Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Identidades e Polinômios Centrais para Álgebras de Matrizes

por

Leomaques Francisco Silva Bernardo

sob orientação de

Prof. Dr. Antônio Pereira Brandão Júnior

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, como requisito parcial para obtenção do título de Mestre em Matemática.

Campina Grande - PB
Junho/2009

Identidades e Polinômios Centrais para Álgebras de Matrizes

por

Leomaques Francisco Silva Bernardo

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Sérgio Mota Alves(UFCG)

Prof. Dr. Plamen Emilov Koshlukov(UNICAMP)

Prof. Dr. Antônio Pereira Brandão Júnior(UFCG)
Orientador

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Junho/2009

Abstract

In this work we study polynomial identities and central polynomials for matrix algebras. More precisely, we present the description of the identities and $\mathbb{Z}_n$-graded and $\mathbb{Z}$-graded central polynomials for the algebra $M_n(K)$ (the $n \times n$ matrices over the field K) when the characteristic of K is zero. Afterwards we give the description of the ordinary (nongraded) central polynomials for the algebra $M_2(K)$, the 2×2 matrices over K, assuming the field of characteristic zero. Finally, we present two classical constructions of central polynomials for $M_n(K)$. These appeared as an answer to a problem posed by Kaplansky in 1956 about the existence of nontrivial central polynomials for that algebra.

Resumo

Neste trabalho apresentamos um estudo sobre identidades e polinômios centrais para a álgebra das matrizes. Mais precisamente, apresentamos a descrição das identidades e polinômios centrais $\mathbb{Z}_n$-graduados e $\mathbb{Z}$-graduados para a álgebra $M_n(K)$ (matrizes $n \times n$ sobre um corpo K), quando característica de K é zero. Depois, apresentamos a descrição dos polinômios centrais ordinários para a álgebra $M_2(K)$ (matrizes 2×2 sobre K), também para um corpo de característica zero. Finalmente, apresentamos duas construções clássicas de polinômios centrais para $M_n(K)$, que surgiram como resposta a um problema sugerido por Kaplansky em 1956 sobre a existência de polinômios centrais não triviais para esta álgebra.

Agradecimentos

Meus sinceros agradecimentos:

A **Deus**, força maior que nos inspira e nos faz persistir diante dos obstáculos.

Aos meus pais, **Gervásio, Fátima, Antônio e Francisca**, pelo amor, educação, e anos de dedicação. Aos meus irmãos, tios, e demais familiares pelo afeto, amizade e apoio nas horas difíceis.

A minha avó, **Da. Francisca**, pelos primeiros ensinamentos, em especial, por ter me ensinado as quatro operações fundamentais.

Aos professores do DME/UFCG pela minha formação. Em especial ao Professor Daniel Cordeiro, pela orientação durante a minha graduação, o incentivo e o enorme apoio.

Ao meu orientador do Mestrado, professor Antônio Pereira Brandão, pela confiança, orientação, companheirismo, seriedade, paciência e toda a ajuda que me concedeu com o seu conhecimento matemático.

Aos professores e funcionários da Pós-Graduação em Matemática da UFCG que contribuíram direta ou indiretamente com a minha formação e para a conclusão deste trabalho.

A minha amiga, professora Marisa, pelo incentivo, a confiança, o carinho, os conselhos. És um grande exemplo a ser seguido.

Aos amigos e companheiros de Mestrado, pessoas que me encorajaram a seguir com esse e outros projetos, em especial, Reginaldo, Suene, Maria Joseane, Marília, Rivaldo e David.

Aos professores da Banca Examinadora que avaliaram o trabalho e cujas sugestões ajudaram a melhorar consideravelmente o nosso trabalho.

A CAPES pelo apoio financeiro.

A todos, meu muito obrigado.

Dedicatória

Aos meus pais, Gervásio e Fátima.

Sumário

Introdução

A teoria das álgebras com identidades polinomiais é de grande importância na Teoria de Anéis. Uma identidade polinomial de uma álgebra A é um polinômio $f(x_1, x_2, \ldots, x_n)$ em variáveis não comutativas que se anula quando avaliado em quaisquer elementos de A. Dizemos que A é uma PI-álgebra quando existe um polinômio não nulo nestas condições. Podemos citar como exemplo de PI-álgebras as álgebras comutativas, as de dimensão finita e as nilpotentes. Uma vez que as identidades polinomiais dizem muito sobre a estrutura de uma álgebra, seu estudo passa a ser de grande relevância.

A teoria das álgebras com identidades polinomiais ou PI-teoria teve início com trabalhos de matemáticos como Jacobson, Kaplansky, Levitzki, Dubnov e Ivanov (podemos citar como exemplos [26], [27], [37], [14]), que tratavam da estrutura de anéis (ou álgebras) que satisfazem uma identidade polinomial, e começou a se desenvolver mais intensamente por volta de 1950 quando foi provado o Teorema de Amitsur-Levitzki [10], o qual afirma que a álgebra $M_n(K)$ das matrizes $n \times n$ sobre um corpo K satisfaz a identidade "standard"de grau $2n$. Ao longo dos anos a PI-teoria tem sido desenvolvida e exposta através de excelentes trabalhos (artigos e livros) de matemáticos como Nagata, Higman, Posner, Amitsur, Herstein, Procesi, Rowen, Shirshov, Drensky (podemos citar como exemplos [39], [25], [42], [3], [23], [24], [43], [49], [50], [51], [13]) entre outros.

Uma das questões centrais na PI-teoria está relacionada à descrição das identidades polinomiais de uma álgebra, isto é, a determinação de uma base para o T-ideal (ideal das identidades) desta álgebra. Em 1950, Specht levantou o seguinte questionamento: "*Toda álgebra associativa possui uma base finita para suas identidades polinomiais?*". Esta pergunta ficou conhecida como Problema de Specht. Em 1987, Kemer, em seu importante trabalho ([29],[30]) sobre a estrutura dos T-ideiais em característica zero, deu uma resposta afirmativa para este problema. Contudo, Kemer não mostra como determinar uma tal base finita e portanto não resolve o problema da descrição das identidades de uma álgebra, problema este que continua em aberto até hoje, tendo sido resolvido apenas para algumas álgebras em particular.

O trabalho de Kemer sobre T-ideais tornou-se importante não somente por responder afirmativamente ao famoso Problema de Specht, mas por ter tratado das álgebras T-primas, álgebras cujos T-ideais são T-primos. Kemer mostra em seu trabalho que os únicos T-ideais T-primos não-triviais em característica zero são os T-ideais das álgebras $M_n(K)$, $M_n(E)$ e $M_{a,b}(E)$, onde E é a álgebra de Grassmann de dimensão infinita e $M_{a,b}(E)$ é a subálgebra de $M_{a+b}(E)$ que consiste das matrizes que têm na diagonal principal um bloco $a \times a$ e outro $b \times b$ com entradas em E_0, o centro de E, e na diagonal secundária blocos com entradas em E_1, a parte anticomutativa de E. A partir do trabalho de Kemer foi mostrado que em característica zero vale as seguintes igualdades $T(M_{a,b}(E) \otimes E) = T(M_{a+b}(E))$, $T(M_{a,b}(E) \otimes M_{c,d}(E)) = T(M_{ac+bd,ad+bc}(E))$ e $T(E \otimes E) = T(M_{1,1}(E))$, onde $T(A)$ denota o T-ideal das identidades da álgebra A. Este resultado é conhecido como o Teorema do Produto Tensorial de Kemer e do qual segue que o produto tensorial $A \otimes B$ de álgebras T-primas é PI-equivalente a uma álgebra T-prima.

Ainda se conhece pouco sobre as descrições das identidades das álgebras T-primas. As identidades da álgebra de Grassmann E foram descritas em característica zero por Latyshev [35] e por Krakowski e Regev [34] (veja também o artigo [20] para as identidades de E sobre corpos infinitos de característica diferente de 2). A descrição das identidades de $M_n(K)$ é conhecida apenas no caso $n = 2$ e foi dada por Razmyslov [44] e Drensky [10], em característica zero, e por Koshlukov [31], para corpos infinitos de característica diferente de 2. No caso de K ser um corpo finito as identidades de $M_n(K)$ foram descritas por Maltsev e Kuzmin [38] no caso $n = 2$ e por Genov e Siderov quando $n = 3$ ou 4 ([18] e [19]). Em característica zero, se conhece a descrição das identidades de $E \otimes E$, e consequentemente de $M_{1,1}(E)$, o qual foi feita por Popov [41]. Vale salientar que em característica positiva ainda não se tem descrição para as identidades destas álgebras e nem é válida a igualdade $T(E \otimes E) = T(M_{1,1}(E))$.

Uma das maiores ferramentas no trabalho de Kemer foi o uso de identidades graduadas. Este tipo de identidade é uma generalização das identidades ordinárias e tem uma estreita relação com elas. Dessa forma, as identidades graduadas têm grande importância na PI-teoria e por essa razão se tornaram objetos de estudos independentes.

As álgebras E, $M_2(K)$, $M_{1,1}(E)$ e $E \otimes E$ possuem $\mathbb{Z}_2$-graduações naturais e os geradores de suas identidades $\mathbb{Z}_2$-graduadas já são conhecidos. As identidades $\mathbb{Z}_2$-graduadas de $M_2(K)$ e de $M_{1,1}(E)$ foram descritas por Di Vincenzo [9], em característica zero, e por Koshlukov e Azevedo [32], para corpos infinitos de característica diferente de 2. No caso das álgebras $M_n(K)$, as identidades $\mathbb{Z}$-graduadas e as $\mathbb{Z}_n$-graduadas foram descritas para n qualquer por Vasilovsky ([54] e [55]), em característica zero, e por Azevedo ([5] e [4]), para corpos infinitos. Apresentaremos neste trabalho a descrição das identidades $\mathbb{Z}$-graduadas e as $\mathbb{Z}_n$-graduadas para $M_n(K)$, no caso de K ser um corpo de característica zero.

Além das identidades graduadas, existem outros tipos importantes de identidades: identidades fracas, identidades traço e identidades com involução. Neste trabalho trataremos apenas de identidades fracas, os quais serão importantes para a construção de um polinômio central para a álgebra $M_n(K)$ (veja [6]) que será apresentada no último capítulo.

Um outro conceito também de grande importância na PI-teoria é o de polinômio central. Um polinômio $f(x_1, x_2, \ldots, x_n)$ é dito central para uma álgebra A se resulta em um elemento do centro de A quando avaliado em quaisquer elementos desta álgebra. Como exemplo de polinômios centrais podemos citar as identidades polinomiais, conhecidas por polinômios centrais triviais. Em 1956, Kaplansky [28] apresentou uma lista de problemas em aberto que motivaram diversos pesquisadores nas décadas seguintes. Um dos problemas era sobre a existência de polinômio central não trivial para a álgebra das matrizes $M_n(K)$, onde $n > 2$ (no caso $n = 2$ o polinômio de Hall $[x_1, x_2][x_3, x_4] + [x_3, x_4][x_1, x_2]$ já era conhecido). A solução para este problema só foi dada 1972-1973 independentemente por Formanek [15] e Razmyslov [45] (veja também [47]). Mais tarde, outros polinômios centrais para $M_n(K)$ foram construídos, veja por exemplo [22], [12] e [21].

Assim como na descrição de identidades, a descrição dos polinômios centrais de uma álgebra é uma questão de grande importância na PI-Teoria, embora ainda se conheça pouco neste sentido. No caso das álgebras $M_n(K)$, geradores dos polinômios centrais são conhecidos apenas no caso $n = 2$, e foram determinados por Okhitin [40], quando $char K = 0$, e por Colombo e Koshlukov [8], quando K é infinito e de característica diferente de 2. Uma descrição detalhada da estrutura de módulo dos polinômios centrais para $M_2(K)$, quando $char K = 0$, pode ser vista em Formanek [16]. No caso da álgebra exterior, um estudo dos polinômios centrais é feita em [1]. Também foram descritos os polinômios centrais graduados para a álgebra $M_n(K)$, com as graduações dadas pelos grupos $\mathbb{Z}$ e $\mathbb{Z}_n$. Nesta descrição as identidades $\mathbb{Z}$-graduadas e as $\mathbb{Z}_n$-graduadas de $M_n(K)$ representaram uma importante ferramenta.

A importância dos conceitos de identidades polinomiais e polinômios centrais e o fato de se saber pouco sobre as descrições das identidades e dos polinômios centrais da álgebra das matrizes sobre um corpo são motivações importantes para o estudo de tais polinômios. Neste trabalho nos propusemos a fazer este estudo.

O nosso trabalho está organizado em quatro capítulos. No primeiro capítulo são apresentados conceitos e resultados básicos necessários para o desenvolvimento do trabalho. No segundo apresentamos as descrições das identidades e polinômios centrais $\mathbb{Z}$-graduados e $\mathbb{Z}_n$-graduados para a álgebra $M_n(K)$, onde K é um corpo de característica zero. Nestas descrições consideramos as graduações naturais de $M_n(K)$ pelos grupos $\mathbb{Z}_n$ e $\mathbb{Z}$. No terceiro capítulo é apresentada a descrição dos polinômios centrais para a álgebra $M_2(K)$, quando $char K = 0$. Finalmente, no quarto capítulo apresentamos as construções de polinômios centrais feitas por Formanek [15] e Razmyslov [45] para a álgebra $M_n(K)$, construções que surgiram como resposta ao problema sugerido por Kaplansky e a construção dada por Latyshev e Shmelkin [36] de um polinômio central em uma variável para a álgebra $M_n(K)$, onde K é um corpo finito.

Capítulo 1

Conceitos Básicos

Neste capítulo apresentaremos os conceitos e resultados necessários para o desenvolvimento deste trabalho. Vamos iniciar com uma discussão sobre álgebras, nosso objeto de estudo. No texto K denotará um corpo e, a menos de alguma menção em contrário, todas as álgebras e espaços vetoriais serão definidos sobre K.

1.1 Álgebras

Definição 1.1.1 *Uma K-**álgebra** (álgebra sobre K ou simplesmente álgebra) é um par $(A, *)$, onde A é um espaço vetorial e $*$ é uma operação binária em A que é uma aplicação bilinear, ou seja, $* : A \times A \longrightarrow A$ satisfaz*

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

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

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

para quaisquer $a, b, c \in A$ e $\lambda \in K$.

Na definição acima, $*$ é chamado de produto ou multiplicação. Para simplificar a notação, vamos denotar uma K-álgebra $(A, *)$ por A, e escreveremos ab, ao invés de $a*b$, para $a, b \in A$. Definimos $a_1a_2a_3$ como sendo $(a_1a_2)a_3$ e, indutivamente, $a_1a_2 \ldots a_na_{n+1}$ como sendo $(a_1a_2 \ldots a_n)a_{n+1}$ para $a_i \in A$. Um subconjunto β é uma base da álgebra A se β é uma base de A como espaço vetorial. Neste caso, definimos a *dimensão* de A como sendo a dimensão do espaço vetorial A.

Definição 1.1.2 *Uma álgebra A é dita ser:*

- ***associativa*** *se $(ab)c = a(bc)$, para quaisquer $a, b, c \in A$.*

- ***comutativa*** *se* $ab = ba$, *para quaisquer* $a, b \in A$.

- ***unitária****(ou com unidade), se o produto possui elemento neutro, isto é, se existe um elemento* $1_A \in A$ *chamado de unidade de* A *tal que* $1_A a = a 1_A = a$ *para todo* $a \in A$.

- ***álgebra de Lie*** *se para quaisquer* $a, b, c \in A$ *valem* $a^2 = aa = 0$ *e* $(ab)c + (bc)a + (ca)b = 0$ *(identidade de Jacobi).*

- ***nil*** *se para cada* $a \in A$, *existe* $n \in \mathbb{N}$ *tal que* $a^n = 0$. *O elemento* a *é chamado de nilpotente e o menor natural* n *com tal propriedade é denominado índice de nilpotência de* a. *Quando existe* $n \in \mathbb{N}$ *tal que* $a^n = 0$ *para todo* $a \in A$, *dizemos que* A *é nil de índice limitado.*

- ***nilpotente*** *se existe* $n \in \mathbb{N}$ *tal que o produto de quaisquer* $n + 1$ *elementos de* A *com qualquer disposição de parênteses é igual a zero (se* A *é de Lie ou associativa, isto equivale a dizer que* $a_1 a_2 \ldots a_n a_{n+1} = 0$ *para quaisquer* $a_1, a_2, \ldots, a_n, a_{n+1} \in A$*). Neste caso, definimos o índice (ou classe) de nilpotência de* A *como sendo o menor* n *que satisfaz esta condição.*

Observe que se A é uma álgebra nilpotente, então é nil de índice limitado. Claramente, uma álgebra nil não pode ter unidade.

Observação 1.1.3 *Se* A *e* B *são espaços vetoriais,* β *uma base de* A *e* $f : \beta \longrightarrow B$ *é uma aplicação qualquer, então existe uma única aplicação linear* $F : A \longrightarrow B$ *estendendo* f. *Além disso, se* $g : \beta \times \beta \longrightarrow A$ *é uma aplicação qualquer, então existe uma única aplicação bilinear* $G : A \times A \longrightarrow A$ *estendendo* g. *Assim, para definir uma estrutura de álgebra em* A, *basta definir o produto para os elementos de uma base. Uma vez definido o produto, verifica-se que* A *é uma álgebra associativa se, e somente se,* $(v_1 v_2) v_3 = v_1 (v_2 v_3)$ *para quaisquer* $v_1, v_2, v_3 \in \beta$. *Isto deve-se ao fato de que a aplicação* $h : A \times A \times A \longrightarrow A$, *definida por* $h(a, b, c) = (ab)c - a(bc)$, *sendo trilinear, é nula se, e somente se, é nula em* $\beta \times \beta \times \beta$.

