Identidades Graduadas para Álgebras de Matrizes

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por Sérgio Sardinha de Azevedo* e aprovada pela comissão julgadora.

Campinas, 24 de fevereiro de 2003.

Prof. Dr. Plamen Koshlukov
Orientador

Banca Examinadora
1. Said Sidki
2. Miguel A. A. Ferrero
3. Francisco Cesar Polcino Millies
4. Antonio Paques
5. Plamen Koshlukov

Tese apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de Doutor em Matemática.

*Apoio FAPESP, Processo No. 98/16449-5.

Conteúdo

Resumo

O estudo das identidades polinomiais graduadas foi motivado pelas suas várias aplicações na Teoria de Identidades Polinomiais, como a teoria estrutural desenvolvida por A. Kemer. Posteriormente tornou-se um objeto de estudo próprio. As identidades graduadas podem fornecer informações interessantes sobre as identidades polinomiais ordinárias. Trabalhando inicialmente com matrizes de ordem n sobre corpos infinitos, encontramos bases para as identidades graduadas dessa álgebra considerando $\mathbb{Z}_n$-graduação e $\mathbb{Z}$-graduação. Depois, provamos que, a menos de isomorfismos, existem duas $\mathbb{Z}_2$-graduações não-triviais para a álgebra das matrizes 2×2 sobre um corpo finito de característica diferente de 2. Além disso, essas graduações podem ser diferenciadas por meio de identidades graduadas. Por fim, encontramos bases para as identidades $\mathbb{Z}_2$-graduadas das álgebras $M_{1,1}(E)$ e $E \otimes E$ sobre um corpo infinito de característica diferente de 2. Como corolário, conseguimos uma prova bastante elementar para um teorema de Kemer, a saber, as álgebras $M_{1,1}(E)$ e $E \otimes E$ são PI equivalentes.

Abstract

The study of graded polynomial identities was motivated by its many applications to Polynomial Identities Theory, like the structure theory developed by A. Kemer. Afterwards it has become an independent object of study. The graded identities can give us interesting information about the ordinary identities. At first working with matrices of order n over infinite fields, we have found bases for the graded identities of this algebra considering $\mathbb{Z}_n$-grading and $\mathbb{Z}$-grading. We have also proved that, up to isomorphism, there exist two non-trivial $\mathbb{Z}_2$-gradings for the algebra of the matrices 2×2 over a finite field of characteristic different from 2. Besides, these gradings can be recognized through graded identities. Finally, we have found bases for the $\mathbb{Z}_2$-graded identities of the algebras $M_{1,1}(E)$ and $E \otimes E$ over an infinite field of characteristic different from 2. As a corollary, we have obtained a rather elementary proof for a theorem of Kemer, namely the algebras $M_{1,1}(E)$ and $E \otimes E$ are PI equivalent.

Introdução

A Teoria de Identidades Polinomiais começou a desenvolver-se mais intensamente por volta de 1950. Nesse ano, foi publicado o famoso Teorema de Amitsur-Levitzki afirmando que o polinômio standard de grau $2n$ é uma identidade polinomial da álgebra das matrizes de ordem n sobre um corpo (veja [1]). Também em 1950, W. Specht [43] levantou um problema que viria a ficar conhecido como o Problema de Specht: *Toda álgebra associativa possui uma base finita para suas identidades polinomiais?* Essa pergunta passou a ser uma das questões centrais da Teoria de Identidades Polinomiais e foi finalmente respondida de modo afirmativo por Kemer em 1987 (veja [23]), no caso de álgebras sobre corpo de característica 0.

Um dos principais problemas sobre identidades polinomiais é encontrar uma base das identidades de álgebras específicas. Em 1973, Razmyslov [39] encontrou uma base para as identidades polinomiais da álgebra das matrizes de ordem 2 sobre um corpo de característica 0. A base encontrada por Ramyslov tinha nove identidades, mas Drensky [15] em 1981 melhorou esse resultado encontrando uma base minimal com duas identidades. Entre 1978 e 1982, foram descobertas bases para as matrizes de ordens 2, 3 e 4 sobre corpos finitos (veja [17, 18, 35]). A base das identidades polinomiais para as matrizes triangulares superiores foi encontrada por vários autores, ainda no caso de um corpo qualquer, ver [16, Capítulo 5].

Além do caso da álgebra das matrizes 2×2, conhecem-se bases para as identidades polinomiais da álgebra de Grassmann e do quadrado tensorial da álgebra de Grassmann sobre corpos de característica 0. No entanto, fora esses resultados pouco se conhece ainda hoje sobre bases para identidades polinomiais de outras álgebras. Assim, surge o interesse por pesquisar outros tipos de identidades polinomiais como identidades fracas, identidades com traço e identidades graduadas, que fornecem informações sobre as identidades polinomiais ordinárias. Ressaltamos que as identidades fracas e as graduadas têm várias aplicações no estudo de álgebras não associativas tais como as de Lie, de Jordan e alternativas. As identidades com traço da álgebra das matrizes, por exemplo, foram descritas por Procesi [38] e por Razmyslov [40].

O interesse pelo estudo de identidades graduadas sobre um corpo de característica 0 é justificado pela relação entre as identidades graduadas e as ordinárias, que é uma das peças chave da teoria estrutural de T-ideais desenvolvida por Kemer (veja [23]) e utilizada para resolver o Problema de Specht em característica 0. Embora em característica positiva não exista tal relação, as identidades graduadas são ainda de interesse (veja por exemplo [5, 7, 8]). Mais tarde, elas se tornaram um objeto de estudo independente. As aplicações que as identidades graduadas podem encontrar na Teoria de PI álgebras são várias. Mencionaremos alguns dos mais importantes resultados relacionados a identidades polinomiais graduadas. Em [4] e [9], foi provado que se G é um grupo abeliano finito e A é uma álgebra G-graduada, então A é uma PI álgebra se e somente se sua componente de grau 0 é uma PI álgebra.

Di Vincenzo [11] descreveu bases para as identidades $\mathbb{Z}_2$-graduadas de várias álgebras importantes e obteve como corolário uma prova bastante elementar do conhecido fato de que as álgebras $M_{1,1}(E)$ e $E\otimes E$ satisfazem as mesmas identidades polinomiais para corpos de característica 0. Aqui E denota a álgebra de Grassmann de dimensão infinita e $M_{1,1}(E)$ é a álgebra das matrizes 2×2 sobre E cuja diagonal principal contém elementos pares de E e cuja outra diagonal contém elementos ímpares. Os resultados de [11] foram generalizados em [29] para corpos infinitos de característica diferente de 2. Além disso, como conseqüência foi obtida uma prova ainda mais elementar da coincidência dos T-ideais de $M_{1,1}(E)$ e $E \otimes E$.

Para corpos de característica 0, Vasilovsky [47, 48] encontrou bases para identidades graduadas da álgebra das matrizes de ordem n, considerando $\mathbb{Z}$-graduações e $\mathbb{Z}_n$-graduações. Em [2, 3], foi provado que esses resultados são válidos para corpos infinitos de qualquer característica. Um dos instrumentos principais utilizados para fazer essa generalização foram as matrizes genéricas (que também foram usadas em [29]).

Recentemente Di Vincenzo e Nardozza [13] desenvolveram um método para encontrar uma base das identidades $G \oplus \mathbb{Z}_2$-graduadas da álgebra $A \otimes E$ a partir das identidades G-graduadas da álgebra A. Como corolário, eles provaram por meio de identidades graduadas um resultado de Kemer, a saber, que as álgebras $M_{1,1}(E) \otimes E$ e $M_2(E)$ satisfazem as mesmas identidades polinomiais. Ressaltamos que ainda não é conhecida uma base das identidades ordinárias da álgebra $M_2(E)$, e a solução deste problema está longe...

Neste texto, apresentamos os trabalhos [2, 3, 29] e também o artigo [30]. Esse último trata de identidades $\mathbb{Z}_2$-graduadas para a álgebra das matrizes 2×2 sobre corpos finitos. Embora sejam conhecidas bases para as identidades polinomiais ordinárias dessas matrizes, o objetivo desse trabalho foi descrever todas as graduações para essa álgebra e mostrar que elas podem ser diferenciadas por identidades graduadas. Vale ressaltar que os métodos utilizados para abordar o problema de matrizes sobre corpos finitos são completamente diferentes daqueles usados para matrizes sobre corpos infinitos.

Resumiremos o conteúdo da tese. No capítulo 1, providenciamos os pré-requisitos para a leitura do texto. São resultados clássicos sobre álgebras, identidades polinomiais e T-ideais, álgebras graduadas e identidades graduadas.

O segundo capítulo trata das identidades graduadas em álgebras matriciais sobre corpos infinitos. Na seção 2.1, descrevemos uma base das identidades $\mathbb{Z}_2$-graduadas da álgebra matricial de ordem 2. Nas próximas duas seções descrevemos as identidades $\mathbb{Z}_n$-graduadas e $\mathbb{Z}$-graduadas da álgebra $M_n(K)$ das matrizes $n \times n$. Os resultados do capítulo 2 estão baseados nos artigos [2, 3, 29] e generalizam trabalhos de Di Vincenzo [11] e Vasilovsky [47, 48].

No terceiro capítulo, estudamos as identidades $\mathbb{Z}_2$-graduadas da álgebra matricial $M_2(K)$ sobre um corpo finito K. Os métodos utilizados nesse capítulo são completamente diferentes dos empregados no restante do texto, por isso o capítulo começa com uma parte introdutória. Nesse capítulo, descrevemos todas as $\mathbb{Z}_2$-graduações da álgebra $M_2(K)$ e mostramos que, a menos de isomorfismo graduado, existem somente duas graduações não-triviais. Em seguida, obtemos bases das identidades graduadas em cada uma dessas graduações, e demonstramos que essas graduações satisfazem identidades graduadas diferentes. O capítulo 3 está baseado principalmente no trabalho [30].

No último capítulo, estudamos as identidades (graduadas e ordinárias) satisfeitas pelas álgebras $M_{1,1}(E)$ e $E \otimes E$. Utilizamos métodos que aperfeiçoam os do capítulo 2, e descrevemos bases das identidades $\mathbb{Z}_2$-graduadas dessas álgebras sobre corpos infinitos de característica $p \neq 2$. Finalmente, obtemos uma nova demonstração do clássico resultado de Kemer de que essas duas álgebras satisfazem as mesmas identidades ordinárias quando $p = 0$. Esse capítulo está baseado no artigo [29].

As aplicações dos resultados desta tese poderão ser teóricas. Nossa opinião é que o conhecimento das identidades $\mathbb{Z}_2$-graduadas satisfeitas por álgebras importantes tais como as álgebras $M_2(K)$, $M_{1,1}(E)$ e $M_2(E)$ sobre corpos de característica positiva poderia resultar em melhor entendimento da estrutura dos respectivos ideais de identidades ordinárias. Nesta direção seria interessante entender melhor a diferença entre as identidades (ordinárias) das álgebras $M_{1,1}(E)$ e $E \otimes E$ (no caso de característica 0, as suas identidades coincidem). Os resultados obtidos sobre as identidades graduadas das matrizes de ordem n poderiam providenciar várias informações sobre os invariantes numéricos dos ideais das identidades graduadas satisfeitas por essas álgebras tais como codimensões graduadas, séries de Hilbert—Poincaré, entre outros. Também poderiam providenciar muita informação útil sobre as identidades ordinárias satisfeitas por essas álgebras. Combinando-se as idéias e os métodos usados nesta tese, poderíamos estudar as identidades satisfeitas por produtos tensoriais de algumas das álgebras aqui consideradas.

Por fim, gostaria de fazer constar aqui meus sinceros agradecimentos ao Prof. Plamen Koshlukov, meu orientador, pelo auxílio na condução desse trabalho e o estímulo prestado para a pesquisa matemática.

Notação

Ao longo de todo o texto, representamos por K um corpo arbitrário de qualquer característica. Todos os espaços vetoriais, álgebras e produtos tensoriais são considerados sobre o corpo K. Denotamos por $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Z}_n$ os conjuntos dos números inteiros positivos, dos números inteiros e dos inteiros módulo n respectivamente. Para cada número inteiro a, denotamos por $\overline{a}$ a classe de equivalência em $\mathbb{Z}_n$ que contém a. Se a e b são números inteiros, denotamos por $a \bmod b$ o resto da divisão de a por b.

Capítulo 1

Álgebras com identidades polinomiais

1.1 Propriedades básicas das álgebras

Definição Um espaço vetorial A sobre um corpo K é chamado uma *álgebra* se A é munido de uma operação binária $*$, chamada *multiplicação*, tal que para quaisquer $a, b, c \in A$ e qualquer $\alpha \in K$
1) $(a+b)*c = a*c+b*c$,
2) $a*(b+c) = a*b+a*c$,
3) $\alpha(a*b) = (\alpha a)*b = a*(\alpha b)$,
4) $a*(b*c) = (a*b)*c$.
Além disso, A é uma álgebra *unitária* se possui um elemento 1 (chamado *identidade*) tal que $1*a = a*1 = a$ para todo $a \in A$.

Na verdade, a definição mais geral de álgebra não exige a propriedade 4. As álgebras que respeitam essa propriedade são denominadas álgebras associativas. Porém, todas as álgebras que aparecem nesse texto são associativas e chamamo-las apenas álgebras. Escrevemos simplesmente ab ao invés de $a*b$.

Definição Um subespaço B de uma álgebra A é uma *subálgebra* se é fechado com relação à multiplicação, ou seja, se $b_1, b_2 \in B$ então $b_1 b_2 \in B$. Uma subálebra I de A é um *ideal* se para qualquer $x \in I$ e para qualquer $a \in A$ temos que $ax \in I$ e $xa \in I$. A subálgebra

$$Z(A) = \{a \in A \mid ax = xa \text{ para todo } x \in A\}$$

é chamada *centro* da álgebra A.

Definição Uma transformação linear $\phi : A \to B$ da álgebra A na álgebra B é um *homomorfismo* se $\phi(ab) = \phi(a)\phi(b)$ para quaisquer a e b em A. Um *isomorfismo* é um homomorfismo bijetor. Um *endomorfismo* é um homomorfismo de uma álgebra nela mesma. Um *automorfismo* é um endomorfismo bijetor.

Enunciamos a seguir o clássico Teorema do Isomorfismo válido para grupos, espaços vetoriais, anéis e álgebras.

Teorema 1.1.1 *Seja $\phi : A \to B$ um homomorfismo de álgebras. Então o núcleo de ϕ*

$$\ker \phi = \{a \in A \mid \phi(a) = 0\}$$

é um ideal de A e a álgebra quociente $A/\ker\phi$ é isomorfa à imagem de ϕ

$$\phi(A) = \{\phi(a) \mid a \in A\}.$$

Damos a seguir dois exemplos de álgebras bastante utilizadas neste texto.

Exemplo O conjunto das matrizes $n \times n$ sobre o corpo K, denotado por $M_n(K)$, é uma álgebra. A matriz $n \times n$ cuja única entrada não-nula é 1 na i-ésima linha e j-ésima coluna, chamada matriz unidade, é indicada por e_{ij}. O centro de $M_n(K)$ é o subespaço unidimensional gerado pela matriz identidade $e = e_{11} + \cdots + e_{nn}$.

Exemplo Seja V um espaço vetorial com base $\{e_i \mid i \in \mathbb{N}\}$. A *álgebra de Grassmann* ou *álgebra exterior* E de V é gerada como espaço vetorial por 1 e pelos produtos $e_{i_1}e_{i_2}\dots e_{i_k}$, onde $i_1 < i_2 < \cdots < i_k$ e $k \in \mathbb{N}$, e a multiplicação em E é induzida por $e_ie_j = -e_je_i$ e $e_i^2 = 0$. Logo $E = E_0 \oplus E_1$ onde E_0 e E_1 são os subespaços de E gerados por todos os produtos de elementos de $\{e_i \mid i \in \mathbb{N}\}$ de comprimento par e ímpar respectivamente. É fácil ver que E_0 é o centro de E e que $ab = -ba$ para quaisquer a e b em E_1.

1.2 Álgebras livres

Definição Sejam $\mathfrak{A}$ uma classe de álgebras e $F \in \mathfrak{A}$ uma álgebra gerada pelo conjunto G. A álgebra F é uma *álgebra livre na classe $\mathfrak{A}$ com conjunto gerador livre G* (ou F é *livremente gerada pelo conjunto G na classe $\mathfrak{A}$*) se para qualquer álgebra $A \in \mathfrak{A}$, toda aplicação de G em A pode ser estendida unicamente a um homomorfismo de F em A.

Vamos construir uma álgebra livre na variedade formada por todas as álgebras. Seja $X = \{x_i \mid i \in \mathbb{N}\}$ um conjunto de variáveis. Denote por $K\langle X\rangle$ a álgebra que é o K-espaço vetorial que tem como base o conjunto dos monômios $X^* = \{x_{i_1}\dots x_{i_n} \mid n = 0, 1, 2, \dots\}$ e multiplicação definida por $(x_{i_1}\dots x_{i_m})(x_{j_1}\dots x_{j_n}) = x_{i_1}\dots x_{i_m}x_{j_1}\dots x_{j_n}$.

Observe que o monômio formado por nenhuma variável, denotado por 1, é a identidade da álgebra $K\langle X\rangle$. Os elementos da álgebra $K\langle X\rangle$, chamados *polinômios*, desempenham nas álgebras um papel semelhante ao das combinações lineares nos espaços vetoriais. Por exemplo, se queremos gerar um espaço vetorial a partir de um subconjunto tomamos todas as combinações lineares de elementos desse subconjunto; de modo similar, se A é uma álgebra gerada pela conjunto G então

$$A = \{f(g_1, \ldots, g_n) \mid f(x_1, \ldots, x_n) \in K\langle X\rangle; g_1, \ldots, g_n \in G\}.$$

O próximo teorema mostra que $K\langle X\rangle$ é livremente gerada por X na classe formada por todas as álgebras.

Teorema 1.2.1 *Se A é uma álgebra e σ é uma aplicação de X em A, então σ estende-se unicamente a um homomorfismo $\phi : K\langle X\rangle \to A$ dado por*

$$\phi(f(x_1, \ldots, x_n)) = f(\sigma(x_1), \ldots, \sigma(x_n)).$$

Demonstração. Inicialmente, estendemos σ à aplicação $\tau : X^* \to A$ definindo $\tau(x_{i_1} \ldots x_{i_k}) = \sigma(x_{i_1}) \ldots \sigma(x_{i_k})$. Agora estendemos τ ao homomorfismo de álgebras $\phi : K\langle X\rangle \to A$ definido por $\phi(\sum_{w\in \mathbf{X}^*} \alpha_w w) = \sum_{w\in \mathbf{X}^*} \alpha_w \tau(w)$. É fácil ver que o homomorfismo ϕ é dado por $\phi(f(x_{i_1}, \ldots, x_{i_n})) = f(\sigma(x_{i_1}), \ldots, \sigma(x_{i_n}))$.

Se φ é um homomorfismo de $K\langle X\rangle$ em A que estende σ, então

$$\varphi(f(x_1, \ldots, x_n)) = f(\sigma(x_1), \ldots, \sigma(x_n)) = \phi(f(x_1, \ldots, x_n)).$$

Portanto, σ estende-se unicamente a um homomorfismo de $K\langle X\rangle$ em A. □

A álgebra $K\langle X\rangle$ é chamada *álgebra livre*.

Na verdade, o homomorfismo que estende a aplicação de um conjunto gerador livre de uma álgebra livre para uma álgebra qualquer é único conforme mostra o próximo lema.

Lema 1.2.1 *Sejam $\mathfrak{A}$ uma classe de álgebras, F uma álgebra livre de $\mathfrak{A}$ com conjunto gerador livre G e A uma álgebra de $\mathfrak{A}$. Toda aplicação de G em A estende-se unicamente a um único homomorfismo de F em A.*

Demonstração. Seja σ uma aplicação de G em A. Se ϕ é um homomorfismo de F em A que estende σ, então $\phi(f(g_1, \ldots, g_n)) = f(\sigma(g_1), \ldots, \sigma(g_n))$. Por outro lado, como

$$F = \{f(g_1, \ldots, g_n) \mid f(x_1, \ldots, x_n) \in K\langle X\rangle; g_1, \ldots, g_n \in G\},$$

existe um único homomorfismo de F em A que estende σ. □

Dizemos que dois conjuntos são *de mesma cardinalidade* se existe uma bijeção entre eles.

Teorema 1.2.2 *Duas álgebras livres de uma mesma classe com conjuntos geradores livres de mesma cardinalidade são isomorfas.*

Demonstração. Sejam F_1 e F_2 duas álgebras livres de uma mesma classe com conjuntos geradores livres G_1 e G_2 respectivamente. Suponhamos que σ seja uma aplicação bijetora de G_1 em G_2. Logo, existe um homomorfismo ϕ_1 de F_1 em F_2 que estende σ. Além disso, existe também um homomorfismo ϕ_2 de F_2 em F_1 que estende σ^{-1}. Por outro lado, o homomorfismo $\phi_2 \circ \phi_1$ estende a aplicação $\sigma^{-1} \circ \sigma$ que é a identidade. Assim, $\phi_2 \circ \phi_1$ é o homomorfismo identidade de F_1 em F_1. Da mesma forma, vemos que $\phi_1 \circ \phi_2$ é o homomorfismo identidade de F_2 em F_2. Portanto, ϕ_1 e ϕ_2 são isomorfismos. □

1.3 Identidades polinomiais

Definição Um polinômio $f(x_1, \ldots, x_n) \in K\langle X\rangle$ ou a expressão $f(x_1, \ldots, x_n) = 0$ é uma *identidade polinomial* da álgebra A se $f(a_1, \ldots, a_n) = 0$ para quaisquer $a_1, \ldots, a_n \in A$ (dizemos também que A *satisfaz* a identidade polinomial f). O conjunto

$$T(A) = \{f \in K\langle X\rangle \mid f \text{ é uma identidade polinomial de } A\}$$

é um ideal de $K\langle X\rangle$ chamado *ideal das identidades*, ou *T-ideal* da álgebra A. Uma *álgebra com identidade polinomial* (ou abreviadamente uma *PI álgebra*, pois a sigla vem do inglês) é uma álgebra que satisfaz uma identidade polinomial não-nula.

Seguem alguns exemplos de PI álgebras.

Exemplo O polinômio $[x_1, x_2] = x_1x_2 - x_2x_1$ é chamado *comutador* de x_1 e x_2. Se A é uma álgebra comutativa então $[x_1, x_2] = 0$ é uma identidade polinomial de A.

Exemplo Uma generalização do polinômio comutador é o *polinômio standard de grau n*

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

onde S_n é o grupo simétrico de grau n que permuta os símbolos 1, 2, ..., n, e $(-1)^\sigma$ é o sinal da permutação σ. Obviamente $s_2(x_1, x_2) = x_1x_2 - x_2x_1 = [x_1, x_2]$. O famoso Teorema de Amitsur-Levitzki afirma que $s_{2n}(x_1, \ldots, x_{2n}) = 0$ é uma identidade polinomial na álgebra das matrizes $M_n(K)$. Há essencialmente cinco provas para esse teorema. A prova original [1], publicada em 1950 por Amitsur e Levitzki, baseia-se em argumentos combinatórios indutivos. Em 1958, Kostant [31] apresentou uma prova utilizando co-homologia. Usando teoria dos grafos, Swan [44] em 1963 também demonstrou esse teorema. As outras duas provas foram feitas por Razmyslov [40] em 1974 e por Rosset [42] em 1976.

Exemplo A álgebra $M_2(K)$ satisfaz a identidade

$$f(x_1, x_2, x_3) = [[x_1, x_2]^2, x_3] = (x_1x_2 - x_2x_1)^2x_3 - x_3(x_1x_2 - x_2x_1)^2,$$

conhecida como identidade de Hall. Verifica-se facilmente essa identidade observando dois fatos de demonstração bastante simples. O primeiro é que se a e b pertencem a $M_n(K)$, $n \in \mathbb{N}$, então o traço de $[a, b]$ é zero; e o segundo é que se a pertence a $M_2(K)$ e o traço de a é zero então $a^2 = \lambda e$, onde $\lambda \in K$ e e é a matriz identidade 2×2.

Exemplo A álgebra das matrizes triangulares superiores $n \times n$ sobre K, denotada por $U_n(K)$, é uma PI álgebra pois satisfaz a identidade

$$f(x_1, \ldots, x_{2n}) = [x_1, x_2][x_3, x_4] \ldots [x_{2n-1}, x_{2n}].$$

Isto decorre dos fatos de que se a e b são elementos de $U_n(K)$ então $[a, b]$ é um elemento de $U_n(K)$ com a diagonal principal nula; e que o produto de n matrizes triangulares superiores $n \times n$ com a diagonal principal nula é a matriz nula.

Exemplo Uma álgebra A é uma *nil álgebra* se para cada $a \in A$ existe um número natural n tal que $a^n = 0$. O menor número n com esta propriedade é chamado *índice de nilpotência* do elemento a. Uma álgebra A é uma *nil álgebra de índice limitado* n se $a^n = 0$ para cada $a \in A$. Toda nil álgebra de índice limitado n é uma PI álgebra, pois satisfaz a identidade $f(x_1) = x_1^n$.

Exemplo Uma álgebra A é *nilpotente* se existe um número natural fixo n tal que o produto de quaisquer n elementos de A é igual a zero. O menor número n com esta propriedade é o *índice de nilpotência* da álgebra A, e A é chamada álgebra *nilpotente de classe* $n-1$. Toda álgebra associativa nilpotente de classe $n-1$ é uma PI álgebra, pois satisfaz a identidade $f(x_1, \ldots, x_n) = x_1 \ldots x_n$.

Após vários exemplos de PI álgebras, podemos nos perguntar: *existem álgebras que não são PI álgebras?* A resposta é sim. A álgebra $K\langle X\rangle$, por exemplo, não satisfaz nenhuma identidade polinomial não-nula. Isto pode ser compreendido através de um argumento simples. Suponhamos, por absurdo, que $f(x_1, \ldots, x_n)$ seja uma identidade polinomial não-nula de $K\langle X\rangle$. Logo, $f(x_1, \ldots, x_n) = f(f_1(x_1), \ldots, f_n(x_n)) = 0$, onde $f_i(x_i) = x_i$ para $1 \leq i \leq n$, o que é um absurdo pois $f(x_1, \ldots, x_n) \neq 0$. Na verdade, basta considerar uma álgebra A que contém como subálgebra a álgebra livre, livremente gerada pelas variáveis x_1 e x_2. Sabe-se que esta álgebra livre contém subálgebras que são livres e livremente geradas por conjuntos de qualquer cardinalidade (segundo um teorema de A. Shirshov, ver [50, Lemma 3.6]). Então A não satisfaz nenhuma identidade polinomial.

O próximo teorema mostra que toda álgebra de dimensão finita é uma PI álgebra.

