r = k$. Suponha o contrário, isto é, que $r < k$. Então é claro que $r \leq k - 2$, pois se $r = k - 1$, sendo r o maior inteiro tal que a congruência acima acontece, obtemos uma contradição. Assim, como I_n é o

ideal gerado por (6.2) e (6.3), e sendo essas, pelo Lema 6.1, identidades da álgebra graduada $\mathcal{M}_n$, usando a definição de congruência temos que

$$x_1x_2 \dots x_r \cdot n|_{(6.4)} = m_\sigma|_{(6.4)} = m|_{(6.4)} \neq 0.$$

Combinando isso com

$$x_1x_2 \dots x_r \cdot n|_{(6.4)} = E_{i_1,j_1} \cdots E_{i_r,j_r} \cdot n|_{(6.4)} = E_{i_1,j_r} \cdot n|_{(6.4)}$$

e

$$m|_{(6.4)} = E_{i_1,j_1} \cdots E_{i_r,j_r} \cdot \{x_{r+1}x_{r+2} \cdots x_k\}|_{(6.4)} = E_{i_r,j_r} \cdot \{x_{r+1}x_{r+2} \cdots x_k\}|_{(6.4)},$$

obtemos

$$n(x_{r+1}, x_{r+2}, \dots, x_k)|_{(6.4)} = x_{r+1}x_{r+2} \cdots x_k|_{(6.4)} \neq 0.$$

Então, pelo Lema 6.4, existe um monômio multilinear $n'(x_{r+2}, x_{r+3}, \dots, x_k)$ tal que

$$n(x_{r+1}, x_{r+2}, \dots, x_k) \equiv x_{r+1} \cdot n'(x_{r+2}, x_{r+3}, \dots, x_k) \pmod{I_n}.$$

Logo

$$m_\sigma \equiv x_1 \cdots x_r \cdot n(x_{r+1}, \dots, x_k) \equiv x_1 \cdots x_r x_{r+1} \cdot n'(x_{r+2}, x_{r+3}, \dots, x_k) \pmod{I_n},$$

contradizendo nossa escolha do número r. Isso completa a demonstração. □

Pelo Lema 6.5 obtemos o seguinte:

Se, para duas permutações $\sigma, \tau \in S_k$, existe uma substituição standard $\mathcal{S}$ tal que

$$m_\sigma(x_1, x_2, \dots, x_k)|_{\mathcal{S}} = m_\tau(x_1, x_2, \dots, x_k)|_{\mathcal{S}} \neq 0,$$

então

$$m_\sigma(x_1, x_2, \dots, x_k) \equiv m_\tau(x_1, x_2, \dots, x_k) \pmod{I_n}.$$

Teorema 6.1. *Toda identidade polinomial graduada da álgebra $\mathbb{Z}_n$-graduada $\mathcal{M}_n$ segue de*

$$x_1x_2 - x_2x_1, \quad \alpha(x_1) = \alpha(x_2) = \overline{0} \tag{6.8}$$

e

$$x_1xx_2 - x_2xx_1, \quad \alpha(x_1) = \alpha(x_2) = -\alpha(x) \tag{6.9}$$

Demonstração. Como $\mathbb{K}$ é um corpo de característica zero precisamos provar apenas que qualquer identidade polinomial graduada multilinear $f(x_1, x_2, \dots, x_k)$ de $\mathcal{M}_n$ pertence a I_n. Para isso, seja r o menor inteiro não-negativo tal que o polinômio f possa ser escrito, módulo I_n, como

uma combinação linear de r monômios multilineares, isto é,

$$f \equiv \sum_{q=1}^{r} a_{\sigma_q} m_{\sigma_q} \pmod{I_n},$$

onde $0 \neq a_{\sigma_q} \in \mathbb{K}$, $\sigma_1, \sigma_2, \ldots, \sigma_r \in S_k$. Precisamos mostrar que $r = 0$. Suponha, por contradição, que $r > 0$. Pelo Lema 6.2, podemos encontrar uma substituição standard $\mathcal{S}$ tal que $m_{\sigma_1}|_{\mathcal{S}} \neq 0$. Como

$$m_{\sigma_q}|_{\mathcal{S}} \in \{E_{i,j} : i, j = 1, 2, \ldots, n\} \cup \{0\}, q = 1, 2, \ldots, r,$$

e

$$a_{\sigma_1} m_{\sigma_1}|_{\mathcal{S}} = \sum_{q=2}^{r} (-a_{\sigma_q}) m_{\sigma_q}|_{\mathcal{S}},$$

segue que existe pelo menos um inteiro $p \in \{2, 3, \ldots, r\}$ tal que $m_{\sigma_p}|_{\mathcal{S}} = m_{\sigma_1}|_{\mathcal{S}}$. Então, pelo Corolário 6.2, $m_{\sigma_p} \equiv m_{\sigma_1} \pmod{I_n}$, tal que

$$f \equiv \sum_{q=1}^{r} a_{\sigma_q} m_{\sigma_q} \equiv (a_{\sigma_1} + a_{\sigma_p}) m_{\sigma_1} + \sum_{q=2}^{p-1} a_{\sigma_q} m_{\sigma_q} + \sum_{q=p+1}^{r} a_{\sigma_q} m_{\sigma_q} \pmod{I_n},$$

ou seja, f pode ser expresso, módulo I_n, como uma combinação linear de $r - 1$ monômios multilineares, o que contradiz a nossa escolha de r. Assim, só podemos ter

$$f \equiv 0 \pmod{I_n}.$$

Isso completa a demonstração do teorema. □

REFERÊNCIAS

[1] BRESAR, M. **Introduction to Noncommutative Algebra**, Springer, 2014

[2] DRENSKY, V. **Free algebras and PI-algebras**, Springer-Verlag, Singapore, 1999.

[3] AMITSUR, S.; LEVITZKI, J. **Minimal identities for algebras**, Proc. Amer. Math. Soc. 1, 449–463 (1950).

[4] ROSSET, S. **A new proof of the Amitsur-Levitzki identity**, Israel J. Math. 23, 187–188 (1976)

[5] GONÇALVES, F.S. **Grafos Eulerianos e Identidades Polinomiais na Álgebra** $M_n(K)$, Dissertação de Mestrado em Matemática, UFSCar: São Carlos, 2013

[6] KEMER, A. **Finite basis property of identities of associative algebras**, Algebra and Logic *26*, 362–397 (1987).

[7] AZEVEDO, S. S., **Graded identities for the matrix algebra of order n over an infinite field**. Communications in Algebra. **30(12)**, (2002), 5849-5860.

[8] VICENZO, O. M. **On the graded identities of** $M_{1,1}(E)$, Israel J. Math. 80(3) (1992), 323–335. MR 94f:16041

[9] SPECHT, **W. Gesetze in ringen** Math. Zeitschrift. *52* (1950), 557-589.

[10] VASILOVSKY, S. Yu. **Zn-graded Polynomial Identities of the Full Matrix of order n**, Proceedings of the American Mathematical Society, *127(12)* (1999), 3517-3524.

[11] DRENSKY, V. **A minimal basis for the identities of a second-order matrix algebra over a field of characteristic 0**, Algebra and Logic *20 (3)*, 188–194 (1981).

[12] RAZMYSLOV, Yu.P. **Finite basing of the identities of a matrix algebra of second order over a field of characteristic zero**, Algebra and Logic, *12* (1973), 83–113.