Em praticamente todo trabalho vamos tratar de álgebras associativas com unidade. De agora em diante, a menos que seja mencionado o contrário, o termo álgebra deverá ser entendido como álgebra associativa unitária. Apresentaremos a seguir alguns exemplos importantes de álgebras.

Exemplo 1.1.4 *O espaço vetorial* $M_n(K)$ *das matrizes* $n \times n$ *com entradas em* K, *munido da multiplicação usual de matrizes, é uma álgebra associativa com unidade a qual é exatamente a matriz identidade* I_n. *Nesta álgebra é importante destacar as* *matrizes unitárias* E_{ij}, *para* $1 \leq i, j \leq n$, *onde* E_{ij} *é a matriz cuja única entrada não nula é* 1 *na i-ésima linha e j-ésima coluna. É fácil ver que elas formam uma base para* $M_n(K)$ *e portanto a dimensão desta álgebra é* n^2. *Mais geralmente, se* A *é uma álgebra, consideremos o espaço vetorial* $M_n(A)$ *de todas as matrizes* $n \times n$ *com entradas em* A. *O produto em* $M_n(A)$ *é análogo ao produto em* $M_n(K)$. *Temos que* $M_n(A)$, *munido deste produto, é uma álgebra.*

Exemplo 1.1.5 *Seja* V *um espaço vetorial com base* $\{e_1, e_2, e_3, \ldots\}$. *Definimos a* ***álgebra de Grassmann (ou álgebra exterior)*** *de* V, *denotada por* E, *como sendo a álgebra com base*

$$\{1, e_{i_1}e_{i_2}\ldots e_{i_k} \mid i_1 < i_2 < \ldots < i_k, k \geq 1\}$$

e cujo produto é definido pelas relações

$$e_i^2 = 0 \text{ e } e_ie_j = -e_je_i \text{ para quaisquer } i, j \in \mathbb{N}.$$

Destacamos em E *os seguintes subespaços vetoriais:*

- E_0, *gerado pelo conjunto* $\{1, e_{i_1}e_{i_2}\ldots e_{i_m} \mid m \text{ é par}\}$
- E_1, *gerado pelo conjunto* $\{e_{i_1}e_{i_2}\ldots e_{i_k} \mid k \text{ é ímpar}\}$

Claramente, $E = E_0 \oplus E_1$ *como espaço vetorial. Desde que* $e_ie_j = -e_je_i$ *temos* $(e_{i_1}\ldots e_{i_m})(e_{j_1}\ldots e_{j_k}) = (-1)^{mk}(e_{j_1}\ldots e_{j_k})(e_{i_1}\ldots e_{i_m})$ *para quaiquer* $m, k \in \mathbb{N}$, *e assim podemos concluir que* $ax = xa$ *para quaisquer* $a \in E_0$ *e* $x \in E$, *e* $bc = -cb$ *para quaisquer* $b, c \in E_1$. *Observamos facilmente que se* $charK = 2$, *então* E *é uma álgebra comutativa.*

Considerando E' *a álgebra com base* $\{e_{i_1}e_{i_2}\ldots e_{i_k} \mid i_1 < i_2 < \ldots < i_k, k \geq 1\}$, *temos que* E' *não tem unidade e é chamada de* ***álgebra exterior sem unidade***.

Se A é uma álgebra associativa e $a, b \in A$, definimos o *comutador* $[a, b] = ab - ba$ e $a \circ b = ab + ba$. Mais geralmente, definimos o *comutador de comprimento* n como sendo $[a_1, \ldots, a_{n-1}, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$, onde $a_i \in A$. A partir de um cálculo direto, podemos mostrar que

$$[ab, c] = a[b, c] + [a, c]b \text{ para quaisquer } a, b, c \in A. \tag{1.1}$$

Se $a \in A$ e $T_a : A \longrightarrow A$ é tal que $T_a(x) = [x, a]$, então por 1.1 segue que T_a é uma derivação. Logo, usando indução sobre n pode-se mostrar que

$$[a_1a_2\ldots a_n, c] = \sum_{i=1}^{n} a_1\ldots a_{i-1}[a_i, c]a_{i+1}\ldots a_n. \tag{1.2}$$

Se A é uma álgebra, V e W subespaços vetoriais de A, definimos o produto VW como sendo o subespaço vetorial de A gerado pelo conjunto $\{xy \mid x \in V, y \in W\}$.

Definição 1.1.6 *Um subespaço vetorial B de uma álgebra A será denominado de* ***subálgebra*** *de A se $BB \subseteq B$ e $1 \in B$. Um subespaço vetorial I de A será denominado de* ***ideal*** *de A se $AI \subseteq I$ e $IA \subseteq I$, ou seja, se ax, $xa \in I$ para quaisquer $a \in A$ e $x \in I$.*

Exemplo 1.1.7 *Considere a álgebra exterior E (Exemplo 1.1.5). Dado $n \in \mathbb{N}$ consideremos o subespaço E_n de E gerado pelo conjunto*

$$\{1, e_{i_1}e_{i_2}\dots e_{i_k} \mid i_1 < i_2 < \dots < i_k \leq n\}.$$

O subespaço E_n é uma subálgebra de E de dimensão 2^n e é a álgebra exterior do espaço vetorial com base $\{e_1, e_2, \dots, e_n\}$.

Exemplo 1.1.8 (Centro de uma álgebra) *Seja A uma álgebra. O conjunto $Z(A) = \{a \in A \mid ax = xa, \forall x \in A\}$ é uma subálgebra de A denominada* ***centro de*** *A. Um fato conhecido da Álgebra Linear elementar é que dado $n \in \mathbb{N}$ tem-se $Z(M_n(K)) = \{\lambda I_{n\times n} \mid \lambda \in K\}$ (matrizes escalares). Se $A = E$(álgebra exterior), então $Z(E) = E_0$ ($charK \neq 2$).*

Exemplo 1.1.9 (Subálgebra gerada) *Sejam A uma álgebra e $\emptyset \neq S \subseteq A$. Consideremos o subespaço B_S de A gerado por $\{1, s_1s_2\dots s_k \mid k \in \mathbb{N}, s_i \in S\}$. Temos que B_S é multiplicativamente fechado e $1 \in B_S$. Portanto, B_S é uma subálgebra de A, chamada de* ***subálgebra gerada por*** *S. Além disso, toda subálgebra de A que contém S deve conter B_S e assim B_S é a menor subálgebra de A contendo S.*

Definição 1.1.10 *Sejam A e B duas álgebras. Uma transformação linear $\varphi : A \longrightarrow B$ é um* ***homomorfismo*** *de álgebras se $\varphi(xy) = \varphi(x)\varphi(y)$ para quaisquer $x, y \in A$ e $\varphi(1_A) = 1_B$. Dizemos que φ é um* ***mergulho****(ou monomorfismo) se φ é um homomorfismo injetivo,* ***isomorfismo*** *se φ é bijetivo,* ***endomorfismo*** *se φ é um homomorfismo e $A = B$ e* ***automorfismo*** *se φ é um endomorfismo bijetivo (endomorfismo e isomorfismo ao mesmo tempo).*

Denotamos por $EndA$ e $AutA$ os conjuntos dos endomorfismos e automorfismos, respectivamente, da álgebra A. Quando existe um isomorfismo $\psi : A \longrightarrow B$, dizemos que as álgebras A e B são isomorfas e denotamos por $A \simeq B$.

Se $\varphi : A \longrightarrow B$ é um homomorfismo de álgebras, o conjunto $Ker\varphi = \{a \in A \mid \varphi(a) = 0\}$, chamado de *núcleo de φ* é um ideal de A, e o conjunto $Im\varphi = \{\varphi(a) \mid a \in A\}$, chamado de *imagem de φ*, é uma subálgebra de B.

Sendo A uma álgebra e I um ideal de A, consideremos no espaço vetorial quociente A/I o produto $(a+I)(b+I) = ab+I$ para $a, b \in A$. Este produto está bem definido (não depende da escolha dos representantes das classes laterais) e torna A/I uma álgebra, conhecida por *álgebra quociente de A por I*. Denotaremos $a+I$ por $\overline{a}$. Seja $\varphi : A \longrightarrow B$ um homomorfismo de álgebras. Se I é um ideal de A e $I \subseteq Ker\varphi$, então a aplicação

$$\begin{array}{rcccc} \overline{\varphi} & : & A/I & \longrightarrow & B \\ & & \overline{a} & \longmapsto & \overline{\varphi}(\overline{a}) = \varphi(a) \end{array}$$

é bem definida e é um homomorfismo de álgebras. Se $I = Ker\varphi$, então $\overline{\varphi}$ é injetora e consequentemente $A/Ker\varphi \simeq Im\overline{\varphi} = Im\varphi$.

Apresentaremos a seguir alguns exemplos importantes de homomorfismos.

Exemplo 1.1.11 *Sejam A uma álgebra e I um ideal de A. A aplicação $\pi : A \longrightarrow A/I$, definida por $\pi(a) = \overline{a}$, é um homomorfismo de álgebras chamado de projeção canônica.*

Exemplo 1.1.12 *Seja A uma álgebra. Dizemos que um elemento $a \in A$ é **invertível** se existe $a^{-1} \in A$ tal que $aa^{-1} = a^{-1}a = 1$. Vamos denotar por $U(A)$ o conjunto dos elementos invertíveis de A. Se $r \in U(A)$, a aplicação $\xi_r : A \longrightarrow A$, definida por $\xi_r(x) = r^{-1}xr$, é um automorfismo de A, chamado de **automorfismo interno determinado por** r.*

Exemplo 1.1.13 *Seja A' uma álgebra sem unidade. Consideremos o espaço vetorial*

$$A = K \oplus A' = \{(\lambda, a) \mid \lambda \in K, a \in A'\}$$

*Definimos em A o seguinte produto $(\lambda_1, a_1)(\lambda_2, a_2) = (\lambda_1\lambda_2, \lambda_1 a_2 + \lambda_2 a_1 + a_1 a_2)$. O conjunto A, munido deste produto, é uma álgebra associativa com unidade (o elemento (1,0)). A aplicação $\Phi : A' \longrightarrow A$ definida por $\Phi(a) = (0, a)$ é um mergulho. Dizemos que A é obtida de A' por **adjunção da unidade**.*

Exemplo 1.1.14 *As álgebras E (álgebra exterior) e $K \oplus E'$ (Exemplo 1.1.13) são isomorfas, pois $\Psi : K \oplus E' \longrightarrow E$, definida por $\Psi(\lambda, x) = \lambda + x$ é um isomorfismo.*

1.2 Identidades Polinomiais

Nesta seção introduziremos o conceito de Identidade Polinomial. Vamos iniciar com a definição de álgebras livres, cuja importância está no fato de ser o "ambiente" onde as identidades polinomiais aparecem.

Definição 1.2.1 *Seja $\mathcal{V}$ uma classe de álgebras. Dizemos que uma álgebra $F \in \mathcal{V}$ é uma **álgebra livre** de $\mathcal{V}$ se existe um subconjunto Y gerador de F tal que para toda álgebra $\mathcal{A} \in \mathcal{V}$ e toda aplicação $h : Y \to \mathcal{A}$ existe um único homomorfismo de álgebras $\varphi : F \to \mathcal{A}$ estendendo h. F é então dita ser livremente gerada por Y e a cardinalidade $|Y|$ do conjunto Y é chamada de posto de F.*

A seguir construíremos uma álgebra livre na classe de todas as álgebras associativas unitárias. Seja $X = \{x_1, x_2, \ldots\}$ um conjunto não-vazio e enumerável de *variáveis* não-comutativas. Uma *palavra* em X é uma sequência $x_{i_1}x_{i_2}\ldots x_{i_n}$ onde $n \in \mathbb{N}$ e $x_{i_j} \in X$. Vamos denotar por 1 a palavra vazia. Dizemos que duas palavras $x_{i_1}x_{i_2}\ldots x_{i_n}$ e $x_{j_1}x_{j_2}\ldots x_{j_m}$ são iguais se $n = m$ e $i_1 = j_1, i_2 = j_2, \ldots, i_n = j_n$. Consideremos $K\langle X\rangle$ o espaço vetorial que tem por base o conjunto de todas as palavras em X. Dessa forma, os elementos de $K\langle X\rangle$, que chamaremos de *polinômios*, são somas (formais) de termos (ou monômios) que são produtos (formais) de um escalar por uma palavra em X. Consideremos em $K\langle X\rangle$ a seguinte multiplicação

$$(x_{i_1}\ldots x_{i_k})(x_{j_1}\ldots x_{j_l}) = x_{i_1}\ldots x_{i_k}x_{j_1}\ldots x_{j_l} \quad onde \quad x_{i_t}, x_{j_s} \in X.$$

O espaço vetorial $K\langle X\rangle$ munido deste produto é uma álgebra associativa (veja a Observação 1.1.3) com unidade, que é a palavra vazia. Observe que X gera $K\langle X\rangle$ como álgebra.

Proposição 1.2.2 *A álgebra $K\langle X\rangle$ é livre na classe das álgebras associativas com unidade.*

Demonstração: Sejam A uma álgebra e $h : X \longrightarrow A$ uma aplicação qualquer, com $h(x_i) = a_i$ para $i \in \mathbb{N}$. Da Observação 1.1.3 segue que existe uma aplicação linear $\varphi_h : K\langle X\rangle \to A$ tal que $\varphi_h(1) = 1_A$ e $\varphi_h(x_{i_1}x_{i_2}\ldots x_{i_n}) = a_{i_1}a_{i_2}\ldots a_{i_n}$. Temos que φ_h é um homomorfismo de álgebras e é o único satisfazendo $\varphi_h|_X = h$. ∎

Definição 1.2.3 *Seja A uma álgebra. Um polinômio $f(x_1, \ldots, x_n) \in K\langle X\rangle$ (ou a expressão $f(x_1, \ldots, x_n) = 0$) é dito ser uma **identidade polinomial** da álgebra A, se $f(a_1, \ldots, a_n) = 0$ para quaisquer $a_1, \ldots, a_n \in A$.*

Observemos que $f = f(x_1, \ldots, x_n)$ é uma identidade polinomial de A se, e somente se, f pertence aos núcleos de todos os homomorfismos de $K\langle X\rangle$ em A. Denotando por $T(A)$ o conjunto de todas as identidades polinomiais de A, dizemos que A é uma

álgebra com identidade polinomial ou **PI-álgebra**[1] se $T(A) \neq \{0\}$. Se A_1 e A_2 são álgebras tais que $T(A_1) = T(A_2)$, dizemos que A_1 e A_2 são **PI-equivalentes**.

Apresentaremos a seguir alguns exemplos de álgebras com identidades polinomiais.

Exemplo 1.2.4 *Se A é uma álgebra comutativa, então o polinômio comutador $f(x_1, x_2) = [x_1, x_2] = x_1x_2 - x_2x_1$ é uma identidade polinomial de A.*

Exemplo 1.2.5 *A álgebra de Grassmann E é uma PI-álgebra, pois o polinômio $[x_1, x_2, x_3]$ é uma identidade polinomial de E. Para ver isto, basta observar que $[a, b] \in E_0 = Z(E)$ para quaisquer $a, b \in E$.*

Exemplo 1.2.6 *A álgebra $M_2(K)$ satisfaz a identidade $f(x_1, x_2, x_3) = [[x_1, x_2]^2, x_3]$ conhecida como a* ***identidade de Hall****. De fato, basta observar que:*

(1) Se $A, B \in M_n(K)$, então $tr([A, B]) = 0$;

(2) Se $A \in M_2(K)$ e $tr(A) = 0$, então $A^2 = \lambda I_2$ onde I_2 é a matriz identidade de $M_2(K)$.

Exemplo 1.2.7 *Considere o polinômio*

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

onde S_n é o grupo simétrico das permutações de $\{1, 2, \ldots, n\}$ e $(-1)^\sigma$ é o sinal da permutação σ. O polinômio s_n é chamado de ***polinômio standard de grau*** *n. Em [2] foi provado que $s_{2n}(x_1, \ldots, x_{2n}) \in T(M_n(K))$, fato conhecido por* ***Teorema de Amitsur-Levitzki****. Posteriormente, foram apresentadas outras demonstrações deste teorema (veja [33], [53], [46] e [48],).*

Os conceitos que apresentaremos a seguir, assim como suas propriedades, são de fundamental importância na PI-teoria.

Definição 1.2.8 *Um ideal I de $K\langle X\rangle$ é dito ser um* ***T-ideal*** *se $\phi(I) \subseteq I$ para todo $\phi \in EndK\langle X\rangle$, ou equivalentemente, se $f(g_1, \ldots, g_n) \in I$ para quaisquer $f(x_1, \ldots, x_n) \in I$ e $g_1, \ldots, g_n \in K\langle X\rangle$.*

Proposição 1.2.9 *O conjunto $T(A)$ das identidades de uma álgebra A é um T-ideal de $K\langle X\rangle$. Reciprocamente, se I é um T-ideal de $K\langle X\rangle$, então existe alguma álgebra B tal que $T(B) = I$.*

[1] a sigla vem do inglês - polinomial identity.

Demonstração: É fácil ver que $T(A)$ é um ideal de $K\langle X\rangle$. Sejam $f(x_1,\ldots,x_n) \in T(A)$ e $\varphi \in EndK\langle X\rangle$, arbitrários. Se $\psi : K\langle X\rangle \to A$ é um homomorfismo qualquer, então $\psi(\varphi(f)) = (\psi\circ\varphi)(f) = 0$, pois $\psi\circ\varphi : K\langle X\rangle \to A$ é um homomorfismo de álgebras e $f \in T(A)$. Daí, $\varphi(f) \in Ker(\psi)$ e portanto $\varphi(f) \in T(A)$.