Teorema 1.3.1 *Se A é uma álgebra de dimensão finita n então ela satisfaz a identidade*

$$s_{n+1}(x_1, \ldots, x_{n+1}) = \sum_{\sigma \in S_{n+1}} (-1)^\sigma x_{\sigma(1)} \ldots x_{\sigma(n+1)}.$$

Demonstração. Da definição de polinômio standard é óbvio que ele é igual a zero se dois de seus argumentos são iguais. Sejam $\{e_1, \ldots, e_n\}$ uma base do espaço vetorial A e $a_1, \ldots, a_{n+1}$ elementos arbitrários da álgebra A. Podemos representar cada um dos elementos a_i na forma de uma combinação linear dos elementos $e_1, \ldots, e_n$ com coeficientes em K. É fácil ver que a expressão $s_{n+1}(a_1, \ldots, a_{n+1})$ é uma combinação linear de termos da forma $s_{n+1}(e_{i_1}, \ldots, e_{i_{n+1}})$, onde cada e_{i_k} é um elemento do conjunto $\{e_1, \ldots, e_n\}$. Mas então existem dois argumentos na expressão $s_{n+1}(e_{i_1}, \ldots, e_{i_{n+1}})$ que necessariamente coincidem e, portanto, ela deve ser igual a zero. Logo, $s_{n+1}(a_1, \ldots, a_{n+1}) = 0$. (Na verdade, a prova vem do fato de que como $a_1, \ldots, a_{n+1}$ são linearmente dependentes então $s_{n+1}(a_1, \ldots, a_{n+1}) = 0$.) □

Definição Um ideal I de uma álgebra A é um *T-ideal* se é invariante sob todos os homomorfismos de A, ou seja, $\phi(I) \subseteq I$ para todo endomorfismo ϕ de A.

Teorema 1.3.2 *O ideal das identidades de uma álgebra é um T-ideal de $K\langle X\rangle$.*

Demonstração. Sejam A uma álgebra, $f(x_1, \ldots, x_n) \in T(A)$ e ϕ um endomorfismo de $K\langle X\rangle$. Como $\phi(f(x_1, \ldots, x_n)) = f(\phi(x_1), \ldots, \phi(x_n))$ e $f(a_1, \ldots, a_n) = 0$ para quaisquer elementos $a_1, \ldots, a_n$ de A, obtemos que $\phi(f(x_1, \ldots, x_n)) \in T(A)$. Portanto, $\phi(T(A)) \subseteq T(A)$. □

Teorema 1.3.3 *Um ideal I de $K\langle X\rangle$ é um T-ideal se, e somente se, $f(f_1, \ldots, f_n) \in I$ para todo $f(x_1, \ldots, x_n) \in I$ e para quaisquer $f_1, \ldots, f_n \in K\langle X\rangle$.*

Demonstração. Suponhamos que I seja um T-ideal de $K\langle X\rangle$. Sejam $f(x_1, \ldots, x_n)$ um polinômio de I e $f_1, \ldots, f_n \in K\langle X\rangle$. A aplicação $\phi : K\langle X\rangle \to K\langle X\rangle$ definida por $\phi(x_i) = f_i$ quando $1 \leq i \leq n$ e $\phi(x_i) = 0$ caso contrário é um endomorfismo de $K\langle X\rangle$. Logo, $f(f_1, \ldots, f_n) = \phi(f(x_1, \ldots, x_n)) \in I$. Suponhamos agora que $f(f_1, \ldots, f_n) \in I$ para todo $f(x_1, \ldots, x_n) \in I$ e para quaisquer $f_1, \ldots, f_n \in K\langle X\rangle$. Se ϕ é um endomorfismo de $K\langle X\rangle$ então

$$\phi(f(x_1, \ldots, x_n)) = f(\phi(x_1), \ldots, \phi(x_n)) \in I,$$

pois $\phi(x_1), \ldots, \phi(x_n) \in K\langle X\rangle$. □

Teorema 1.3.4 *Se I é um T-ideal de $K\langle X\rangle$ então $I = T(K\langle X\rangle/I)$.*

Demonstração. Sejam $f(x_1, \ldots, x_n) \in I$ e $f_1, \ldots, f_n$ elementos de $K\langle X\rangle$. Como $f(f_1, \ldots, f_n) \in I$ devido ao Teorema 1.3.3, temos que

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

Portanto, $I \subseteq T(K\langle X\rangle/I)$. Por outro lado, se $f(x_1, \ldots, x_n) \in T(K\langle X\rangle/I)$ então

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

assim, $f(x_1, \ldots, x_n) \in I$. Portanto, $T(K\langle X\rangle/I) \subseteq I$. □

Definição Se $\mathcal{B}$ é um conjunto gerador de $T(A)$ para uma álgebra A, dizemos que $\mathcal{B}$ é uma *base* das identidades de A. Se $\mathcal{B}$ não contém propriamente nenhuma base de A, $\mathcal{B}$ é chamada *base minimal* de $T(A)$. Se $\mathcal{S}$ é um subconjunto de $K\langle X\rangle$, o T-ideal gerado por $\mathcal{S}$ é denotado por $\langle \mathcal{S}\rangle^T$. Em outras palavras, $\langle \mathcal{S}\rangle^T$ é o ideal em $K\langle X\rangle$ gerado pelos polinômios

$$\{f(g_1, g_2, \ldots, g_n) \mid f(x_1, x_2, \ldots, x_n) \in \mathcal{S}, g_i \in K\langle X\rangle\}.$$

Se um polinômio $f \in K\langle X\rangle$ pertence a $\langle \mathcal{S}\rangle^T$ dizemos que f *segue* de $\mathcal{S}$ ou que f é uma *conseqüência* de $\mathcal{S}$. Dois subconjuntos de $K\langle X\rangle$ são *equivalentes* se eles geram o mesmo T-ideal.

Um dos principais problemas da Teoria de Identidades Polinomiais é encontrar, para uma determinada álgebra, bases para suas identidades polinomiais. Seguem alguns exemplos de bases de identidades polinomiais.

Exemplo Razmyslov [39] encontrou uma base com 9 identidades para a álgebra $M_2(K)$, quando K é um corpo de característica zero. A demonstração desse resultado é bastante complicada, consistindo em demonstrar primeiro que as identidades polinomiais da álgebra de Lie $sl_2(K)$ têm base finita, e em utilizar depois as chamadas *identidades fracas* satisfeitas pelo par $(M_2(K), sl_2(K))$. Recordamos que um polinômio associativo f é uma identidade fraca para este par, se f anula-se sobre os elementos de $sl_2(K)$. Aqui $sl_2(K)$ é a álgebra de Lie das matrizes 2×2 com traço 0, onde a multiplicação é o comutador $[a, b] = ab - ba$ para a, $b \in sl_2(K)$. Drensky, utilizando pesadamente a teoria de representações dos grupos simétrico e geral linear, em [15] melhorou esse resultado encontrando uma base minimal com 2 identidades, a saber

$$\begin{aligned} s_4(x_1, x_2, x_3, x_4) &= \sum_{\sigma \in S_4} (-1)^\sigma x_{\sigma(1)} x_{\sigma(2)} x_{\sigma(3)} x_{\sigma(4)}, \\ h(x_1, x_2, x_3) &= [[x_1, x_2]^2, x_3]. \end{aligned}$$

Em seguida, Vasilovsky em [45] demonstrou que as identidades polinomiais da álgebra de Lie $sl_2(K)$ admitem base que consiste de uma identidade só, desde que o corpo K seja infinito e de característica $p \neq 2$, e desenvolveu métodos interessantes. Esses métodos foram aplicados com sucesso em várias situações, ver por exemplo [46]. Em [25], o resultado de Razmyslov sobre as identidades fracas de $(M_2(K), sl_2(K))$ foi provado verdadeiro para característica $p \neq 2$, e algumas generalizações foram obtidas em [26] e em [27].

Em [28] foi demonstrado que o resultado de Razmyslov e de Drensky sobre as identidades polinomiais da álgebra $M_2(K)$ é válido para corpos infinitos com característica prima $p \geq 7$. Sabe-se também que o resultado acima é válido para corpos infinitos de característica 5, e que em característica 3, a base minimal consiste das duas identidades acima, mais uma identidade polinomial de grau 6, a saber

$$[x_1, x_2] \circ (u \circ v) - (1/8)([x_1, u, v, x_2] + [x_1, v, u, x_2] - [x_2, u, x_1, v] - [x_2, v, x_1, u])$$

onde $u = [x_3, x_4]$, $v = [x_5, x_6]$, $a \circ b = (1/2)(ab + ba)$, e os comutadores compridos são lidos da esquerda para a direita, isto é, $[a, b, c] = [[a, b], c]$ (observe que se a característica de K for 3 então $1/8 = -1$).

Ressaltamos que os métodos utilizados em característica positiva são baseados na teoria de invariantes dos grupos clássicos. Essa teoria foi desenvolvida por Doubilet, Rota e Stein [14] e em seguida por De Concini e Procesi em [10], de modo independente da característica do corpo base. Nesta tese não precisaremos de tais métodos algébricos, combinatórios e geométricos, portanto encerramos a discussão neste ponto.

Exemplo Maltsev e Kuzmin [35] provaram que o ideal das identidades da álgebra das matrizes $M_2(K)$, onde K é um corpo finito com q elementos, é gerado pelos polinômios

$$\begin{aligned} f_1(x_1, x_2) &= (x_1 - x_1^q)(x_2 - x_2^{q^2})(1 - [x_1, x_2]^{q-1}), \\ f_2(x_1, x_2) &= (x_1 - x_1^q) \cdot (x_2 - x_2^q) - [(x_1 - x_1^q) \cdot (x_2 - x_2^q)]^q, \end{aligned}$$

onde $x_1 \cdot x_2 = x_1x_2 + x_2x_1$.

Exemplo Regev e Krakowski [32] descobriram que sobre corpos de característica 0 todas as identidades da álgebra de Grassmann seguem da identidade $[[x_1, x_2], x_3] = 0$. Este último resultado generaliza-se facilmente para o caso de quaisquer corpos infinitos de característica $p \neq 2$. (Quando $p = 2$, a álgebra de Grassmann é comutativa, portanto não muito "interessante" do ponto de vista da PI teoria. Pois no caso de álgebras comutativas, um raciocínio bastante simples mostra que qualquer identidade polinomial que não seja seqüência da comutatividade, implica na nilpotência da álgebra.) Ressaltamos ainda que a álgebra de Grassmann E de um espaço V, $\dim V = \infty$, é um exemplo de uma álgebra PI que não satisfaz nenhuma das identidades standard s_n, $n \geq 1$, em característica 0. Quando a característica do corpo é $p > 2$, a álgebra E satisfaz a identidade s_{p+1}. Um teorema de Kemer, ver [24], afirma que neste último caso, toda PI álgebra satisfaz alguma identidade standard.

Em 1950, Specht [43] formulou o seguinte problema para álgebras associativas sobre corpos de característica zero: *Toda álgebra possui uma base finita para suas identidades polinomiais?* Essa pergunta, que ficou conhecida como Problema de Specht, passou a ser uma das questões centrais da Teoria de Identidades Polinomiais e foi finalmente respondida de modo afirmativo por Kemer em 1987 (vide [23] ou [22]). Anteriormente, em 1973, Kruse [33] e Lvov [34] separadamente provaram que esse problema tem resposta positiva para álgebras finitas. Foi encontrada uma resposta negativa para o Problema de Specht no caso de álgebras infinitas sobre corpos de característica positiva. Não vamos discutir em detalhes os avanços na resolução do Problema de Specht pois é um assunto que merece atenção especial, envolve métodos e técnicas pesados, e não está diretamente relacionado com o conteúdo da presente tese. Mais adiante faremos uma exposição resumida de alguns pontos da teoria desenvolvida por Kemer, com a finalidade de justificar o nosso interesse em estudos de identidades graduadas em álgebras matriciais e de Grassmann. Referências adicionais e resultados clássicos bem como recentes sobre o Problema de Specht e a história da sua solução, podem ser encontradas no artigo de Belov [6].

Definição Seja I um subconjunto de $K\langle X\rangle$. A *variedade* de álgebras $\mathfrak{V}$ definida pelo conjunto I é a classe de todas as álgebras que satisfazem cada identidade de I; o conjunto I é o *conjunto de identidades que definem* a variedade $\mathfrak{V}$. É fácil ver que o ideal I está contido no núcleo de qualquer homomorfismo da álgebra livre $K\langle X\rangle$ numa álgebra da variedade $\mathfrak{V}$. A *variedade trivial* é a classe de álgebras que contém apenas a álgebra nula (em outras palavras é a variedade cujo conjunto de identidades que a definem é $K\langle X\rangle$).

Definição Se $\mathfrak{A}$ é uma classe de álgebras, o conjunto

$$T(\mathfrak{A}) = \{f \in K\langle X\rangle \mid f \in T(A) \text{ para cada } A \in \mathfrak{A}\}$$

é um ideal de $K\langle X\rangle$ chamado *ideal das identidades* da classe de álgebras $\mathfrak{A}$.

Obviamente se $\mathfrak{V}$ é uma variedade de álgebras, o ideal das identidades $T(\mathfrak{V})$ é um conjunto de identidades que definem (ou determinam) a variedade $\mathfrak{V}$. O próximo teorema mostra que toda variedade possui uma álgebra livre.

Teorema 1.3.5 *Sejam $\mathfrak{V}$ uma variedade não-trivial de álgebras e $\pi : K\langle X\rangle \rightarrow$*

$K\langle X\rangle/T(\mathfrak{V})$ a projeção canônica. Então:
(i) a restrição de π a X é injetora;
(ii) a álgebra $K\langle X\rangle/T(\mathfrak{V})$ é livre na variedade $\mathfrak{V}$ com conjunto gerador livre $\pi(X)$.

Demonstração. Provaremos primeiro que a restrição de π a X é injetora. Sejam x_1 e x_2 elementos distintos de X tais que $\pi(x_1) = \pi(x_2)$. Consideremos uma álgebra não-nula A de $\mathfrak{V}$ e um elemento não-nulo a de A. Então existe um homomorfismo $\phi : K\langle X\rangle \to A$ tal que $\phi(x_1) = a$ e $\phi(x_2) = 0$. Como $T(\mathfrak{V})$ está contido no núcleo de ϕ, existe um homomorfismo $\psi : K\langle X\rangle/T(\mathfrak{V}) \to A$ para o qual $\psi \circ \pi = \phi$. Mas

$$a = \phi(x_1) = \psi \circ \pi(x_1) = \psi \circ \pi(x_2) = \phi(x_2) = 0,$$

o que é uma contradição.

A álgebra $K\langle X\rangle/T(\mathfrak{V})$ é gerada pelo conjunto $\pi(X)$ e pertence a $\mathfrak{V}$ desde que satisfaz todas as identidades de $T(\mathfrak{V})$. Mostraremos que essa álgebra é livre em $\mathfrak{V}$ com conjunto de geradores livres $\pi(X)$. Sejam $A \in \mathfrak{V}$ e σ uma aplicação de $\pi(X)$ em A. Como $K\langle X\rangle$ é uma álgebra livre com conjunto gerador livre X, a aplicação $\sigma \circ \pi : X \to A$ estende-se a um homomorfismo $\psi : K\langle X\rangle \to A$. Existe um homomorfismo $\phi : K\langle X\rangle/T(\mathfrak{V}) \to A$ para o qual $\phi \circ \pi = \psi$, pois $T(\mathfrak{V})$ está contido no núcleo de ψ. Se $x \in X$, então

$$\phi(\pi(x)) = \phi \circ \pi(x) = \psi(x) = \sigma \circ \pi(x) = \sigma(\pi(x));$$

ou seja, o homomorfismo ϕ estende a aplicação σ. Conseqüentemente, ϕ é o homomorfismo desejado. Assim, $K\langle X\rangle/T(\mathfrak{V})$ é uma álgebra livre na variedade $\mathfrak{V}$ e $\pi(X)$ é o seu conjunto gerador livre. $\square$

Uma variedade de álgebras é claramente fechada sob as operações de tomar subálgebras, imagens homomorfas e produtos cartesianos. Uma variedade $\mathfrak{V}$ de álgebras é *gerada* por uma classe $\mathfrak{A}$ de álgebras, se toda álgebra de $\mathfrak{V}$ pode ser obtida das álgebras de $\mathfrak{A}$ por uma seqüência finita de aplicações dessas operações; denotamos esse fato por $\mathfrak{V} = Var\mathfrak{A}$ ou, quando a classe $\mathfrak{A}$ contém apenas uma álgebra A, por $\mathfrak{V} = VarA$. O clássico teorema de Birkhoff demonstra que uma classe não vazia de álgebras é variedade se, e somente se, ela é fechada com respeito às três operações acima descritas.

No próximo lema, listamos algumas propriedades básicas das variedades (omitimos a demonstração por ser bastante fácil). É importante frisar que ele só é válido pois o conjunto X é infinito.

Lema 1.3.1 *Sejam $\mathfrak{A}$ e $\mathfrak{B}$ duas classes de álgebras e $\mathfrak{V}$ uma variedade de álgebras.*
(i) $T(\mathfrak{A}) = \cap_{A\in\mathfrak{A}} T(A) = T(Var\mathfrak{A})$;
(ii) se $\mathfrak{A} \subseteq \mathfrak{B}$ então $T(\mathfrak{B}) \subseteq T(\mathfrak{A})$;
(iii) $\mathfrak{A} \subseteq \mathfrak{V}$ se, e somente se, $T(\mathfrak{V}) \subseteq T(\mathfrak{A})$;
(iv) se F é uma álgebra livre em $\mathfrak{V}$ então $T(\mathfrak{V}) = T(F)$.

Corolário 1.3.1 *Se A é uma álgebra então $T(VarA) = T(A)$.*

Vários dos resultados e definições apresentados nesta seção e na anterior poderiam ser generalizados para álgebras não necessariamente associativas (álgebras de Lie, de Jordan, alternativas, entre outras), sobre anéis comutativos com identidade. Porém, como as álgebras tratadas neste texto são principalmente a álgebra das matrizes e a álgebra de Grassmann, desde este primeiro capítulo restringimos as definições a álgebras associativas sobre corpos. Para definições e propriedades mais genéricas sobre esse tema, o livro [50] é muito adequado.

1.4 Polinômios homogêneos, lineares e próprios

Definição Um monômio m tem *grau k em x_i* se a variável x_i ocorre em m exatamente k vezes. Um polinômio f é *homogêneo de grau k em x_i*, se todos os seus monômios têm grau k em x_i; denotamos isso por $\deg_{x_i} f = k$. Um polinômio *linear em x_i* é um polinômio homogêneo de grau 1 em x_i.

Definição Um polinômio é *multi-homogêneo* se para cada variável x_i todos os seus monômios têm o mesmo grau em x_i. Um polinômio é *multilinear* se é linear em cada variável. O *grau* de um monômio é o seu comprimento. O *grau* de um polinômio é o grau de seu maior monômio.

Definição Se f é um polinômio de $K\langle X\rangle$ de grau n e x_k é uma variável de f, podemos escrevê-lo como uma soma

$$f = \sum_{i=0}^{n} f_i$$

onde cada polinômio f_i é homogêneo de grau i na variável x_k. Cada polinômio f_i é uma *componente homogênea de grau i em x_k* do polinômio f.

Os polinômios multilineares e multi-homogêneos desempenham um papel importante na busca de bases para identidades polinômiais sobre determinados tipos de corpos. Esse fato, já observado por Specht [43] em 1950, está desenvolvido em detalhes no próximo lema que também pode ser encontrado em [16], pp. 39–40.

Lema 1.4.1 *Seja*

$$f(x_1, \ldots, x_m) = \sum_{i=0}^{n} f_i(x_1, \ldots, x_m) \in K\langle X\rangle,$$

onde f_i é a componente homogênea de f de grau i em x_1.
(i) Se o corpo K contém mais que n elementos então as identidades polinomiais $f_i = 0$, $i = 0, 1, \ldots, n$, seguem de $f = 0$.
(ii) Se a característica do corpo K é 0 ou maior que o grau de f então $f = 0$ é equivalente a um conjunto de identidades polinomiais multilineares.

Demonstração. (i) Seja $I = \langle f \rangle^T$ o T-ideal de $K\langle X \rangle$ gerado por f. Escolhemos $n+1$ elementos diferentes $\alpha_0, \alpha_1, \ldots, \alpha_n$ de K. Como I é um T-ideal,

$$f(\alpha_j x_1, x_2, \ldots, x_m) = \sum_{i=0}^{n} \alpha_j^i f_i(x_1, x_2, \ldots, x_m) \in I, \quad j = 0, 1, \ldots, n.$$

Consideramos essas equações como um sistema linear com incógnitas f_i, $0 \leq i \leq n$. Desde que o determinante

$$\begin{vmatrix} 1 & \alpha_0 & \alpha_0^2 & \cdots & \alpha_0^n \\ 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^n \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^n \end{vmatrix} = \prod_{i<j} (\alpha_j - \alpha_i)$$

é o determinante de Vandermonde e é diferente de 0, temos que cada $f_i(x_1, \ldots, x_m)$ pertence a I, ou seja, as identidades polinomiais $f_i = 0$ são conseqüências de $f = 0$.

(ii) Pela parte (i), podemos assumir que $f(x_1, \ldots, x_m)$ é multi-homogêneo. Seja $k = \deg_{x_1} f$. Escrevemos $f(y_1 + y_2, x_2, \ldots, x_m) \in I$ na forma

$$f(y_1 + y_2, x_2, \ldots, x_m) = \sum_{i=0}^{k} f_i(y_1, y_2, x_2, \ldots, x_m),$$

onde f_i é a componente homogênea de grau i em y_1. Logo $f_i \in I$, $0 \leq i \leq k$. Como $\deg_{y_i} f_i < k$, $i = 1, \ldots, k-1$, $j = 1, 2$, aplicamos argumentos indutivos e obtemos um conjunto de conseqüências multilineares de $f = 0$. A fim de ver que essas identidades multilineares são equivalentes a $f = 0$, é suficiente ver que

$$f_i(y_1, y_1, x_2, \ldots, x_m) = \binom{k}{i} f(y_1, x_2, \ldots, x_m),$$

e o coeficiente binomial é diferente de 0 porque assumimos que a característica do corpo K é 0 ou maior que o grau do polinômio f. □

Observamos que o item (i) do lema acima significa que o polinômio f gera o mesmo T-ideal como o gerado pelos polinômios f_i, $i = 0, 1, \ldots, n$.

Corolário 1.4.1 *Seja A uma álgebra.*
(i) Se o corpo K é infinito então todas as identidades polinomiais de A seguem de suas identidades multi-homogêneas.
(ii) Se o corpo K tem característica zero então todas as identidades polinomiais de A seguem de suas identidades multilineares.

Quando a álgebra é unitária podemos restringir a busca de identidades polinomiais a um determinado tipo de polinômios conforme explicamos abaixo.

Definição O *comutador de comprimento n* é definido indutivamente por $[x_1, x_2] = x_1x_2 - x_2x_1$ para $n = 2$ e por

$$[x_1, \ldots, x_{n-1}, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$$

para $n \geq 2$. Um polinômio $f \in K\langle X\rangle$ é chamado *polinômio próprio* (ou *comutador*) se é uma combinação linear de produtos de comutadores

$$f(x_1, \ldots, x_m) = \sum \alpha_{i,\ldots,j}[x_{i_1}, \ldots, x_{i_p}] \ldots [x_{j_1}, \ldots, x_{j_q}], \quad \alpha_{i,\ldots,j} \in K.$$

(Assumimos que 1 é um produto de um conjunto vazio de comutadores.) Denotamos por $B(X)$ o conjunto de todos os polinômios próprios em $K\langle X\rangle$.

O próximo lema mostra a importância dos polinômios comutadores para encontrar uma base das identidades de uma álgebra unitária. Sua prova não é complicada e pode ser encontrada em [16], Proposição 4.3.3, pp. 42–44. A demonstração está baseada no teorema de Poincaré, Birkhoff e Witt sobre a álgebra universal envolvente de uma álgebra de Lie, e, mais especificamente, que a álgebra $K\langle X\rangle$ é a universal envolvente da álgebra livre de Lie livremente gerada pelo conjunto X.

Lema 1.4.2 *Se A é uma álgebra unitária sobre um corpo infinito, então todas as identidades polinomiais de A seguem das suas identidades próprias (ou seja, daquelas em $T(A) \cap B(X)$). Se A é uma álgebra unitária sobre um corpo de característica 0, então todas as identidades polinomiais de A seguem das suas identidades próprias multilineares.*

1.5 Álgebras graduadas

As bases de identidades polinomiais para álgebras são ainda pouco conhecidas. Os poucos resultados descobertos até agora resumem-se basicamente em bases para as seguintes álgebras: matrizes de ordem 2 sobre corpos de característica diferente de 2, as matrizes de ordem 3 e 4 sobre corpos finitos, matrizes triangulares superiores de qualquer ordem sobre corpos infinitos, a álgebra de Grassmann, e o quadrado tensorial da álgebra de Grassmann sobre corpos de característica 0. Assim, somos levados a pesquisar outros tipos de identidades polinomiais como identidades fracas (já discutimos de modo informal tais identidades), identidades com traço (isto é, além das operações usuais da álgebra, temos mais uma operação unária — o traço, e os "polinômios" envolvem, além das variáveis usuais, traços), e identidades graduadas, que fornecem informações sobre as identidades polinomiais ordinárias. As identidades com traço da álgebra $M_n(K)$, por exemplo, foram descritas por Procesi [38] e por Razmyslov [40]. Esse resultado é um dos mais abrangentes e gerais, e de grande importância para a PI teoria.

O interesse no estudo de identidades graduadas sobre um corpo de característica 0 é justificado pela relação entre as identidades graduadas e as ordinárias que é uma das peças chave da teoria estrutural de T-ideais desenvolvida por Kemer (veja [23]). Embora em característica positiva não exista tal relação, as identidades graduadas são ainda de interesse (veja por exemplo [7, 8]).

Até o final desta seção, fixamos G como um grupo abeliano aditivo.

Definição Uma *álgebra G-graduada* $A = \sum_{g\in G} A_g$ é uma álgebra que pode ser expressa como a soma direta da família de subespaços $\{A_g \mid g \in G\}$ de A tais que $A_g A_h \subseteq A_{g+h}$ para quaisquer g, $h \in G$.

Definição Uma álgebra G-graduada A possui *G-graduação trivial* se $A_0 = A$ e $A_g = 0$ para $0 \neq g \in G$.

Definição Uma aplicação $\phi : A \to B$ entre álgebras G-graduadas é um *homomorfismo G-graduado* se $\phi(A_g) \subseteq B_g$ para todo $g \in G$. Do mesmo modo, são definidos *isomorfismo*, *endomorfismo* e *automorfismo G-graduados*.

Definição Um subespaço B de uma álgebra G-graduada A é *G-graduado* se é a soma direta das interseções $B \cap A_g$.

Definição Seja A um álgebra G-graduada. Um elemento a de A é *homogêneo* se existe $g \in G$ tal que $a \in A_g$; nesse caso, dizemos que g é o *grau homogêneo* do elemento a e denotamos $\alpha(a) = g$. Se $a = \sum_{a_g \in A_g} a_g$, dizemos que a_g é a *componente homogênea de grau g* de a.

Os próximos dois lemas têm demonstrações bastante diretas.