Seja I um T-ideal de $K\langle X\rangle$. Tomemos a álgebra quociente $B = K\langle X\rangle/I$ e a projeção canônica $\pi : K\langle X\rangle \longrightarrow K\langle X\rangle/I$. Se $f \in T(B)$, então $f \in Ker(\pi)$. Como $Ker(\pi) = I$, temos $T(B) \subseteq I$. Por outro lado, se $f(x_1,\ldots,x_n) \in I$ e $g_1,\ldots,g_n \in K\langle X\rangle$, então $f(g_1,\ldots,g_n) \in I$ e daí $f(\overline{g_1},\ldots,\overline{g_n}) = \overline{f(g_1,\ldots,g_n)} = \overline{0}$. Logo, $f \in T(B)$, o que conclui a demonstração. ■

Não é difícil ver que a intersecção de uma família qualquer de T-ideais é ainda um T-ideal. Segue então a seguinte definição.

Definição 1.2.10 *Seja S um subconjunto de $K\langle X\rangle$. Definimos o* ***T-ideal gerado por*** *S, denotado por $\langle S\rangle^T$, como sendo a interseção de todos os T-ideais de $K\langle X\rangle$ que contém S. Dessa forma, $\langle S\rangle^T$ é o menor T-ideal contendo S.*

Do ponto de vista prático, o T-ideal gerado por S coincide com o subespaço vetorial de $K\langle X\rangle$ gerado pelo conjunto

$$\{h_1 f(g_1,\ldots,g_n)h_2 \mid f \in S, h_1, h_2, g_1,\ldots,g_n \in K\langle X\rangle\}.$$

Se A é uma álgebra e $S \subseteq T(A)$ é tal que $T(A) = \langle S\rangle^T$ dizemos que S é uma **base das identidades** de A. Se um polinômio $f(x_1,\ldots,x_n) \in \langle S\rangle^T$ dizemos que f segue de S, ou que f é uma consequência de S.

Um dos problemas centrais da PI-teoria é encontrar, para uma dada álgebra, bases para suas identidades polinomiais. Sendo A uma álgebra, caso $T(A)$ possua uma base finita e todo T-ideal I com $I \supseteq T(A)$ também tem base finita, dizemos que A satisfaz a **propriedade de Specht** (W. Specht). A questão da existência da base finita para as identidades das álgebras associativas sobre corpos de característica zero é conhecida como **problema de Specht** e, em [30], Kemer deu uma resposta positiva para esta questão.

Vejamos agora alguns exemplos de bases de identidades de algumas álgebras importantes.

Exemplo 1.2.11 *Se A é uma álgebra comutativa com unidade e K é um corpo infinito, então $T(A) = \langle [x_1, x_2] \rangle^T$. Dizemos então que todas as identidades de $\mathcal{A}$ seguem (ou são consequências) do polinômio $[x_1, x_2]$.*

Exemplo 1.2.12 *Se K é um corpo infinito de característica diferente de 2, então $T(E) = \langle [x_1, x_2, x_3] \rangle^T$ (veja [34] e [20]). No caso de K ser finito Stojanova-Venkova [52] descreveu as identidades da álgebra exterior não-unitária e de dimensão finita e Siderov [7] descreveu as identidades quando a dimensão é infinita.*

Exemplo 1.2.13 *Em 1973, Razmyslov [44] provou que $T(M_2(K))$ é finitamente gerado para $charK = 0$, determinando uma base com 9 identidades. Posteriormente, Drensky [10] mostrou que $T(M_2(K)) = \langle s_4(x_1, x_2, x_3, x_4), [[x_1, x_2]^2, x_3] \rangle^T$, também quando $charK = 0$. Em 2001, Koshlukov [31] generalizou este resultado de Drensky para K infinito de característica diferente de 2 e 3. Quando $charK = 3$, uma terceira identidade é necessária para gerar o T-ideal (veja [8]). Para $charK = 2$, o problema da descrição de $T(M_2(K))$ ainda está em aberto.*

1.3 Variedades e Álgebras Relativamente Livres

Apresentaremos nesta seção um breve estudo sobre variedades de álgebras e álgebras relativamente livres.

Definição 1.3.1 *Seja S um subconjunto de $K\langle X \rangle$. A classe $\mathcal{B}$ de todas as álgebras que têm todos os polinômios de S como identidades é chamada de* ***variedade*** *(de álgebras associativas) definida por S. A* ***variedade trivial*** *é a classe de álgebras que contém apenas a álgebra nula (isto é, é a variedade cujo conjunto de identidades que a definem é $K\langle X \rangle$).*

Se $\mathcal{B}$ é uma classe de álgebras, seja $T(\mathcal{B})$ a interseção de todos os T-ideais $T(A)$ com $A \in \mathcal{B}$. A variedade de álgebras definida por $T(\mathcal{B})$ é chamada de **variedade gerada por** $\mathcal{B}$ e denotada por $var\mathcal{B}$. Se $\mathcal{B} = \{R\}$, então denotamos $var\mathcal{B}$ simplesmente por $varR$. Observe que a variedade definida por S é igual à variedade definida por $\langle S \rangle^T$.

Teorema 1.3.2 (Birkhoff) *Uma classe não-vazia de álgebras $\mathcal{B}$ é uma variedade se, e somente se, é fechada a produtos diretos, subálgebras e álgebras quocientes.*

Demonstração: Veja [13], página 24. ∎

Definição 1.3.3 *Seja $\mathcal{V}$ uma variedade de álgebras. Para um conjunto fixo Y, a álgebra $F \in \mathcal{V}$ é uma* ***álgebra relativamente livre de*** *$\mathcal{V}$, se F é livre na classe $\mathcal{V}$ (livremente gerada por Y, veja definição 1.2.1). A cardinalidade de Y é chamada o* ***posto de*** *F.*

Teorema 1.3.4 *Toda variedade $\mathcal{V}$ (não-trivial) possui alguma álgebra relativamente livre. Além disso, duas álgebras relativamente livres de mesmo posto em $\mathcal{V}$ são isomorfas.*

Demonstração: Seja $T(\mathcal{V}) = \bigcap_{R\in\mathcal{V}} T(R)$ e considere $\pi : K\langle X\rangle \longrightarrow K\langle X\rangle/T(\mathcal{V})$ a projeção canônica. Sejam x_1 e x_2 dois elementos distintos de X tais que $\pi(x_1) = \pi(x_2)$. Consideremos uma álgebra não-nula A de $\mathcal{V}$ e um elemento não-nulo $a \in A$. Então existe um homomorfismo $\psi : K\langle X\rangle \longrightarrow A$ tal que $\psi(x_1) = a$ e $\psi(x_2) = 0$. Como $T(\mathcal{V}) \subseteq Ker\psi$, existe um homomorfismo $\phi : K\langle X\rangle/T(\mathcal{V}) \longrightarrow A$ tal que $\phi \circ \pi = \psi$. Mas, $a = \psi(x_1) = (\phi\circ\pi)(x_1) = (\phi\circ\pi)(x_2) = \psi(x_2) = 0$, o que é uma contradição. Logo, $\pi|_X$ é injetora e portanto $\pi(X)$ é enumerável.

A álgebra $K\langle X\rangle/T(\mathcal{V})$ é gerada pelo conjunto $\pi(X)$ e pertence a $\mathcal{V}$, pois satisfaz todas as identidades de $T(\mathcal{V})$. Vamos mostrar que esta álgebra é livre em $\mathcal{V}$, com conjunto gerador livre $\pi(X)$. Sejam $A \in \mathcal{V}$ e σ uma aplicação de $\pi(X)$ em A. Como $K\langle X\rangle$ é a álgebra livre com conjunto gerador X, a aplicação $\sigma\circ\pi : X \longrightarrow A$ estende-se a um homomorfismo $\theta : K\langle X\rangle \longrightarrow A$. Existe um homomorfismo $\rho : K\langle X\rangle/T(\mathcal{V}) \longrightarrow A$ para o qual $\rho\circ\pi = \theta$, pois $T(\mathcal{V}) \subseteq Ker\theta$. Se $x \in X$, temos que $\rho(\pi(x)) = (\rho\circ\pi)(x) = \theta(x) = (\sigma\circ\pi)(x) = \sigma(\pi(x))$, ou seja, o homomorfismo ρ estende a aplicação σ. Portanto, $K\langle X\rangle/T(\mathcal{V})$ é uma álgebra livre na variedade $\mathcal{V}$.

Suponhamos agora F_1 e F_2 álgebras relativamente livres de mesmo posto em $\mathcal{V}$. Sendo F_1 e F_2 livremente geradas por Y_1 e Y_2 respectivamente, tomemos uma bijeção $g : Y_1 \longrightarrow Y_2$. Temos então que existem homomorfismos de álgebras $\varphi_1 : F_1 \longrightarrow F_2$ e $\varphi_2 : F_2 \longrightarrow F_1$ estendendo g e g^{-1}, respectivamente. Logo, $(\varphi_2\circ\varphi_1)(y) = y$ e $(\varphi_1\circ\varphi_2)(z) = z$, para quaisquer $y \in Y_1$ e $z \in Y_2$. Segue então que $\varphi_2\circ\varphi_1 = Id_{F_1}$ e $\varphi_1\circ\varphi_2 = Id_{F_2}$, e portanto φ_1 e φ_2 são isomorfismos. ■

As idéias de variedades e álgebras livres são na verdade mais gerais do que acabamos de apresentar. Para mais detalhes, veja [13], Seções 1.2, 1.2 e 2.3.

1.4 Álgebras envolventes

Seja A uma álgebra associativa. Considere em A o produto $[a,b] = ab - ba$, para $a, b \in A$. Com este produto temos em A uma nova estrutura de álgebra, que denotaremos por $A^{(-)}$. Como $[a,a] = 0$ e $[a,b,c] + [b,c,a] + [c,a,b] = 0$ (identidade de Jacobi) para quaisquer $a, b, c \in A$, segue que $A^{(-)}$ é uma álgebra de Lie. Se uma álgebra de Lie L é isomorfa a uma subálgebra de $A^{(-)}$, dizemos que A é uma *álgebra envolvente de* L.

Exemplo 1.4.1 *Seja L uma álgebra de Lie com base $\{u, v\}$ tal que $u * v = v$. A álgebra $M_2(K)$ é uma álgebra envolvente de L, pois o subespaço vetorial V de $M_2(K)$ gerado por $\{E_{11}, E_{12}\}$ é uma subálgebra de $M_2(K)^{(-)}$ e a aplicação linear $\varphi : L \longrightarrow V$ que satisfaz $\varphi(u) = E_{11}$ e $\varphi(v) = E_{12}$ é um isomorfismo de álgebras.*

Definição 1.4.2 *Seja L uma álgebra de Lie. Diz-se que uma álgebra associativa U é uma **álgebra universal envolvente de** L, e denotamos por $U = U(L)$, se L é uma subálgebra de $U^{(-)}$ e U satisfaz a seguinte propriedade universal: para qualquer álgebra associativa R e qualquer homomorfismo de álgebras de Lie $\varphi : L \to R^{(-)}$ existe um único homomorfismo de álgebras associativas $\psi : U \to R$ que estende φ, ou seja, tal que $\psi|_L = \varphi$.*

Os teoremas que serão apresentados a seguir nos ajudarão a determinar uma base de $K\langle X \rangle$.

Teorema 1.4.3 (Poincaré, Birkhoff, Witt) *Toda álgebra de Lie L possui uma única (a menos de isomorfismos) álgebra universal envolvente $U(L)$. Se L tem uma base $\{e_i \mid i \in I\}$ onde o conjunto de indices I é ordenado, então $U(L)$ tem uma base dada por*

$$e_{i_1} \ldots e_{i_p},\ i_1 \leq \ldots \leq i_p,\ i_k \in I,\ p = 0, 1, 2, \ldots$$

onde $p = 0$ nos dá a unidade de $U(L)$.

Demonstração: Veja [13], página 11. ■

Sendo $X = \{x_1, x_2, \ldots\}$, consideremos

$$ComX = \{[x_{i_1}, x_{i_2}, \ldots, x_{i_k}] \mid\ k \geq 2,\ x_{i_j} \in X\}.$$

Sejam $B(X)$ a subálgebra (com unidade) de $K\langle X \rangle$ gerada por $ComX$ e $L(X)$ o subespaço vetorial de $K\langle X \rangle$ gerado por $X \cup ComX$. Os polinômios de $B(X)$ são chamados de *polinômios próprios*. Consideremos agora a álgebra de Lie $K\langle X \rangle^{(-)}$. Mostra-se que se $u, v \in X \cup ComX$, então $[u, v] \in L(X)$. Portanto, $L(X)$ é uma subálgebra de Lie de $K\langle X \rangle^{(-)}$.

Teorema 1.4.4 (Witt) $U(L(X)) = K\langle X \rangle$.

Demonstração: Veja [13], página 14, teorema 1.3.5. ■

Pode ser demonstrado que a álgebra $L(X)$ é livre na classe das álgebras de Lie. De fato, sejam L uma álgebra de Lie e $h : X \longrightarrow L$ uma aplicação qualquer. Por $K\langle X\rangle$ ser livremente gerada por X, existe um homomorfismo $\varphi : K\langle X\rangle \longrightarrow U(L)$ estendendo h. Temos que $\varphi([x_{i_1}, x_{i_2}, \ldots, x_{i_k}]) = [\varphi(x_{i_1}), \varphi(x_{i_2}), \ldots, \varphi(x_{i_k})]$ para $k \geq 2$, e assim $\varphi(L(X)) \subseteq L$. além disso, é imediato ver que se $f_1, f_2 \in L(X)$, então $\varphi([f_1, f_2]) = [\varphi(f_1), \varphi(f_2)]$. Logo, $\varphi|_{L(X)} : L(X) \longrightarrow L$ é um homomorfismo de álgebras de Lie que estende h. Dizemos então que $L(X)$ é uma *álgebra de Lie livre, livremente gerada por* X.

Consideremos agora uma base ordenada de $L(X)$ consistindo dos elementos

$$x_1, x_2, \ldots, x_n, \ldots, u_1, u_2, \ldots, u_m, \ldots$$

onde $\{u_1, u_2, \ldots\} \subseteq ComX$ é uma base de $[L(X), L(X)]$, o subespaço vetorial de $L(X)$ gerado por $ComX$. Dos teoremas 1.4.3 e 1.4.4 segue que $K\langle X\rangle$ possui uma base formada pelos elementos

$$x_{i_1}^{n_1} x_{i_2}^{n_2} \ldots x_{i_k}^{n_k} u_{j_1} u_{j_2} \ldots u_{j_q}, \ k, q, n_i \geq 0 \tag{1.3}$$

onde $i_1 < i_2 < \ldots < i_k$, $j_1 \leq j_2 \leq \ldots \leq j_q$. Note que os elementos com $k = 0$ formam uma base para $B(X)$ e que se $f(x_1, x_2, \ldots, x_n) \in K\langle X\rangle$, então

$$f(x_1, x_2, \ldots, x_n) = \sum_a \alpha_a x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} g_a, \tag{1.4}$$

onde $a = (a_1, a_2, \ldots, a_n)$, $a_i \geq 0$, $\alpha_a \in K$ e $g_a \in B(X)$. Além disso, pela independência dos elementos em 1.3, temos esta maneira de se expressar f única.

1.5 Polinômios multi-homogêneos e multilineares

Definição 1.5.1 *Sejam $m \in K\langle X\rangle$ um monômio e $x_i \in X$. Definimos o **grau** de x_i em m, denotado por $deg_{x_i} m$, como sendo o número de ocorrências de x_i em m. Um polinômio $f \in K\langle X\rangle$ é dito **homogêneo** em x_i se todos os seus monômios têm o mesmo grau em x_i. f é dito **multi-homogêneo** quando é homogêneo em todas as variáveis e é **multilinear** se é multi-homogêneo em cada monômio e cada variável tem grau exatamente 1.*

Se $m = m(x_1, x_2, \ldots, x_k)$ é um monômio de $K\langle X\rangle$, o **multigrau** de m é a k-upla $(a_1, a_2, \ldots, a_k)$ onde $a_i = deg_{x_i} m$. A soma de todos os monômios de $f \in K\langle X\rangle$ com um dado multigrau, é dito ser uma **componente multi-homogênea** de f. Notemos ainda que $f \in K\langle X\rangle$ é multi-homogêneo se, e somente se, possui uma única componente multi-homogênea. Além disso, $f(x_1, x_2, \ldots, x_k) \in K\langle X\rangle$ é multilinear se é multi-homogêneo com multigrau $(1, 1, \ldots, 1)$. Neste caso, f tem a forma

$$\sum_{\sigma \in S_k} a_\sigma x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(k)},\ a_\sigma \in K.$$

Os próximos resultados nos darão uma importante ferramenta no trabalho de determinar geradores para T-ideais sobre determinados tipos de corpos.

Proposição 1.5.2 *Sejam I um T-ideal de $K\langle X\rangle$ e $f(x_1, x_2, \ldots, x_k) \in I$. Se K é infinito então cada componente multi-homogênea de f pertence a I. Consequentemente, I é gerado por seus polinômios multi-homogêneos.*

Demonstração: Seja n o maior grau em x_1 de algum monômio de f. Para cada $i = 0, 1, \ldots, n$, consideremos $f_i(x_1, x_2, \ldots, x_k)$ como sendo a soma de todos os monômios que têm grau i em x_1 (a componente de grau i em x_1). Temos claramente que $f = f_0 + f_1 + \ldots + f_n$. Como K é infinito, podemos escolher $n+1$ elementos distintos $\alpha_0, \ldots, \alpha_n \in K$. Para cada $j = 0, 1, 2, \ldots, n$ temos $g_j = f(\alpha_j x_1, x_2, \ldots, x_k) = f_0 + \alpha_j f_1 + \ldots + \alpha_j^n f_n$ e assim

$$\begin{pmatrix} 1 & \alpha_0 & \ldots & \alpha_0^n \\ 1 & \alpha_1 & \ldots & \alpha_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \ldots & \alpha_n^n \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_n \end{pmatrix}$$

Observe que $g_0, g_1, \ldots, g_n \in I$, pois I é um T-ideal. Além disso, a primeira matriz na igualdade anterior é uma matriz de Vandermonde invertível. Logo, devemos ter $f_0, f_1, \ldots, f_n \in I$.

Agora, para cada $i = 0, 1, \ldots, n$ e cada $t = 0, 1, 2, \ldots$, tomemos f_{i_t} como sendo a componente homogênea em f_i de grau t em x_2. Usando então os mesmos argumentos anteriores, concluímos que $f_{i_t} \in I$ e assim, repetindo o processo para cada variável, temos a primeira afirmação. Finalmente, observando que f é a soma de suas componentes multi-homogêneas, concluímos que I é gerado por seus polinômios multi-homogêneos. ■

Proposição 1.5.3 *Se I é um T-ideal de $K\langle X\rangle$ e $charK = 0$, então I é gerado por seus polinômios multilineares.*

Demonstração: Como $charK = 0$, temos que K é infinito e portanto, pela proposição 1.5.2, podemos assumir que $f(x_1, x_2, \ldots, x_n) \in I$ é um polinômio multi-homogêneo. Seja $n = deg_{x_1} f$. Tomando y_1 e y_2 variáveis de X distintas de $x_1, x_2, \ldots, x_n$, consideremos o polinômio $h(y_1, y_2, x_2, \ldots, x_n) = f(y_1 + y_2, x_2, \ldots, x_n)$. Sendo $h_1(y_1, y_2, x_2, \ldots, x_k)$ a componente homogênea de $h(y_1, y_2, x_2, \ldots, x_k)$ de grau 1 em y_1, temos que $deg_{y_2} h_1 = n - 1$ e que $h_1(x_1, x_1, x_2, \ldots, x_k) = nf(x_1, x_2, \ldots, x_k)$. Por $charK = 0$, segue que f é consequência de $h_1(y_1, y_2, \ldots, x_k)$. Notemos que $deg_{y_2} h_1 = n - 1$ e assim, caso seja necessário, continuamos o processo para as variáveis $y_2, x_2, \ldots, x_k$ em h_1. Continuando com este processo (chamado de *processo de linearização*), concluímos que f é consequência de algum polinômio multilinear de I e assim segue o resultado. ■

Proposição 1.5.4 *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.*

Demonstração: Seja $f(x_1, \ldots, x_m)$ uma identidade polinomial de A. Como K é infinito, podemos assumir que f é multi-homogênea. Utilizando 1.4, vamos escrever f da seguinte forma:

$$f = \sum \alpha_a x_1^{a_1} \ldots x_m^{a_m} \omega_a(x_1, \ldots, x_m), \ \alpha_a \in K,$$

onde $\omega_a(x_1, \ldots, x_m) \in B(X)$ e a soma é feita sobre todas as m-uplas $a = (a_1, \ldots, a_m)$ tais que $a_i \leq deg_{x_i} f$, $1 \leq i \leq m$. Definimos então o conjunto

$$M(f) = \{M_1, \ldots, M_l\} = \{a_1 \mid a = (a_1, \ldots, a_m) \ e \ \alpha_a \neq 0\},$$

onde $M_1 > \ldots > M_l > 0$. A demonstração da proposição segue da seguinte afirmação:

Se $f \in T(A)$ e f é multi-homogênea, então

$$g_j = \sum_{a_1=M_j} \alpha_a x_2^{a_2} \dots x_m^{a_m} \omega_a(x_1, \dots, x_m) \in T(A)$$

para $j = 1, 2, \dots, l$.

Demonstremos esta afirmação. É fácil ver que $\omega_a(x_1 + 1, x_2, \dots, x_m) = \omega_a(x_1, x_2, \dots, x_m)$. Como $f(x_1 + 1, x_2, \dots, x_m)$ também é identidade polinomial de A, concluímos que

$$f(x_1 + 1, x_2, \dots, x_m) = \sum \alpha_a \sum_{i=0}^{a_1} \binom{a_1}{i} x_1^i x_2^{a_2} \dots x_m^{a_m} \omega_a(x_1, \dots, x_m) \in T(A).$$

Como f é multi-homogênea, $a_1 + deg_{x_1}\omega_a(x_1, x_2, \dots, x_m) = deg_{x_1} f$ e assim a componente homogênea de $f(x_1 + 1, \dots, x_m)$ com menor grau possível em relação a x_1 se obtém quando $a_1 = M_1$ e é dada por

$$\sum_{a_1=M_1} \alpha_a x_2^{a_2} \dots x_m^{a_m} \omega_a(x_1, \dots, x_m), \tag{1.5}$$

onde o sub-índice do somatório indica que a soma é feita sobre todos os $a = (a_1, \dots, a_m)$ onde $a_1 = M_1$. Como o corpo é infinito, da proposição 1.5.2, segue que o polinômio 1.5 pertence a $T(A)$. Suponhamos que a afirmação seja verdadeira para $j = 1, 2, \dots, k$, onde k é um número natural menor que l. Subtraindo $x_1^{M_1} g_1 + x_2^{M_2} g_2 + \dots + x_k^{M_k} g_k$ de $f(x_1, \dots, x_m)$ obtemos

$$h(x_1, \dots, x_m) = \sum_{a_1 > M_k} \alpha_a x_1^{a_1} \dots x_m^{a_m} \omega_a(x_1, \dots, x_m) \in T(\mathcal{A}).$$

É claro que $M(h) = \{M_{k+1}, \dots, M_l\}$ e aplicando os mesmos argumentos anteriores a este polinômio, concluímos que

$$\sum_{a_1=M_{k+1}} x_2^{a_2} \dots x_m^{a_m} \omega_a(x_1, \dots, x_m) \in T(A)$$

o que prova a afirmação. ■

1.6 T-espaços e polinômios centrais

Definição 1.6.1 *Sejam A uma álgebra e $f(x_1, \dots, x_n) \in K\langle X \rangle$. Dizemos que f é um* ***polinômio central*** *para A se f tem termo constante nulo e $f(a_1, \dots, a_n) \in Z(A)$ para quaisquer $a_1, \dots, a_n \in A$*

Conforme esta definição, dizer que f é um polinômio central para A significa dizer que $[f, g]$ é uma identidade de A para todo polinômio $g \in K\langle X\rangle$. Logo, se duas álgebras são PI-equivalentes, então elas têm os mesmos polinômios centrais.

Exemplo 1.6.2 *Sendo A uma álgebra, toda identidade de A é um polinômio central para A. As identidades são ditas* ***polinômios centrais triviais****.*

Exemplo 1.6.3 *O polinômio $f(x_1, x_2, x_3, x_4) = [x_1, x_2] \circ [x_3, x_4]$ (polinômio de Hall) é um polinômio central para a álgebra $M_2(K)$. Conforme veremos no capítulo 3, Okhitin [40] descreveu os polinômios centrais para a álgebra $M_2(K)$, no caso de $charK = 0$. Posteriormente, Colombo e Koshlukov [8] generalizaram esta descrição para o caso de K ser infinito e de característica diferente de 2. Veremos também, no capítulo 4, algumas construções de polinômios centrais para $M_n(K)$ as quais estão nos artigos [15], [45] e [36].*

Exemplo 1.6.4 *Seja E a álgebra exterior sobre um corpo K. Temos que $f(x_1, x_2) = [x_1, x_2]$ é um polinômio central para E. Caso $charK = p$, segue que $g(x) = x^p$ é um polinômio central para E. Apresentaremos mais adiante a descrição dos polinômios centrais para E quando $charK = 0$.*

Definição 1.6.5 *Um subespaço V de $K\langle X\rangle$ é um T-espaço se $\varphi(V) \subseteq V$ para todo $\varphi \in EndK\langle X\rangle$*

Proposição 1.6.6 *Um subespaço V de $K\langle X\rangle$ é um T-espaço se, e somente se, $f(g_1, \ldots, g_n) \in V$ para quaisquer $f(x_1, \ldots, x_n) \in V$ e $g_1, \ldots, g_n \in K\langle X\rangle$.*

Demonstração: Sabemos que dado um subconjunto $\{f_i \mid i \in \mathbb{N}\}$, existe um único endomorfismo φ de $K\langle X\rangle$ tal que $\varphi(x_i) = f_i$ para todo $i \in \mathbb{N}$. Suponhamos que V seja um T-espaço de $K\langle X\rangle$. Dados $g_1, \ldots, g_n \in K\langle X\rangle$, existe um endomorfismo φ de $K\langle X\rangle$ tal que $\varphi(x_i) = g_i$, para $i = 1, \ldots, n$, e $\varphi(x_i) = 0$, caso contrário. Logo, por V ser um T-epaço, $\varphi(f(x_1, \ldots, x_n)) = f(\varphi(x_1), \ldots, \varphi(x_n)) = f(g_1, \ldots, g_n) \in V$, para qualquer $f(x_1, \ldots, x_n) \in V$. Por outro lado, suponhamos que $f(g_1, \ldots, g_n) \in V$ para quaisquer $f(x_1, \ldots, x_n) \in V$ e $g_1, \ldots, g_n \in K\langle X\rangle$. Se $\varphi \in EndK\langle X\rangle$, então $\varphi(f(x_1, \ldots, x_n)) = f(\varphi(x_1), \ldots, \varphi(x_n)) \in V$, pois $\varphi(x_1), \ldots, \varphi(x_n) \in K\langle X\rangle$. ■

Apresentaremos a seguir alguns exemplos de T-espaços importantes.

Exemplo 1.6.7 *Todo T-ideal de $K\langle X\rangle$ é um T-espaço.*

Exemplo 1.6.8 *Sejam A uma álgebra e W um subespaço de A. O conjunto*

$$\mathcal{L} = \{f(x_1, \ldots, x_n) \in K\langle X\rangle \mid f(a_1, \ldots, a_n) \in W \text{ para } a_1, \ldots, a_n \in A\}$$

é um T-espaço de $K\langle X\rangle$. Destacamos o caso particular $W = Z(A)$, no qual está nosso maior interesse. Daí, temos o T-espaço

$$\{f(x_1, \ldots, x_n) \in K\langle X\rangle \mid f(a_1, \ldots, a_n) \in Z(A) \text{ para } a_1, \ldots, a_n \in A\}$$

*que é conhecido por **espaço dos polinômios centrais** de A e denotado por $C(A)$. Por $Z(A)$ ser uma subálgebra de A, temos que $C(A)$ é multiplicativamente fechado, condição que nem todo T-espaço satisfaz.*

É importante observar que os elementos de $C(A)$ são da forma $h+c$, onde h é um polinômio central (de acordo com a definição 1.6.1), e c é uma constante. Além disso, o conjunto dos polinômios centrais de uma álgebra pode não ser um T-espaço. De acordo com o exemplo 1.6.4, no caso $char K = p$, vimos que $g(x) = x^p$ é um polinômio central para E. Entretanto, $g(x + 1) = x^p + 1$ tem termo constante não-nulo e não é central.

É fácil ver que a interseção e a soma de uma família de T-espaços ainda são T-espaços. De maneira análoga a definição de T-ideal gerado por um conjunto, temos o de T-espaço gerado. Dado um subconjunto S de $K\langle X\rangle$, definimos o *T-espaço gerado por S* como sendo a interseção de todos os T-espaços que contêm S, ou seja, o *menor T-espaço* de $K\langle X\rangle$ que contém S. O próximo resultado nos dá uma importante caracterização do T-espaço gerado por um conjunto.

Proposição 1.6.9 *Se $S \subseteq K\langle X\rangle$ e V é o T-espaço de $K\langle X\rangle$ gerado por S, então V é o subespaço de $K\langle X\rangle$ gerado por*

$$\{f(g_1, \ldots, g_n) \mid f \in S,\ g_1, \ldots, g_n \in K\langle X\rangle\}.$$

Demonstração: Notemos inicialmente que este conjunto é exatamente igual a

$$(End K\langle X\rangle)S = \{\varphi(f) \mid f \in S,\ \varphi \in End K\langle X\rangle\}.$$

Consideremos V_1 como sendo o subespaço de $K\langle X\rangle$ gerado por $(End K\langle X\rangle)S$. Como $S \subseteq V$ e V é um T-espaço, temos que $\varphi(f) \in V$, onde $f \in S$ e $\varphi \in End K\langle X\rangle$, ou seja, $(End K\langle X\rangle)S \subseteq V$. Logo, $V_1 \subseteq V$. Observemos agora que $\psi(g) \in (End K\langle X\rangle)S$ quaisquer que sejam $\psi \in End K\langle X\rangle$ e $g \in (End K\langle X\rangle)S$. Logo, V_1 é um T-espaço de $K\langle X\rangle$. Além disso, $S \subseteq V_1$ e por V ser o T-espaço gerado por S, segue que $V \subseteq V_1$. Portanto, $V = V_1$. ■

Observação 1.6.10 *De acordo com as proposições 1.5.2 e 1.5.3 todo T-ideal é gerado por seus polinômios multi-homogêneos caso o corpo base seja infinito e por seus polinômios multilineares quando o corpo base tem característica zero. Analogamente, mostra-se que todo T-espaço é gerado por seus polinômios multilineares no caso do corpo base ter característica zero e por seus polinômios multi-homogêneos no caso do corpo base ser infinito.*

A seguir veremos alguns exemplos importantes.

Exemplo 1.6.11 *Consideremos $M_2(K)$ a álgebra das matrizes de ordem sobre K, onde K denota um corpo de característica diferente de 2. Seja*

$$V = \{f(x_1, \ldots, x_k) \in K\langle X\rangle \mid tr(f(A_1, \ldots, A_k)) = 0 \text{ para } A_1, \ldots, A_k \in M_2(K)\}.$$

Notemos que V é um T-espaço de $K\langle X\rangle$ e que $V \cap C(M_2(K)) = T(M_2(K))$. De fato, é imediato que $T(M_2(K)) \subseteq V$ e $T(M_2(K)) \subseteq C(M_2(K))$, de onde segue que $T(M_2(K)) \subseteq V \cap C(M_2(K))$. Sejam $f(x_1, \ldots, x_k) \in V \cap C(M_2(K))$ e $A_1, \ldots, A_k \in M_2(K)$. Logo, por $f(x_1, \ldots, x_k) \in C(M_2(K))$, temos

$$f(A_1, \ldots, A_k) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},\ \lambda \in K.$$

Por outro lado, $f(x_1, \ldots, x_k) \in V$, isto é, $tr(f(A_1, \ldots, A_k)) = 2\lambda = 0$. Mas $charK \neq 2$, de onde segue que $\lambda = 0$. Portanto, $f(x_1, \ldots, x_k) \in T(M_2(K))$. Sendo assim, $V \cap C(M_2(K)) = T(M_2(K))$.

O T-espaço V não é multiplicativamente fechado, pois $[x_1, x_2]^2 \notin V$. Basta considerarmos $x_1 = E_{12} - E_{21}$ e $x_2 = E_{22}$.

Exemplo 1.6.12 *Seja V o T-espaço de $K\langle X\rangle$ gerado por $[x_1, x_2]$ e $[x_1, x_2][x_3, x_4]$. Da igualdade (1.1) temos*

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

e

$$[x_1, x_2, x_3x_4] = x_3[x_1, x_2, x_4] + [x_1, x_2, x_3]x_4.$$

Da primeira igualdade segue que $[x_1, x_2, x_3]x_4 \in V$ e da segunda obtemos

$$x_3[x_1, x_2, x_4]x_5 = [x_1, x_2, x_3x_4]x_5 - [x_1, x_2, x_3]x_4x_5.$$

Sendo assim, $x_3[x_1, x_2, x_4]x_5 \in V$ e portanto o T-ideal $\langle[x_1, x_2, x_3]\rangle^T \subseteq V$. Usando agora a igualdade (1.2), concluímos que

$$[[x_3, x_4] \ldots [x_{2n-1}, x_{2n}], x_2] \in \langle[x_1, x_2, x_3]\rangle^T$$

para todo $n \geq 3$. Dessa forma, como

$$[x_1[x_3, x_4] \dots [x_{2n-1}, x_{2n}], x_2] = [x_1, x_2] \dots [x_{2n-1}, x_{2n}] + x_1[[x_3, x_4] \dots [x_{2n-1}, x_{2n}], x_2]$$

temos que $[x_1, x_2][x_3, x_4] \dots, [x_{2n-1}, x_{2n}] \in V$ e portanto V é multiplicativamente fechado.

Mostraremos agora que, no caso de char$K = 0$, $C(E) = V$ (E é a álgebra de Grasmann). Como $[x_1, x_2]$ e $[x_1, x_2][x_3, x_4]$ são polinômios centrais para E, temos $V \subseteq C(E)$. Além disso, $T(E) \subseteq V$, pois $T(E)$ é exatamente igual ao T-ideal $\langle [x_1, x_2, x_3] \rangle^T$. Consideremos agora $f(x_1, \dots, x_k) \in C(E)$ multilinear. Logo,

$$f(x_1, \dots, x_k) = \sum_{\sigma \in S_k} a_\sigma x_{\sigma(1)} \dots x_{\sigma(k)}, \ a_\sigma \in K.$$

Para todo $\sigma \in S_k$, temos

$$x_{\sigma(1)} \dots x_{\sigma(k)} = x_1 x_{\sigma(i+1)} \dots x_{\sigma(k)} x_{\sigma(1)} \dots x_{\sigma(i-1)} + [x_{\sigma(1)} \dots x_{\sigma(i-1)}, x_1 x_{\sigma(i+1)} \dots x_{\sigma(k)}],$$

onde $\sigma(i) = 1$. Dessa forma, $f(x_1, \dots, x_k) \equiv x_1 g(x_2, \dots, x_k)$ (mod V), onde g é um polinômio multilinear. Logo, $x_1 g(x_2, \dots, x_k) \in C(E)$ e consequentemente $g(x_2, \dots, x_k) \in C(E)$ (faça $x_1 = 1$). Entretanto, g e $x_1 g$ pertencentes a $C(E)$ só é possível caso g seja identidade de E. Daí, $x_1 g \in T(E)$ e portanto $f(x_1, \dots, x_k) \in V$.