Lema 1.5.1 *Sejam A uma álgebra G-graduada e B uma subálgebra de A. As afirmações a seguir São equivalentes:*
(i) B é uma subálgebra G-graduada de A;

(ii) B é uma álgebra G-graduada tal que $B_g \subseteq A_g$ para cada $g \in G$;
(iii) As componentes homogêneas de cada elemento de B pertencem a B.

O centro $Z(A)$ de uma álgebra G-graduada A é uma subálgebra G-graduada. Para ver isso, considere a_g a componente homogênea de grau g de um elemento $a \in Z(A)$ e x um elemento homogêneo de A. Como $ax = xa$, temos que $a_g x = x a_g$. Assim, o elemento a_g comuta com qualquer elemento homogêneo de A e, portanto, com qualquer elemento de A. Logo, $a_g \in Z(A)$.

Lema 1.5.2 *Se I é um ideal G-graduado de uma álgebra G-graduada A então A/I é uma álgebra G-graduada considerando $(A/I)_g = \{a + I \mid a \in A_g\}$.*

É fácil ver que se $\phi : A \to B$ é um homomorfismo G-graduado então $\ker \phi$ é um ideal G-graduado de A e $\phi(A)$ é uma subálgebra G-graduada de B tal que $\phi(A)_g = \phi(A_g)$ para todo $g \in G$. Além disso, o Teorema do Isomorfismo é válido para álgebra graduadas, ou seja, a álgebra quociente $A/\ker \phi$ é isomorfa à imagem $\phi(A)$.

Podemos definir uma G-graduação para a álgebra livre $K\langle X\rangle$. Seja $\{X_g \mid g \in G\}$ uma família de subconjuntos disjuntos e enumeráveis de X tais que $X = \cup_{g\in G} X_g$. Uma variável $x \in X$ tem grau homogêneo g, denotado por $\alpha(x) = g$, se $x \in X_g$. O conjunto dos monômios

$$\{x_{i_1} x_{i_2} \dots x_{i_k} \mid x_{i_1}, x_{i_2}, \dots, x_{i_k} \in X, k \in \mathbb{N}\}$$

é uma base da álgebra livre $K\langle X\rangle$ como espaço vetorial. O grau homogêneo de um monômio $\mathsf{m} = x_{i_1} x_{i_2} \dots x_{i_k}$ é definido como $\alpha(\mathsf{m}) = \alpha(x_{i_1}) + \alpha(x_{i_2}) + \cdots + \alpha(x_{i_k})$. Para $g \in G$, denote por $K\langle X\rangle_g$ o subespaço de $K\langle X\rangle$ gerado por todos os monômios com grau homogêneo g. Note que $K\langle X\rangle_g K\langle X\rangle_h \subseteq K\langle X\rangle_{g+h}$ para quaisquer g e h em G. Portanto, esta decomposição define uma G-graduação para a álgebra $K\langle X\rangle$.

Definição Um ideal I de uma álgebra G-graduada A é um *T_G-ideal* se é invariante sob todos os endomorfismos G-graduados de A, ou seja, $\phi(I) \subseteq I$ para todo endomorfismo G-graduado ϕ de A.

Definição Um polinômio $f(x_1, \dots, x_m) \in K\langle X\rangle$, ou a expressão $f(x_1, \dots, x_m) = 0$, é uma *identidade polinomial G-graduada* da álgebra G-graduada A se $f(a_1, \dots, a_m) = 0$ para quaisquer $a_1, \dots, a_m \in \cup_{\alpha\in G} A_\alpha$ tais que $a_i \in A_{\alpha(x_i)}$, $i = 1, \dots, m$. O conjunto $\mathrm{T}_G(A)$ de todas as identidades graduadas de uma álgebra G-graduada A é um T_G-ideal de $K\langle X\rangle$ chamado *ideal das identidades G-graduadas* da álgebra A.

As álgebras graduadas com identidades polinômiais possuem propriedades análogas às álgebras não-graduadas com respeito a T-ideais, variedades, polinômios lineares, polinômios homogêneos, etc.

O próximo lema fornece alguma informação sobre as identidades ordinárias a partir de identidades graduadas.

Lema 1.5.3 *Se A e B são álgebras G-graduadas tais que $T_G(A) \subseteq T_G(B)$ então $T(A) \subseteq T(B)$.*

Demonstração. Seja $f(x_1, \ldots, x_m)$ uma identidade qualquer de A e sejam

$$b_1 = \sum_{g \in G} b_{1g}, \ldots, b_m = \sum_{g \in G} b_{mg}$$

elementos de B. Como $f \in T(A)$, temos que

$$f(\sum_{g \in G} x_{1g}, \ldots, \sum_{g \in G} x_{mg}) \in T_G(A) \subseteq T_G(B).$$

Logo $f(b_1, \ldots, b_m) = f(\sum_{g \in G} b_{1g}, \ldots, \sum_{g \in G} b_{mg}) = 0$. Assim $T(A) \subseteq T(B)$. □

Corolário 1.5.1 *Se duas álgebras têm as mesmas identidades graduadas então elas têm as mesmas identidades ordinárias.*

Daremos abaixo um contra-exemplo para a inversa desse corolário.

Um grupo importante para estudar identidades graduadas são os inteiros módulo 2. Para esse grupo utilizamos algumas notações particulares.

Definição Numa álgebra $\mathbb{Z}_2$-graduada A, o subespaço A_0 é chamado *subespaço par* e seus elementos são os *elementos pares*, ao passo que o subespaço A_1 é chamado *subespaço ímpar* e seus elementos são os *elementos ímpares*.

A álgebra de Grassmann $E = E_0 \oplus E_1$ é uma álgebra $\mathbb{Z}_2$-graduada, onde E_0 é o subespaço par e E_1 é o subespaço ímpar.

A álgebra livre $K\langle X \rangle$ também tem algumas notações especiais no caso de $\mathbb{Z}_2$-graduação. Sejam $Y = \{y_i \mid i \in \mathbb{N}\}$ e $Z = \{z_i \mid i \in \mathbb{N}\}$ dois subconjuntos disjuntos de X tais que $X = Y \cup Z$. Assumimos que as variáveis do conjunto Y têm grau par e as variáveis do conjunto Z têm grau ímpar. Portanto, um monômio tem grau par (ímpar) se possui um número par (ímpar) de variáveis do conjunto Z.

Do mesmo modo que no caso das identidades ordinárias, estamos interessados em encontrar bases para as identidades graduadas. A fim de encontrarmos uma base para as identidades $\mathbb{Z}_2$-graduadas da álgebra de Grassmann, vamos recordar um fato simples de álgebra linear.

Lema 1.5.4 *Sejam U_1 e U_2 dois subespaços de um espaço vetorial V tais que $U_1 \subseteq U_2$. Se $v_1, \ldots, v_n$ são elementos de V tais que o conjunto $\{v_1 + U_1, \ldots, v_n + U_1\}$ gera V/U_1 e o conjunto $\{v_1 + U_2, \ldots, v_n + U_2\}$ é linearmente independente em V/U_2 então $U_1 = U_2$.*

Demonstração. Seja u um elemento de U_2. Por hipótese, existem escalares $\alpha_1, \ldots, \alpha_n$ tais que $u + U_1 = \alpha_1(v_1 + U_1) + \cdots + \alpha_n(v_n + U_n)$; logo, $u - \alpha_1 v_1 + \cdots + \alpha_n v_n \in U_1 \subseteq U_2$. Assim, $0 + U_2 = u + U_2 = \alpha_1 v_1 + \cdots + \alpha_n v_n + U_2 = \alpha_1(v_1 + U_2) + \cdots + \alpha_n(v_n + U_2)$. Portanto, $\alpha_1 = \cdots = \alpha_n = 0$ e $u \in U_1$. □

Proposição 1.5.1 *Se o corpo K é infinito e de característica diferente de 2 então todas as identidades polinomiais $\mathbb{Z}_2$-graduadas da álgebra de Grassmann seguem de $y_1y_2 = y_2y_1$, $y_1z_1 = z_1y_1$ e $z_1z_2 = -z_2z_1$. Se o corpo K é infinito e de característica 2 então todas as identidades polinomiais $\mathbb{Z}_2$-graduadas da álgebra de Grassmann seguem de $y_1y_2 = y_2y_1$, $y_1z_1 = z_1y_1$, $z_1z_2 = z_2z_1$ e $z_1^2 = 0$.*

Demonstração. Suponhamos que K tenha característica diferente de 2. Seja I o ideal das identidades $\mathbb{Z}_2$-graduadas de $K\langle X\rangle$ gerado pelas identidades graduadas $y_1y_2 = y_2y_1$, $y_1z_1 = z_1y_1$ e $z_1z_2 = -z_2z_1$. Claramente $I \subseteq T_2(E)$. Seja C o conjunto dos monômios $y_{i_1} \ldots y_{i_k} z_{j_1} \ldots z_{j_l}$ tais que $i_1 \leq \cdots \leq i_k$ e $j_1 < \cdots < j_l$. É fácil ver que o conjunto $\{\mathsf{m} + I \mid \mathsf{m} \in C\}$ gera o espaço vetorial $K\langle X\rangle/I$. Vamos provar que o conjunto $\{\mathsf{m} + T_2(E) \mid \mathsf{m} \in C\}$ é linearmente independente no espaço vetorial $K\langle X\rangle/T_2(E)$. Sejam $\mathsf{m}_1, \ldots, \mathsf{m}_n$ elementos de C e $\alpha_1, \ldots, \alpha_n$ elementos do corpo K tais que $\alpha_1\mathsf{m}_1 + \ldots + \alpha_n\mathsf{m}_n \in T_2(E)$; queremos mostrar que $\alpha_1 = \cdots = \alpha_n = 0$. Como o corpo K é infinito, pelo Lema 1.4.1, podemos supor que $\alpha_i\mathsf{m}_i \in T_2(E)$ para cada $i \in \{1, \ldots, n\}$. Fazendo as substituições $y_i \mapsto 1$ e $z_i \mapsto e_i$ no monômio m_i, temos que $\alpha_i = 0$. Aplicando o Lema 1.5.4, concluímos a prova. Se o corpo K tem característica 2, pelo mesmo raciocínio concluímos a prova. □

Podemos agora dar um exemplo que mostra que a recíproca do Corolário 1.5.1 não é válida. Consideremos na álgebra de Grassmann E duas graduações. A primeira é a graduação da proposição anterior. A outra é a graduação trivial, onde $y_1y_2 = y_2y_1$ não é uma identidade graduada. Portanto, uma mesma álgebra pode ter identidades graduadas diferentes conforme a graduação.

Enunciamos um lema para identidades $\mathbb{Z}_2$-graduadas correspodente ao Lema 1.4.2.

Lema 1.5.5 *Se $f(y_1, \ldots, y_m, z_1, \ldots, z_n) \in K\langle X\rangle$ é um polinômio multi-homogêneo, então ele é equivalente como identidade graduada a uma coleção finita de identidades graduadas tais que as variáveis $y_1, \ldots, y_m$ aparecem em cada um deles apenas em comutadores.*

Demonstração. A prova é a mesma que a da Proposição 4.3.3 de [16]. Note que podemos substituir x_i por $x_i + 1$ apenas quando $x_i \in Y$, pois $1 \in K\langle X\rangle$ pertence a $K\langle X\rangle_0$. □

Denote como $B_2(X)$ o conjunto dos polinômios f em $K\langle X\rangle$ tais que toda variável y_i aparece em comutadores na expansão de f.

Corolário 1.5.2 *Se I é um T_2-ideal de $K\langle X\rangle$ então I é gerado como T_2-ideal pelo conjunto $I \cap B_2(X)$.*

No próximo capítulo consideraremos álgebras graduadas e suas identidades polinomiais. Recordamos agora alguns fatos da teoria de A. Kemer [23] sobre a estrutura dos T-ideais. Essa teoria foi desenvolvida para álgebras sobre corpos de característica 0, portanto assumimos até o fim desta seção que a característica do corpo K é 0.

Sejam U e V duas variedades de álgebras, denotamos por UV o produto de U e V, isto é, a classe de todas as álgebras A que possuem um ideal I tal que $I \in V$, $A/I \in U$. Definimos a álgebra $M_{k,l}(E)$ como sendo a subálgebra de $M_{k+l}(E)$ que consiste das matrizes $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ tais que $A \in M_k(E_0)$, $D \in M_l(E_0)$ e B e C são matrizes $k \times l$ e $l \times k$, respectivamente, com entradas de E_1.

Um T-ideal I em $K\langle X\rangle$ é chamado T-primo, se ele é primo dentro da classe de todos T-ideais. Em outras palavras, se I_1 e I_2 são T-ideais e $I_1 I_2 \subseteq I$ então $I_1 \subseteq I$ ou $I_2 \subseteq I$. O T-ideal J é semiprimo, se $J_1^2 \subseteq J$ implica $J_1 \subseteq J$ para todo T-ideal J_1. Isto quer dizer que não existem T-ideais nilpotentes e não nulos na álgebra $K\langle X\rangle/J$.

Os seguintes resultados foram demonstrados em [23, Capítulo 1].

1. Se V é uma variedade não trivial então $V = N_k W$ onde N_k é a variedade das álgebras nilpotentes de índice k, e W é a maior variedade semiprima que está contida em V.

2. O T-ideal I é semiprimo se e somente se $I = I_1 \cap I_2 \cap \ldots \cap I_q$ para algum q e alguns T-ideais primos I_j.

3. Os únicos T-ideais que são T-primos são 0, $K\langle X\rangle$ e os T-ideais das álgebras $M_n(K)$, $M_n(E)$ e $M_{k,l}(E)$.

Se $A = A_0 \oplus A_1$ é uma álgebra $\mathbb{Z}_2$-graduada, denotamos por $E(A)$ o envelope de Grassmann de A, isto é, $E(A) = A_0 \otimes E_0 \oplus A_1 \otimes E_1$.

Kemer demonstrou ainda os seguintes resultados, ver [23, Capítulo 1].

1. Todo T-ideal não-trivial coincide com o T-ideal do envelope de Grassmann de uma álgebra $\mathbb{Z}_2$-graduada e finitamente gerada.

2. O T-ideal de qualquer álgebra $\mathbb{Z}_2$-graduada e finitamente gerada coincide com o T-ideal de alguma álgebra $\mathbb{Z}_2$-graduada de dimensão finita.

3. Dos dois resultados acima segue que todo T-ideal não-trivial coincide com o T-ideal do envelope de Grassmann de alguma álgebra $\mathbb{Z}_2$-graduada de dimensão finita.

Um dos corolários mais importantes dos resultados mencionados acima foi a solução positiva do problema de Specht em característica 0.

Como a teoria de Kemer está baseada fortemente em propriedades de identidades $\mathbb{Z}_2$-graduadas, isso induziu vários estudos sobre as identidades de álgebras $\mathbb{Z}_2$-graduadas. Indicamos o artigo [5] para detalhes e mais referências.

Quando consideramos álgebras sobre corpos de característica positiva, a teoria de Kemer não se aplica imediatamente. Em primeiro lugar, surgem novos T-ideais que são T-primos (os chamados T-ideais irregulares). A sua descrição está bem longe de ser completa, e uma parte da teoria de Kemer pode ser transferida somente para álgebras livres e finitamente geradas. Por outro lado, o problema de Specht em característica positiva tem resposta negativa. Mas as identidades graduadas podem ser usadas no estudo das identidades polinomiais em álgebras mesmo em característica positiva. Alguns exemplos nós exibiremos nos capítulos a seguir. Outros podem ser encontrados em [5] e na bibliografia desse artigo.

Capítulo 2

Matrizes sobre corpos infinitos

2.1 Identidades $\mathbb{Z}_2$-graduadas de $M_2(K)$

A álgebra $M_2(K)$ possui a seguinte $\mathbb{Z}_2$-graduação não-trivial

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

Di Vincenzo [11] provou que sobre corpos de característica 0 todas as identidades graduadas dessa álgebra seguem de $y_1y_2 = y_2y_1$ e $z_1z_2z_3 = z_3z_2z_1$. Ao estudar identidades polinômiais sobre corpos de característica 0, conforme vimos no Lema 1.4.1, temos uma vantagem pois podemos considerar apenas os polinômios multilineares. Porém, para corpos de característica positiva não podemos contar com esse recurso. No caso de corpos infinitos, as contas são mais complicadas que no caso de característica 0, mas ainda temos uma vantagem semelhante que é o fato de poder considerar apenas polinômios multi-homogêneos (*vide* Lema 1.4.1). Assim, foi provado que o resultado de Di Vincenzo é válido para corpos infinitos de qualquer característica, veja [29]. Reproduziremos nesta seção a demonstração desse fato.

É bem conhecido o resultado clássico que a álgebra das matrizes genéricas de ordem n é isomorfa à álgebra relativamente livre $K\langle X\rangle/T(M_n(K))$ da variedade das matrizes $n \times n$ (veja por exemplo Seção 7.2 de [16], pp. 86–87). Usaremos uma idéia semelhante para álgebras graduadas. Todas as seções deste capítulo utilizam um método bastante semelhante. Considerando uma álgebra G-graduada A, inicialmente construímos uma álgebra graduada livre F que é isomorfa à álgebra $K\langle X\rangle/T_G(A)$. A seguir trabalhamos na álgebra graduada F ao invés da álgebra $K\langle X\rangle/T_G(A)$.

Até o final desta seção, assumimos que K é um corpo infinito.

Seja $\Omega = K[t_i, u_i, v_i, w_i \mid i \in \mathbb{N}]$ a álgebra dos polinômios comutativos gerada pelas variáveis t_i, u_i, v_i e w_i. A álgebra $M_2(\Omega)$ possui uma graduação semelhante à de $M_2(K)$, a saber,

$$M_2(\Omega)_0 = \left\{ \begin{pmatrix} f_1 & 0 \\ 0 & f_4 \end{pmatrix} \mid f_1, f_4 \in \Omega \right\} \text{ e } M_2(\Omega)_1 = \left\{ \begin{pmatrix} 0 & f_2 \\ f_3 & 0 \end{pmatrix} \mid f_2, f_3 \in \Omega \right\}.$$

Denote por F a subálgebra $\mathbb{Z}_2$-graduada de $M_2(\Omega)$ gerada pelas matrizes

$$A_i = \begin{pmatrix} t_i & 0 \\ 0 & w_i \end{pmatrix} \text{ e } B_i = \begin{pmatrix} 0 & u_i \\ v_i & 0 \end{pmatrix}$$

para $i \in \mathbb{N}$.

Lema 2.1.1 *A álgebra $\mathbb{Z}_2$-graduada relativamente livre $K\langle X\rangle/T_2(M_2(K))$ é isomorfa à álgebra F.*

Demonstração. A prova é análoga àquela para matrizes genéricas. A aplicação $\phi : K\langle X\rangle \to F$ definida por $\phi(f(y_1, \ldots, y_m, z_1, \ldots, z_n)) = f(A_1, \ldots, A_m, B_1, \ldots, B_n)$ é um homomorfismo $\mathbb{Z}_2$-graduado. Claramente, ϕ é sobrejetora. Além disso, um simples cálculo mostra que $\ker \phi = T_2(M_2(K))$ e ϕ induz um isomorfismo. $\square$

Seja I o ideal das identidades $\mathbb{Z}_2$-graduadas de $K\langle X\rangle$ gerado pelas identidades graduadas $y_1y_2 = y_2y_1$ e $z_1z_2z_3 = z_3z_2z_1$.

Lema 2.1.2 *A álgebra $\mathbb{Z}_2$-graduada $M_2(K)$ satisfaz todas as identidades graduadas do T_2-ideal I.*

Demonstração. Basta verificar que as identidades $y_1y_2 = y_2y_1$ e $z_1z_2z_3 = z_3z_2z_1$ pertencem a $T_2(M_2(K))$. $\square$

Uma *seqüência básica* $s = (a_1, \ldots, a_p, b_1, \ldots, b_q, c_1, \ldots, c_r, d_1, \ldots, d_s)$ é uma seqüência de números naturais tais que
(i) $p \geq 0$, $q \geq 0$, $r \geq 0$, $s \geq 0$;
(ii) $a_1 \leq \cdots \leq a_p$, $b_1 \leq \cdots \leq b_q$, $c_1 \leq \cdots \leq c_r$, $d_1 \leq \cdots \leq d_s$;
(iii) $s \leq r \leq s + 1$;
(iv) se $r = 0$ então $q = 0$.
À seqüência básica s associamos o monômio

$$\mathsf{m}_s = \begin{cases} y_{a_1} \ldots y_{a_p} z_{c_1} y_{b_1} \ldots y_{b_q} z_{d_1} z_{c_2} z_{d_2} \ldots z_{c_s} z_{d_s} & \text{se } \ r = s, \\ y_{a_1} \ldots y_{a_p} z_{c_1} y_{b_1} \ldots y_{b_q} z_{d_1} z_{c_2} z_{d_2} \ldots z_{c_s} z_{d_s} z_{d_{s+1}} & \text{se } \ r = s + 1. \end{cases}$$

Seja C o conjunto de todos os monômios associados a seqüências básicas. Note que o monômio 1 pertence a C, pois está associado à seqüência vazia.

Lema 2.1.3 *O conjunto* $\{\mathsf{m} + T_2(M_2(K)) \mid \mathsf{m} \in C\}$ *é linearmente independente no espaço vetorial* $K\langle X\rangle/T_2(M_2(K))$.

Demonstração. Sejam $\mathsf{m}_1,\ldots,\mathsf{m}_n$ elementos de C e $\alpha_1,\ldots,\alpha_n$ elementos do corpo K tais que $\alpha_1\mathsf{m}_1 + \cdots + \alpha_n\mathsf{m}_n \in T_2(M_2(K))$. Vamos provar que $\alpha_1 = \cdots = \alpha_n = 0$. Como o corpo K é infinito, podemos supor que os monômios $\mathsf{m}_1,\ldots,\mathsf{m}_n$ são multi-homogêneos. Denote por $\overline{\mathsf{m}}$ o elemento de $M_2(\Omega)$ obtido pelas substituições $y_i \mapsto A_i$ e $z_i \mapsto B_i$ no monômio $\mathsf{m} \in C$. Se $s = (a_1,\ldots,a_p,b_1,\ldots,b_q,c_1,\ldots,c_r,d_1,\ldots,d_s)$ é uma seqüência básica então

$$\overline{\mathsf{m}}_s = \begin{cases} \omega_1 e_{11} + \omega_2 e_{22} & \text{se} \quad r = s, \\ \omega_1 e_{12} + \omega_2 e_{21} & \text{se} \quad r = s+1, \end{cases}$$

onde

$$\begin{aligned} \omega_1 &= t_{a_1}\ldots t_{a_p} u_{b_1}\ldots u_{b_q} v_{c_1}\ldots v_{c_s} w_{d_1}\ldots w_{d_s} \\ \omega_2 &= t_{b_1}\ldots t_{b_q} u_{a_1}\ldots u_{a_p} v_{d_1}\ldots v_{d_s} w_{c_1}\ldots w_{c_s}. \end{aligned}$$

Assim, é fácil ver que existe uma bijeção entre C e o subconjunto $\{\overline{\mathsf{m}} \mid \mathsf{m} \in C\}$ de F. Desse modo, se $\alpha_1\mathsf{m}_1 + \cdots + \alpha_n\mathsf{m}_n \in T_2(F)$ então $\alpha_1 = \cdots = \alpha_n = 0$, pois as matrizes $\overline{\mathsf{m}}_1,\ldots,\overline{\mathsf{m}}_n$ são linearmente independentes em F. Pelo Lema 2.1.1, sabemos que $\alpha_1\mathsf{m}_1 + \cdots + \alpha_n\mathsf{m}_n \in T_2(F)$ e a prova do lema está concluída. $\square$

Apresentamos agora o principal teorema desta seção.

Teorema 2.1.1 *Todas as identidades polinomiais graduadas da álgebra* $\mathbb{Z}_2$*-graduada* $M_2(K)$ *seguem das identidades* $y_1y_2 = y_2y_1$ *e* $z_1z_2z_3 = z_3z_2z_1$.

Demonstração. Se $f \in K\langle X\rangle_0$ então $y_if - fy_i$ pertence a I. Assim todo elemento de $K\langle X\rangle/I$ é uma combinação linear de elementos da forma $\mathsf{m}_1 z_{e_1}\mathsf{m}_2 z_{e_2} z_{e_3}\ldots z_{e_k} + I$ onde m_1 e m_2 são monômios formados apenas por y_i's. Devido à identidade $y_1y_2 = y_2y_1$, podemos supor que os índices das variáveis em m_1 e m_2 crescem (com possíveis repetições). Pela identidade $z_1z_2z_3 = z_3z_2z_1$, assumimos que $e_1 \le e_3 \le e_5 \le \cdots$ e $e_2 \le e_4 \le e_6 \le \cdots$. Note que se $e_1 > e_3$ num monômio, então usamos o fato de que $z_{e_1}(\mathsf{m}_2 z_{e_2})z_{e_3} - z_{e_3}(\mathsf{m}_2 z_{e_2})z_{e_1}$ pertence a I. Assim, concluímos que o conjunto $\{\mathsf{m} + I \mid \mathsf{m} \in C\}$ gera o espaço vetorial $K\langle X\rangle/I$. Sabemos, pelo Lema 2.1.2, que $I \subseteq T_2(M_2(K))$. Aplicando os Lemas 2.1.3 e 1.5.4, concluímos a prova. $\square$

2.2 Identidades $\mathbb{Z}_n$-graduadas de $M_n(K)$

Podemos generalizar o resultado da seção anterior considerando na álgebra $M_n(K)$ uma $\mathbb{Z}_n$-graduação. Vasilovsky [48] provou que quando K é um corpo de característica 0 todas as identidades $\mathbb{Z}_n$-graduadas da álgebra $M_n(K)$ seguem das identidades $x_1x_2 = x_2x_1$ com $\alpha(x_1) = \alpha(x_2) = 0$ e $x_1x_2x_3 = x_3x_2x_1$ com $\alpha(x_1) = -\alpha(x_2) = \alpha(x_3)$. Utilizando matrizes genéricas foi provado [2] que o resultado de Vasilovsky é válido para corpos infinitos.

Até o final desta seção, assumimos que K é um corpo infinito.

Inicialmente vamos definir uma $\mathbb{Z}_n$-graduação para $M_n(K)$. Para cada $\alpha \in \mathbb{Z}_n$, seja $M_n(K)_\alpha$ o subespaço de $M_n(K)$ gerado por todas as matrizes unidade e_{ij} tais que $\overline{j-i} = \alpha$. Assim, $M_n(K)_0$ consiste das matrizes da forma

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

e, para $0 < t \leq n-1$, $M_n(K)_{\overline{t}}$ consiste das matrizes da forma

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

onde $a_{1,t+1}$, $a_{2,t+2}$, $\ldots$, $a_{n-t,n}$, $a_{n-t+1,1}$, $\ldots$, $a_{n,t} \in K$. Como $e_{ij}e_{js} = e_{is}$ e $e_{ij}e_{rs} = 0$ se $j \neq r$, segue que $M_n(K)_{\overline{p}}M_n(K)_{\overline{q}} \subseteq M_n(K)_{\overline{p+q}}$ para p, $q \in \{0, 1, \ldots, n-1\}$; portanto a decomposição acima define uma $\mathbb{Z}_n$-graduação para a álgebra $M_n(K)$.

Seja $\Omega = K[y_i^{(\alpha)} \mid i \in \mathbb{N}, \alpha \in \mathbb{Z}_n]$ a álgebra dos polinômios comutativos gerada pelas variáveis $y_i^{(\alpha)}$. Para cada $\alpha \in \mathbb{Z}_n$, seja $M_n(\Omega)_\alpha$ o subespaço de $M_n(\Omega)$ que consiste das matrizes da forma

$$\begin{pmatrix} 0 & \cdots & 0 & f_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & f_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & f_{n-i} \\ f_{n-i+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & f_n & 0 & 0 & \cdots & 0 \end{pmatrix},$$

onde $f_1, \ldots, f_n \in \Omega$ e $\bar{i} = \alpha$. O próximo lema mostra que a decomposicão acima define uma $\mathbb{Z}_n$-graduacão para a álgebra $M_n(\Omega)$.

Lema 2.2.1 *Sejam*

$$A = \begin{pmatrix} 0 & \cdots & 0 & a_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & a_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & a_{n-i} \\ a_{n-i+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & a_n & 0 & 0 & \cdots & 0 \end{pmatrix},$$

$$B = \begin{pmatrix} 0 & \cdots & 0 & b_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & b_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & b_{n-j} \\ b_{n-j+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & b_n & 0 & 0 & \cdots & 0 \end{pmatrix}$$

matrizes de $M_n(\Omega)$, onde $0 \leq i, j \leq n-1$. Então

$$AB = \begin{pmatrix} 0 & \cdots & 0 & a_1 b_{i_1} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & a_2 b_{i_2} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & a_x b_{i_x} \\ a_{x+1} b_{i_{x+1}} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & a_n b_{i_n} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

onde $i_k = (i+k-1) \bmod n+1$ e $x = n-(i+j) \bmod n$.

Demonstração. O elemento a_1 está na posição $(1, i+1)$ da matriz A. Logo, como $k = 1$, temos que $i_1 = i + 1 = (i + k - 1) \bmod n + 1$.

Para $k \geq 2$, a posição do elemento a_k é $(k, i + k)$ se $i + k \leq n$ ou $(k, i + k - n)$ se $i + k > n$. Logo, a posição de a_k é $(k, (i + k - 1) \bmod n + 1)$. Portanto, $i_k = (i + k - 1) \bmod n + 1$.

O elemento $a_x b_{i_x}$ está na última coluna da matriz AB. Por outro lado, como b_{n-j} está na última coluna da matriz B, sabemos que $n - j = i_x$. Portanto, $n - j = (i + x - 1) \bmod n + 1$. Há dois possíveis casos:

Caso 1: $0 \leq i + x - 1 < n$. Então $n - j = i + x$, donde $x = n - (i + j)$. Como $1 \leq x \leq n$, temos que $0 \leq i + j \leq n - 1$. Logo $x = n - (i + j) \bmod n$.

Caso 2: $n \leq i + x - 1 \leq 2n - 2$. Então $n - j = i + x - n$, donde $x = n - (i + j - n)$. Como $1 \leq x \leq n$, temos que $0 \leq i + j - n \leq n - 1$. Logo $x = n - (i + j - n) \bmod n = n - (i + j) \bmod n$. $\square$

Denote por F a subálgebra $\mathbb{Z}_n$-graduada de $M_n(\Omega)$ gerada pelas matrizes

$$A_i = \begin{pmatrix} 0 & \cdots & 0 & y_i^{(\bar{0})} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & y_i^{(\bar{1})} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & y_i^{(-\alpha(x_i)-\bar{1})} \\ y_i^{(-\alpha(x_i))} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & y_i^{(\overline{n-1})} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

para $i \in \mathbb{N}$.

Lema 2.2.2 *A álgebra $\mathbb{Z}_n$-graduada relativamente livre $K\langle X\rangle/T_n(M_n(K))$ é isomorfa à álgebra F.*

Demonstração. A aplicação $\phi : K\langle X\rangle \to F$ definida por $\phi(f(x_1, \ldots, x_m)) = f(A_1, \ldots, A_m)$ é um homomorfismo $\mathbb{Z}_n$-graduado. Claramente, ϕ é sobrejetora. Além disso, um simples cálculo mostra que $\ker \phi = T_n(M_n(K))$ e ϕ induz um isomorfismo. $\square$

Seja I o ideal das identidades $\mathbb{Z}_n$-graduadas de $K\langle X\rangle$ gerado pelas identidades graduadas $x_1x_2 = x_2x_1$ com $\alpha(x_1) = \alpha(x_2) = 0$ e $x_1x_2x_3 = x_3x_2x_1$ com $\alpha(x_1) = -\alpha(x_2) = \alpha(x_3)$.

Lema 2.2.3 *A álgebra $\mathbb{Z}_n$-graduada $M_n(K)$ satisfaz todas as identidades graduadas do T_n-ideal I.*

Demonstração. Como quaisquer duas matrizes diagonais comutam, a identidade graduada $x_1x_2 = x_2x_1$ com $\alpha(x_1) = \alpha(x_2) = 0$ é válida em $M_n(K)$. Sendo multilineares as identidades $x_1x_2x_3 = x_3x_2x_1$ com $\alpha(x_1) = -\alpha(x_2) = \alpha(x_3)$, é suficiente mostrar que elas são válidas para $x_1 = e_{ij} \in M_n(K)_{\bar{t}}$, $x_3 = e_{kl} \in M_n(K)_{\bar{t}}$ e $x_2 = e_{rs} \in M_n(K)_{\overline{-t}}$, onde $0 < t \leq n-1$. Observe que

$$j = \begin{cases} i+t & \text{se } j-i \geq 0, \\ i+t-n & \text{se } j-i < 0; \end{cases}$$
$$k = \begin{cases} l-t & \text{se } l-k \geq 0, \\ l-t+n & \text{se } l-k < 0; \end{cases}$$
$$r = \begin{cases} s+t & \text{se } s-r < 0, \\ s+t-n & \text{se } s-r \geq 0. \end{cases}$$

Note que $e_{ij}e_{rs}e_{kl} \neq 0$ se e somente se $j = r$ e $s = k$. Afirmamos que nesse caso $i = s = k$ e $j = r = l$. Observe que se $j = i+t$ e $r = s+t-n$ então, como $j = r$, segue que $n = s-i$, o que é impossível. Por isso, as igualdades $j = i+t$ e $r = s+t-n$ não podem ocorrer simultaneamente. O mesmo vale para as igualdades $k = l-t+n$ e $r = s+t$. Assim, quando $j = i+t$, temos que $r = s+t$ e $k = l-t$, de modo que $k = s = r-t = j-t = i$ e $r = j = i+t = k+t = l$. Analogamente, quando $j = i+t-n$, temos que $r = s+t-n$ e $k = l-t+n$, donde $k = s = r-t+n = j-t+n = i$ e $r = j = i+t-n = k+t-n = l$. Logo, $e_{ij}e_{rs}e_{kl} \neq 0$ se e somente se $i = s = k$ e $j = r = l$. Similarmente, temos que $e_{kl}e_{rs}e_{ij} \neq 0$ se e somente se $k = s = i$ e $l = r = j$. Portanto, se $e_{ij}e_{rs}e_{kl} \neq 0$ então $e_{ij}e_{rs}e_{kl} = e_{il} = e_{kj} = e_{kl}e_{rs}e_{ij}$, senão, $e_{ij}e_{rs}e_{kl} = 0 = e_{kl}e_{rs}e_{ij}$. □

Lema 2.2.4 *Para todo monômio $0 \neq \mathsf{m}(x_1, \ldots, x_m) \in K\langle X\rangle$ de comprimento q, existem inteiros $1 \leq i_1 \leq \cdots \leq i_q \leq m$ e elementos $\alpha_1, \ldots, \alpha_q$ de $\mathbb{Z}_n$ tais que*

$$\mathsf{m}(A_1, \ldots, A_m) = \begin{pmatrix} 0 & \cdots & 0 & \omega_{\bar{0}} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_{\bar{1}} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_{-\alpha(\mathsf{m})-\bar{1}} \\ \omega_{-\alpha(\mathsf{m})} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_{\overline{n-1}} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

onde $\omega_\delta = y_{i_1}^{(\alpha_1+\delta)} \ldots y_{i_q}^{(\alpha_q+\delta)}$.

Demonstração. Usamos indução sobre q. Se $q = 1$, obviamente temos o resultado. Se $q > 1$, então existe um monômio $0 \neq \mathsf{n}(x_1, \ldots, x_m) \in K\langle X\rangle$ tal que

$\mathsf{m}(x_1, \ldots, x_m) = \mathsf{n}(x_1, \ldots, x_m)x_i$, onde $1 \leq i \leq m$. Pela hipótese de indução e o Lema 2.2.1, podemos concluir a prova. $\square$

Lema 2.2.5 *Sejam* $\mathsf{m}(x_1, \ldots, x_m)$ *e* $\mathsf{n}(x_1, \ldots, x_m)$ *dois monômios de* $K\langle X\rangle$. *Se as matrizes* $\mathsf{m}(A_1, \ldots, A_m)$ *e* $\mathsf{n}(A_1, \ldots, A_m)$ *têm na primeira linha a mesma entrada não-nula então* $\mathsf{m}(x_1, \ldots, x_m) \equiv \mathsf{n}(x_1, \ldots, x_m)(\mathrm{mod} I)$.

Demonstração. Se $\mathsf{m}(A_1, \ldots, A_k)$ e $\mathsf{n}(A_1, \ldots, A_k)$ têm na primeira linha a mesma entrada não-nula, vemos pelo Lema 2.2.4 que $\mathsf{m}(A_1, \ldots, A_k) = \mathsf{n}(A_1, \ldots, A_k)$. Seja q o comprimento de m. Usaremos indução sobre q. Se $q = 1$, obviamente temos o resultado. Suponhamos então que $q > 1$.

Suponhamos que x_p é uma variável de $\mathsf{m}(x_1, \ldots, x_k)$ e m_1 e m_2 são dois monômios de $K\langle X\rangle$ tais que $\mathsf{m} = \mathsf{m}_1 x_p \mathsf{m}_2$. Pelo Lema 2.2.4, sabemos que existem monômios $\omega_1, \ldots, \omega_n, \eta_1, \ldots, \eta_n$ de Ω e inteiros $0 \leq i, j \leq n-1$ tais que

$$\mathsf{m}_1(A_1, \ldots, A_k) = \begin{pmatrix} 0 & \cdots & 0 & \omega_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_{n-i} \\ \omega_{n-i+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_n & 0 & 0 & \cdots & 0 \end{pmatrix}$$

e

$$\mathsf{m}_2(A_1, \ldots, A_k) = \begin{pmatrix} 0 & \cdots & 0 & \eta_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \eta_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \eta_{n-j} \\ \eta_{n-j+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \eta_n & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Observe que os graus homogêneos de $\mathsf{m}_1(A_1, \ldots, A_k)$ e $\mathsf{m}_2(A_1, \ldots, A_k)$ em F são respectivamente $\bar{i}$ e $\bar{j}$. Pelo Lema 2.2.1, temos que $\mathsf{m}_1(A_1, \ldots, A_k)A_p$ é igual a

$$\begin{pmatrix} 0 & \cdots & 0 & \omega_1 y_p^{(\alpha_1)} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \omega_x y_p^{(\alpha_x)} \\ \omega_{x+1} y_p^{(\alpha_{x+1})} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_n y_p^{(\alpha_n)} & 0 & \cdots & 0 \end{pmatrix}$$

onde $\alpha_r = \overline{(i+r-1)}$ e $x = n - (i + a_p))$ mod n, sendo $\alpha(x_p) = \overline{a_p}$. Logo a matriz $\mathsf{m}(A_1, \ldots, A_k) = \mathsf{m}_1(A_1, \ldots, A_k)A_p\mathsf{m}_2(A_1, \ldots, A_k)$ é igual a

$$\begin{pmatrix} 0 & \cdots & 0 & \omega_1 y_p^{(i_1)}\eta_{j_1} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & \omega_y y_p^{(i_y)}\eta_{j_y} \\ \omega_{y+1} y_p^{(i_{y+1})}\eta_{j_{y+1}} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_n y_p^{(i_n)}\eta_{j_n} & 0 & \cdots & 0 \end{pmatrix}$$

onde $j_s = (n - x + s - 1)$ mod $n + 1$ e $y = n - (n - x + j)$ mod n. Assim a variável $y_p^{(\alpha_1)}$ deve aparecer pelo menos uma vez na primeira linha de $\mathsf{n}(A_1, \ldots, A_k)$. Aplicando o mesmo raciocínio a n, existem dois monômios n_1 e n_2 em $K\langle X\rangle$ tais que $\mathsf{n} = \mathsf{n}_1 x_p \mathsf{n}_2$ e $\mathsf{n}_1(A_1, \ldots, A_k)$ tem grau $\bar{i}$ em F, porque caso contrário a variável $y_p^{(\alpha_1)}$ não apareceria na primeira linha de $\mathsf{n}(A_1, \ldots, A_k)$. Como $\mathsf{m}_1(A_1, \ldots, A_k)$ e $\mathsf{n}_1(A_1, \ldots, A_k)$ têm o mesmo grau em F, $\alpha(\mathsf{m}_1) = \alpha(\mathsf{n}_1)$. Portanto podemos concluir que se x_p é uma variável de $\mathsf{m}(x_1, \ldots, x_k)$ e $\mathsf{m}_1, \ldots, \mathsf{m}_l$ são monômios de $K\langle X\rangle$ tais que $\mathsf{m} = \mathsf{m}_1 x_p \mathsf{m}_2 x_p \mathsf{m}_3 \ldots \mathsf{m}_{l-1} x_p \mathsf{m}_l$, então existem monômios $\mathsf{n}_1, \ldots, \mathsf{n}_l$ em $K\langle X\rangle$ e uma bijeção (correspondência biunívoca) $\varphi : \{1, \ldots, l\} \to \{1, \ldots, l\}$ tais que $\mathsf{n} = \mathsf{n}_1 x_p \mathsf{n}_2 x_p \mathsf{n}_3 \ldots \mathsf{n}_{l-1} x_p \mathsf{n}_l$ e $\alpha(\mathsf{m}_1 x_p \mathsf{m}_2 \ldots \mathsf{m}_t) = \alpha(\mathsf{n}_1 x_p \mathsf{n}_2 \ldots \mathsf{n}_{\varphi(t)})$.

Seja x_i a primeira variável de m. Logo existem dois monômios n_1 e n_2 de $K\langle X\rangle$ tais que $\mathsf{n} = \mathsf{n}_1 x_i \mathsf{n}_2$ e $\alpha(\mathsf{n}_1) = 0$. Temos três possíveis casos:

Caso 1. Existem dois monômios m_1 e m_2 em $K\langle X\rangle$ tais que $\mathsf{m} = x_i \mathsf{m}_1 x_i \mathsf{m}_2$ e $\alpha(x_i \mathsf{m}_1) = 0$. Então existem três monômios n_3,n_4,n_5 em $K\langle X\rangle$ tais que $\mathsf{n} = \mathsf{n}_3 x_i \mathsf{n}_4 x_i \mathsf{n}_5$,$\alpha(\mathsf{n}_3) = 0$ e $\alpha(\mathsf{n}_3 x_i \mathsf{n}_4) = 0$.

Caso 2. Existem duas variáveis x_a e x_b, e seis monômios m_1,m_2,n_3,n_4,n_5, n_6 em $K\langle X\rangle$ tais que $\mathsf{m} = \mathsf{m}_1 x_a x_b \mathsf{m}_2$, $\mathsf{n} = \mathsf{n}_3 x_a \mathsf{n}_4 x_i \mathsf{n}_5 x_b \mathsf{n}_6$, $\mathsf{n}_1 = \mathsf{n}_3 x_a \mathsf{n}_4$, $\alpha(\mathsf{m}_1) = \alpha(\mathsf{n}_3)$ e $\alpha(\mathsf{m}_1 x_a) = \alpha(\mathsf{n}_3 x_a \mathsf{n}_4 x_i \mathsf{n}_5)$. Então um simples cálculo mostra-nos que $\alpha(\mathsf{n}_4 x_i \mathsf{n}_5) = 0$.

Caso 3. Nenhum dos casos 1 ou 2 ocorre. Considere $\mathsf{m} = x_{i_1} \ldots x_{i_q}$. Seja r um inteiro de $\{1, \ldots, q-1\}$ e sejam n_3,n_4,n_5,n_6 monômios de $K\langle X\rangle$ tais que $\mathsf{n}_1 = \mathsf{n}_3 x_{i_r} \mathsf{n}_4$, $\alpha(\mathsf{n}_3) = \alpha(x_{i_1} \ldots x_{i_{r-1}})$, $\mathsf{n} = \mathsf{n}_5 x_{i_{r+1}} \mathsf{n}_6$, $\alpha(\mathsf{n}_5) = \alpha(x_{i_1} \ldots x_{i_r})$. Então o comprimento de n_5 é menor que o comprimento de n_1, para que não ocorram os casos anteriores (se o comprimento de n_5 é igual ao comprimento de n_1 então ocorre o caso 1, se é maior ocorre o caso 2). Aplicando a mesma idéia a $r+1$, $r+2$, ..., concluímos que existe $r_0 \in \{1, \ldots, q\}$ tal que para $r \geq r_0$, todo x_{i_r} aparece em n_1 o mesmo número de vezes que em $x_{i_{r_0}} x_{i_{r_0+1}} \ldots x_{i_q}$, e toda variável de n_1 está em $x_{i_{r_0}} x_{i_{r_0+1}} \ldots x_{i_q}$. Logo n_1 e $x_{i_{r_0}} x_{i_{r_0+1}} \ldots x_{i_q}$ possuem o mesmo grau em cada variável. Sejam m_3, m_4, m_5 monômios de $K\langle X\rangle$ tais que $\mathsf{m} = \mathsf{m}_3 \mathsf{m}_4 x_j \mathsf{m}_5$ onde x_j é a primeira variável de n, $\alpha(\mathsf{m}_3 \mathsf{m}_4) = 0$ e $\mathsf{m}_4 x_j \mathsf{m}_5 = x_{i_{r_0}} x_{i_{r_0+1}} \ldots x_{i_q}$; portanto $\alpha(\mathsf{m}_4 x_j \mathsf{m}_5) = \alpha(x_{i_{r_0}} x_{i_{r_0+1}} \ldots x_{i_q}) = \alpha(\mathsf{n}_1) = 0$.

Trocando as letras m e n se ocorre o caso 3, podemos concluir que existem quatro monômios n_7, n_8, n_9, n_{10} em $K\langle X\rangle$ tais que $\mathsf{n} = \mathsf{n}_7\mathsf{n}_8 x_i \mathsf{n}_9\mathsf{n}_{10}$, $\alpha(\mathsf{n}_7\mathsf{n}_8) = 0$ e $\alpha(\mathsf{n}_8 x_i \mathsf{n}_9) = 0$. Definimos

$$\mathsf{w}(x_1,\ldots,x_k) = \begin{cases} x_i\mathsf{n}_9\mathsf{n}_7\mathsf{n}_8\mathsf{n}_{10} & \text{, se} \quad \alpha(\mathsf{n}_8) = 0, \\ x_i\mathsf{n}_9\mathsf{n}_8\mathsf{n}_7\mathsf{n}_{10} & \text{, se} \quad \alpha(\mathsf{n}_8) \neq 0. \end{cases}$$

Se $\alpha(\mathsf{n}_8) = 0$ então $\alpha(x_i\mathsf{n}_9) = 0$ e, usando a identidade $x_1x_2 = x_2x_1$ com $\alpha(x_1) = \alpha(x_2) = 0$, temos que $\mathsf{w}(x_1,\ldots,x_k) \equiv \mathsf{n}(x_1,\ldots,x_k)(\mathrm{mod} I)$. Por outro lado, se $\alpha(\mathsf{n}_8) \neq 0$ então $\alpha(\mathsf{n}_7) = \alpha(x_i\mathsf{n}_9) = -\alpha(\mathsf{n}_8)$ e, usando a identidade $x_1x_2x_3 = x_3x_2x_1$ com $\alpha(x_1) = -\alpha(x_2) = \alpha(x_3)$, temos que $\mathsf{w}(x_1,\ldots,x_k) \equiv \mathsf{n}(x_1,\ldots,x_k)(\mathrm{mod} I)$.

Como

$$\mathsf{w}(x_1,\ldots,x_k) - \mathsf{n}(x_1,\ldots,x_k) \in I \subseteq T_n(M_n(K)) = T_n(R),$$

temos que

$$\mathsf{w}(A_1,\ldots,A_k) = \mathsf{n}(A_1,\ldots,A_k) = \mathsf{m}(A_1,\ldots,A_k).$$

Se w_0 e m_0 são monômios de $K\langle X\rangle$ tais que $\mathsf{w} = x_i\mathsf{w}_0$ e $\mathsf{m} = x_i\mathsf{m}_0$ então usando o Lema 2.2.1 é fácil ver que $\mathsf{w}_0(A_1,\ldots,A_k) = \mathsf{m}_0(A_1,\ldots,A_k)$. Pela hipótese de indução, temos que $\mathsf{w}_0(x_1,\ldots,x_k) \equiv \mathsf{m}_0(x_1,\ldots,x_k)(\mathrm{mod} I)$, portanto $\mathsf{w}(x_1,\ldots,x_k) \equiv \mathsf{m}(x_1,\ldots,x_k)(\mathrm{mod} I)$. □

Teorema 2.2.1 *Todas as identidades polinomiais graduadas da álgebra $\mathbb{Z}_n$-graduada $M_n(K)$ seguem de*

$$x_1x_2 = x_2x_1, \quad \alpha(x_1) = \alpha(x_2) = 0,$$

e

$$x_1x_2x_3 = x_3x_2x_1, \quad \alpha(x_1) = -\alpha(x_2) = \alpha(x_3).$$

Demonstração. Pelo Lema 2.2.3, sabemos que $I \subseteq T_n(M_n(K))$. Por isso, basta mostrarmos a inclusão contrária. Como o corpo K é infinito, pelo Lema 2.2.1, precisamos apenas provar que qualquer identidade polinomial graduada multi-homogênea $f(x_1,\ldots,x_m) = 0$ de $M_n(K)$ pertence a I. Seja r o menor inteiro não-negativo para o qual o polinômio f pode ser expresso módulo I como uma combinação linear de r monômios multi-homogêneos:

$$f \equiv \sum_{q=1}^{r} a_q\mathsf{m}_q(\mathrm{mod} I)$$

onde $0 \neq a_q \in K$, m_1, m_2, $\ldots$, $\mathsf{m}_r \in K\langle X\rangle$. Mostraremos que $r = 0$. Suponhamos pelo contrário que $r > 0$. Pelo Lema 2.2.2, sabemos que $f \in T_n(F)$. Como

$$a_1\mathsf{m}_1(A_1,\ldots,A_m) = -\sum_{q=2}^{r} a_q\mathsf{m}_q(A_1,\ldots,A_m)$$

segue que existe $p \in \{2, 3, \ldots, r\}$ tal que $\mathsf{m}_1(A_1, \ldots, A_m)$ e $\mathsf{m}_p(A_1, \ldots, A_m)$ têm na primeira linha a mesma entrada não-nula. Então, pelo Lema 2.2.5, $\mathsf{m}_1 \equiv \mathsf{m}_p(\mathrm{mod} I)$ e

$$f \equiv (a_1 + a_p)\mathsf{m}_1 + \sum_{q=2}^{p-1} a_q \mathsf{m}_q + \sum_{q=p+1}^{r} a_q \mathsf{m}_q (\mathrm{mod} I).$$

Portanto f pode ser expresso módulo I como uma combinação linear de no máximo $r - 1$ monômios multi-homogêneos, o que contradiz nossa escolha do número r. $\square$

2.3 Identidades $\mathbb{Z}$-graduadas de $M_n(K)$

Ao tentar descrever as identidades $\mathbb{Z}_n$-graduadas da álgebra $M_n(K)$, Vasilovsky [47] encontrou uma base para as identidade $\mathbb{Z}$-graduadas dessa álgebra. Mais precisamente, ele provou que quando K é um corpo de característica 0 as identidades $\mathbb{Z}$-graduadas da álgebra $M_n(K)$ seguem de

$$\begin{aligned} x_1 &= 0, \quad |\alpha(x_1)| \geq n, \\ x_1 x_2 &= x_2 x_1, \quad \alpha(x_1) = \alpha(x_2) = 0, \\ x_1 x_2 x_3 &= x_3 x_2 x_1, \quad \alpha(x_1) = -\alpha(x_2) = \alpha(x_3). \end{aligned}$$

Esse resultado também pode ser generalizado para corpos infinitos [3].

Até o final desta seção, assumimos que K é um corpo infinito.

Para cada $\alpha \in \mathbb{Z}$, seja $M_n(K)_\alpha$ o subespaço de $M_n(K)$ gerado por todas as matrizes unidade e_{ij} tais que $j - i = \alpha$. Assim, $M_n(K)_0$ consiste das matrizes da forma

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}, \quad a_1, a_2, \ldots, a_n \in K;$$

para $1 \leq \alpha \leq n-1$, $M_n(K)_\alpha$ consiste das matrizes da forma

$$\begin{pmatrix} 0 & \cdots & 0 & a_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & a_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & a_{n-\alpha} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad a_1, a_2, \ldots, a_{n-\alpha} \in K$$

enquanto $M_n(K)_{-\alpha}$ consiste das matrizes da forma

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{n-\alpha} & 0 & \cdots & 0 \end{pmatrix}, \quad a_1, a_2, \ldots, a_{n-\alpha} \in K.$$

Finalmente $M_n(K)_\alpha = 0$ para $|\alpha| \geq n$. Como $e_{ij}e_{js} = e_{is}$ e $e_{ij}e_{rs} = 0$ se $j \neq r$, segue que $M_n(K)_\alpha M_n(K)_\beta \subseteq M_n(K)_{\alpha+\beta}$ para α e β em $\mathbb{Z}$; portanto a decomposição acima define uma $\mathbb{Z}$-graduação para a álgebra $M_n(K)$.

Seja $\Omega = K[y_i^{(k)} \mid i \in \mathbb{N}, 1 \leq k \leq n]$ a álgebra dos polinômios comutativos gerada pelas variáveis $y_i^{(k)}$. Se $0 \leq i \leq n-1$ então $M_n(\Omega)_\alpha$ consiste de todas as matrizes da forma

$$\begin{pmatrix} 0 & \cdots & 0 & f_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & f_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & f_{n-\alpha} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

com $f_1, \ldots, f_{n-\alpha} \in \Omega$, analogamente $M_n(\Omega)_{-\alpha}$ consiste das matrizes da forma

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ f_1 & 0 & \cdots & 0 & 0 & \cdots & \\ 0 & f_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & f_{n-\alpha} & 0 & \cdots & 0 \end{pmatrix}$$

com $f_1, \ldots, f_{n-\alpha} \in \Omega$, e se $|\alpha| \geq n$ então $M_n(\Omega)_\alpha = 0$. O próximo lema, cuja prova é de verificação direta, mostra que a decomposição acima define uma $\mathbb{Z}$-graduação para a álgebra $M_n(\Omega)$.