Observação 1.6.13 *No caso de char$K = p > 0$ temos $V \neq C(E)$. De fato, consideremos a álgebra $U_2(K)$ (matrizes triangulares superiores) e o T-espaço*

$$W = \{f(x_1, \dots, x_k) \in K\langle X \rangle \mid f(A_1, \dots, A_k) \text{ tem diagonal nula e os } A_i' s \in U_2(K)\}.$$

É imediato ver que $[x_1, x_2]$ e $[x_1, x_2][x_3, x_4]$ pertencem a W, donde $V \subseteq W$. Considerando o polinômio $h(x) = x^p$ de $C(E)$, verificamos que h não pertence a W (basta considerar $x_1 = E_{11}$). Portanto, $h(x) \in C(E) - V$.

Hoje se sabe que $C(E)$ não é finitamente gerado para char$K = p > 0$ (veja [1]).

No que foi tratado até agora sobre T-espaços e polinômios centrais, vimos que o conjunto $C(A)$ é sempre um T-espaço de $K\langle X \rangle$ qualquer que seja a álgebra A. Quando fala-se em descrever os polinômios centrais de A, entende-se por determinar um subconjunto de $C(A)$ que possa gerá-lo como T-espaço. Existem T-espaços que não são multiplicativamente fechados (veja o exemplo 1.6.11) e também T-espaços multiplicativamente fechados que não são espaços de polinômios centrais para nenhuma álgebra, conforme veremos a seguir.

Proposição 1.6.14 *Se char$K = p > 2$, então não existe álgebra A tal que $C(A) = V$.*

Demonstração: Suponhamos que $C(A) = V$ para alguma álgebra associativa A. Então, $[x_1, x_2] \in C(A)$ e consequentemente $[x_1, x_2, x_3] \in T(A)$. Usando indução é possível mostrar que

$$[y, \underbrace{x, \ldots, x}_{n}] = \sum_{j=0}^{n} (-1)^j \binom{n}{j} x^j y x^{n-j}$$

para $n \geq 1$, em toda álgebra associativa. Logo, para $n = p$, temos $[y, x, \ldots, x] = yx^p - x^p y = [y, x^p]$. Daí, concluímos que $[x_2, x_1^p] \in T(A)$ e portanto $x_1^p \in C(A)$, o que contradiz a hipótese de que $C(A) = V$ (veja a observação 1.6.13). ∎

1.7 Identidades e polinômios centrais graduados

Nesta seção apresentaremos os conceitos de identidades e polinômios centrais para álgebras graduadas. Estas idéias serão fundamentais para o próximo capítulo. No que segue, G denotará um grupo abeliano com notação aditiva.

Definição 1.7.1 *Seja A uma álgebra. Uma G-**graduação** em A é uma família $\{A_g \mid g \in G\}$ de subespaços de A tais que*

$$A = \bigoplus_{g \in G} A_g \quad e \quad A_g A_h \subseteq A_{g+h}$$

*para quaisquer $g, h \in G$. Definimos uma **álgebra** G-**graduada** como sendo uma álgebra munida de uma G-graduação.*

Na definição acima, o subespaço A_g é chamado de *componente homogênea* de grau g e os seus elementos de *elementos homogêneos* de grau g.

A seguir apresentaremos alguns exemplos de álgebras graduadas.

Exemplo 1.7.2 *Toda álgebra A admite uma G-graduação. Basta considerar $A_0 = A$ e $A_g = \{0\}$ para todo $g \in G - \{0\}$. Esta graduação é chamada de **graduação trivial**.*

Exemplo 1.7.3 *A álgebra exterior E possui uma $\mathbb{Z}_2$-graduação natural dada por $E = E_0 \oplus E_1$, onde E_0 e E_1 são os subespaços definidos no exemplo 1.1.5.*

Exemplo 1.7.4 *Considere n um inteiro positivo e $A = M_n(K)$. Para cada $\gamma \in \mathbb{Z}_n$, tomemos o subespaço $M_\gamma = \langle E_{ij} \mid \overline{j - i} = \gamma \rangle$. Para cada $k \in \mathbb{Z}$, consideremos*

$$M_k = \begin{cases} \{0\}, & se \quad |k| \geq n \\ \langle E_{ij} \mid j - i = k \rangle, & se \quad |k| < n \end{cases}$$

Observe que $M_{\bar{0}} = M_0$ *é exatamente o conjunto das matrizes diagonais. Do fato do conjunto* $\{E_{ij} \mid 1 \leq i, j \leq n\}$ *ser uma base de* A *segue que*

$$A = \bigoplus_{\gamma \in \mathbb{Z}_n} M_\gamma \quad e \quad A = \bigoplus_{k \in \mathbb{Z}} M_k$$

Agora para ver que estas decomposições definem uma $\mathbb{Z}_n$*-graduação e uma* $\mathbb{Z}$*-graduação, respectivamente, em* $M_n(K)$*, basta notarmos que*

$$E_{ij}E_{kl} = \begin{cases} 0, & se \quad j \neq k \\ E_{il}, & se \quad j = k \end{cases}$$

donde segue que $M_{\gamma_1}M_{\gamma_2} \subseteq M_{\gamma_1+\gamma_2}$ *para* $\gamma_1, \gamma_2 \in \mathbb{Z}_n$ *e* $M_{k_1}M_{k_2} \subseteq M_{k_1+k_2}$ *para* $k_1, k_2 \in \mathbb{Z}$*.*

Proposição 1.7.5 *Se* A *é uma álgebra* G*-graduada, então* $1 \in A_0$*.*

Demonstração: Temos que existem $g_1, \ldots, g_n \in G - \{0\}$ tais que

$$1 = a_0 + a_{g_1} + \ldots + a_{g_n}$$

com $a_0 \in A_0$ e $a_{g_i} \in A_{g_i}$, para $i = 1, \ldots, n$. Tomando agora $h \in G$ e $a_h \in A_h$, arbitrários, temos

$$a_h = a_h a_0 + a_h a_{g_1} + \ldots + a_h a_{g_n}$$

Notando que $a_h a_0 \in A_h$, $a_h a_{g_i} \in A_{h+g_i}$ e $h, h+g_1, \ldots, h+g_n$ são dois a dois distintos, concluímos que $a_h a_{g_i} = 0$ para $i = 1, \ldots, n$ e portanto $a_h a_0 = a_h$. Multiplicando a primeira igualdade por a_0, obtemos $a_0 = a_0 a_0 + a_{g_1} a_0 + \ldots + a_{g_n} a_0$. Usando agora o fato de $a_h a_0 = a_h$, temos $a_0 = a_0 + a_{g_1} + \ldots + a_{g_n}$, isto é, $a_{g_1} + \ldots + a_{g_n} = 0$ e portanto $a_0 = 1$. ∎

Definição 1.7.6 *Uma aplicação* $\psi : A \longrightarrow B$ *entre álgebras* G*-graduadas é chamada* ***homomorfismo*** G***-graduado****, se* ψ *é um homomorfismo de álgebras que satisfaz* $\psi(A_g) \subseteq B_g$ *para todo* $g \in G$*.*

Vamos agora tratar de identidades e polinômios centrais G-graduados. Antes, precisaremos do conceito de álgebra associativa livre G-graduada. Para definí-lo, consideremos uma família $\{X_g \mid g \in G\}$ de conjuntos enumeráveis e dois a dois disjuntos. Tomemos então $X = \bigcup_{g \in G} X_g$ e consideremos a álgebra associativa livre unitária $K\langle X \rangle$. Definimos agora

$$\omega(1) = 0 \quad e \quad \omega(x_1 x_2 \ldots x_m) = \omega(x_1) + \omega(x_2) + \ldots + \omega(x_m)$$

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

$$K\langle X\rangle_g = \langle m \mid m \text{ é monômio de } K\langle X\rangle,\, \omega(m) = g\rangle$$

temos

$$K\langle X\rangle = \bigoplus_{g\in G} K\langle X\rangle_g \quad e \quad K\langle X\rangle_g K\langle X\rangle_h \subseteq K\langle X\rangle_{g+h}$$

para quaisquer $g, h \in G$, e assim $K\langle X\rangle$ é chamada *álgebra associativa livre G-graduada*. Se $f \in K\langle X\rangle_g$, dizemos que f é homogêneo de G-grau g e usamos a notação $\omega_G(f) = g$.

Definição 1.7.7 *Seja $A = \bigoplus_{g\in G} A_g$ uma álgebra G-graduada. Dizemos que um polinômio $f = f(x_1, \ldots, x_n) \in K\langle X\rangle$ é*

i) uma ***identidade polinomial*** *G*-***graduada*** *para A, se $f(a_1, \ldots, a_n) = 0$ para quaisquer $a_i \in A_{\omega(x_i)}$ com $i = 1, 2, \ldots, n$.*

ii) um ***polinômio central*** *G*-***graduado*** *para A, se $f(a_1, \ldots, a_n) \in Z(A)$ para quaisquer $a_i \in A_{\omega(x_i)}$ com $i = 1, 2, \ldots, n$.*

Exemplo 1.7.8 *Consideremos a álgebra exterior E com sua $\mathbb{Z}_2$-graduação natural (conforme o Exemplo 1.7.3). Como $ab = -ba$ para quaisquer $a, b \in E_1$, temos que $f(x_1, x_2) = x_1 \circ x_2$ é uma identidade $\mathbb{Z}_2$-graduada de E, onde $K\langle X\rangle$ é a álgebra livre $\mathbb{Z}_2$-graduada, e $\omega(x_1) = \omega(x_2) = 1$. Por $E_0 = Z(E)$, temos que todo polinômio $f \in K\langle X\rangle_0$ é um polinômio central $\mathbb{Z}_2$-graduada para E.*

No estudo das identidades e polinômios centrais ordinários (de acordo com as definições 1.2.3 e 1.6.1), os conceitos de T-ideal e T-espaço são de extrema importância. Para o caso de identidades e polinômios centrais G-graduados temos conceitos análogos, a saber, os de T_G-ideal e T_G-espaço.

Definição 1.7.9 *Seja $K\langle X\rangle$ a álgebra associativa livre G-graduada. Um ideal I de $K\langle X\rangle$ é dito ser um T_G-ideal se $\varphi(I) \subseteq I$ para todo endomorfismo G-graduado φ de $K\langle X\rangle$. Um subespaço V de $K\langle X\rangle$ é dito ser um T_G-espaço se $\varphi(V) \subseteq V$ para todo endomorfismo G-graduado φ de $K\langle X\rangle$.*

Não é difícil ver que I é um T_G-ideal se, e somente se, $f(g_1, \ldots, g_n) \in I$, para quaisquer $f(x_1, \ldots, x_n) \in I$ e $g_i \in K\langle X\rangle_{\omega(x_i)}$. Uma idéia análoga para T_G-espaço.

As idéias de T_G-ideal e T_G-espaços gerados por um dado subconjunto S de $K\langle X\rangle$ são análogas as idéias de T-ideal e T-espaços gerados. Denotamos por $\langle S\rangle^{T_G}$ o T_G-ideal gerado por S.

Se A é uma álgebra G-graduada, então o conjunto $T_G(A)$ das identidades G-graduadas de A é um T_G-ideal de $K\langle X\rangle$ e o conjunto $C_G(A)$ dos polinômios centrais G-graduados de A é um T_G-espaço de $K\langle X\rangle$. As proposições 1.5.2 e 1.5.3 também são válidas no caso de T_G-ideal e T_G-espaço.

O próximo resultado mostra uma importante relação entre os conceitos de identidades ordinárias e graduadas.

Proposição 1.7.10 *Sejam A e B duas álgebras. Se A e B possuem G-graduações tais que $T_G(A) \subseteq T_G(B)$, então $T(A) \subseteq T(B)$. Ademais, se $T_G(A) = T_G(B)$, então $T(A) = T(B)$.*

Demonstração: Consideremos a álgebra associativa livre $K\langle Y\rangle$, onde $Y = \{y_1, y_2, \ldots\}$ e seja $f(y_1, y_2, \ldots, y_n) \in T(A)$. Dados $b_1, b_2, \ldots, b_n \in B$, tomemos $b_{i_g} \in B_g$, para $i = 1, \ldots, n$ e $g \in G$, tais que $b_i = \sum_{g\in G} b_{i_g}$. Para cada $b_{i_g} \neq 0$, tomemos $x_{i_g} \in X_g$ e consideremos o polinômio $f_1 = f(\sum_{g\in G} x_{1_g}, \ldots, \sum_{g\in G} x_{n_g}) \in K\langle X\rangle$. Como $f \in T(A)$, temos $f_1 \in T_G(A)$ e daí $f_1 \in T_G(B)$. Fazendo então as substituições $x_{i_g} = b_{i_g}$, para $i = 1, \ldots, n$ e $g \in G$, temos

$$f(b_1, b_2, \ldots, b_n) = f\left(\sum_{g\in G} b_{1_g}, \sum_{g\in G} b_{2_g}, \ldots, \sum_{g\in G} b_{n_g}\right) = 0$$

e assim $f \in T(B)$.

Se $T_G(A) = T_G(B)$, então $T_G(A) \subseteq T_G(B)$ e $T_G(B) \subseteq T_G(A)$, donde temos a última afirmação. ■

É importante observar que a recíproca do resultado acima é falsa. Considere na álgebra exterior E a $\mathbb{Z}_2$-graduação natural $E = E_0 \oplus E_1$ e a $\mathbb{Z}_2$-graduação trivial $E = E \oplus \{0\}$. Temos que $f(y_1, y_2) = [y_1, y_2]$, com $\omega(y_1) = \omega(y_2) = 0$, é identidade $\mathbb{Z}_2$-graduada de E com respeito a primeira graduação, mas não é identidade graduada com respeito a graduação trivial.

Capítulo 2

Identidades e Polinômios Centrais Graduados para a Álgebra $M_n(K)$

Neste capítulo vamos apresentar as descrições das identidades e polinômios centrais $\mathbb{Z}$-graduados e $\mathbb{Z}_n$-graduados para a álgebra $M_n(K)$, onde K é um corpo de característica zero. Nestas descrições estaremos considerando as graduações naturais de $M_n(K)$ pelos grupos $\mathbb{Z}_n$ e $\mathbb{Z}$, as quais foram definidas na seção 1.7.

As identidades $\mathbb{Z}_n$-graduadas e as $\mathbb{Z}$-graduadas de $M_n(K)$ foram descritas primeiramente por Vasilovsky ([55] e [54]) em característica zero. Posteriormente, Azevedo ([4] e [5]) generalizou esta descrição para corpos infinitos quaisquer.

Algumas idéias usadas na descrição dos polinômios centrais $\mathbb{Z}_n$-graduados e os $\mathbb{Z}$-graduados encontram-se em [6], onde a descrição foi feita para corpos infinitos e com uso de matrizes genéricas. Aqui apresentaremos a descrição apenas no caso de K ser um corpo de característica zero, onde utilizamos idéias sobre monômios multilineares contidas em [55] e [54].

Os conceitos e resultados básicos necessários sobre álgebras graduadas podem ser encontradas na seção 1.7.

Em todo este capítulo K denotará um corpo de característica zero.

2.1 Identidades Polinomiais $\mathbb{Z}_n$-graduadas

Em toda esta seção $K\langle X\rangle$ denotará a álgebra associativa livre $\mathbb{Z}_n$-graduada, onde $X = \bigcup_{\gamma\in\mathbb{Z}_n} X_\gamma$, e $M_n(K)$ a álgebra das matrizes com a $\mathbb{Z}_n$-graduação dada no Exemplo 1.7.4. Vamos considerar as notações introduzidas na seção 1.7 e denotar $T_{\mathbb{Z}_n}$

simplesmente por T_n.

A seguir apresentaremos os resultados necessários para a demonstração do teorema que descreve as identidades $\mathbb{Z}_n$-graduadas para a álgebra $M_n(K)$ (veja [55]).