Lema 2.3.1 *Sejam*

$$A = \begin{pmatrix} 0 & \cdots & 0 & a_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & a_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & a_{n-i} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & \cdots & 0 & b_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & b_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & b_{n-j} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ c_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & c_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & c_{n-k} & 0 & \cdots & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & d_{n-l} & 0 & \cdots & 0 \end{pmatrix}$$

matrizes de $M_n(\Omega)$, *onde* $0 \leq i, j \leq n-1$ *e* $1 \leq k, l \leq n-1$.
(a) Se $i + j < n$ *então*

$$AB = \begin{pmatrix} 0 & \cdots & 0 & a_1 b_{i+1} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & a_2 b_{i+2} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & a_{n-i-j} b_{n-j} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

senão $AB = 0$;
(b) Se $i \geq k$ *então*

$$AC = \begin{pmatrix} 0 & \cdots & 0 & a_1 c_{i-k+1} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & a_2 c_{i-k+2} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & a_{n-i} c_{n-k} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

onde a_1c_{i-k+1} *está na* $(i-k+1)$*-ésima coluna e*

$$CA = \begin{pmatrix} 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & c_1a_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & c_2a_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & c_{n-i}a_{n-i} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

onde c_1a_1 *está na* $(k+1)$*-ésima linha.*

Senão

$$AC = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ a_{k-i+1}c_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_{k-i+2}c_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{n-i}c_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

onde $a_{k-i+1}c_1$ *está na* $(k-i+1)$*-ésima linha e*

$$CA = \begin{pmatrix} 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & c_1a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & c_2a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & c_{n-k}a_{n-k} & 0 & \cdots & 0 \end{pmatrix}$$

onde c_1a_1 *está na* $(i+1)$*-ésima coluna;*

(c) Se $k + l < n$ então

$$CD = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ c_{l+1}d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & c_{l+2}d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & c_{n-k}d_{n-k-l} & 0 & \cdots & 0 \end{pmatrix},$$

senão $CD = 0$.

Denote por F a subálgebra $\mathbb{Z}$-graduada de $M_n(\Omega)$ gerada pelas matrizes

$$A_i = \begin{pmatrix} 0 & \cdots & 0 & y_i^{(1)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & y_i^{(2)} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & y_i^{(n-\alpha(x_i))} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

quando $0 \leq \alpha(x_i) \leq n - 1$,

$$A_i = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ y_i^{(1)} & 0 & \cdots & 0 & 0 & \cdots & \\ 0 & y_i^{(2)} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & y_i^{(n+\alpha(x_i))} & 0 & \cdots & 0 \end{pmatrix}$$

quando $-n + 1 \leq \alpha(x_i) \leq -1$, e $A_i = 0$ quando $|\alpha(x_i)| \geq n$.

Lema 2.3.2 *A álgebra $\mathbb{Z}$-graduada relativamente livre $K\langle X\rangle/T_{\mathbb{Z}}(M_n(K))$ é isomorfa à álgebra F.*

Demonstração. A aplicação $\phi : K\langle X\rangle \to F$ definida por $\phi(f(x_1, \ldots, x_m)) = f(A_1, \ldots, A_m)$ é um homomorfismo $\mathbb{Z}$-graduado. Claramente, ϕ é sobrejetora. Além disso, um simples cálculo mostra que $\ker\phi = T_{\mathbb{Z}}(M_n(K))$ e ϕ induz um isomorfismo. □

Seja I o ideal das identidades $\mathbb{Z}$-graduadas de $K\langle X\rangle$ gerado pelas identidades graduadas

$$\begin{aligned} x_1 &= 0, \quad |\alpha(x_1)| \geq n, \\ x_1x_2 &= x_2x_1, \quad \alpha(x_1) = \alpha(x_2) = 0, \\ x_1x_2x_3 &= x_3x_2x_1, \quad \alpha(x_1) = -\alpha(x_2) = \alpha(x_3). \end{aligned}$$

Lema 2.3.3 *A álgebra $\mathbb{Z}$-graduada $M_n(K)$ satisfaz todas as identidades graduadas do $T_{\mathbb{Z}}$-ideal I.*

Demonstração. Como $M_n(K)_\alpha = 0$ quando $|\alpha| \geq n$, $M_n(K)$ satisfaz as identidades graduadas $x_1 = 0$ para $|\alpha(x_1)| \geq n$. Quaisquer duas matrizes diagonais comutam; portanto a identidade graduada $x_1x_2 = x_2x_1$ com $\alpha(x_1) = \alpha(x_2) = 0$ é válida em $M_n(K)$. Sendo multilineares as identidades $x_1x_2x_3 = x_3x_2x_1$ com $\alpha(x_1) = -\alpha(x_2) = \alpha(x_3)$, é suficiente mostrar que elas são válidas para $x_1 = e_{ij} \in M_n(K)_\alpha$, $x_3 = e_{kl} \in M_n(K)_\alpha$ e $x_2 = e_{rs} \in M_n(K)_{-\alpha}$, com $|\alpha| \leq n-1$. Note que $e_{ij}e_{rs}e_{kl} \neq 0$ se e somente se $j = r$ e $s = k$; em tal caso $i = j - \alpha = r - \alpha = s = k$ e $j = i + \alpha = k + \alpha = l$. Logo, $e_{ij}e_{rs}e_{kl} \neq 0$ se e somente se $i = s = k$ e $j = r = l$. Similarmente, temos que $e_{kl}e_{rs}e_{ij} \neq 0$ se e somente se $k = s = i$ e $l = r = j$. Portanto, se $e_{ij}e_{rs}e_{kl} \neq 0$ então $e_{ij}e_{rs}e_{kl} = e_{il} = e_{kj} = e_{kl}e_{rs}e_{ij}$, senão, $e_{ij}e_{rs}e_{kl} = 0 = e_{kl}e_{rs}e_{ij}$. □

Lema 2.3.4 *Para todo monômio $0 \neq \mathsf{m}(x_1, \ldots, x_m) \in K\langle X\rangle$ de comprimento q, existem inteiros $1 \leq i_1 \leq \cdots \leq i_q \leq m$ e $\{k_1, \ldots, k_q\} \subseteq \{1, \ldots, n\}$ tais que*
(i) se $|\alpha(\mathsf{m})| \geq n$ então $\mathsf{m}(A_1, \ldots, A_m) = 0$;
(ii) se $0 \leq \alpha(\mathsf{m}) \leq n-1$ então $\mathsf{m}(A_1, \ldots, A_m)$ é igual a

$$\begin{pmatrix} 0 & \cdots & 0 & y_{i_1}^{(k_1)} \cdots y_{i_q}^{(k_q)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & y_{i_1}^{(k_1+1)} \cdots y_{i_q}^{(k_q+1)} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & y_{i_1}^{(k_1+x)} \cdots y_{i_q}^{(k_q+x)} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

onde $x = n - \alpha(\mathsf{m}) - 1$;

(iii) se $-n+1 \leq \alpha(\mathsf{m}) \leq -1$ *então* $\mathsf{m}(A_1,\ldots,A_m)$ *é iqual a*

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ y_{i_1}^{(k_1)}\ldots y_{i_q}^{(k_q)} & 0 & \cdots & 0 & 0 & \cdots & \\ 0 & y_{i_1}^{(k_1+1)}\ldots y_{i_q}^{(k_q+1)} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & y_{i_1}^{(k_1+x)}\ldots y_{i_q}^{(k_q+x)} & 0 & \cdots & 0 \end{pmatrix}$$

onde $x = n+\alpha(\mathsf{m})-1$.

Demonstração. Usamos indução sobre q. Se $q=1$, obviamente temos o resultado. Se $q>1$, então existe um monômio $0 \neq \mathsf{n}(x_1,\ldots,x_m) \in K\langle X\rangle$ tal que $\mathsf{m}(x_1,\ldots,x_m) = \mathsf{n}(x_1,\ldots,x_m)x_i$, onde $1 \leq i \leq m$. Pela hipótese de indução e o Lema 2.3.1, podemos concluir a prova. $\square$

Lema 2.3.5 *Sejam* $\mathsf{m}(x_1,\ldots,x_m)$ *e* $\mathsf{n}(x_1,\ldots,x_m)$ *dois monômios de* $K\langle X\rangle$ *e suponha que* $|\alpha(\mathsf{m})| < n$. *Se as matrizes* $\mathsf{m}(A_1,\ldots,A_m)$ *e* $\mathsf{n}(A_1,\ldots,A_m)$ *têm na mesma posição a mesma entrada não-nula então* $\mathsf{m}(A_1,\ldots,A_m) \equiv \mathsf{n}(A_1,\ldots,A_m)(\mathrm{mod} I)$.

Demonstração. Se $\mathsf{m}(x_1,\ldots,x_m)$ e $\mathsf{n}(x_1,\ldots,x_m)$ têm na mesma posição a mesma entrada não-nula, vemos pelo Lema 2.3.4 que $\mathsf{m}(A_1,\ldots,A_m) = \mathsf{n}(A_1,\ldots,A_m)$. Seja q o comprimento de m. Usaremos indução sobre q. Se $q=1$, obviamente temos o resultado. Suponhamos então que $q>1$.

Suponhamos que x_p seja uma variável de $\mathsf{m}(x_1,\ldots,x_m)$ e m_1 e m_2 sejam dois monômios de $K\langle X\rangle$ tais que $\mathsf{m} = \mathsf{m}_1 x_p \mathsf{m}_2$. Denote $i=\alpha(\mathsf{m}_1)$, $j=\alpha(x_p)$ e $k=\alpha(\mathsf{m}_2)$. Suponhamos que $i \geq 0$, $j \geq 0$ e $k \geq 0$. Pelo Lema 2.3.4, sabemos que existem monômios $\omega_1,\ldots,\omega_{n-i},\eta_1,\ldots,\eta_{n-k}$ de Ω tais que

$$\mathsf{m}_1(A_1,\ldots,A_m) = \begin{pmatrix} 0 & \cdots & 0 & \omega_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_{n-i} \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

e

$$\mathsf{m}_2(A_1,\ldots,A_m)=\begin{pmatrix} 0 & \cdots & 0 & \eta_1 & 0 & \cdots & 0\\ 0 & \cdots & 0 & 0 & \eta_2 & \cdots & 0\\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & 0 & 0 & 0 & \cdots & \eta_{n-k}\\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0\\ \vdots & & \vdots & \vdots & \vdots & & \vdots\\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Pelo Lema 2.3.1, temos que $\mathsf{m}_1(A_1,\ldots,A_m)A_p$ é igual a

$$\begin{pmatrix} 0 & \cdots & 0 & \omega_1 y_p^{(i+1)} & \cdots & 0\\ \vdots & & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & 0 & 0 & \cdots & \omega_{n-i-j}y_p^{(n-j)}\\ 0 & \cdots & 0 & 0 & \cdots & 0\\ \vdots & & \vdots & \vdots & & \vdots\\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Logo a matriz $\mathsf{m}(A_1,\ldots,A_m)=\mathsf{m}_1(A_1,\ldots,A_m)A_p\mathsf{m}_2(A_1,\ldots,A_m)$ é igual a

$$\begin{pmatrix} 0 & \cdots & 0 & \omega_1 y_p^{(i+1)}\eta_{i+j+1} & \cdots & 0\\ \vdots & & \vdots & \vdots & \ddots & \vdots\\ 0 & \cdots & 0 & 0 & \cdots & \omega_{n-i-j-k}y_p^{(n-j-k)}\eta_{n-k}\\ 0 & \cdots & 0 & 0 & \cdots & 0\\ \vdots & \ddots & \vdots & \vdots & & \vdots\\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Assim, a variável $y_p^{(i+1)}$ aparece ao menos uma vez na primeira linha de $\mathsf{n}(A_1,\ldots,A_m)$. Aplicando o mesmo raciocínio para n, existem dois monômios n_1 e n_2 em $K\langle X\rangle$ tais que $\mathsf{n}=\mathsf{n}_1x_p\mathsf{n}_2$ e $\mathsf{n}_1(A_1,\ldots,A_m)$ têm grau i em F, porque senão a variável $y_p^{(i+1)}$ não apareceria na primeira linha de $\mathsf{n}(A_1,\ldots,A_m)$. Como $\mathsf{m}_1(A_1,\ldots,A_m)$ e $\mathsf{n}_1(A_1,\ldots,A_m)$ têm o mesmo grau em F, $\alpha(\mathsf{m}_1)=\alpha(\mathsf{n}_1)$. Portanto podemos concluir que se x_p é uma variável de $\mathsf{m}(x_1,\ldots,x_m)$ e $\mathsf{m}_1,\ldots,\mathsf{m}_l$ são monômios de $K\langle X\rangle$ tais que $\mathsf{m}=\mathsf{m}_1x_p\mathsf{m}_2x_p\mathsf{m}_3\ldots\mathsf{m}_{l-1}x_p\mathsf{m}_l$, então existem monômios $\mathsf{n}_1,\ldots,\mathsf{n}_l$ em $K\langle X\rangle$ e uma bijeção $\varphi:\{1,\ldots,l\}\to\{1,\ldots,l\}$ tais que $\mathsf{n}=\mathsf{n}_1x_p\mathsf{n}_2x_p\mathsf{n}_3\ldots\mathsf{n}_{l-1}x_p\mathsf{n}_l$ e $\alpha(\mathsf{m}_1x_p\mathsf{m}_2\ldots\mathsf{m}_t)=\alpha(\mathsf{n}_1x_p\mathsf{n}_2\ldots\mathsf{n}_{\varphi(t)})$. Pelo mesmo raciocínio, temos que a última afirmação é verdadeira quando $i<0$, $j<0$ ou $k<0$. De fato, temos que analisar mais sete casos, mas eles são tratados do mesmo modo.

Seja x_i a primeira variável de m. Logo existem dois monômios n_1 e n_2 de $K\langle X\rangle$ tais que $\mathsf{n} = \mathsf{n}_1 x_i \mathsf{n}_2$ e $\alpha(\mathsf{n}_1) = 0$. Temos três possíveis casos:

Caso 1. Existem dois monômios m_1 e m_2 em $K\langle X\rangle$ tais que $\mathsf{m} = x_i \mathsf{m}_1 x_i \mathsf{m}_2$ e $\alpha(x_i \mathsf{m}_1) = 0$. Então existem três monômios $\mathsf{n}_3, \mathsf{n}_4, \mathsf{n}_5$ em $K\langle X\rangle$ tais que $\mathsf{n} = \mathsf{n}_3 x_i \mathsf{n}_4 x_i \mathsf{n}_5$, $\alpha(\mathsf{n}_3) = 0$ e $\alpha(\mathsf{n}_3 x_i \mathsf{n}_4) = 0$.

Caso 2. Existem duas variáveis x_a e x_b, e seis monômios m_1, m_2, n_3, n_4, n_5, n_6 em $K\langle X\rangle$ tais que $\mathsf{m} = \mathsf{m}_1 x_a x_b \mathsf{m}_2$, $\mathsf{n} = \mathsf{n}_3 x_a \mathsf{n}_4 x_i \mathsf{n}_5 x_b \mathsf{n}_6$, $\mathsf{n}_1 = \mathsf{n}_3 x_a \mathsf{n}_4$, $\alpha(\mathsf{m}_1) = \alpha(\mathsf{n}_3)$ e $\alpha(\mathsf{m}_1 x_a) = \alpha(\mathsf{n}_3 x_a \mathsf{n}_4 x_i \mathsf{n}_5)$. Então um cálculo fácil mostra que $\alpha(\mathsf{n}_4 x_i \mathsf{n}_5) = 0$.

Caso 3. Os casos 1 e 2 não ocorrem. Considere $\mathsf{m} = x_{i_1} \dots x_{i_q}$. Sejam r um inteiro do conjunto $\{1, \dots, q-1\}$ e n_3, n_4, n_5, n_6 monômios de $K\langle X\rangle$ tais que $\mathsf{n}_1 = \mathsf{n}_3 x_{i_r} \mathsf{n}_4$, $\alpha(\mathsf{n}_3) = \alpha(x_{i_1} \dots x_{i_{r-1}})$, $\mathsf{n} = \mathsf{n}_5 x_{i_{r+1}} \mathsf{n}_6$, $\alpha(\mathsf{n}_5) = \alpha(x_{i_1} \dots x_{i_r})$. Então o comprimento de n_5 é menor que o comprimento de n_1, para que os casos prévios não ocorram (se o comprimento de n_5 é igual ao comprimento de n_1 então caímos no caso 1, se é maior caímos no caso 2). Concluímos que existe $r_0 \in \{1, \dots, q\}$ tal que os monômios n_1 e $x_{i_{r_0}} x_{i_{r_0+1}} \dots x_{i_q}$ possuem o mesmo grau em cada variável. Sejam m_3, m_4, m_5 monômios de $K\langle X\rangle$ tais que $\mathsf{m} = \mathsf{m}_3 \mathsf{m}_4 x_j \mathsf{m}_5$ onde x_j é a primeira variável de n, $\alpha(\mathsf{m}_3 \mathsf{m}_4) = 0$ e $\mathsf{m}_4 x_j \mathsf{m}_5 = x_{i_{r_0}} x_{i_{r_0+1}} \dots x_{i_q}$; portanto $\alpha(\mathsf{m}_4 x_j \mathsf{m}_5) = \alpha(x_{i_{r_0}} x_{i_{r_0+1}} \dots x_{i_q}) = \alpha(\mathsf{n}_1) = 0$.

Trocando as letras m e n se tivermos o caso 3, podemos concluir que existem quatro monômios n_7, n_8, n_9, n_{10} em $K\langle X\rangle$ tais que $\mathsf{n} = \mathsf{n}_7 \mathsf{n}_8 x_i \mathsf{n}_9 \mathsf{n}_{10}$, $\alpha(\mathsf{n}_7 \mathsf{n}_8) = 0$ e $\alpha(\mathsf{n}_8 x_i \mathsf{n}_9) = 0$. Definiremos

$$\mathsf{w}(x_1, \dots, x_k) = \begin{cases} x_i \mathsf{n}_9 \mathsf{n}_7 \mathsf{n}_8 \mathsf{n}_{10} & \text{se} \quad \alpha(\mathsf{n}_8) = 0, \\ x_i \mathsf{n}_9 \mathsf{n}_8 \mathsf{n}_7 \mathsf{n}_{10} & \text{se} \quad \alpha(\mathsf{n}_8) \neq 0. \end{cases}$$

Se $\alpha(\mathsf{n}_8) = 0$ então $\alpha(x_i \mathsf{n}_9) = 0$ e, usando a identidade $x_1 x_2 = x_2 x_1$ com $\alpha(x_1) = \alpha(x_2) = 0$, temos $\mathsf{w}(x_1, \dots, x_m) \equiv \mathsf{n}(x_1, \dots, x_m)(\text{mod} I)$. Por outro lado, se $\alpha(\mathsf{n}_8) \neq 0$ então $\alpha(\mathsf{n}_7) = \alpha(x_i \mathsf{n}_9) = -\alpha(\mathsf{n}_8)$ e, usando a identidade $x_1 x_2 x_3 = x_3 x_2 x_1$ com $\alpha(x_1) = -\alpha(x_2) = \alpha(x_3)$, neste caso temos que $\mathsf{w}(x_1, \dots, x_m) \equiv \mathsf{n}(x_1, \dots, x_m)(\text{mod } I)$.

Como $\mathsf{w}(x_1, \dots, x_m) - \mathsf{n}(x_1, \dots, x_m) \in I \subseteq T_{\mathbb{Z}}(M_n(K)) = T_{\mathbb{Z}}(F)$, temos que $\mathsf{w}(A_1, \dots, A_m) = \mathsf{n}(A_1, \dots, A_m) = \mathsf{m}(A_1, \dots, A_m)$. Se w_0 e m_0 são monômios de $K\langle X\rangle$ tais que $\mathsf{w} = x_i \mathsf{w}_0$ e $\mathsf{m} = x_i \mathsf{m}_0$, então usando o Lema 2.3.1 é fácil ver que $\mathsf{w}_0(A_1, \dots, A_m) = \mathsf{m}_0(A_1, \dots, A_m)$. Pela hipótese de indução, $\mathsf{w}_0(x_1, \dots, x_m) \equiv \mathsf{m}_0(x_1, \dots, x_m)(\text{mod} I)$, portanto $\mathsf{w}(x_1, \dots, x_m) \equiv \mathsf{m}(x_1, \dots, x_m)(\text{mod} I)$. $\square$

Teorema 2.3.1 *Todas as identidades polinomiais graduadas da álgebra $\mathbb{Z}$-graduada $M_n(K)$ seguem de*

$$\begin{aligned} x_1 &= 0, \quad |\alpha(x_1)| \geq 0, \\ x_1 x_2 &= x_2 x_1, \quad \alpha(x_1) = \alpha(x_2) = 0, \\ x_1 x_2 x_3 &= x_3 x_2 x_1, \quad \alpha(x_1) = -\alpha(x_2) = \alpha(x_3). \end{aligned}$$

Demonstração. Pelo Lema 2.3.3, sabemos que $I \subseteq T_{\mathbb{Z}}(M_n(K))$. Por isso, basta mostrarmos a inclusão contrária. Como o corpo K é infinito, pelo Lema 1.4.1, precisamos apenas provar que qualquer identidade polinomial graduada multi-homogênea $f(x_1, \dots, x_m) = 0$ de $M_n(K)$ pertence a I. Seja r o menor inteiro não-negativo para o qual o polinômio f pode ser expresso módulo I como uma combinação linear de r monômios multi-homogêneos:

$$f \equiv \sum_{q=1}^{r} a_q \mathsf{m}_q (\mathrm{mod} I)$$

onde $0 \neq a_q \in K$, $\mathsf{m}_1, \mathsf{m}_2, \dots, \mathsf{m}_r \in K\langle X \rangle$; observe que $|\alpha(\mathsf{m}_i)| < n$ para todo $i \in \{1, \dots, r\}$, pois senão $\mathsf{m}_i \in I$. Mostraremos que $r = 0$. Suponhamos pelo contrário que $r > 0$. Pelo Lema 2.3.2, sabemos que $f \in T_{\mathbb{Z}}(F)$. Como

$$a_1 \mathsf{m}_1(A_1, \dots, A_m) = -\sum_{q=2}^{r} a_q \mathsf{m}_q(A_1, \dots, A_m)$$

segue que existe $p \in \{2, 3, \dots, r\}$ tal que $\mathsf{m}_1(A_1, \dots, A_m)$ e $\mathsf{m}_p(A_1, \dots, A_m)$ têm na mesma posição a mesma entrada não-nula. Então, pelo Lema 2.3.5, $\mathsf{m}_1 \equiv \mathsf{m}_p (\mathrm{mod} I)$ e

$$f \equiv (a_1 + a_p)\mathsf{m}_1 + \sum_{q=2}^{p-1} a_q \mathsf{m}_q + \sum_{q=p+1}^{r} a_q \mathsf{m}_q (\mathrm{mod} I).$$

Portanto f pode ser expresso módulo I como uma combinação linear de no máximo $r - 1$ monômios multi-homogêneos, o que contradiz nossa escolha do número r. □

Capítulo 3

Matrizes 2×2 sobre corpos finitos

3.1 Introdução

Ao longo de todo este capítulo, assumimos que K é um corpo finito com q elementos e característica $p \neq 2$, ou seja, $K = GF(q)$ e $q = p^n$. Por conveniência, identificaremos o corpo K com o centro da álgebra $M_2(K)$.

Maltsev e Kuzmin [35] provaram que todas as identidades polinomiais da álgebra $M_n(K)$ seguem de duas identidades, a saber

$$(x_1 - x_1^q)(x_2 - x_2^{q^2})(1 - [x_1, x_2]^{q-1}) = 0,$$

e

$$(x_1 - x_1^q) \cdot (x_2 - x_2^q) - [(x_1 - x_1^q) \cdot (x_2 - x_2^q)]^q = 0,$$

onde $x_1 \cdot x_2 = x_1x_2 + x_2x_1$. As técnicas utilizadas para tratar o caso de matrizes sobre corpos finitos são completamente diferentes daquelas empregadas para o caso de corpos infinitos, devido sobretudo ao fato de que no primeiro caso não podemos restringir-nos ao estudo de polinômios multi-homogêneos. Foi mencionado no primeiro capítulo que o interesse no estudo de identidades graduadas é que elas podem nos fornecer informações interessantes acerca das identidades ordinárias que são o nosso principal objeto de estudo. No entanto, no caso das matrizes de ordem 2 sobre corpos finitos, embora já seja conhecida uma base para as identidades ordinárias, é interessante estudar suas identidades graduadas por vários motivos. O artigo [30] é um estudo sobre todas as possíveis $\mathbb{Z}_2$-graduações de $M_n(K)$ e suas identidades graduadas. Um dos resultados interessantes é que além da graduação trivial, existem apenas mais duas $\mathbb{Z}_2$-graduações que podem ser distingüidas através de identidades graduadas.

Nas próximas seções apresentaremos os resultados de [30], que estão baseados principalmente no trabalho de Maltsev e Kuzmin [35] para identidades ordinárias e no artigo de Wall [49] para álgebras $\mathbb{Z}_2$-graduadas.

3.2 Graduações para a álgebra das matrizes 2×2

Fixemos duas graduações não-triviais em $M_2(K)$. A primeira será denotada por Ω e defina como

$$\Omega_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in K \right\} \quad \text{e} \quad \Omega_1 = \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \mid b, c \in K \right\}.$$

A segunda será denotada por Ω^α, onde $0 \neq \alpha \in K$, e definida como

$$\Omega_0^\alpha = \left\{ \begin{pmatrix} a & d \\ \alpha d & a \end{pmatrix} \mid a, d \in K \right\} \quad \text{e} \quad \Omega_1^\alpha = \left\{ \begin{pmatrix} b & c \\ -\alpha c & -b \end{pmatrix} \mid b, c \in K \right\}.$$

Lema 3.2.1 *Seja $A = A_0 \oplus A_1$ uma graduação para $M_2(K)$. Então:*
(i) existe um elemento invertível u_A em $M_2(K)$ tal que $u_A^2 \in K$,

$$A_0 = \{a \in A \mid au_A = u_A a\} \text{ e } A_1 = \{a \in A \mid au_A = -u_A a\};$$

(ii) $u_A^q = u_A$ ou $u_A^q = -u_A$, onde $q = |K|$;
(iii) se $B = B_0 \oplus B_1$ é uma graduação de $M_2(K)$ e existe uma matriz invertível P em $M_2(K)$ tal que $P^{-1} u_A P = u_B$ então a aplicação $\phi \colon A \to B$ definida por $\phi(x) = P^{-1} x P$ é um isomorfismo graduado.

Demonstração. Como $M_2(K)$ é uma álgebra (não-graduada) simples e central, então A é uma álgebra graduada simples e central. Pelo Lema 6 de [49], sabemos que existe $u_A \in A$ tal que $A_0 = \{a \in A \mid au_A = u_A a\}$, $A_1 = \{a \in A \mid au_A = -u_A a\}$ e $0 \neq u_A^2 \in K$. Além disso, $u_A^q = u_A$ ou $u_A^q = -u_A$; para $u_A^q = (u_A^2)^{(q-1)/2} u_A = (\alpha I)^{(q-1)/2} u_A = \pm u_A$ onde I é a matriz identidade.

A terceira afirmação segue facilmente do fato que $B_0 = \{b \in B \mid b\phi(u_A) = \phi(u_A) b\}$ e $B_1 = \{b \in B \mid b\phi(u_A) = -\phi(u_A) b\}$. Então observe que se $a \in A_0$ então

$$\phi(a)\phi(u_A) = \phi(au_A) = \phi(u_A a) = \phi(u_A)\phi(a),$$

logo $\phi(a) \in B_0$. Similarmente, se $a \in A_1$ então

$$\phi(a)\phi(u_A) = \phi(au_A) = -\phi(u_A a) = -\phi(u_A)\phi(a),$$

portanto $\phi(a) \in B_1$. $\square$

Observação Para as graduações Ω e Ω^α podem-se escolher elementos

$$u_\Omega = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ e } u_{\Omega^\alpha} = \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix}$$

respectivamente. Para a graduação trivial T, o elemento u_T pode ser escolhido como a matriz identidade.

Agora estamos preparados para mostrar que existem apenas duas graduações não-triviais para $M_2(K)$ (a menos de isomorfismos graduados). Mais precisamente, quando $A = A_0 \oplus A_1$ é uma graduação para $M_2(K)$, se $u_A^q = u_A$ então A é isomorfa a Ω^α para algum quadrado perfeito $0 \neq \alpha \in K$, senão A é isomorfa a Ω^α para qualquer $\alpha \in K$ que não é quadrado perfeito. Além disso, quando $\alpha \neq 0$ é um quadrado perfeito em K então as graduações Ω e Ω^α são isomorfas. Provaremos esses fatos nos próximos lemas.

Lema 3.2.2 *Toda graduação não-trivial $A = A_0 \oplus A_1$ de $M_2(K)$ tal que $u_A^q = u_A$ é isomorfa a Ω.*

Demonstração. Se $u_A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ então $u_A^2 = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix}$. Portanto, como $u_A^2 \in K$, temos que $b = c = 0$ ou $a = -d$. No primeiro caso $A_0 = M_2(K)$ e $A_1 = 0$, o que é uma contradição. Então $a = -d$. O polinômio característico de u_A é $f(x) = x^2 - (a^2+bc)$ cujas raízes são $\pm\lambda$ onde $\lambda = \sqrt{a^2+bc}$. Mas $u_A^2 \neq 0$ implica que $a^2 + bc \neq 0$. Logo existe uma matriz invertível $P \in M_2(GF(q^2))$ tal que $P^{-1}u_AP = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix}$. Assim

$$\begin{pmatrix} \lambda^q & 0 \\ 0 & (-\lambda)^q \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix}^q = (P^{-1}u_AP)^q = P^{-1}u_A^qP = P^{-1}u_AP = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix}.$$

Portanto $\lambda^q = \lambda \in GF(q)$, $P \in M_2(K)$ e a aplicação $\phi : A \to \Omega$ definida por $\phi(x) = P^{-1}xP$ é um isomorfismo graduado. $\square$

Observação Se $\alpha \neq 0$ é um quadrado perfeito em K então $u_{\Omega^\alpha}^q = u_{\Omega^\alpha}$. Por exemplo, quando $\alpha = 1$ temos a graduação Ω^1 onde $u_{\Omega^1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Seus autovalores são -1 e 1. Portanto, existe uma matriz invertível $P \in M_2(GF(q))$ tal que $P^{-1}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}P = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Logo $P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ e $P^{-1} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix}$. O isomorfismo graduado $\phi : \Omega^1 \to \Omega$ tal que $\phi(x) = P^{-1}xP$ é o seguinte:

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \frac{1}{2}\begin{pmatrix} a+b+c+d & a-b+c-d \\ a+b-c-d & a-b-c+d \end{pmatrix}.$$

Corolário 3.2.1 *Toda graduação de $M_2(K)$ que satisfaz a identidade $y_1^q = y_1$ é isomorfa a Ω.*

Lema 3.2.3 *Toda graduação não-trivial $A = A_0 \oplus A_1$ de $M_2(K)$ tal que $u_A^q = -u_A$ é isomorfa a Ω^α, para algum $\alpha \in K$ que não é um quadrado perfeito.*

Demonstração. Se $u_A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ então $u_A^2 = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix}$. Portanto, $b = c = 0$ ou $a = -d$. Se $b = c = 0$ obtemos a graduação trivial, assim $a = -d$. O polinômio característico de u_A é $f(x) = x^2 - (a^2+bc)$ cujas raízes são $\pm\lambda$ onde $\lambda = \sqrt{a^2+bc}$. Como $u_A^2 \neq 0$, temos que $a^2+bc \neq 0$. Além disso, $\lambda \notin K$, pois $u_A^q \neq u_A$; ou seja, a^2+bc não é um quadrado perfeito em K. Como α e a^2+bc não são quadrados perfeitos em K então $\alpha(a^2+bc)$ é um quadrado perfeito em K, pois K^* é um grupo cíclico. Escolha $\beta \in K$ tal que $\beta^2 = \alpha(a^2+bc)$, e considere a matriz $u'_A = \frac{\alpha}{\beta}\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$. Seu polinômio característico é $f(x) = x^2 - \alpha$ cujas raízes são $\sqrt{\alpha}$ e $-\sqrt{\alpha}$, e existe uma matriz invertível $P \in M_2(K(\sqrt{\alpha}))$ tal que $P^{-1}u'_AP = \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{pmatrix}$. Mas o polinômio característico de u_{Ω^α} é também $f(x) = x^2 - \alpha$, e para alguma matriz invertível $Q \in M_2(K(\sqrt{\alpha}))$ temos que $Q^{-1}u_{\Omega^\alpha}Q = \begin{pmatrix} \sqrt{\alpha} & 0 \\ 0 & -\sqrt{\alpha} \end{pmatrix}$. Assim $(PQ^{-1})^{-1}u'_APQ^{-1} = u_{\Omega^\alpha}$ e a aplicação $\phi : A \to \Omega^\alpha$, definida por $\phi(x) = P^{-1}xP$, é um isomorfismo graduado. □

Observação Se α não é um quadrado perfeito em K então $u_{\Omega^\alpha}^q = -u_{\Omega^\alpha}$. Assim, para $K = \mathbb{Z}_3$ e $\alpha = -1$, obtemos a graduação

$$\Omega_0^{-1} = \left\{ \begin{pmatrix} a & d \\ -d & a \end{pmatrix} \mid a, d \in K \right\} \text{ e } \Omega_1^{-1} = \left\{ \begin{pmatrix} b & c \\ c & -b \end{pmatrix} \mid b, c \in K \right\}$$

onde $u_{\Omega^{-1}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Além disso, $u_{\Omega^{-1}}^3 = -u_{\Omega^{-1}}$ porque -1 não é um quadrado perfeito em $\mathbb{Z}_3$.

3.3 Irredutibilidade subdireta

Definiremos irredutibilidade subdireta para álgebras do mesmo modo que é feito para anéis (veja por exemplo o livro de Herstein [19], pp. 52–53).

Definição O *produto direto* das álgebras A_i, para i em algum conjunto de índices I, é o conjunto

$$\Pi_{i\in I}A_i = \{f : I \to \cup_{i\in I}A_i \mid f(i) \in A_i \text{ para todo } i \in I\}.$$

Estabelecemos nele uma estrutura de álgebra, definindo as operações $(f+g)(i) = f(i)+g(i)$, $(fg)(i) = f(i)g(i)$ e $(\alpha f)(i) = \alpha f(i)$.

Definição Seja π_i a projeção de $\Pi_{i\in I}A_i$ em A_i. Uma álgebra A é chamada uma *soma subdireta* das álgebras $\{A_i\}_{i\in I}$ se existe um monomorfismo $\phi : A \to \Pi_{i\in I}A_i$ tal que

$$(\pi_i \circ \phi)(A) = A_i$$

para cada $i \in I$.

Lema 3.3.1 *Uma álgebra A é a soma subdireta das álgebras $\{A_i\}_{i\in I}$ se, e somente se, existem epimorfismos $\phi_i : A \to A_i$ tais que $\cap_{i\in I} \ker \phi_i = 0$.*

Demonstração. Suponha que A seja uma soma subdireta, ou seja, existe um monomorfismo $\phi : A \to \Pi_{i\in I}A_i$ tal que $(\pi_i \circ \phi)(A) = A_i$ para cada $i \in I$. Considere os epimorfismos $\phi_i = \pi_i \circ \phi$. Observe que

$$\begin{aligned} \cap_{j\in I} \ker \pi_j &= \cap_{j\in I}\{f \in \Pi_{i\in I}A_i \mid f(j) = 0\} = \\ &= \{f \in \Pi_{i\in I}A_i \mid f(j) = 0 \text{ para todo } j \in I\} = 0 \end{aligned}$$

e

$$\begin{aligned} \cap_{i\in I} \ker \phi_i &= \cap_{i\in I} \ker(\pi_i \circ \phi) = \cap_{i\in I}\{a \in A \mid \phi(a) \in \ker \pi_i\} = \\ &= \{a \in A \mid \phi(a) \in \cap_{i\in I} \ker \pi_i\} = \\ &= \{a \in A \mid \phi(a) = 0\} = \ker \phi = 0. \end{aligned}$$

Suponha agora que existem epimorfismos $\phi_i : A \to A_i$ tais que $\cap_{i\in I} \ker \phi_i = 0$. Para cada $a \in A$, definimos $f_a : I \to \cup_{i\in I}A_i$ como $f_a(i) = \phi_i(a)$. Claramente, $f_a \in \Pi_{i\in I}A_i$, e $\phi : A \to \Pi_{i\in I}A_i$, definido por $\phi(a) = f_a$, é um homomorfismo. Além disso, $(\pi_i \circ \phi)(A) = A_i$ e

$$\ker \phi = \{a \in A \mid f_a = 0\} = \{a \in A \mid \phi_i(a) = 0 \text{ para todo } i \in I\} = \cap_{i\in I} \ker \phi_i = 0.$$

Portanto, A é uma soma subdireta das álgebras $\{A_i\}_{i\in I}$. □

Definição Uma álgebra A é *subdiretamente irredutível* se a interseção de todos os seus ideais não-nulos não é zero.

Lema 3.3.2 *Se A é uma K-álgebra graduada e finita então existe um conjunto $\mathfrak{A}$ de álgebras graduadas finitas e subdiretamente irredutíveis tal que $VarA = Var\mathfrak{A}$.*

Demonstração. Para $0 \neq a \in A$, seja I_a um ideal graduado de A maximal com relação à exclusão de a. (Segundo o Lema de Zorn tal I_a existe. Ressaltamos que A é finita, portanto a mesma conclusão pode ser obtida sem o uso do lema de Zorn.) As projeções $\pi_a : A \to A/I_a$ são epimorfismos graduados e $\cap_{0 \neq a \in A} \ker \pi_a = \cap_{a \in A} I_a = 0$. Logo A é uma soma subdireta das álgebras A/I_a. Como $a + I_a$ não é zero e pertence a todo ideal não-nulo de A/I_a, então A/I_a é subdiretamente irredutível. Seja $\mathfrak{A}$ o conjunto das álgebras graduadas A/I_a.

Suponha que $a \in A$; então obviamente $T_2(A) \subseteq T_2(A/I_a)$. Se o polinômio $f(y_1, \ldots, y_m, z_1, \ldots, z_n)$ pertence a $T_2(A/I_a)$ então $f(a_1, \ldots, a_m, b_1, \ldots, b_n) \in \ker \pi_a$ para quaisquer $a \in A$, $a_1, \ldots, a_m \in A_0$, $b_1, \ldots, b_n \in A_1$. Logo $f \in \cap_{a \in \Omega} T_2(A/I_a)$. □

O próximo lema é análogo ao resultado 2.2 de [33].

Lema 3.3.3 *Toda variedade de álgebras graduadas é gerada por suas álgebras finitamente geradas.*

Definição O *expoente* de uma variedade de álgebras graduadas $\mathfrak{V}$ é o maior limitante inferior do conjunto de todos os inteiros positivos r tais que $ra = 0$ para todo elemento a pertencente a qualquer algebra de $\mathfrak{V}$. O *índice* de $\mathfrak{V}$ é o menor limitante superior do conjunto de todos os índices de nilpotência de suas álgebras nilpotentes. Uma variedade de álgebras graduadas é *localmente finita* se suas álgebras finitamente geradas são finitas.

O próximo lema é análogo ao Corolário 2.9 de [34].

Lema 3.3.4 *Uma variedade de álgebras graduadas com índice e expoente finitos é localmente finita.*

Teorema 3.3.1 *Uma variedade $\mathfrak{V}$ de álgebras graduadas com índice e expoente finitos é gerada por um conjunto de álgebras graduadas finitas e subdiretamente irredutíveis.*

Demonstração. De acordo com os dois lemas anteriores, $\mathfrak{V}$ é gerada por um conjunto de álgebras graduadas finitas. Logo $\mathfrak{V}$ é gerada por um conjunto de álgebras graduadas finitas e subdiretamente irredutíveis. □

3.4 Identidades graduadas de Ω

Considere os dois polinômios de $K\langle X \rangle$, que são $f_1(y_1) = y_1^q - y_1$ e

$f_2(y_1, y_2, z_1, z_2) = (y_1 + z_1 - (y_1 + z_1)^q)(y_2 + z_2 - (y_2 + z_2)^{q^2})(1 - [y_1 + z_1, y_2 + z_2]^{q-1})$.

O próximo teorema fornece uma base para as identidades graduadas de Ω.

Teorema 3.4.1 *Todas as identidades polinomiais graduadas de Ω seguem de $f_1 = 0$ e $f_2 = 0$.*

A prova desse teorema, que está baseada na demonstração do teorema de Maltsev e Kuzmin [35] para identidades polinomiais ordinárias, será dada pelos próximos dois lemas. Denotemos por $\mathfrak{V}$ a variedade das álgebras graduadas que satisfazem as identidades $f_1 = 0$ e $f_2 = 0$.

Lema 3.4.1 $Var\Omega \subseteq \mathfrak{V}$.

Demonstração. Como $a^q = a$ para todo $a \in K$ então $f_1 = 0$ é uma identidade graduada de Ω. Por [35], sabemos que $(x_1 - x_1^q)(x_2 - x_2^{q^2})(1 - [x_1, x_2]^{q-1}) = 0$ é uma identidades polinomial de $M_2(K)$. Portanto, $f_2 = 0$ é uma identidade graduada de Ω. $\square$

Lema 3.4.2 $\mathfrak{V} \subseteq Var\Omega$.

Demonstração. Seja $N = N_0 \oplus N_1$ uma álgebra nilpotente de $\mathfrak{V}$. Então N_0 é também uma álgebra nilpotente de $\mathfrak{V}$. O índice de nilpotência s de N_0 é 2; pois se $s > 2$, podemos tomar elementos $a_1, \ldots, a_{s-1} \in N_0$ tais que $a_1 \ldots a_{s-1} \neq 0$. Pela identidade $f_1 = 0$, sabemos que $0 = (a_1 \ldots a_{s-1})^q - a_1 \ldots a_{s-1} = a_1 \ldots a_{s-1}$, o que é uma contradição. Assim se $a \in N_0$ então $a = a^q = 0$. Portanto, $N_0 = 0$ e $N = N_1$. Além disso, como $N_1 N_1 \subseteq N_0 = 0$, temos que $N^2 = 0$.

A variedade $\mathfrak{V}$ tem índice e exponente finitos. Pelo Teorema 3.3.1, $\mathfrak{V}$ é gerada por um conjunto de álgebras graduadas finitas e subdiretamente irredutíveis. Para provar o lema, é suficiente mostrar que cada uma dessas álgebras pertence a $Var\Omega$. Provaremos ainda mais: cada uma delas é isomorficamente mergulhada em Ω. Até o final da prova, assumiremos que A é uma álgebra finita e subdiretamente irredutível de $\mathfrak{V}$.

Se a álgebra A é nilpotente então $A_0 = 0$, $A_1 = A$, $A^2 = 0$ e $\dim_K A = 1$; pois se a_1, $a_2 \in A$ fossem linearmente independentes, os subespaços gerados por a_1 e a_2 seriam ideais com interseção nula. Assim a aplicação $\phi\colon A \to \Omega$ definida por $\phi(\alpha g) = \alpha e_{12}$ é um monomorfismo graduado, onde g é um gerador de A.

Suponhamos agora que A seja uma álgebra não-graduada simples, ou seja, $A = M_k(GF(p^t))$ e $p^t \geq q$. Se $k \geq 3$ então $f_2(a_0, b_0, a_1, b_1) = e_{13} \neq 0$ onde $a_0, b_0 \in A_0$ e $a_1, b_1 \in A_1$ são tais que $e_{12} = a_0 + a_1$ e $e_{23} = b_0 + b_1$.

Logo $k \leq 2$. Seja $k = 2$. Se $a_0, b_0 \in A_0$ e $a_1, b_1 \in A_1$ são tais que $\alpha e_{11} = a_0 + a_1$ e $e_{12} = b_0 + b_1$, então $f_2(a_0, b_0, a_1, b_1) = (\alpha^q - \alpha)e_{12} = 0$. Logo $\alpha - \alpha^q = 0$, $q \geq p^t$ e $A = M_2(GF(q))$. Pelo Corolário 3.2.1, temos que Ω e A são isomorfas.

Vamos considerar agora $k = 1$, ou seja, $A = GF(p^t)$. Se $0 \neq a \in A_1$ então

$$a^{q^2} = (a^2)^{(q+1)(q-1)/2} a = (a^2 a^2)^{(q-1)/2} a = (a^2)^{q-1} a = a^{2q} a^{-2} a = a^2 a^{-2} a = a.$$

Se $a_0 \in A_0$ e $a_1 \in A_1$, então $(a_0+a_1)^{q^2} = a_0^{q^2}+a_1^{q^2} = a_0+a_1$. Portanto, $\alpha^{q^2}-\alpha = 0$ para qualquer $\alpha \in A$, donde $q^2 \geq p^t$, $A = GF(q)$ ou $A = GF(q^2)$. Se $A = GF(q)$ então existe um homomorfismo graduado injetor de A em Ω. Se $A = GF(q^2)$ então a única graduação possível é $A_0 \cong GF(q)$ e $A_1 \cong GF(q)$ e, pelo Lema 5 de [49], existe $u \in A_1$ tal que $A_1 = A_0u$ e $u^2 = a \neq 0$ pertence a $GF(q)$. Logo, $A = GF(q)\mathbf{1} + GF(q)u$ onde $\mathbf{1}$ é a identidade multiplicativa de A. Assim a aplicação $\phi : A \to \Omega$ definida como

$$\phi(\alpha\mathbf{1} + \beta u) = \begin{pmatrix} \alpha & \beta a \\ \beta & \alpha \end{pmatrix}$$

é um homomorfismo graduado e injetor.

Suponha agora que $A = B \oplus N$ como uma soma direta de espaços vetoriais onde B é uma subálgebra não-graduada semi-simples de A e N é o radical de Jacobson de A. O radical de Jacobson é graduado [23] e, como N é nilpotente, $N^2 = 0$. Se $x \in A_0 \cap N$ então $f_1 = 0$ implica que $x = x^q = 0$ assim $N \subseteq A_1$. Logo $A_1 = A_1 \cap B \oplus N$. Se $x \in A_1 \cap B$ e $u \in N$, então $ux, xu \in A_0 \cap N$, ou seja, $ux = xu = 0$. Portanto $x = 0$, pois o ideal de A gerado por x tem interseção nula com N. Logo $A_1 = N$. Como $A/N \cong B$ e $A/N \cong A_0$, temos que $A_0 \cong B$. Assim A_0 é uma subálgebra não-graduada semi-simples de A.

Seja $A_0 = B_1 \oplus \cdots \oplus B_s$ a decomposição (não-graduada) de A_0 em álgebras simples. A identidade $f_1 = 0$ implica que $B_i = GF(q)$ para todo i. Seja e_i a identidade da subálgebra B_i. Como A é subdiretamente irredutível então $AN \neq 0$ ou $NA \neq 0$. Suponha que $AN \neq 0$. Como a interseção dos ideais e_iN é zero, apenas um deles é não-nulo, digamos e_1N. Como N se decompõem numa soma direta de ideais $N = e_1N \oplus (1 - e_1)N$, temos $(1 - e_1)N = 0$ e $N = e_1N$. Similarmente os ideais Ne_i têm interseção nula, portanto no máximo um deles pode ser diferente de 0. Há três casos possíveis.

Caso 1: $NA = 0$. Então $A_0 = B_1 = GF(q)$ e N é um espaço vetorial unidimensional sobre $GF(q)$. A aplicação $\phi : A \to M_2(GF(q))$ definida como

$$\phi(\alpha + \beta u) = \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix},$$

onde $\alpha, \beta \in GF(q)$ e $0 \neq u \in N$ está fixado é um homomorfismo graduado injetor.

Caso 2: $Ne_1 \neq 0$, $N = e_1Ne_1$. Novamente $A_0 = B_1 = GF(q)$ e N é um $(GF(q), GF(q))$-bimódulo. Como A é subdiretamente irredutível, N não pode ter sub-bimódulos não-nulos com interseção nula. Portanto existe um automorfismo σ de $GF(q)$ tal que $x\alpha = \sigma(\alpha)x$ para todo $x \in N$ e todo $\alpha \in GF(q)$ (veja [36], p. 315). Assim cada subespaço de N é um sub-bimódulo e portanto N é um espaço vetorial unidimensional sobre $GF(q)$. A aplicação $\phi : A \to M_2(GF(q))$ definida como

$$\phi(\alpha + \beta u) = \begin{pmatrix} \alpha & \beta \\ 0 & \sigma(\alpha) \end{pmatrix},$$

onde $\alpha, \beta \in GF(q)$ e $0 \neq u \in N$, é um homomorfismo graduado injetor.

Caso 3: $Ne_2 \neq 0$, $N = e_1Ne_2$. Neste caso $A_0 = B_1 \oplus B_2 = GF(q) \oplus GF(q)$, $NB_1 = B_2N = 0$ e N é um $(GF(q), GF(q))$-bimódulo. Repetindo o raciocínio do caso 2, sabemos que existe um automorfismo σ de $GF(q)$ tal que $x\alpha = \sigma(\alpha)x$, para todo $x \in N$ e para todo $\alpha \in GF(q)$, e N é um espaço vetorial unidimensional sobre $GF(q)$. A aplicação $\phi : A \to M_2(GF(q))$ definida como

$$\phi(\alpha + \beta + \gamma u) = \begin{pmatrix} \alpha & \gamma \\ 0 & \sigma(\beta) \end{pmatrix},$$

onde $\alpha, \gamma \in B_1$, $\beta \in B_2$ e $0 \neq u \in N$ está fixado, é um homomorfismo graduado injetor. $\square$

Observação Listamos algumas outras identidades para Ω:

$$\begin{aligned}
f_3(y_1, y_2) &= y_1y_2 - y_2y_1, \\
f_4(z_1, z_2, z_3) &= z_1z_2z_3 - z_3z_2z_1, \\
f_5(y_1, z_1) &= (y_1 \cdot z_1)^q - z_1^{q-1}(y_1 \cdot z_1), \\
f_6(z_1, z_2) &= (z_1^{2(q-1)} - 1)z_1z_2(1 - [z_1, z_2]^{q-1}), \\
f_7(z_1, z_2) &= (z_1^{2(q-1)} - 1)z_2z_1(1 - [z_1, z_2]^{q-1}), \\
f_8(y_1, y_2, z_1, z_2) &= (X_1 - X_1^{q^2})(1 - [X_1, X_2]^{q-1})(X_2 - X_2^q), \\
f_9(y_1, y_2, z_1, z_2) &= (X_1 - X_1^q) \cdot (X_2 - X_2^q) - ((X_1 - X_1^q) \cdot (X_2 - X_2^q))^q,
\end{aligned}$$

onde $X_i = y_i + z_i$, $i = 1, 2$. A identidade $f_3 = 0$ segue da identidade $f_1 = 0$ (veja por exemplo [19], p. 73). As identidades $f_8 = 0$ e $f_9 = 0$ são conhecidas por [35], e podemos trocar a identidade $f_2 = 0$ no Teorema 3.4.1 por qualquer uma delas.

3.5 Identidades graduadas de Ω^α não sendo α um quadrado perfeito

Considere $g_1(y_1) = y_1^{q^2} - y_1$, $g_2(z_1) = z_1^{2q-1} - z_1$ e

$$g_3(y_1, y_2, z_1, z_2) = (y_1 + z_1 - (y_1 + z_1)^q)(y_2 + z_2 - (y_2 + z_2)^{q^2})(1 - [y_1 + z_1, y_2 + z_2]^{q-1})$$

três polinômios de $K\langle X \rangle$.

O próximo teorema apresenta uma base para as identidades graduadas de Ω^α.

Teorema 3.5.1 *Todas as identidades polinomiais graduadas de Ω^α seguem de $g_1 = 0$, $g_2 = 0$ e $g_3 = 0$.*

Seja $\mathfrak{V}$ a variedade de álgebras graduadas definida pelas identidades $g_1 = 0$, $g_2 = 0$ e $g_3 = 0$.

Lema 3.5.1 *$Var\Omega^\alpha \subseteq \mathfrak{V}$.*

Demonstração. Seja $y_1 = \begin{pmatrix} a & d \\ \alpha d & a \end{pmatrix}$ uma matriz de Ω_0^α. Seu polinômio característico é $f(x) = x^2 - (a^2 + \alpha d^2)$ com autovalores $\pm\lambda$ onde $\lambda = \sqrt{a^2 + \alpha d^2}$. Observemos primeiro que

$$\lambda^{q^2} = (\sqrt{a^2 + \alpha d^2})^{q^2} = (a^2 + \alpha d^2)^{(q+1)(q-1)/2}\lambda = (a^2 + \alpha d^2)^{(q-1)}\lambda = \lambda.$$

Similarmente obtemos $(-\lambda)^{q^2} = -\lambda$. Então, como existe uma matriz invertível P na álgebra $M_2(GF(q^2))$ tal que $P^{-1}y_1P = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix}$, temos que $y_1^{q^2} = y_1$. Agora seja $z_1 = \begin{pmatrix} b & c \\ -\alpha c & -b \end{pmatrix} \in \Omega_1^\alpha$. Como $z_1^2 = \begin{pmatrix} b^2 - \alpha c^2 & 0 \\ 0 & b^2 - \alpha c^2 \end{pmatrix}$ e $b^2 - \alpha c^2 \neq 0$ pois α não é um quadrado perfeito em K, temos $(z_1^2)^{q-1} = 1$. Então $z_1^{2q-1} = z_1$. Finalmente, por [35], sabemos que $(x_1 - x_1^q)(x_2 - x_2^{q^2})(1 - [x_1, x_2]^{q-1}) = 0$ é uma identidade polinomial de $M_2(K)$; portanto, $g_3 = 0$ é uma identidade graduada de Ω^α. $\square$

Lema 3.5.2 *$\mathfrak{V} \subseteq Var\Omega^\alpha$.*

Demonstração. Seja $N = N_0 \oplus N_1$ uma álgebra nilpotente de $\mathfrak{V}$. Logo N_0 é também um álgebra nilpotente de $\mathfrak{V}$. O índice de nilpotência s de N_0 é 2; pois se $s > 2$, podemos escolher elementos $a_1, \ldots, a_{s-1} \in N_0$ tais que $a_1 \ldots a_{s-1} \neq 0$ e, por $g_1 = 0$, obtemos

$$0 = (a_1 \ldots a_{s-1})^{q^2} - a_1 \ldots a_{s-1} = a_1 \ldots a_{s-1},$$

o que é uma contradição. Assim se $a \in N_0$ então $a = a^{q^2} = 0$ e portanto $N_0 = 0$. Além disso, como $N_1N_1 \subseteq N_0 = 0$, temos que $N_1^2 = 0$. Se $a \in N_1$ então $a = a^{2q-1} = 0$, $N_1 = 0$ e $N = 0$.