Lema 2.1.1 *A álgebra $M_n(K)$ satisfaz as seguintes identidades $\mathbb{Z}_n$-graduadas*

$$x_1x_2 - x_2x_1 = 0, \quad \omega(x_1) = \omega(x_2) = \overline{0} \tag{2.1}$$

$$x_1x_2x_3 - x_3x_2x_1 = 0, \quad \omega(x_1) = \omega(x_3) = -\omega(x_2). \tag{2.2}$$

Demonstração: Observe inicialmente que se $A \in M_{\overline{0}}$, então A é uma matriz diagonal. Desde que duas matrizes diagonais comutam, temos que $M_n(K)$ satisfaz a identidade graduada 2.1. Por outro lado, as identidades 2.2 são multilineares. Logo, precisamos mostrar que as identidades em 2.2 são satisfeitas para

$$x_1 = E_{i_1j_1}, \quad x_2 = E_{i_2j_2}, \quad x_3 = E_{i_3j_3},$$

onde $E_{i_1j_1},\ E_{i_3j_3} \in M_{\overline{t}}$ e $E_{i_2j_2} \in M_{\overline{n-t}}$, onde $0 < t \leq n-1$. Note que para o caso $t = 0$, as matrizes $E_{i_1j_1}, E_{i_2j_2}, E_{i_3j_3}$ são diagonais e portanto comutam entre si. Por $E_{i_1j_1},\ E_{i_3j_3} \in M_{\overline{t}}$ e $E_{i_2j_2} \in M_{\overline{n-t}}$ segue que

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

$$i_2 = \begin{cases} j_2 + t, & se \quad j_2 + t \leq n, \\ j_2 + t - n, & se \quad j_2 + t > n; \end{cases}$$

$$i_3 = \begin{cases} j_3 - t, & se \quad j_3 - t \geq 1, \\ j_3 - t + n, & se \quad j_3 - t < 1. \end{cases}$$

Notemos que $E_{i_1j_1}E_{i_2j_2}E_{i_3j_3} \neq 0$ se, e somente se, $j_1 = i_2$ e $j_2 = i_3$. Mostraremos que, neste caso, $i_1 = j_2 = i_3$ e $j_1 = i_2 = j_3$. Observemos que se $j_1 = i_1 + t$ e $i_2 = j_2 + t - n$, então por $j_1 = i_2$, segue que $j_2 - i_1 = n$, o que é um absurdo. Então as igualdades $j_1 = i_1 + t$ e $i_2 = j_2 + t - n$ não ocorrem simultaneamente. Da mesma forma, as equações $j_2 = i_2 - t$ e $i_3 = j_3 - t + n$ não podem ocorrer simultaneamente. Então quando $j_1 = i_1 + t$, devemos ter $i_2 = j_2 + t$ e $i_3 = j_3 - t$, o que nos dá

$$i_3 = j_2 = i_2 - t = j_1 - t = i_1. \tag{2.3}$$

Usando 2.3, obtemos

$$i_2 = j_1 = i_1 + t = i_3 + t = j_3.$$

Analogamente, quando $j_1 = i_1 + t - n$, teremos $i_2 = j_2 + t - n$ e $i_3 = j_3 - t + n$, de onde

$$i_3 = j_2 = i_2 - t + n = j_1 - t + n = i_1. \tag{2.4}$$

Usando 2.4, obtemos

$$i_2 = j_1 = i_1 + t - n = i_3 + t - n = j_3.$$

Desta forma, $E_{i_1j_1}E_{i_2j_2}E_{i_3j_3} \neq 0$ se, e somente se, $E_{i_3j_3}E_{i_2j_2}E_{i_1j_1} \neq 0$. Neste caso, $i_1 = j_2 = i_3$ e $j_1 = i_2 = j_3$, e daí

$$E_{i_1j_1}E_{i_2j_2}E_{i_3j_3} = E_{i_1j_3} = E_{i_3j_1} = E_{i_3j_3}E_{i_2j_2}E_{i_1j_1}.$$

Caso contrário,

$$E_{i_1j_1}E_{i_2j_2}E_{i_3j_3} = 0 = E_{i_3j_3}E_{i_2j_2}E_{i_1j_1}$$

o que conclui a demonstração. ■

Vamos denotar por I_n o T_n ideal gerado pelas identidades graduadas 2.1 e 2.2. Pelo Lema 2.1.1 temos $I_n \subseteq T_n(M_n(K))$. Para $x_1, x_2, \ldots, x_k \in X$ e $\sigma \in S_k$, considere

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

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

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

Obviamente, $\omega(m) = \omega(m_\sigma) = \omega(x_1) + \omega(x_2) + \ldots + \omega(x_k)$. Sabe-se que cada polinômio graduado multilinear $f(x_1, x_2, \ldots, x_k)$ pode ser escrito da forma

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

onde $a_\sigma \in K$.

Uma substituição $\mathcal{S}$ do tipo

$$x_1 = E_{i_1j_1}, x_2 = E_{i_2j_2}, \ldots, x_k = E_{i_kj_k}, \tag{2.5}$$

onde

$$\overline{j_s - i_s} = \omega(x_s),\ \ s = 1, 2, \ldots, k \tag{2.6}$$

é conhecida como *substituição Standard*. Observe que $E_{i_s j_s} \in M_{\omega(x_s)},\ s = 1, 2, \ldots, k$. Para um polinômio graduado $f(x_1, x_2, \ldots, x_k)$ e uma substituição Standard $\mathcal{S}$, denotaremos por $f|_{\mathcal{S}}$ o valor de f correspondente a substituição $\mathcal{S}$. Claramente, se um polinômio graduado multilinear f é tal que $f|_{\mathcal{S}} = 0$ para cada substituição Standard $\mathcal{S}$, então f é uma identidade graduada de $M_n(K)$. Notemos que quando uma substituição $\mathcal{S}$ (veja 2.5) é feita, o valor do monômio $m_\sigma(x_1, x_2, \ldots, x_k)$ é diferente de zero, somente se

$$j_{\sigma(1)} = i_{\sigma(2)},\ j_{\sigma(1)} = i_{\sigma(2)}, \ldots,\ j_{\sigma(k-1)} = i_{\sigma(k)}. \tag{2.7}$$

Neste caso, $m_\sigma|_{\mathcal{S}} = E_{i_{\sigma(1)} j_{\sigma(k)}}$.

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

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

Lema 2.1.2 *Para cada $\sigma \in S_k$, existe uma substituição Standard $\mathcal{S}$ tal que*

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

Demonstração: A demonstração será feita por indução sobre k. O caso $k = 1$ é trivial. Basta considerar $x_1 = E_{ij}$ tal que $\overline{j - i} = \omega(x_1)$. Suponhamos que para qualquer monômio de comprimento k, $m_1(x_1, x_2, \ldots, x_k) = x_{l_1} x_{l_2} \ldots x_{l_k}$, onde $l_1, l_2, \ldots, l_k \in \{1, 2, \ldots, k\}$, existe uma substituição Standard $\mathcal{S}$ tal que

$$m_1(x_1, x_2, \ldots, x_k)|_{\mathcal{S}} \neq 0.$$

Seja $m_2(x_1, x_1, \ldots, x_k, x_{k+1}) = x_{t_1} x_{t_2} \ldots x_{t_k} x_{t_{k+1}}$, onde

$$\{t_1, t_2, \ldots, t_k, t_{k+1}\} = \{1, 2, \ldots, k, k + 1\}.$$

Suponhamos que $\omega(x_{t_{k+1}}) = \bar{t}$, para algum $0 \leq t < n$. Para $x_{t_1} x_{t_2} \ldots x_{t_k}$, existe uma substituição Standard $\mathcal{S}'$

$$x_{t_1} = E_{i_1 j_1},\quad x_{t_2} = E_{i_2 j_2},\quad \ldots,\quad x_{t_k} = E_{i_k j_k}, \tag{2.8}$$

tal que

$$x_{t_1}x_{t_2}\ldots x_{t_k}|_{\mathcal{S}'} = E_{i_1j_1}E_{i_2j_2}\ldots E_{i_kj_k} = E_{i_1j_k} \neq 0. \tag{2.9}$$

Consideremos agora a substituição Standard $\mathcal{S}$ formada pelos elementos 2.8 e $x_{t_{k+1}} = E_{j_ki_{k+1}}$, onde

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

Logo, por 2.9

$$m_2(x_1, x_2, \ldots, x_k, x_{k+1})|_{\mathcal{S}} = E_{i_1j_k}E_{j_ki_{k+1}} = E_{i_1i_{k+1}} \neq 0.$$

■

Nos resultados enunciados a seguir $\mathcal{S}$ denotará uma substituição Standard (conforme 2.5).

Lema 2.1.3 *Se $m_\sigma|_{\mathcal{S}} \neq 0$, então para $1 \leq p \leq q \leq k$*

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

Demonstração: Por 2.6 e 2.7, temos

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

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

■

Lema 2.1.4 *Se para uma permutação $\sigma \in S_k$, existir uma substituição Standard $\mathcal{S}$ tal que*

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

então

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

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

Demonstração: Caso $\sigma(1) = 1$, a demonstração é trivial. Suponhamos que $\sigma(1) \neq 1$. Logo, $1 \neq \sigma^{-1}(1)$, e assim $1 = \sigma^{-1}(\sigma(1)) < \sigma^{-1}(1)$. Além disso, existe um inteiro positivo u tal que $\sigma(1) = 1 + u$. Daí, $1 = \sigma^{-1}(\sigma(1)) = \sigma^{-1}(1 + u) < \sigma^{-1}(1)$. Seja u_0 o menor inteiro positivo tal que $\sigma^{-1}(1 + u_0) < \sigma^{-1}(1)$. Obviamente,

$$1 \leq \sigma^{-1}(1 + u_0) < \sigma^{-1}(1) \leq \sigma^{-1}(u_0). \tag{2.10}$$

Desde que $m_\sigma|_{\mathcal{S}} = m|_{\mathcal{S}} \neq 0$, temos

$$E_{i_1j_1}E_{i_2j_2}\dots E_{i_kj_k} = E_{i_{\sigma(1)}j_{\sigma(1)}}E_{i_{\sigma(2)}j_{\sigma(2)}}\dots E_{i_{\sigma(k)}j_{\sigma(k)}} \neq 0,$$

e daí, $i_1 = i_{\sigma(1)}$, $j_t = i_{t+1}$, $t = 1, \dots, k-1$ e, para $s > 1$, $j_{\sigma(s-1)} = i_{\sigma(s)}$. Considerando $p = \sigma^{-1}(u_0 + 1)$, $q = \sigma^{-1}(1)$ e $r = \sigma^{-1}(u_0)$, por 2.10 temos $1 \leq p < q \leq r$ e $j_{\sigma(q-1)} = i_{\sigma(q)} = i_1 = i_{\sigma(1)}$, $j_{\sigma(r)} = i_{\sigma(p)}$. Ademais, se $p > 1$, $j_{\sigma(p-1)} = i_{\sigma(p)}$. Vamos considerar inicialmente o caso $p > 1$. Das igualdades

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

temos que

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

para algum $t_o \in \mathbb{Z}$. Pelo Lema 2.1.3, temos

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

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

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

Consequentemente, usando 2.2, segue que

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

$$\equiv m_\sigma^{[q,r]}m_\sigma^{[p,q-1]}m_\sigma^{[1,p-1]}m_\sigma^{[r+1,k]} = x_{\sigma(q)}x_{l_2}\dots x_{l_k} = x_1x_{l_2}\dots x_{l_k} \ (mod\ I_n).$$

Consideremos agora $p = 1$. Neste caso, $j_{\sigma(q-1)} = i_{\sigma(q)} = i_{\sigma(1)} = j_{\sigma(r)}$, e pelo Lema 2.1.3

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

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

Portanto, por 2.1 segue que

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

$$\equiv m_\sigma^{[q,r]}m_\sigma^{[1,q-1]}m_\sigma^{[r+1,k]} = x_{\sigma(q)}x_{l_2}\dots x_{l_k} = x_1x_{l_2}\dots x_{l_k} \ (mod\ I_n).$$

■

Lema 2.1.5 *Se para uma permutação $\sigma \in S_k$, existir uma substituição Standard $\mathcal{S}$ tal que*

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

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

Demonstração: Pelo Lema 2.1.4, $m_\sigma(x_1, x_2, \ldots, x_k) \equiv x_1 n(x_2, x_3, \ldots, x_k)$ $(mod\ I_n)$. Seja r o maior inteiro positivo tal que

$$m_\sigma(x_1, x_2, \ldots, x_k) \equiv x_1 x_2 \ldots x_r n(x_{r+1}, \ldots, x_k)\ (mod\ I_n), \tag{2.11}$$

para algum monômio $n = n(x_{r+1}, \ldots, x_k)$ multilinear. Mostraremos que $r = k$. Suponhamos por contradição que $r < k$. Então, obviamente $r \leq k - 2$. Desde que $I_n \subseteq T_n(M_n(K))$, por 2.11 temos

$$x_1 x_2 \ldots x_r n(x_{r+1}, \ldots, x_k)|_{\mathcal{S}} = m_\sigma(x_1, x_2, \ldots, x_k)|_{\mathcal{S}} = m(x_1, x_2, \ldots, x_k)|_{\mathcal{S}} \neq 0.$$

Combinando a igualdade anterior com

$$x_1 x_2 \ldots x_r n|_{\mathcal{S}} = E_{i_1 j_1} E_{i_2 j_2} \ldots E_{i_r j_r} n|_{\mathcal{S}} = E_{i_1 j_r} n|_{\mathcal{S}}$$

e

$$m|_{\mathcal{S}} = E_{i_1 j_1} E_{i_2 j_2} \ldots E_{i_r j_r} \{x_{r+1} x_{r+2} \ldots x_k\}|_{\mathcal{S}},$$

temos que

$$n(x_{r+1}, \ldots, x_k)|_{\mathcal{S}} = x_{r+1} x_{r+2} \ldots x_k|_{\mathcal{S}} = E_{j_r j_k} \neq 0.$$

Pelo Lema 2.1.4, existe um monômio $n'(x_{r+2}, \ldots, x_k)$ multilinear tal que

$$n(x_{r+1}, \ldots, x_k) \equiv x_{r+1} n'(x_{r+2}, \ldots, x_k)\ (mod\ I_n).$$

Logo,

$$m_\sigma \equiv x_1 \ldots x_r n(x_{r+1}, x_{r+2} \ldots, x_k) \equiv x_1 \ldots x_r x_{r+1} n'(x_{r+2}, \ldots, x_k)\ (mod\ I_n),$$

o que contradiz a escolha do número r. Portanto, $r = k$. ∎

Corolário 2.1.6 *Se para duas permutações $\sigma, \tau \in S_k$, existir uma substituição Standard $\mathcal{S}$ tal que*

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

então $m_\sigma(x_1, x_2, \ldots, x_k) \equiv m_\tau(x_1, x_2, \ldots, x_k)$ (mod I_n).

Demonstração: Consideremos $x_1^{'} = x_{\tau(1)}, x_2^{'} = x_{\tau(2)}, \ldots, x_k^{'} = x_{\tau(k)}$. Sendo assim,

$$m_\tau(x_1, x_2, \ldots, x_k) = m(x_1^{'}, x_2^{'}, \ldots, x_k^{'}).$$

Tomemos agora $\mu = \tau^{-1} \circ \sigma$. Daí, temos

$$m_\mu(x_1^{'}, x_2^{'}, \ldots, x_k^{'}) = m_\sigma(x_1, x_2, \ldots, x_k).$$

Por $m_\sigma|_{\mathcal{S}} = m_\tau|_{\mathcal{S}} \neq 0$, temos que $m_\mu(x_1^{'}, x_2^{'}, \ldots, x_k^{'})|_{\mathcal{S}} = m(x_1^{'}, x_2^{'}, \ldots, x_k^{'})|_{\mathcal{S}} \neq 0$. Pelo Lema 2.1.5, segue que

$$m_\mu(x_1^{'}, x_2^{'}, \ldots, x_k^{'}) \equiv m(x_1^{'}, x_2^{'}, \ldots, x_k^{'}) \ (mod\ I_n)$$

e portanto,

$$m_\sigma(x_1, x_2, \ldots, x_k) \equiv m_\tau(x_1, x_2, \ldots, x_k) \ (mod\ I_n).$$

■

A seguir apresentaremos o resultado central desta seção.

Teorema 2.1.7 *Todas as identidades polinomiais da álgebra $\mathbb{Z}_n$-graduada $M_n(K)$ seguem de*

$$x_1x_2 - x_2x_1 = 0, \quad \omega(x_1) = \omega(x_2) = \overline{0};$$

$$x_1x_2x_3 - x_3x_2x_1 = 0, \quad \omega(x_1) = \omega(x_3) = -\omega(x_2),$$

ou seja, $T_n(M_n(K)) = I_n$.

Demonstração: Como a característica do corpo base é zero, precisamos mostrar que uma identidade polinomial $\mathbb{Z}_n$-graduada e multilinear arbitrária $f(x_1, x_2, \ldots, x_k)$ de $M_n(K)$ está em I_n. Seja r o menor inteiro não-negativo tal que f pode ser escrito, módulo I_n, como uma combinação linear de r monômios multilineares, isto é,

$$f \equiv \sum_{q=1}^{r} a_{\sigma_q} m_{\sigma_q} \ (mod\ I_n), \tag{2.12}$$

onde $0 \neq a_{\sigma_q} \in K$ e $\sigma_1, \sigma_2, \ldots, \sigma_r \in S_k$. Mostraremos que $r = 0$. De fato, suponhamos por contradição que $r > 0$. Em virtude do Lema 2.1.2, existe uma substituição Standard $\mathcal{S}$ tal que $m_{\sigma_1}|_{\mathcal{S}} \neq 0$. Por $I_n \subseteq T_n(M_n(K))$, temos que

$$f|_{\mathcal{S}} - \left(\sum_{q=1}^{r} a_{\sigma_q} m_{\sigma_q}\right)\Bigg|_{\mathcal{S}} = \left(f - \sum_{q=1}^{r} a_{\sigma_q} m_{\sigma_q}\right)\Bigg|_{\mathcal{S}} = 0$$

e daí

$$\left.\left(\sum_{q=1}^{r} a_{\sigma_q} m_{\sigma_q}\right)\right|_{\mathcal{S}} = 0$$

o que nos dá

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

Combinando esta última igualdade com o fato que

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

concluímos que existe um menor inteiro $p \in \{2, 3, \ldots, r\}$ tal que $m_{\sigma_p}|_{\mathcal{S}} = m_{\sigma_1}|_{\mathcal{S}}$. Portanto, pelo Corolário 2.1.6, $m_{\sigma_p} \equiv m_{\sigma_1}$ $(mod\ I_n)$ e daí, por 2.12

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

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

ou seja, f pode ser escrito, módulo I_n, como uma combinação de menos que r monômios multilineares, o que contradiz a escolha do número r. Logo,

$$f \equiv 0 \ (mod\ I_n)$$

e assim $T_n(M_n(K)) = I_n$. ■

2.2 Polinômios Centrais $\mathbb{Z}_n$-graduados

Apresentaremos nesta seção a descrição do espaço dos polinômios centrais $\mathbb{Z}_n$-graduados para a álgebra $M_n(K)$.

Vamos considerar $K\langle X\rangle$ a álgebra associativa livre $\mathbb{Z}_n$-graduada, onde $X = \bigcup_{\gamma \in \mathbb{Z}_n} X_\gamma$. Denotaremos $T_{\mathbb{Z}_n}$ e $C_{\mathbb{Z}_n}$ simplesmente por T_n e C_n, respectivamente.

Nesta e nas próximas seções consideremos, para cada inteiro positivo m, o m-ciclo $\theta_m = (1\ 2\ \ldots\ m)$ do grupo simétrico S_m e o subgrupo cíclico $H_m = \langle\theta_m\rangle$ de S_m.