A variedade $\mathfrak{V}$ tem índice e expoente finitos. Pelo Teorema 3.3.1, $\mathfrak{V}$ é gerada por um conjunto de álgebras graduadas finitas e subdiretamente irredutíveis. Para provar o lema, é suficiente mostrar que cada uma dessas álgebras pertence a $Var\Omega^\alpha$. Provaremos ainda mais: cada uma delas está isomorficamente mergulhada em Ω^α. Até o final da prova, consideramos A como uma álgebra finita e subdiretamente irredutível de $\mathfrak{V}$.

Suponhamos que $A = B \oplus N$ como uma soma direta de espaços vetoriais onde B é uma subálgebra (não-graduada) semi-simples de A e N é o radical de Jacobson de A. Como N é um ideal graduado e é nilpotente, $N = 0$. Assim considerando $A = B_1 \oplus \cdots \oplus B_s$ a decomposição de A em álgebras não-graduadas simples, vemos, devido à irredutibilidade subdireta de A, que $s = 1$, ou seja, A é uma álgebra simples.

Suponhamos agora que A seja uma álgebra não-graduada simples, ou seja, $A = M_k(GF(p^t))$ e $p^t \geq q$. Observe que $k \leq 2$, pois se $k \geq 3$ então $g_3(a_0, b_0, a_1, b_1) = e_{13} \neq 0$ onde $a_0, b_0 \in A_0$ e $a_1, b_1 \in A_1$ são tais que $e_{12} = a_0 + a_1$ e $e_{23} = b_0 + b_1$.

Consideremos $k = 2$. Se $a_0, b_0 \in A_0$ e $a_1, b_1 \in A_1$ são tais que $\alpha e_{11} = a_0 + a_1$ e $e_{12} = b_0 + b_1$ então $g_3(a_0, b_0, a_1, b_1) = (\alpha^q - \alpha)e_{12} = 0$; logo $\alpha - \alpha^q = 0$, $q \geq p^t$ e $A = M_2(GF(q))$. Pelo Lema 3.2.1 temos duas possibilidades: $u_A^q = u_A$ ou $u_A^q = -u_A$. Se $u_A^q = u_A$ então A é isomorfa a Ω, e isso é uma contradição porque Ω não satisfaz $g_2 = 0$. Logo temos que $u_A^q = -u_A$. Pelo Lema 3.2.3 existe um isomorfismo graduado entre Ω^α e A.

Vamos considerar agora $k = 1$, ou seja, $A = GF(p^t)$. Se $0 \neq a \in A_1$ então $a^{q^2} = (a^2)^{(q+1)(q-1)/2} a = (a^{2q} a^2)^{(q-1)/2} a = (a^2)^{q-1} a = a^{2q-1} = a$. Se $a_0 \in A_0$ e $a_1 \in A_1$, então $(a_0 + a_1)^{q^2} = a_0^{q^2} + a_1^{q^2} = a_0 + a_1$. Portanto $\alpha^{q^2} - \alpha = 0$ para qualquer $\alpha \in A$ e, sendo $q^2 \geq p^t$, $A = GF(q)$ ou $A = GF(q^2)$. Se $A = GF(q)$ então existe um homomorfismo graduado injetor de A em Ω^α. Se $A = GF(q^2)$ então a única graduação possível é $A_0 \cong K$ e $A_1 \cong K$ e, pelo Lema 5 de [49], existe um elemento $u \in A_1$ tal que $A_1 = A_0 u$ e $0 \neq u^2 = a \in K$. Logo $A = Ka + Ku$, e a aplicação $\phi : A \to \Omega^\alpha$ definida como

$$\phi(\beta a + \gamma u) = \begin{pmatrix} \beta a + \gamma u & 0 \\ 0 & \beta a - \gamma u \end{pmatrix}$$

é um homomorfismo graduado injetor. □

Observação Listamos algumas outras identidades para Ω^α:

$$\begin{aligned}
g_4(y_1, y_2) &= y_1 y_2 - y_2 y_1, \\
g_5(z_1, z_2, z_3) &= z_1 z_2 z_3 - z_3 z_2 z_1, \\
g_6(y_1, z_1) &= z_1^{2q-2} y_1 - y_1, \\
g_7(y_1, z_1) &= (y_1 \cdot z_1)^q - z_1^{q-1}(y_1 \cdot z_1), \\
g_8(y_1, y_2, z_1, z_2) &= (X_1 - X_1^{q^2})(1 - [X_1, X_2]^{q-1})(X_2 - X_2^q), \\
g_9(y_1, y_2, z_1, z_2) &= (X_1 - (X_1)^q) \cdot (X_2 - X_2^q) - ((X_1 - X_1^q) \cdot (X_2 - X_2^q))^q,
\end{aligned}$$

onde $X_i = y_i + z_i$, $i = 1, 2$. A identidade $g_4 = 0$ segue de $g_1 = 0$. As identidades $g_8 = 0$ e $g_9 = 0$ são conhecidas por [35], e podemos trocar a identidade $g_3 = 0$ no Teorema 3.5.1 por qualquer uma delas.

Corolário 3.5.1 *As graduações não-isomorfas da álgebra das matrizes de ordem dois sobre um corpo finito são distinguidas por suas identidades polinomiais.*

De fato é suficiente considerar a identidade graduada $y_1^q = y_1$. Ela é satisfeita se e somente se a graduação é isomorfa a Ω.

Capítulo 4

Matrizes sobre a álgebra de Grassmann

4.1 Introdução

Denote por $M_2(E)$ a álgebra das matrizes de ordem 2 com entradas na álgebra de Grassmann E. A álgebra

$$M_{1,1}(E) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in E_0 \text{ e } b, c \in E_1 \right\}$$

é uma subálgebra de $M_2(E)$ interessante para o estudo de identidades polinomiais.

Definição Duas álgebras são *PI equivalentes* se satisfazem as mesmas identidades polinomiais ordinárias.

Um corolário da teoria desenvolvida por A. Kemer [21] foi a descrição do comportamento das álgebras T-primas em relação ao produto tensorial. Mais precisamente, Kemer demonstrou o seguinte resultado em característica 0, ver [21].

1. $T(M_{a,b}(K) \otimes E) = T_{a+b}(E)$;
2. $T(M_{a,b}(E) \otimes M_{c,d}(E)) = T(M_{r,s}(E))$ onde $r = ac + bd$ e $s = ad + bc$;
3. $T(M_{1,1}(E)) = T(E \otimes E)$.

A última PI-equivalência é um fato interessante. Ela também é uma conseqüência da teoria de estrutura de T-ideais de Kemer para variedades de álgebras associativas (veja [23], p. 24). Popov em [37] descreveu uma base das identidades polinomiais satisfeitas pela álgebra $E \otimes E$. Sem utilizar a teoria de Kemer, Regev [41] encontrou ainda outra prova (para as três afirmações acima). Di Vincenzo em [11], providenciou mais uma demonstração, também elementar, da terceira afirmação do resultado de Kemer, nessa vez utilizando-se de identidades graduadas. Tal interesse justifica-se pelo fato de que os T-ideais "mais simples" que são T-primos em característica 0, são os de K, E, $M_2(K)$, $M_{1,1}(E)$, $E \otimes E$, $M_2(E)$. As identidades polinomiais dessas álgebras foram descritas, exceto as de $M_2(E)$.

Em [29] foi apresentada uma nova prova da PI equivalência de $M_{1,1}(E)$ e $E \otimes E$ em característica 0, usando identidades graduadas. Além disso, nesse artigo são apresentadas bases para as identidades $\mathbb{Z}_2$-graduadas das álgebras $M_{1,1}(E)$ e $E \otimes E$. Utilizando-se métodos semelhantes aos de [29], pode ser demonstrado que quando o corpo base tem característica positiva p, as duas últimas álgebras não são PI equivalentes, e provavelmente é possível abordar a questão da PI equivalência de outros produtos tensoriais. Mas tal questão seria tema de futuros trabalhos.

Neste capítulo apresentaremos os resultados de [29].

4.2 Identidades $\mathbb{Z}_2$-graduadas de $M_{1,1}(E)$

A álgebra $M_{1,1}(E)$ possui a seguinte $\mathbb{Z}_2$-graduação não-trivial

$$M_{1,1}(E)_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in E_0 \right\} \text{ e } M_{1,1}(E)_1 = \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \mid b, c \in E_1 \right\}.$$

Di Vincenzo [11] provou que sobre corpos de característica 0 todas as identidades graduadas dessa álgebra seguem de $y_1y_2 = y_2y_1$ e $z_1z_2z_3 = -z_3z_2z_1$. Em [29] foi provado que o resultado de Di Vincenzo é válido para corpos infinitos de característica diferente de 2. Reproduziremos nesta seção a demonstração desse fato.

Até o final desta seção, assumimos que K é um corpo infinito de característica diferente de 2.

Sejam $V_0 = \{t_i, w_i \mid i \in \mathbb{N}\}$ e $V_1 = \{u_i, v_i \mid i \in \mathbb{N}\}$ dois conjuntos disjuntos de variáveis e considere a $\mathbb{Z}_2$-graduação usual sobre a álgebra livre $K\langle V_0 \cup V_1\rangle$, assumindo que as variáveis de V_0 são pares e as de V_1 são ímpares. Assim

$$K\langle V_0 \cup V_1\rangle = K\langle V_0 \cup V_1\rangle_0 \oplus K\langle V_0 \cup V_1\rangle_1.$$

Seja T o ideal $\mathbb{Z}_2$-graduado de $K\langle V_0 \cup V_1\rangle$ gerado pelas relações $fg = (-1)^{\alpha\beta}gf$ para $f \in K\langle V_0 \cup V_1\rangle_\alpha$ e $g \in K\langle V_0 \cup V_1\rangle_\beta$. Seja Ω a álgebra quociente de $K\langle V_0 \cup V_1\rangle$ por T. A álgebra Ω, que é também uma álgebra $\mathbb{Z}_2$-graduada considerando a $\mathbb{Z}_2$-graduação herdada de $K\langle V_0 \cup V_1\rangle$, é conhecida como *álgebra supercomutativa livre* (veja por exemplo [8], Seção 2). Além disso, a álgebra Ω é isomorfa a $K[V_0] \otimes E(V_1)$, onde $E(V_1)$ é a álgebra de Grassmann do espaço vetorial com base V_1, conforme o próximo lema.

Lema 4.2.1 *Sejam $K[V_0]$ a álgebra dos polinômios comutativos gerada por V_0 e $E(V_1)$ a álgebra de Grassmann do espaço vetorial com base V_1. A aplicação*

$$\phi : K[V_0] \otimes E(V_1) \to \Omega$$

definida por $\phi(a \otimes b) = ab + T$ é um isomorfismo de álgebras.

Demonstração. É fácil ver que ϕ é um homomorfismo de álgebras sobrejetor. Sejam $a = y_1 \ldots y_p$ e $b = z_1 \ldots z_q$ monômios não-nulos de $K[V_0]$ e de $E(V_1)$ respectivamente. Se fizermos as seguintes substituições $y_1 = \cdots = y_p = 1$ e $z_1 = e_1, \ldots, z_q = e_q$, teremos que $ab \notin T_2(E)$. Como $T \subseteq T_2(E)$, temos que ϕ é injetora. □

A álgebra $M_2(\Omega)$ possui uma graduação semelhante à de $M_2(K)$, a saber,

$$M_2(\Omega)_0 = \left\{ \begin{pmatrix} f_1 & 0 \\ 0 & f_4 \end{pmatrix} \mid f_1, f_4 \in \Omega \right\} \text{ e } M_2(\Omega)_1 = \left\{ \begin{pmatrix} 0 & f_2 \\ f_3 & 0 \end{pmatrix} \mid f_2, f_3 \in \Omega \right\}.$$

Denote por F a subálgebra $\mathbb{Z}_2$-graduada de $M_2(\Omega)$ gerada pelas matrizes

$$A_i = \begin{pmatrix} t_i & 0 \\ 0 & w_i \end{pmatrix} \text{ e } B_i = \begin{pmatrix} 0 & u_i \\ v_i & 0 \end{pmatrix}$$

para $i \in \mathbb{N}$.

Lema 4.2.2 *A álgebra $\mathbb{Z}_2$-graduada relativamente livre $K\langle X\rangle/T_2(M_{1,1}(E))$ é isomorfa à álgebra F.*

Demonstração. A aplicação $\phi : K\langle X\rangle \to F$ definida por

$$\phi(f(y_1, \ldots, y_m, z_1, \ldots, z_n)) = f(A_1, \ldots, A_m, B_1, \ldots, B_n)$$

é um homomorfismo $\mathbb{Z}_2$-graduado. Claramente, ϕ é sobrejetora. Além disso, um simples cálculo mostra que $\ker \phi = T_2(M_{1,1}(E))$ e ϕ induz um isomorfismo. □

Seja I o ideal das identidades $\mathbb{Z}_2$-graduadas de $K\langle X\rangle$ gerado pelas identidades graduadas $y_1y_2 = y_2y_1$ e $z_1z_2z_3 = -z_3z_2z_1$.

Lema 4.2.3 *A álgebra $\mathbb{Z}_2$-graduada $M_{1,1}(E)$ satisfaz todas as identidades graduadas do T_2-ideal I.*

Demonstração. Basta verificar que as identidades $y_1y_2 = y_2y_1$ e $z_1z_2z_3 = -z_3z_2z_1$ pertencem a $T_2(M_{1,1}(E))$. A prova pode ser verificada diretamente, usando as relações $ab = (-1)^{\alpha\beta}ba$ para $a \in E_\alpha$ e $b \in E_\beta$. □

Uma *seqüência básica* $s = (a_1, \ldots, a_p, b_1, \ldots, b_q, c_1, \ldots, c_r, d_1, \ldots, d_s)$ é uma seqüência de números naturais tais que
(i) $p \geq 0$, $q \geq 0$, $r \geq 0$, $s \geq 0$;
(ii) $a_1 \leq \cdots \leq a_p$, $b_1 \leq \cdots \leq b_q$, $c_1 < \cdots < c_r$, $d_1 < \cdots < d_s$;
(iii) $s \leq r \leq s + 1$;
(iv) se $r = 0$ então $q = 0$.
À seqüência básica s associamos o monômio

$$\mathsf{m}_s = \begin{cases} y_{a_1} \ldots y_{a_p} z_{c_1} y_{b_1} \ldots y_{b_q} z_{d_1} z_{c_2} z_{d_2} \ldots z_{c_s} z_{d_s} & \text{se} \quad r = s, \\ y_{a_1} \ldots y_{a_p} z_{c_1} y_{b_1} \ldots y_{b_q} z_{d_1} z_{c_2} z_{d_2} \ldots z_{c_s} z_{d_s} z_{d_{s+1}} & \text{se} \quad r = s + 1. \end{cases}$$

Seja C o conjunto de todos os monômios associados a seqüências básicas. Note que o monômio 1 pertence a C, pois está associado à seqüência vazia.

Lema 4.2.4 *O conjunto $\{\mathsf{m} + T_2(M_{1,1}(E)) \mid \mathsf{m} \in C\}$ é linearmente independente no espaço vetorial $K\langle X\rangle/T_2(M_{1,1}(E))$.*

Demonstração. Sejam $\mathsf{m}_1, \ldots, \mathsf{m}_n$ elementos de C e $\alpha_1, \ldots, \alpha_n$ elementos do corpo K tais que $\alpha_1 \mathsf{m}_1 + \cdots + \alpha_n \mathsf{m}_n \in T_2(M_{1,1}(E))$. Vamos provar que $\alpha_1 = \cdots = \alpha_n = 0$. Como o corpo K é infinito, podemos supor que os monômios m_1, ..., m_n são multihomogêneos. Denote por $\overline{\mathsf{m}}$ o elemento de $M_2(\Omega)$ obtido pelas substituições $y_i \mapsto A_i$ e $z_i \mapsto B_i$ no monômio $\mathsf{m} \in C$. Se $s = (a_1, \ldots, a_p, b_1, \ldots, b_q, c_1, \ldots, c_r, d_1, \ldots, d_s)$ é uma seqüência básica então

$$\overline{\mathsf{m}}_s = \pm \begin{cases} \omega_1 e_{11} + \omega_2 e_{22} & \text{se} \quad r = s, \\ \omega_1 e_{12} + \omega_2 e_{21} & \text{se} \quad r = s + 1, \end{cases}$$

onde

$$\begin{aligned} \omega_1 &= t_{a_1} \ldots t_{a_p} u_{b_1} \ldots u_{b_q} v_{c_1} \ldots v_{c_s} w_{d_1} \ldots w_{d_s}, \\ \omega_2 &= t_{b_1} \ldots t_{b_q} u_{a_1} \ldots u_{a_p} v_{d_1} \ldots v_{d_s} w_{c_1} \ldots w_{c_s}. \end{aligned}$$

Assim, é fácil ver que existe uma bijeção entre C e o subconjunto $\{\overline{\mathsf{m}} \mid \mathsf{m} \in C\}$ de F. Desse modo, se $\alpha_1 \mathsf{m}_1 + \cdots + \alpha_n \mathsf{m}_n \in T_2(F)$ então $\alpha_1 = \cdots = \alpha_n = 0$, pois as matrizes $\overline{\mathsf{m}}_1$, ..., $\overline{\mathsf{m}}_n$ são linearmente independentes em F. Pelo Lema 4.2.2, sabemos que $\alpha_1 \mathsf{m}_1 + \cdots + \alpha_n \mathsf{m}_n \in T_2(F)$ e a prova do lema está concluída. □

Apresentamos agora o principal teorema desta seção.

Teorema 4.2.1 *Todas as identidades polinomiais graduadas da álgebra $\mathbb{Z}_2$-graduada $M_{1,1}(E)$ seguem das identidades $y_1 y_2 = y_2 y_1$ e $z_1 z_2 z_3 = -z_3 z_2 z_1$.*

Demonstração. Se $f \in K\langle X\rangle_0$ então $y_i f - f y_i$ pertence a I. Assim todo elemento de $K\langle X\rangle/I$ é uma combinação linear de elementos da forma $\mathsf{m}_1 z_{e_1} \mathsf{m}_2 z_{e_2} z_{e_3} \ldots z_{e_k} + I$ onde m_1 e m_2 são monômios formados apenas por y_i's. Devido à identidade $y_1 y_2 = y_2 y_1$, podemos supor que os índices das variáveis em m_1 e m_2 crescem (com possíveis repetições). Pela identidade $z_1 z_2 z_3 = -z_3 z_2 z_1$, assumimos que $e_1 < e_3 < e_5 < \cdots$ e $e_2 < e_4 < e_6 < \cdots$. Note que se $e_1 > e_3$ num monômio, então usamos o fato de que $z_{e_1}(\mathsf{m}_2 z_{e_2}) z_{e_3} = -z_{e_3}(\mathsf{m}_2 z_{e_2}) z_{e_1}$ pertence a I. Assim, concluímos que o conjunto $\{\mathsf{m} + I \mid \mathsf{m} \in C\}$ gera o espaço vetorial $K\langle X\rangle/I$. Sabemos, pelo Lema 4.2.3, que $I \subseteq T_2(M_{1,1}(E))$. Aplicando os lemas 4.2.4 e 1.5.4, concluímos a prova. $\square$

Observação Se um polinômio multi-homogêneo $f \in K\langle X\rangle$ não é uma identidade de $M_{1,1}(E)$ e a variável z_i ocorre nos monômios de f então $\deg_{z_i} f \leq 2$. Pois se há três letras z_i num monômio, ao menos duas delas estarão numa das seqüências c_i ou d_i. Mas devido à identidade $z_1 z_2 z_3 = -z_3 z_2 z_1$ tais monômios desaparecem.

Observação Em [11] o teorema acima foi provado usando propriedades da involução $*$ definida no espaço de polinômios multilineares, veja [23], pp. 17–18 para a definição exata. Como o nosso corpo pode ser de característica positiva os elementos multilineares de um T_2-ideal podem não determinar o T_2-ideal. Em [11] o resultado correspondentes é uma conseqüência direta das propriedades da involução $*$ e da descrição da base para as identidades $\mathbb{Z}_2$-graduadas de $M_2(K)$. Isso é válido pois se decompomos $M_2(K) = A_0 \oplus A_1$ de acordo com a graduação usual então $M_{1,1}(E) \cong A_0 \otimes E_0 \oplus A_1 \otimes E_1$ é o envelope de Grassmann de $M_2(K)$.

Observação Note que o polinômio $[y^p, z]$ não desaparece em $M_{1,1}(E)$ se considerado como uma identidade $\mathbb{Z}_2$-graduada. (Aqui y é uma variável par, z é uma variável ímpar e p é a característica do corpo K.) Escolha por exemplo $y = e_{11} + 2e_{22}$, $z = ge_{12} + ge_{21}$ onde $g \neq 0$ é um elemento arbitrário de E_1. Então $y^p = e_{11} + 2^p e_{22}$ e como $2^p = 2 \neq 1$ em K temos que $[y^p, z] = g((1 - 2^p)e_{12} + (2^p - 1)e_{21}) \neq 0$.

Agora observe que podemos escolher outro modelo para a álgebra F. Sejam $a_i^{(0)}$, $b_i^{(0)}$ variáveis comutativas e $a_i^{(1)}$, $b_i^{(1)}$ variáveis anticomutativas, e forme a álgebra supercomutativa livre $K(a_i^{(j)}, b_i^{(j)} \mid i \in \mathbb{N}, j = 0, 1)$ que é livremente gerada por elas. Considere as matrizes da forma

$$C_i = a_i^{(0)} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b_i^{(0)} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad D_i = a_i^{(1)} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + b_i^{(1)} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

e gere uma álgebra L com 1 e com elas, assumindo que C_i são elementos pares, e que D_i são elementos ímpares. Então L é uma álgebra $\mathbb{Z}_2$-graduada.

Lema 4.2.5 *A álgebra L é isomorfa à álgebra F.*

Demonstração. O homomorfismo $\varphi : F \to L$ definido por $\varphi(A_i) = C_i$ e $\varphi(B_i) = D_i$ é obviamente um isomorfismo $\mathbb{Z}_2$-graduado. $\square$

É imediato que as matrizes $a_i^{(0)}(e_{11}+e_{22})$ comutam com as de L. Denote por $B_2(L)$ a subálgebra de L que é gerada por 1 e por todos os elementos de L tais que toda "variável" par aparece neles apenas em comutadores. Como as matrizes $a_i^{(0)}(e_{11}+e_{22})$ são centrais, elas desaparecerão dos polinômios em $B_2(L)$.

Lema 4.2.6 *As matrizes* $E_i = b_i^{(0)}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *e* $D_i = \begin{pmatrix} 0 & c_i^{(1)} \\ d_i^{(1)} & 0 \end{pmatrix}$ *satisfazem as seguintes relações:*
i) E_iE_j *são centrais;*
ii) $E_iE_j = E_jE_i$*;*
iii) $E_iD_j = -D_jE_i$*;*
iv) $D_i^2D_j = -D_jD_i^2$*.*

Demonstração. Segue de verificação direta. $\square$

Agora seja $B_2(M_{1,1})$ a subálgebra de F gerada por $1 = e_{11}+e_{22}$ e pelos polinômios tais que toda variável par aparece apenas em comutadores. Em outras palavras, $B_2(F) = B_2(X)/(T_2(M_{1,1}(E)) \cap B_2(X))$. Então $B_2(F)$ é canonicamente isomorfa a $B_2(L)$, e identificaremos $B_2(F)$ e $B_2(L)$.

A proposição a seguir é uma adaptação de Lemas 2.2 e 2.3 de [12].

Proposição 4.2.1 *Se* $f \in B_2(L)$ *é um polinômio multi-homogêneo, então* f *é uma combinação linear de elementos da forma*

$$E_{i_1}^{\alpha_1}E_{i_2}^{\alpha_2}\dots E_{i_k}^{\alpha_k}D_{j_1}^2D_{j_2}^2\dots D_{j_l}^2 g(D_{n_1}, D_{n_2}, \dots, D_{n_m})$$

onde $i_1 < i_2 < \dots < i_k$, $j_1 < j_2 < \dots < j_l$, $\{j_1, j_2, \dots, j_l\}$ *e* $\{n_1, n_2, \dots, n_m\}$ *são disjuntos, e o polinômio* g *é multilinear.*

Demonstração. Primeiro, como $1 = e_{11} + e_{22}$ é central, não há matrizes do tipo $a_i^{(0)}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ na expansão de f. Então usando o lema anterior obtemos que

$$f = E_{i_1}^{\alpha_1}E_{i_2}^{\alpha_2}\dots E_{i_k}^{\alpha_k}h(D_1, D_2, \dots, D_t)$$

onde h é um polinômio multi-homogêneo. Se o grau de h em algum D_i fosse maior que 2 então h seria uma identidade $\mathbb{Z}_2$-graduada para $M_{1,1}(E)$, veja observação acima. Logo podemos supor que o grau de h em qualquer uma de suas variáveis é ≤ 2.

Agora escreva h como a soma de monômios, e divida cada um desses monômios em duas seqüências ascendentes como foi feito antes para os monômios associados a seqüências básicas. Se houvesse dois D_i's iguas numa das seqüências de um monômio, então esse monômio desapareceria devido a $z_1 z_2 z_1 = 0$. Portanto se D_i aparece duas vezes no monômio então deve participar uma vez em cada seqüência. Mas isso significa que podemos escrever, a menos de sinal, o monômio como $\ldots D_i^2 \ldots$. Então usamos o fato de que $D_i^2 D_j = -D_j D_i^2$ a fim de levar D_i^2 para o começo do monômio. Finamente, observe que $D_i^2 D_j^2 = D_j^2 D_i^2$ para todo i e j. □

4.3 Um pouco de combinatória

Para as demonstrações da próxima seção, precisaremos de um pouco de combinatória. Seja $(i_1, i_2, \ldots, i_n)$ uma permutação dos símbolos $\{1, 2, \ldots, n\}$, e assuma que

$$\{1, 2, \ldots, n\} = A \cup B, \quad A \cap B = \emptyset.$$

Pode-se considerar a coloração desses símbolos nas cores A e B como a motivação para a terminologia usada. Então o par (i_α, i_β), $1 \leq \alpha, \beta \leq n$, forma uma inversão colorida (com relação à partição A, B) se $1 \leq \alpha < \beta \leq n$, $i_\alpha > i_\beta$ e $\alpha \in A$, $\beta \in B$. Se q é o número de todas as inversões coloridas em $(i_1, i_2, \ldots, i_n)$ então $(-1)^q$ é o sinal colorido dessa permutação com relação à partição A, B. Consideraremos as partições A, B de $\{1, 2, \ldots, n\}$ como pares não-ordenados, ou seja, não diferenciaremos (A, B) de (B, A). Então há exatamente 2^{n-1} partições de $\{1, 2, \ldots, n\}$ incluindo a trivial. Obviamente o sinal colorido da permutação principal (ou trivial) $(1, 2, \ldots, n)$ é igual a 1 para todas as partições pois a permutação principal não contém nenhuma inversão (ordinária).