Apresentaremos a seguir um tipo importante de polinômios centrais não-triviais para a álgebra $M_n(K)$. Para isso, precisaremos do conceito de *sequência completa* em $\mathbb{Z}_n$.

Definição 2.2.1 *Sejam* $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}_n$. *Dizemos que a n-upla* $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *é uma sequência completa se* $\{\alpha_1, \alpha_1 + \alpha_2, \ldots, \alpha_1 + \alpha_2 + \ldots + \alpha_n\} = \mathbb{Z}_n$ *e* $\alpha_1 + \alpha_2 + \ldots + \alpha_n = \overline{0}$.

Exemplo 2.2.2 *A sequência* $(\overline{1}, \overline{2}, \overline{3}, \overline{2})$ *é uma sequência completa em* $\mathbb{Z}_4$. *Dado* $\gamma \in \mathbb{Z}_n$, *temos que* $(\gamma, \gamma, \ldots, \gamma)$ *é uma sequência completa se, e somente se,* γ *é um gerador do grupo* $\mathbb{Z}_n$.

Lema 2.2.3 *Seja* $m(x_1, x_2, \ldots, x_k) = x_1 x_2 \ldots x_k$ *um monômio multilinear de* $K\langle X\rangle$ *com* $\omega(m) = \overline{0}$. *Se uma substituição Standard* $\mathcal{S}$ *(conforme 2.5)*

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

é tal que $m|_{\mathcal{S}} \neq 0$, *então* $m_\sigma|_{\mathcal{S}} \neq 0$ *para todo* $\sigma \in H_k$.

Demonstração: Sendo $m|_{\mathcal{S}} \neq 0$, temos $j_1 = i_2,\ j_2 = i_3,\ \ldots,\ j_{k-1} = i_k$. Como $m|_{\mathcal{S}} = E_{i_1 j_k}$ e $\omega(m) = \overline{0}$, devemos ter $i_1 = j_k$. Observemos que $m_{\theta_k}|_{\mathcal{S}} = E_{i_2 j_k} E_{i_1 j_1} = E_{i_2 i_2} \neq 0$. O resultado segue então indutivamente. ■

Proposição 2.2.4 *O polinômio multilinear*

$$f(x_1, x_2, \ldots, x_n) = \sum_{\sigma \in H_n} x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n)}$$

onde $(\omega(x_1), \omega(x_2), \ldots, \omega(x_n))$ *é uma sequência completa em* $\mathbb{Z}_n$, *é um polinômio central* $\mathbb{Z}_n$*-graduado, que não é identidade para a álgebra* $M_n(K)$.

Demonstração: Como f é multilinear , basta mostrar que $f|_{\mathcal{S}} \in Z(M_n(K))$ para toda substituição Standard $\mathcal{S}$. Observemos inicialmente que $\omega(x_1 x_2 \ldots x_n) = \omega(x_1) + \omega(x_2) + \ldots + \omega(x_n) = \overline{0}$. Vamos considerar $m = m(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n$. Pelo Lema 2.2.3, se $m|_{\mathcal{S}} = 0$, então $m_\sigma|_{\mathcal{S}} = 0$ para todo $\sigma \in H_n$, e daí $f|_{\mathcal{S}} = 0$. Suponhamos então $\mathcal{S}$ uma substituição Standard

$$x_1 = E_{i_1 j_1},\ x_2 = E_{i_2 j_2},\ \ldots,\ x_n = E_{i_n j_n}$$

tal que $m|_{\mathcal{S}} \neq 0$. Claramente devemos ter $j_1 = i_2,\ j_2 = i_3,\ \ldots,\ j_{n-1} = i_n$ e também $j_n = i_1$, pois $\omega(m) = \omega(x_1) + \omega(x_2) + \ldots + \omega(x_n) = \overline{0}$. Logo,

$$f|_{\mathcal{S}} = E_{i_1 i_1} + E_{i_2 i_2} + \ldots + E_{i_n i_n}.$$

Notando agora que

$$\omega(x_1) = \overline{i_2 - i_1},\ \omega(x_2) = \overline{i_3 - i_2},\ \ldots,\ \omega(x_{n-1}) = \overline{i_n - i_{n-1}},\ \omega(x_n) = \overline{i_1 - i_n},$$

temos

$$\omega(x_1)+\omega(x_2)=\overline{i_3-i_1},\ \ldots,\ \omega(x_1)+\ldots+\omega(x_{n-1})=\overline{i_n-i_1}.$$

Como $(\omega(x_1),\omega(x_2),\ldots,\omega(x_n))$ é uma sequência completa, devemos ter $\overline{i_2-i_1},\overline{i_3-i_1}$, $\ldots,\overline{i_n-i_1}$ não-nulos e dois a dois distintos, donde segue que $i_1,i_2,\ldots,i_n$ devem ser dois a dois incôgruos módulo n. Mas, $\{i_1,i_2,\ldots,i_n\}\subseteq\{1,2,\ldots,n\}$. Logo, temos a igualdade destes dois conjuntos e portanto $f|_{\mathcal{S}}=I_n\in Z(M_n(K))$. ■

Sejam I_n o T_n-ideal das identidades $\mathbb{Z}_n$-graduadas de $M_n(K)$ e $C_n(M_n(K))$ o T_n-espaço dos polinômios centrais $\mathbb{Z}_n$-graduados de $M_n(K)$. Claramente, temos $I_n\subseteq C_n(M_n(K))$. Tomemos agora V como sendo o T_n espaço gerado pelos polinômios

$$\begin{aligned} z_1[x_1,x_2]z_2\ , &\qquad \omega(x_1)=\omega(x_2)=\overline{0};\\ z_1(x_1x_2x_3-x_3x_2x_1)z_2\ , &\qquad \omega(x_1)=\omega(x_3)=-\omega(x_2);\\ \sum_{\sigma\in H_n} x_{\sigma(1)}x_{\sigma(2)}\ldots x_{\sigma(n)}\ , &\qquad (\omega(x_1),\omega(x_2),\ldots,\omega(x_n))\text{ sequência completa,}\end{aligned}\tag{2.13}$$

onde z_1 e z_2 são variavéis em X.

Do fato de todos os polinômios em 2.13 serem centrais segue que $V\subseteq C_n(M_n(K))$. Observando agora que o T_n-espaço gerado pelos dois primeiros polinômios em 2.13 é exatamente I_n, concluímos que $I_n\subset V$.

Lema 2.2.5 *Se o polinômio multilinear*

$$f(x_1,x_2,\ldots,x_k)=\lambda_1m_1(x_1,x_2,\ldots,x_k)+\ldots+\lambda_nm_n(x_1,x_2,\ldots,x_k)\ (k\geq n)$$

é tal que existe uma substituição Standard $\mathcal{S}$ tal que $f|_{\mathcal{S}}=\lambda I_n$, para algum $0\neq\lambda\in K$, então $f\in V$.

Demonstração: Como $f|_{\mathcal{S}}=\lambda I_n$, devemos ter $\lambda_1=\lambda_2=\ldots=\lambda_n=\lambda$ e $\omega(m_i)=\overline{0}$ para cada $i=1,\ldots,n$. Vamos supor que $m_1(x_1,x_2,\ldots,x_k)=x_1x_2\ldots x_k$. Seja $\mathcal{S}$ uma substituição Standard

$$x_1=E_{i_1j_1},\ x_2=E_{i_2j_2},\ \ldots,\ x_k=E_{i_kj_k}$$

satisfazendo as hipóteses do Lema. Por $f|_{\mathcal{S}}=\lambda I_n$, para cada $i=1,\ldots,n$, existe $j\in\{1,\ldots,n\}$ tal que $m_j|_{\mathcal{S}}=E_{ii}$. Logo, existem $1=l_1<l_2<\ldots<l_n$ de modo que

$\{i_{l_1}, i_{l_2}, \ldots, i_{l_n}\} = \{1, 2, \ldots, n\}$. Sendo assim,

$$m_1(x_1, x_2, \ldots, x_k) = \overbrace{x_{l_1} \ldots x_{l_2-1}}^{t_1} \overbrace{x_{l_2} \ldots x_{l_3-1}}^{t_2} \ldots \overbrace{x_{l_n} \ldots x_k}^{t_n}.$$

Logo,

$$\omega(t_1) = \overline{i_{l_2} - i_1},\ \omega(t_2) = \overline{i_{l_3} - i_{l_2}},\ \ldots,\ \omega(t_{n-1}) = \overline{i_{l_n} - i_{l_{n-1}}},\ e\ \omega(t_n) = \overline{i_1 - i_{l_n}}.$$

A sequência $(\omega(t_1), \omega(t_2), \ldots, \omega(t_n))$ é uma sequência completa em $\mathbb{Z}_n$. De fato,

$$\omega(t_1) + \omega(t_2) + \ldots + \omega(t_n) = \overline{i_{l_2} - i_1} + \overline{i_{l_3} - i_{l_2}} + \ldots + \overline{i_{l_n} - i_{l_{n-1}}} + \overline{i_1 - i_{l_n}} = \overline{0}.$$

Além disso,

$$\omega(t_1) = \overline{i_{l_2} - i_{l_1}},\ \omega(t_1) + \omega(t_2) = \overline{i_{l_3} - i_{l_1}},\ \ldots,\ \omega(t_1) + \omega(t_2) + \ldots + \omega(t_{n-1}) = \overline{i_{l_n} - i_{l_1}}.$$

Daí, sendo $\{i_{l_1}, i_{l_2}, \ldots, i_{l_n}\} = \{1, 2, \ldots, n\}$, devemos ter $\overline{i_{l_2} - i_{l_1}},\ \overline{i_{l_3} - i_{l_1}},\ \ldots,\ \overline{i_{l_n} - i_{l_1}}$ não-nulos e dois a dois distintos.

Consideremos agora o monômio

$$\overbrace{x_{l_2} \ldots x_{l_3-1}}^{t_2} \ldots \overbrace{x_{l_n} \ldots x_k}^{t_n} \overbrace{x_{l_1} \ldots x_{l_2-1}}^{t_1}$$

e observemos que $t_2 \ldots t_n t_1|_{\mathcal{S}} = E_{i_{l_2} i_{l_2}}$. Por $f|_{\mathcal{S}} = \lambda I_n$, existe algum $q \in \{1, 2, \ldots, n\}$ tal que $m_q|_{\mathcal{S}} = t_2 \ldots t_n t_1|_{\mathcal{S}} = E_{i_{l_2} i_{l_2}}$ e pelo Corolário 2.1.6, concluímos que $m_q \equiv t_2 \ldots t_n t_1\ (mod\ I_n)$. Como $\{t_{\sigma(1)} t_{\sigma(2)} \ldots t_{\sigma(n)}|_{\mathcal{S}};\ \sigma \in H_n\} = \{E_{11}, E_{22}, \ldots, E_{nn}\}$ continuamos com este raciocínio, usando novamente o Corolário 2.1.6, e concluímos que

$$f(x_1, x_2, \ldots, x_k) = \lambda(m_1 + m_2 + \ldots + m_n) \equiv \lambda \sum_{\sigma \in H_n} t_{\sigma(1)} t_{\sigma(2)} \ldots t_{\sigma(n)}\ (mod\ I_n),$$

e daí

$$f(x_1, x_2, \ldots, x_k) \equiv \lambda \sum_{\sigma \in H_n} t_{\sigma(1)} t_{\sigma(2)} \ldots t_{\sigma(n)}\ (mod\ V),$$

pois $I_n \subseteq V$. Além disso, $\sum_{\sigma \in H_n} t_{\sigma(1)} t_{\sigma(2)} \ldots t_{\sigma(n)} \in V$, donde segue que $f(x_1, x_2, \ldots, x_k) \in V$. ■

Teorema 2.2.6 *Seja K um corpo de característica zero. Então $C_n(M_n(K)) = V$.*

Demonstração: Seja $f(x_1, x_2, \ldots, x_k) \in C_n(M_n(K))$. Podemos supor f multilinear. Suponhamos ainda que f não é identidade $\mathbb{Z}_n$-graduada para $M_n(K)$. Podemos escrever f na forma

$$f = \lambda_1 m_1 + \lambda_2 m_2 + \ldots + \lambda_l m_l$$

onde $m_1, m_2, \ldots, m_l$ são monômios multilineares em $x_1, x_2, \ldots, x_k$. Por f não ser identidade $\mathbb{Z}_n$-graduada para $M_n(K)$, existe uma substituição Standard $\mathcal{S}$ tal que $f|_{\mathcal{S}} = \lambda I_n$, para algum $0 \neq \lambda \in K$. Logo, $l \geq n$. Observemos ainda que para cada $i = 1, 2, \ldots, l$, temos $m_i|_{\mathcal{S}} = 0$ ou $m_i|_{\mathcal{S}} = E_{jj}$. Temos também que para cada $i = 1, \ldots, n$, existe $j_i \in \{1, 2, \ldots, l\}$ tal que $m_{j_i}|_{\mathcal{S}} = E_{ii}$. Juntando os termos $m'_{j_i}s$ tais que $m_{j_i}|_{\mathcal{S}} = E_{ii}$ e usando o Corolário 2.1.6, concluímos que

$$f(x_1, x_2, \ldots, x_k) \equiv \alpha_1 m_{j_1} + \alpha_2 m_{j_2} + \ldots + \alpha_n m_{j_n} + \beta_1 m_{t_1} + \ldots + \beta_r m_{t_r} \ (mod\ V),$$

onde $r < l$, $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_r \in K$. Pelo Lema 2.2.5, temos

$$\alpha_1 m_{j_1} + \alpha_2 m_{j_2} + \ldots + \alpha_n m_{j_n} \in V,$$

donde segue que

$$f(x_1, x_2, \ldots, x_k) \equiv \beta_1 m_{t_1} + \ldots + \beta_r m_{t_r} \ (mod\ V).$$

Por $f \in C_n(M_n(K))$, temos que $\beta_1 m_{t_1} + \ldots + \beta_r m_{t_r} \in C_n(M_n(K))$. Se $r < n$, então $\beta_1 m_{t_1} + \ldots + \beta_r m_{t_r} \in I_n \subseteq V$. Caso contrário, repetimos os mesmos argumentos usados inicialmente. ■

2.3 Identidades Polinomiais $\mathbb{Z}$-graduadas

Nesta e na próxima seções denotaremos por $K\langle X \rangle$ a álgebra associativa livre $\mathbb{Z}$-graduada, onde $X = \bigcup_{m \in \mathbb{Z}} X_m$ e $M_n(K)$ a álgebra $\mathbb{Z}$-graduada, definida na seção 1.7.

Os resultados apresentados a seguir serão usados na demonstração do teorema que descreve as identidades $\mathbb{Z}$-graduadas para a álgebra $M_n(K)$.

Lema 2.3.1 *A álgebra $M_n(K)$ satisfaz as seguintes identidades*

$$x = 0 \ , \qquad |\omega(x)| \geq n; \tag{2.14}$$

$$x_1 x_2 - x_2 x_1 = 0 \ , \qquad \omega(x_1) = \omega(x_2) = 0; \tag{2.15}$$

$$x_1 x_2 x_3 - x_3 x_2 x_1 = 0 \ , \qquad \omega(x_1) = \omega(x_3) = -\omega(x_2). \tag{2.16}$$

Demonstração: Desde que $M_k = \{0\}$ quando $|k| \geq n$, temos que $M_n(K)$ satisfaz as identidades graduadas 2.14. Por outro lado, M_0 é o conjunto das matrizes diagonais . Logo, 2.15 é uma identidade graduada para $M_n(K)$.

As identidades 2.16 são multilineares. Dessa forma, é suficiente mostrar que as identidades 2.16 são satisfeitas quando

$$x_1 = E_{i_1j_1}, \quad x_2 = E_{i_2j_2}, \quad x_3 = E_{i_3j_3},$$

onde $E_{i_1j_1},\ E_{i_3j_3} \in M_k$ e $E_{i_2j_2} \in M_{-k}$ e $|k| \leq n-1$. Notemos que $E_{i_1j_1}E_{i_2j_2}E_{i_3j_3} \neq 0$ se, e somente se,

$$j_1 = i_2 \text{ e } j_2 = i_3. \tag{2.17}$$

Mostraremos que neste caso, $i_1 = j_2 = i_3$ e $j_1 = i_2 = j_3$. De fato, por $E_{i_1j_1},\ E_{i_3j_3} \in M_k$, $E_{i_2j_2} \in M_{-k}$ e 2.17, temos

$$i_2 = j_1 = i_1 + k, \tag{2.18}$$

por 2.18

$$i_3 = j_2 = i_2 - k = i_1, \tag{2.19}$$

e por 2.19

$$j_3 = i_3 + k = i_1 + k = j_1.$$

Similarmente, $E_{i_3j_3}E_{i_2j_2}E_{i_1j_1} \neq 0$, somente se $j_1 = i_2 = j_3$ e $i_1 = j_2 = i_3$. Desta forma, $E_{i_1j_1}E_{i_2j_2}E_{i_3j_3} \neq 0$ se, e somente se, $E_{i_3j_3}E_{i_2j_2}E_{i_1j_1} \neq 0$. Neste caso, $i_1 = j_2 = i_3$ e $j_1 = i_2 = j_3$, e daí

$$E_{i_1j_1}E_{i_2j_2}E_{i_3j_3} = E_{i_1j_3} = E_{i_3j_1} = E_{i_3j_3}E_{i_2j_2}E_{i_1j_1}.$$

Caso contrário,

$$E_{i_1j_1}E_{i_2j_2}E_{i_3j_3} = 0 = E_{i_3j_3}E_{i_2j_2}E_{i_1j_1}$$

o que conclui a demonstração. ■

Denotaremos por J_n o $T_{\mathbb{Z}}$-ideal gerado pelas identidades graduadas de 2.14 a 2.16 e SSt o conjunto de todas as substituições Standard (conforme Seção 2.1). Aqui $\omega(x_s) = j_s - i_s$. Recordemos que dados um monômio $m_\sigma(x_1, x_2, \ldots, x_k)$, $\sigma \in S_k$, e dois inteiros $1 \leq p \leq q \leq k$, denotamos por $m_\sigma^{[p,q]}$ a *subpalavra* obtida de m_σ descartando os $p-1$ primeiros e os últimos $k-q$ fatores, ou seja,

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

Nos resultados enunciados a seguir $\mathcal{S}$ denotará uma substituição Standard.