Proposição 4.3.1 *Seja $i = (i_1, i_2, \ldots, i_n)$ uma permutação fixa de $(1, 2, \ldots, n)$. Então o sinal colorido de i é ou igual a 1 para todas as partições, ou igual ao número -1 para todas as partições, ou senão igual a 1 para 2^{n-2} partições e -1 para as restantes 2^{n-2} partições.*

Demonstração. A prova é um raciocínio combinatório elementar. É fácil mostrar que as transposições $(t, t+2)$ mudam o sinal colorido de cada permutação, para toda partição (A, B). A fim de provar esse fato, consideremos todas as quatro possibilidades para três símbolos consecutivos na permutação: todos pertencendo a A ou seja $a_1 a_2 a_3$, ou dois pertencendo a A e um a B ou seja $a_1 a_2 b$, $a_1 b a_2$, $b a_1 a_2$. Aqui a_1, $a_2 \in A$, $b \in B$.

Usando a observação acima, é suficiente provar a proposição apenas para permutações i tais que $i_1 < i_3 < \ldots$ e $i_2 < i_4 < \ldots$.

Usamos indução sobre n, $n = 1$ e 2 são óbvios. Para $n = 3$, apresentamos uma tabela com os sinais coloridos de todas as permutações de $\{1, 2, 3\}$ abaixo. Em particular, isso mostra que a afirmação é verdadeira para $n = 3$.

permutações

partições		123	132	231	213	312	321
	123	$+$	$-$	$+$	$-$	$+$	$-$
	$12;3$	$+$	$+$	$+$	$-$	$-$	$-$
	$13;2$	$+$	$+$	$-$	$+$	$-$	$-$
	$23;1$	$+$	$-$	$-$	$+$	$+$	$-$

Suponhamos que $n > 3$ e que a afirmação foi provada para todo $m < n$. Sejam $i = (i_1, i_2, \ldots, i_n)$ e $i' = (i_1, i_2, \ldots, i_{n-1})$ a permutação de $n-1$ símbolos $\{1, 2, \ldots, n\} \setminus \{i_n\}$ obtida de i apagando sua última entrada. Então a proposição é verdadeira para i' devido à indução. Note que ou $i_n = n$ ou $i_{n-1} = n$ pois $i_1 < i_3 < \ldots$ e $i_2 < i_4 < \ldots$. Agora considere dois casos para i_{n-1} e i_n.

Caso 1. Assumindo que $i_{n-1} < i_n$, temos $i_n = n$. Se (A, B) é uma partição de $\{1, 2, \ldots, n\} \setminus \{i_n\}$ formamos duas partições de $\{1, 2, \ldots, n\}$. Elas são $(A \cup \{i_n\}, B)$ e $(A, B \cup \{i_n\})$. Os sinais coloridos de i com relação a essas duas partições serão iguais ao sinal colorido de i' com relação a (A, B).

Caso 2. Se $i_{n-1} > i_n$ então $i_{n-1} = n$. Logo i_{n-1} forma inversão apenas com i_n. Defina $i'' = (i_1, i_2, \ldots, i_{n-2}, i_n)$. Então a nossa afirmação se mantém para i''. Seja (C, D) uma partiçaõ de $\{1, 2, \ldots, n-1\}$ e ε o sinal colorido de i'' com relação a (C, D). Formamos duas partições $(C \cup \{n\}, D)$ e $(C, D \cup \{n\})$ de $\{1, 2, \ldots, n\}$. Numa delas $i_{n-1} = n$ e i_n pertencem a conjuntos diferentes da partição, logo o sinal colorido de i com relação a essa partição será ε. Analogamente na outra partição $i_{n-1} = n$ e i_n estão no mesmo conjunto e, como eles formam uma inversão, isso produz o sinal colorido $-\varepsilon$.

Ambos os casos foram tratados e a prova da proposição está completa. □

O corolário a seguir mostra uma aplicação elementar e interessante da combinatória desenvolvida acima

Corolário 4.3.1 *O sinal colorido de $\sigma = (n, n-1, \ldots, 2, 1)$ é igual a 1 para todas as partições quando $n \equiv 1 \pmod 4$ e -1 quando $n \equiv 3 \pmod 4$. Se n é par então o sinal colorido de σ é igual a 1 para 2^{n-2} partições, e -1 para as restantes partições.*

Demonstração. Suponhamos que $\{1, 2, \ldots, n\} = A \cup B$, $|A| = a$, $|B| = b$ e $a + b = n$. Então haverá $q = a(a-1)/2 + b(b-1)/2$ inversões coloridas em σ. Logo

$$q = (a^2 + b^2 - a - b)/2 = (n^2 - n)/2 - ab = n(n-1)/2 - ab.$$

Se n é ímpar então ou a ou b é par, e isso conclui a prova para $n \equiv 1$ e $3 \pmod 4$.

Se $n = 2m$ é par, usando o fato de que $\sum_{j=0}^{n} (-1)^j \binom{n}{j} = 0$, obtemos a igualdade $\sum_{j=0}^{m-1} (-1)^j \binom{n}{j} + (1/2)(-1)^m \binom{n}{m} = 0$. (Note que no último caso $\binom{n}{m} = \binom{2m}{m}$ é sempre par.) □

Proposição 4.3.2 *Seja $i = (i_1, i_2, \ldots, i_n)$ uma permutação dos símbolos $(1, 2, \ldots, n)$ e suponhamos que $i_1 < i_3 < \ldots$ e $i_2 < i_4 < \ldots$. Se $i \neq (1, 2, \ldots, n)$ então o sinal colorido de i é igual a 1 para 2^{n-2} partições e -1 para as restantes 2^{n-2} partições de $\{1, 2, \ldots, n\}$.*

Demonstração. Segue da prova da Proposição 4.3.1. Usamos indução finita sobre n. No primeiro caso considerado lá, devido à hipótese de indução e a $i \neq (1, 2, \ldots, n)$ obtemos 2^{n-2} vezes o sinal colorido 1, e 2^{n-2} vezes o sinal colorido -1. O mesmo é válido para o segundo caso. $\square$

Observação Note que com os resultados anteriores demos uma descrição combinatória da estrutura linear das álgebras Meson, veja por exemplo [20], pp. 115 e 264–272. É claro que o nosso objetivo não era a descrição dessas álgebras, mas isso surgiu "de graça", como uma conseqüência da combinatória acima. As álgebras Meson têm um papel importante na teoria de representações de álgebras de Jordan, ver [20]. Elas aparecem de maneira natural na teoria de álgebras de Clifford e têm várias aplicações.

4.4 Identidades $\mathbb{Z}_2$-graduadas de $E \otimes E$

Consideramos o quadrado tensorial da álgebra de Grassmann G juntamente com sua $\mathbb{Z}_2$-graduação definida como $E \otimes E = (E_0 \otimes E_0 \oplus E_1 \otimes E_1) \oplus (E_0 \otimes E_1 \oplus E_1 \otimes E_0)$. Denote por I o ideal das identidades $\mathbb{Z}_2$-graduadas satisfeitas por $E \otimes E$. Primeiro vamos construir um modelo para a álgebra $\mathbb{Z}_2$-graduada relativamente livre na variedade das álgebras $\mathbb{Z}_2$-graduadas definida por $E \otimes E$.

Sejam $a_i^{(0)}$, $b_i^{(0)}$, $c_i^{(0)}$, $d_i^{(0)}$ variáveis comutativas e $a_i^{(1)}$, $b_i^{(1)}$, $c_i^{(1)}$, $d_i^{(1)}$ variáveis anticomutativas, $i \in \mathbb{N}$. Consideramos a álgebra supercomutativa livre $K(V_0; V_1)$ livremente gerada pelos conjuntos $V_0 = \{a_i^{(0)}, b_i^{(0)}, c_i^{(0)}, d_i^{(0)}\}$ e $V_1 = \{a_i^{(1)}, b_i^{(1)}, c_i^{(1)}, d_i^{(1)}\}$ de variáveis pares e ímpares respectivamente. Denote por F' a subálgebra do produto tensorial $K(V_0; V_1) \otimes K(V_0; V_1)$ gerada por todos os elementos da forma

$$Y_i = a_i^{(0)} \otimes b_i^{(0)} + a_i^{(1)} \otimes b_i^{(1)}, \qquad Z_i = c_i^{(0)} \otimes d_i^{(1)} + c_i^{(1)} \otimes d_i^{(0)}.$$

Então $F' = F'_0 \oplus F'_1$ é uma álgebra $\mathbb{Z}_2$-graduada e a sua graduação é a natural, ou seja, consideramos Y_i como variáveis pares e Z_i como variáveis ímpares.

Lema 4.4.1 *A álgebra $\mathbb{Z}_2$-graduada relativamente livre $K\langle X\rangle / T_2(E \otimes E)$ é isomorfa à álgebra F'.*

Demonstração. A prova é bastante direta. O homomorfismo de $K\langle X\rangle$ em F' definido por $y_i \mapsto Y_i$ e $z_i \mapsto Z_i$ é sobrejetor e seu núcleo é igual a I, logo ele induz um isomorfismo. □

Precisaremos de algumas propriedades elementares da álgebra $E \otimes E$. É fácil ver que seu centro é igual a $E_0 \otimes E_0$.

Lema 4.4.2 *Os polinômios $y_1y_2 - y_2y_1$ e $z_1z_2z_3 + z_3z_2z_1$ são identidades graduadas para $E \otimes E$. Se a característica de K é $p > 2$ então o polinômio $y_1^pz_1 - z_1y_1^p$ é também uma identidade graduada para $E \otimes E$.*

Demonstração. O primeiro polinômio é uma identidade $\mathbb{Z}_2$-graduada de $E\otimes E$ pois a componente par $E_0 \otimes E_0 \oplus E_1 \otimes E_1$ é uma álgebra comutativa. O segundo polinômio é também uma identidade $\mathbb{Z}_2$-graduada para $E \otimes E$ como mostra um cálculo direto.

Para o terceiro, seja $a \in E_0 \otimes E_0 \oplus E_1 \otimes E_1$, então $a = \sum(e_i \otimes f_i + g_i \otimes h_i)$ onde e_i, $f_i \in E_0$, g_i, $h_i \in E_1$. Portanto

$$a^p = \sum(e_i^p \otimes f_i^p + g_i^p \otimes h_i^p) = \sum e_i^p \otimes f_i^p$$

pois $g_i^p = h_i^p = 0$ e os termos mistos desaparecem devido aos coeficientes binomiais que são divisíveis por p. O elemento $\sum e_i^p \otimes f_i^p$ é central em $E \otimes E$, e isso completa a prova. □

Observação Observe que de acordo com a seção 4.2, a última identidade graduada não é satisfeita pela álgebra $M_{1,1}(E)$. Logo ela não é uma conseqüência das duas primeiras identidades do lema.

Precisaremos das seguintes relações satisfeitas por $E \otimes E$. Sua dedução é direta e pode ser encontrada em [12], lema 2.2.

Lema 4.4.3 *As seguintes igualdades são válidas para a álgebra $E \otimes E$:*

1. $z_1zz_1 = 0$, $z_1uz_1vz_1 = 0$, $z_1^2z_2^2 = z_2^2z_1^2$, $z_1^2z_2 = -z_2z_1^2$;

2. $t_1ut_2 = t_2ut_1$, $zt = -tz$,

para todo t, t_1, $t_2 \in E_1 \otimes E_1$, z, z_1, $z_2 \in E_0 \otimes E_1 \oplus E_1 \otimes E_0$, u, $v \in E \otimes E$.

Observe que as identidades graduadas do item (1) do lema acima são conseqüências das identidades $y_1y_2 = y_2y_1$ e $z_1z_2z_3 = -z_3z_2z_1$. Isso foi provado na seção 4.2 quando estabelecemos que elas são válidas na álgebra $M_{1,1}(E)$.

Já deduzimos que $T_2(M_{1,1}(E)) \subseteq T_2(E \otimes E)$. Portanto, a álgebra $\mathbb{Z}_2$-graduada relativamente livre F' é uma imagem homomórfica de F e de L. Logo temos o seguinte lema.

Lema 4.4.4 *A álgebra $B_2(F') = B_2(X)/(B_2(X) \cap I)$ é uma imagem homomorfa de $B_2(L)$ (e de $B_2(F)$ também).*

Demonstração. Para demonstrarmos a afirmação do Lema, observamos que temos a inclusão $T_2(M_{1,1}(E)) \subseteq T_2(E \otimes E) = I$, portanto $B_2(X)/(B_2(X) \cap I)$ é uma imagem homomórfica do quociente $B_2(X)/(B_2(X) \cap T_2(M_{1,1}(E)))$. $\square$

Lema 4.4.5 *Sejam $g_i(z_1, z_2, \ldots, z_n)$ polinômios multilineares que são linearmente independentes módulo o T_2-ideal $T_2(M_{1,1}(E))$. Então os polinômios*

$$y_1^{i_1} y_2^{i_2} \ldots y_k^{i_k} z_{n+1}^2 z_{n+2}^2 \ldots z_{n+r}^2 g_i(z_1, z_2 \ldots, z_n)$$

são linearmente independentes módulo o T_2-ideal $T_2(M_{1,1}(E))$.

Demonstração. Defina $y_1 = E_1 + E_2 + \ldots + E_{i_1}$, $\ldots$, $y_k = E_{t+1} + \ldots + E_{t+i_k}$ para $t = i_1 + \ldots + i_{k-1}$, $z_{n+1} = D_{n+1} + D_{n+2}$, $\ldots$, $z_{n+r} = D_{n+2r-1} + D_{n+2r}$. Isso produz um múltiplo não-nulo e então aplica-se a independência de g_i. $\square$

Corolário 4.4.1 *Os monômios multilineares*

$$m_{ij} = z_{i_1} z_{j_1} z_{i_2} z_{j_2} \ldots z_{i_m} \widehat{z_{j_m}},$$

onde $i_1 < i_2 < \ldots < i_m$ e $j_1 < j_2 < \ldots < j_{m-1} < j_m$, são linearmente independentes mólulo as identidades graduadas da álgebra $E \otimes E$. Aqui se o grau do monômio é ímpar, z_{j_m} não aparece.

Demonstração. Suponhamos, pelo contrário, que os respectivos monômios são linearmente dependentes e que $\sum \alpha_{ij} m_{ij} = 0$. Então a última equação será uma identidade graduada para $E \otimes E$. Devido à homogeneidade, podemos supor que todos os m_{ij} são monômios em z_1, z_2, $\ldots$, z_k. Suponhamos que $m = z_1 z_2 \ldots z_{k-1} z_k$ participa nessa combinação linear com coeficiente não-nulo α. Escolhemos a partição $A \cup B$ do conjunto $\{1, 2, \ldots, k-1, k\}$ e seja $z_i \mapsto e_i \otimes 1$ sempre que $i \in A$, $z_j \mapsto 1 \otimes e_j$, $j \in B$. O valor da combinação será 0. Some os valores para todas as partições A e B. Os elementos de $E_1 \otimes E_0$ anticomutam e o mesmo é válido para $E_0 \otimes E_1$. Os elementos de $E_0 \otimes E_1$ comutam com os de $E_1 \otimes E_0$. Assim aplica-se a Proposição 4.3.2 e se obtém que $2^h \alpha = 0$ para algum inteiro positivo h. (Os outros monômios participantes na combinação linear darão contribuição nula devido a Proposição 4.3.2, pois eles são distintos de m. Então o sinal $+1$ aparecerá 2^{k-2} vezes, o mesmo número de ocorrências como o de -1.) Isso é uma contradição pois a característica de K é diferente de 2, e $2^h \neq 0$. $\square$

Corolário 4.4.2 *Seja $f(y_1, \dots, y_m, z_1, \dots, z_n) \in B_2(F) \equiv B_2(L)$ um polinômio graduado. (Aqui usamos as letras y_i para E_i e z_i para D_i, veja a definição de L na seção 4.2.) Então módulo o ideal I das identidades graduadas de $E \otimes E$ o polinômio f é igual a um polinômio da forma*

$$y_1^{\alpha_1} y_2^{\alpha_2} \dots y_m^{\alpha_m} z_{i_1}^2 z_{i_2}^2 \dots z_{i_k}^2 g_j(z_{j_1}, z_{j_2}, \dots, z_{j_l})$$

onde $\{i_1, i_2, \dots, i_k\} \cap \{j_1, j_2, \dots, j_l\} = \emptyset$, $i_1 < i_2 < \dots < i_k$ e g_j é um polinômio multilinear. Se a característica de K é $p > 0$ impomos também que $\alpha_i < p$, $i = 1$, $\dots$, m.

Além disso, se os polinômios multilineares g_j são linearmente independentes módulo I então os polinômios acima são linearmente independentes também.

Demonstração. A prova é a mesma que para $B_2(F)$. Note que se $a \in E_1 \otimes E_1$ então $a^p = 0$. □

Teorema 4.4.1 *Se a característica do corpo K é igual a 0 então o ideal das identidades $\mathbb{Z}_2$-graduadas da álgebra $E \otimes E$ é gerado pelas identidades $y_1 y_2 = y_2 y_1$ e $z_1 z_2 z_3 = -z_3 z_2 z_1$. Quando a característica de K é $p > 2$, o ideal das identidades é gerado pelas duas identidades anteriores e por $y_1^p z_1 = z_1 y_1^p$.*

Demonstração. Já mostramos que essas identidades são de fato identidades de $E \otimes E$. Como as duas primeiras formam uma base para as identidades graduadas de $M_{1,1}(E)$, podemos trabalhar na álgebra relativamente livre determinadas por elas, ou seja, em F. Como já mostramos é suficiente considerar apenas os polinômios nos quais as variáveis pares aparecem apenas em comutadores. Nesses casos, o último corolário completa a prova do teorema. □

Como um corolário do último teorema obtemos outra prova da coincidência dos T-ideais das álgebras $M_{1,1}(E)$ e $E \otimes E$ sobre um corpo de característica 0. Notamos que é um fato sábido. Suas provas conhecidas usam ou a teoria estrutural de T-ideais (veja [23], p. 24) ou a descrição da base de $T(E \otimes E)$ dada por Popov, [37] (veja [11], teorema 2), ou outros métodos e resultados mais complexos (veja [41], teorema 4.7). A prova que damos é elementar.

Corolário 4.4.3 *Se a característica do corpo K é 0 então as álgebras $M_{1,1}(E)$ e $E \otimes E$ são PI equivalentes. Em outras palavras, $T(M_{1,1}(E)) = T(E \otimes E)$.*

Demonstração. Pelo Lema 1.5.3, sabemos que se duas álgebras graduadas satisfazem as mesmas identidades graduadas então elas satisfazem as mesmas identidades ordinárias. Conforme mostramos para o caso de característica 0, as identidades $\mathbb{Z}_2$-graduadas de $M_{1,1}(E)$ e de $E \otimes E$ seguem das identidades $y_1 y_2 = y_2 y_1$ e $z_1 z_2 z_3 = -z_3 z_2 z_1$. Portanto, as álgebras $M_{1,1}(E)$ e $E \otimes E$ satisfazem as mesmas identidades polinômiais ordinárias quando a característica de K é 0. □

Bibliografia

[1] S. A. Amitsur, J. Levitzki, *Minimal identities for algebras*, Proc. Amer. Math. Soc. **1**, 449–463 (1950).

[2] S. S. Azevedo, *Graded identities for the matrix algebra of order n over an infinite field*, Commun. Algebra **30 (12)**, 5849–5860 (2002).

[3] S. S. Azevedo, *A basis for $\mathbb{Z}$-graded identities of matrices over infinite fields*, submetido.

[4] Yu. Bahturin, A. Giambruno, D. Riley, *Group graded algebras satisfying a polynomial identity*, Israel J. Math. **104**, 145–155 (1998).

[5] Yu. Bahturin, A. Giambruno, M. Zaicev, *Codimension growth and graded identities*, Algebra (Moscow, 1998), 57–76, de Gruyter, Berlin, 2000.

[6] A. Ya. Belov, *On non-specht varieties*, Fundam. Prikl. Mat. **5 (1)**, 47–66 (1999).

[7] A. Berele, *Magnum PI*, Israel J. Math. **51 (1–2)**, 13–19 (1985).

[8] A. Berele, *Generic verbally prime PI-algebras and their GK-dimensions*, Commun. Algebra **21 (5)**, 1487–1504 (1993).

[9] J. Bergen, M. Cohen, *Actions of commutative Hopf algebras*, Bull. London Math. Soc. **18 (2)**, 159–164 (1986).

[10] C. de Concini, C. Procesi, *A characteristic free approach to invariant theory*, Adv. Math. **21 (3)**, 330–354 (1976).

[11] O. M. Di Vincenzo, *On the graded identities of $M_{1,1}(E)$*, Israel J. Math. **80 (3)**, 323–335 (1992).

[12] O. M. Di Vincenzo, V. Drensky, *Polynomial identities for tensor products of Grassmann algebras*, Mathematica Pannonica **4**, 249–272 (1993).

[13] O. M. Di Vincenzo, V. Nardozza, *Graded polynomial identities for tensor products by the Grassmann algebra*, Commun. Algebra, a aparecer (2002).

[14] P. Doubilet, G.-C. Rota, J. Stein, *On the foundations of combinatorial theory*, Stud. Appl. Math. **3**, No. 9, 185–216 (1974).

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

[16] V. Drensky, *Free algebras and PI-algebras*, Springer–Verlag, Singapore, 2000.

[17] G. K. Genov, *Basis for identities of a third order matrix algebra over a finite field*, Algebra and Logic **20**, 241–257 (1981).

[18] G. K. Genov, P. N. Siderov, *A basis for identities of the algebra of fourth-order matrices over a finite field I, II*, Serdica **8**, 313–323, 351–366 (1982) [Russian].

[19] I. N. Herstein, *Noncommutative rings*, Carus Math. Monographs, Math. Assoc. Amer., New York, 1968.

[20] N. Jacobson, *Structure and representations of Jordan algebras*, Amer. Math. Soc. Colloquium Publ. **39**, Amer. Math. Soc., Providence, RI, 1968.

[21] A. R. Kemer, *Varieties and $\mathbb{Z}_2$-graded algebras*, Izv. Akad. Nauk SSSR, Ser. Mat. **48**, 1042–1059 (1984). Translation: Math. USSR, Izv. **25**, 359–374 (1985).

[22] A. R. Kemer, *Finite bases for identities of associative algebras*, Algebra and Logic **27**, 597–641 (1987).

[23] A. R. Kemer, *Ideals of identities of associative algebras*, Translations Math. Monographs **87**, Amer. Math. Soc., Providence, 1991.

[24] A. Kemer, *The standard identity in characteristic p. A conjecture of I. B. Volichenko*, Israel J. Math. **81**, 343–355 (1993).

[25] P. Koshlukov, *Weak polynomial identities for the matrix algebra of order two*, J. Algebra **188**, No. 7, 610–625 (1997).

[26] P. Koshlukov, *Finitely based ideals of weak polynomial identities*, Commun. Algebra **26**, No. 10, 3335–3359 (1998).

[27] P. Koshlukov, *Ideals of identities of representations of nilpotent Lie algebras*, Commun. Algebra **28**, No. 7, 3095–3113 (2000).

[28] P. Koshlukov, *Basis of the identities of the matrix algebra of order two over a field of characteristic* $p \neq 2$, J. Algebra **241**, 410–434 (2001).

[29] P. Koshlukov, S. S. Azevedo, *Graded identities for T-prime algebras over fields of positive characteristic*, Israel J. Math. **128**, 157–176 (2002).

[30] P. Koshlukov, S. S. Azevedo, *A basis for the graded identities of the matrix algebra of order two over a finite field of characteristic* $p \neq 2$, Finite Fields Appl. **8**, 597–609 (2002).

[31] B. Kostant, *A theorem of Frobenius, a theorem of Amitsur-Levitzki and cohomology theory*, J. Math. Mech. **7**, 237–264 (1958).

[32] D. Krakowski, A. Regev, *The polynomial identities of the Grassmann algebra*, Trans. Amer. Math. Soc. **181**, 429–438 (1973).

[33] R. L. Kruse, *Identities satisfied by a finite ring*, J. Algebra **26**, 298–318 (1973).

[34] I. V. Lvov, *Varieties of associative rings*, Algebra and Logic **12**, 150–167 (1973).

[35] Yu. N. Maltsev, E. N. Kuzmin, *A basis for identities of the algebra of second order matrices over a finite field*, Algebra and Logic **17**, 18–21 (1978).

[36] B. R. McDonald, *Finite rings with identities*, Marcel Dekker, New York, 1974.

[37] A. P. Popov, *Identities of the tensor square of a Grassmann algebra*, Algebra and Logic **21**, 296-316 (1982).

[38] C. Procesi, *The invariant theory of* $n \times n$ *matrices*, Adv. Math. **19 (3)**, 306–381 (1976).

[39] Yu. P. Razmyslov, *Finite basing of the identities of a matrix algebra of second order over a field of characteristic zero*, Algebra and Logic **12**, 47–63 (1973).

[40] Yu. P. Razmyslov, *Trace identities of full matrix algebras over a field of characteristic zero*, Math. USSR Izvestiya **8**, 727–760 (1974).

[41] A. Regev, *Tensor products of matrix algebras over the Grassmann algebra*, J. Algebra **133**, 512–526 (1990).

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

[43] W. Specht, *Gesetze in Ringen*, Math. Zeitschrift **52**, 557–589 (1950).

[44] R. G. Swan, *An application of graph theory to algebra*, Proc. Amer. Math. Soc. **14**, 367–373 (1963). Correção: **21**, 379–380 (1969).

[45] S. Yu. Vasilovsky, *The basis of identities of a three-dimensional simple Lie algebra over an infinite field*, Algebra and Logic **28**, No. 5, 355–368 (1989).

[46] S. Vasilovsky, *A finite basis for polynomial identities of the Jordan algebras of bilinear form*, Siberian Adv. Math. **1**, No. 4, 1–43 (1991).

[47] S. Yu. Vasilovsky, *$\mathbb{Z}$-graded polynomial identities of the full matrix algebra*, Commun. Algebra **26 (2)**, 601–612 (1998).

[48] S. Yu. Vasilovsky, *$\mathbb{Z}_n$-graded polynomial identities of the full matrix algebra of order n*, Proc. Amer. Math. Soc. **127 (12)**, 3517–3524 (1999).

[49] C. T. C. Wall, *Graded Brauer groups*, J. Reine Angew. Math. **213**, 187–199 (1963).

[50] K. A. Zhevlakov, A. M. Slinko, I. P. Shestakov, A. I. Shirshov, *Rings that are nearly associative*, Pure and Appl. Math. **104**, Academic Press, 1982.