Lema 2.3.2 *Seja $\sigma \in S_k$. Se $m_\sigma|_{\mathcal{S}} \neq 0$, então para $1 \leq p \leq q \leq k$*

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

Demonstração: Por 2.6 e 2.7, temos

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

$$= (j_{\sigma(q)} - i_{\sigma(q)}) + (j_{\sigma(q-1)} - i_{\sigma(q-1)}) + \ldots + (j_{\sigma(p)} - i_{\sigma(p)}) = j_{\sigma(q)} - i_{\sigma(p)}.$$

■

Lema 2.3.3 *Sejam $\sigma \in S_k$ e*

$$x_1 = E_{i_1 j_1}, x_2 = E_{i_2 j_2}, \ldots, x_k = E_{i_k j_k}, \tag{2.20}$$

uma substituição Standard tal que $\max\{i_1, j_1, i_2, j_2, \ldots, i_k, j_k\} = n - t$, *onde* $t \geq 1$ *(respectivamente* $\min\{i_1, j_1, i_2, j_2, \ldots, i_k, j_k\} = 1 + r$, *onde* $r \geq 1$*).*

(i) Se $m_\sigma(x_1, x_2, \ldots, x_k)|_{(2.20)} = 0$, então quando a substituição Standard

$$x_1 = E_{i'_1 j'_1},\ x_2 = E_{i'_2 j'_2},\ \ldots,\ x_k = E_{i'_k j'_k}, \tag{2.21}$$

com $i'_s = i_s + t$ e $j'_s = j_s + t$ (resp. $i'_s = i_s - r$ e $j'_s = j_s - r$), $s = 1, 2, \ldots, k$ é feita, temos

$$m_\sigma(x_1, x_2, \ldots, x_k)|_{(2.21)} = 0.$$

(ii) Se $m_\sigma(x_1, x_2, \ldots, x_k)|_{(2.20)} = E_{i_{\sigma(1)} j_{\sigma(k)}}$, então $m_\sigma(x_1, x_2, \ldots, x_k)|_{(2.21)} = E_{i'_{\sigma(1)} j'_{\sigma(k)}}$.

Demonstração: **(i)** Da igualdade

$$m_\sigma|_{(2.20)} = E_{i_{\sigma(1)} j_{\sigma(1)}} E_{i_{\sigma(2)} j_{\sigma(2)}} \ldots E_{i_{\sigma(k)} j_{\sigma(k)}} = 0,$$

nós temos que $j_{\sigma(s)} \neq i_{\sigma(s+1)}$ para algum $s \in \{1, 2, \ldots, k-1\}$. Então

$$j'_{\sigma(s)} = j_{\sigma(s)} + t \neq i_{\sigma(s+1)} + t = i'_{\sigma(s+1)}\ (resp.\ j'_{\sigma(s)} = j_{\sigma(s)} - r \neq i_{\sigma(s+1)} - r = i'_{\sigma(s+1)}).$$

Portanto, $m_\sigma|_{(2.21)} = 0$.

(ii) Para $s = 1, \ldots, k-1$, a igualdade $j_{\sigma(s)} = i_{\sigma(s+1)}$, nos dá $j'_{\sigma(s)} = i'_{\sigma(s+1)}$. Portanto,

$$m_\sigma|_{(2.21)} = E_{i'_{\sigma(1)} j'_{\sigma(1)}} E_{i'_{\sigma(2)} j'_{\sigma(2)}} \ldots E_{i'_{\sigma(k)} j'_{\sigma(k)}} = E_{i'_{\sigma(1)} j'_{\sigma(k)}},$$

concluindo assim a demonstração. ■

Para um monômio graduado $\mathtt{n}(x_1, x_2, \ldots, x_r) = x_{i_1} x_{i_2} \ldots x_{i_r}$ e $1 \leq p \leq q \leq r$, denotaremos por $|\omega(\mathtt{n}^{[p,q]})|$ o valor absoluto do grau homogêneo da subpalavra $\mathtt{n}^{[p,q]}$. Consideremos

$$\widehat{\omega}(\mathtt{n}) = \max\{|\omega(\mathtt{n}^{[p,q]})| \ / \ 1 \leq p \leq q \leq r\}.$$

É claro que se $\widehat{\omega}(\mathtt{n}) \geq n$, então $\mathtt{n} \in J_n$. De fato, existe uma subpalavra $\mathtt{n}^{[p',q']}$, $1 \leq p' \leq q' \leq r$, tal que $\widehat{\omega}(\mathtt{n}) = |\omega(\mathtt{n}^{[p',q']})| \geq n$. Daí,

$$\mathtt{n} = \mathtt{n}^{[1,p'-1]} \mathtt{n}^{[p',q']} \mathtt{n}^{[q'+1,r]} \in J_n,$$

pois $\mathtt{n}^{[p',q']} \in J_n$.

Lema 2.3.4 *Se*

$$x_0 \left(\sum_{\sigma \in P} a_\sigma m_\sigma(x_1, x_2, \ldots, x_k) \right) = 0,$$

onde $P \subseteq S_k$, é uma identidade graduada de $M_n(K)$ tal que $\widehat{\omega}(x_0 m_\sigma) \leq n-1$, para todo $\sigma \in P$, então

$$\sum_{\sigma \in P} a_\sigma m_\sigma(x_1, x_2, \ldots, x_k) \in T_{\mathbb{Z}}(M_n(K)).$$

Demonstração: Suponhamos por contradição que existe uma substituição Standard $\mathcal{S}$ tal que

$$\left(\sum_{\sigma \in P} a_\sigma m_\sigma \right) \Bigg|_{\mathcal{S}} = \sum_{i,j=1}^{n} b_{ij} E_{ij} \neq 0, \ b_{ij} \in K. \tag{2.22}$$

Podemos supor sem perda de generalidade que se $\omega(x_0) \geq 0$, então

$$\max\{i_1, j_1, i_2, j_2, \ldots, i_k, j_k\} = n,$$

pois se $\max\{i_1, j_1, i_2, j_2, \ldots, i_k, j_k\} = n - t$ com $t \geq 1$, então, pelo Lema 2.3.3, a substituição $\mathcal{S}'$ da forma $x_s = E_{i'_s j'_s}$, com $i'_s = i_s + t$ e $j'_s = j_s + t$, $s = 1, 2, \ldots, k$ é tal que $\max\{i'_1, j'_1, i'_2, j'_2, \ldots, i'_k, j'_k\} = n$ e

$$\left(\sum_{\sigma \in P} a_\sigma m_\sigma \right) \Bigg|_{\mathcal{S}'} \neq 0.$$

Similarmente, nós podemos supor que se $\omega(x_0) < 0$, então

$$\min\{i_1, j_1, i_2, j_2, \ldots, i_k, j_k\} = 1.$$

Nós podemos supor ainda que para qualquer coeficiente $b_{ij} \neq 0$ em 2.22, $1 \leq i - \omega(x_0) \leq n$. Para verificar isto, observemos que $i \in \{i_{\sigma(1)} \mid \sigma \in P,\ m_\sigma|_{\mathcal{S}} \neq 0\}$. Logo, é suficiente provar que $1 \leq i_{\sigma(1)} - \omega(x_0) \leq n$, para cada $\sigma \in P$ com $m_\sigma|_{\mathcal{S}} \neq 0$.

Primeiro, consideremos o caso onde $\omega(x_0) \geq 0$ e $\max\{i_1, j_1, i_2, j_2, \ldots, i_k, j_k\} = n$. Em decorrência de 2.7, para $\sigma \in P$ com $m_\sigma|_{\mathcal{S}} \neq 0$, se $\max\{j_1, j_2, \ldots, j_k\} < n$, então $i_{\sigma(1)} = n$. Logo,

$$\omega(x_0) \geq 0, \text{ ou seja, } n - \omega(x_0) \leq n, \text{ de onde, } i_{\sigma(1)} - \omega(x_0) \leq n.$$

Além disso,

$$\omega(x_0) \leq |\omega(x_0)| \leq \widehat{\omega}(x_0 m_\sigma) \leq n-1, \text{ ou seja, } 1 \leq n - \omega(x_0), \text{ isto é, } 1 \leq i_{\sigma(1)} - \omega(x_0).$$

Portanto, $1 \leq i_{\sigma(1)} - \omega(x_0) \leq n$. Agora vamos supor que $\max\{j_1, j_2, \ldots, j_k\} = n$. Escolha um $\sigma \in P$ arbitrário tal que $m_\sigma|_{\mathcal{S}} \neq 0$ e consideremos $n = j_{\sigma(r)}$, para algum $1 \leq r \leq k$. Pelo Lema 2.3.2, temos

$$\omega(x_0 m_\sigma^{[1,r]}) = \omega(x_0) + j_{\sigma(r)} - i_{\sigma(1)} = \omega(x_0) + n - i_{\sigma(1)}.$$

Combinando isto com $\omega(x_0 m_\sigma^{[1,r]}) \leq |\omega(x_0 m_\sigma^{[1,r]})| \leq \widehat{\omega}(x_0 m_\sigma) \leq n-1$, obtemos que

$$\omega(x_0) + n - i_{\sigma(1)} \leq n-1, \text{ isto é, } \omega(x_0) - i_{\sigma(1)} \leq -1, \text{ de onde, } 1 \leq i_{\sigma(1)} - \omega(x_0).$$

Além disso, $i_{\sigma(1)} \leq n \leq \omega(x_0) + n$, isto é, $i_{\sigma(1)} - \omega(x_0) \leq n$. Daí, $1 \leq i_{\sigma(1)} - \omega(x_0) \leq n$.

Consideremos agora o caso onde $\omega(x_0) < 0$ e $\min\{i_1, j_1, i_2, j_2, \ldots, i_k, j_k\} = 1$. Em virtude de 2.7, se $\min\{j_1, j_2, \ldots, j_k\} > 1$, então $i_{\sigma(1)} = 1$ para todo $\sigma \in P$ tal que $m_\sigma|_{\mathcal{S}} \neq 0$. Daí,

$$\omega(x_0) < 0, \text{ ou seja, } 1 = i_{\sigma(1)} < i_{\sigma(1)} - \omega(x_0).$$

Além do mais, por $-\omega(x_0) \leq |\omega(x_0)| \leq \widehat{\omega}(x_0 m_\sigma) \leq n-1$, temos que $-\omega(x_0) \leq n-1$, ou seja, $i_{\sigma(1)} - \omega(x_0) = 1 - \omega(x_0) \leq n$. Suponhamos agora que $\min\{j_1, j_2, \ldots, j_k\} = 1$. Escolha um $\sigma \in P$ arbitrário tal que $m_\sigma|_{\mathcal{S}} \neq 0$ e tome $r \in \{1, 2, \ldots, k\}$ tal que $1 = j_{\sigma(r)}$. Pelo Lema 2.3.2, temos

$$\omega(x_0 m_\sigma^{[1,r]}) = \omega(x_0) + j_{\sigma(r)} - i_{\sigma(1)} = \omega(x_0) + 1 - i_{\sigma(1)}.$$

Combinando isto com

$$-\omega(x_0 m_\sigma^{[1,r]}) \leq |\omega(x_0 m_\sigma^{[1,r]})| \leq \widehat{\omega}(x_0 m_\sigma) \leq n-1,$$

obtemos que $-\omega(x_0) - 1 + i_{\sigma(1)} \leq n - 1$, isto é, $i_{\sigma(1)} - \omega(x_0) \leq n$. Por outro lado,

$$\omega(x_0) < 0, \text{ isto é}, 1 \leq i_{\sigma(1)} < i_{\sigma(1)} - \omega(x_0), \text{ ou seja}, 1 \leq i_{\sigma(1)} - \omega(x_0).$$

Logo, $1 \leq i_{\sigma(1)} - \omega(x_0) \leq n$.

Finalmente, escolha $i_0, j_0 \in \{1, 2, \ldots, n\}$ tal que $b_{i_0 j_0} \neq 0$. Pelo que foi exposto anteriormente, $1 \leq i_0 - \omega(x_0) \leq n$. Considerando a substituição Standard $\mathcal{S}'$ formada por $\mathcal{S}$ e $x_0 = E_{i_0 - \omega(x_0), i_0}$, temos que

$$\left(x_0 \sum_{\sigma \in P} a_\sigma m_\sigma \right) \Bigg|_{\mathcal{S}'} = E_{i_0 - \omega(x_0), i_0} \left(\sum_{i,j=1}^{n} b_{ij} E_{ij} \right) = \sum_{j=1}^{n} b_{i_0 j} E_{i_0 - \omega(x_0), j} \neq 0,$$

contradizendo a hipótese do Lema. ■

Corolário 2.3.5 *Para qualquer monômio graduado* $m_\sigma(x_1, x_2, \ldots, x_k)$ *com* $\widehat{\omega}(m_\sigma) \leq n - 1$, *existe uma substituição Standard* $\mathcal{S}$ *tal que* $m_\sigma(x_1, x_2, \ldots, x_k)|_{\mathcal{S}} \neq 0$.

Demonstração: Para $k = 1$, $m_\sigma(x_1) = x_1$. Logo, por $\widehat{\omega}(m_\sigma) \leq n - 1$, segue que $|\omega(x_1)| \leq n - 1$. Basta então escolher $x_1 = E_{i_1 j_1}$ tal que $j_1 - i_1 = \omega(x_1)$.

Suponhamos que para qualquer monômio multilinear m de tamanho k, onde $\widehat{\omega}(m) \leq n - 1$, existe uma substituição Standard $\mathcal{S}$ tal que $m(x_1, x_2, \ldots, x_k)|_{\mathcal{S}} \neq 0$. Consideremos o monômio $\mathtt{n}(x_1, x_2, \ldots, x_k, x_{k+1}) = x_{i_1} x_{i_2} \ldots x_{i_k} x_{i_{k+1}}$, com $i_1, i_2, \ldots, i_k$, $i_{k+1} \in \{1, 2, \ldots, k, k+1\}$, tal que $\widehat{\omega}(\mathtt{n}) \leq n - 1$. Observe que

$$\mathtt{n}(x_1, x_2, \ldots, x_k, x_{k+1}) = x_{i_1} \mathtt{n}'(x_{i_2}, \ldots, x_{i_k}, x_{i_{k+1}}).$$

Logo, $\widehat{\omega}(\mathtt{n}) = \widehat{\omega}(x_{i_1} \mathtt{n}') \leq n - 1$. Portanto, pelo Lema 2.3.4 $\mathtt{n} = x_{i_1} \mathtt{n}'$ não pode ser identidade $\mathbb{Z}$-graduada para $M_n(K)$, pois do contrário $\mathtt{n}'$ também seria identidade. Além disso, de $\widehat{\omega}(x_{i_1} \mathtt{n}') \leq n - 1$ segue que $\widehat{\omega}(\mathtt{n}') \leq n - 1$, o que contradiz a hipótese de indução. ■

Denotemos por Λ_0 o conjunto de todos os monômios $m_\sigma(x_1, x_2, \ldots, x_k)$, $\sigma \in S_k$, tal que $\widehat{\omega}(m_\sigma) = n - 1$.

Lema 2.3.6 *Para qualquer monômio* $m_\sigma(x_1, x_2, \ldots, x_k) \in \Lambda_0$, *existe uma única substituição Standard* $\mathcal{S}$ *tal que* $m_\sigma|_{\mathcal{S}} \neq 0$.

Demonstração: Sejam $m_\sigma^{[p,q]}$ uma subpalavra de m_σ com $|\omega(m_\sigma^{[p,q]})| = n-1$ e $\mathcal{S}$ uma substituição Standard tal que $m_\sigma|_\mathcal{S} \neq 0$. Se $\omega(m_\sigma^{[p,q]}) = -n+1$, então $m_\sigma^{[p,q]}|_\mathcal{S} = E_{n1}$. Logo, $E_{i_{\sigma(p)}j_{\sigma(q)}} = E_{n1}$, ou seja, $i_{\sigma(p)} = n$ e $j_{\sigma(q)} = 1$. Suponhamos uma substituição Standard $\mathcal{S}'$ tal que $m_\sigma|_{\mathcal{S}'} \neq 0$. Sendo assim, $i'_{\sigma(p)} = n$ e $j'_{\sigma(q)} = 1$. Consequentemente,

$$i_{\sigma(p)} = i'_{\sigma(p)} \text{ e } j_{\sigma(q)} = j'_{\sigma(q)}. \tag{2.23}$$

Temos que

$$m_\sigma|_\mathcal{S} = E_{i_{\sigma(1)}j_{\sigma(1)}} \dots E_{i_{\sigma(p-1)}j_{\sigma(p-1)}} E_{i_{\sigma(p)}j_{\sigma(p)}} \dots E_{i_{\sigma(q)}j_{\sigma(q)}} E_{i_{\sigma(q+1)}j_{\sigma(q+1)}} \dots E_{i_{\sigma(k)}j_{\sigma(k)}},$$

e

$$m_\sigma|_{\mathcal{S}'} = E_{i'_{\sigma(1)}j'_{\sigma(1)}} \dots E_{i'_{\sigma(p-1)}j'_{\sigma(p-1)}} E_{i'_{\sigma(p)}j'_{\sigma(p)}} \dots E_{i'_{\sigma(q)}j'_{\sigma(q)}} E_{i'_{\sigma(q+1)}j'_{\sigma(q+1)}} \dots E_{i'_{\sigma(k)}j'_{\sigma(k)}}.$$

Por 2.7 e 2.23, temos que $j_{\sigma(p-1)} = i_{\sigma(p)} = i'_{\sigma(p)} = j'_{\sigma(p-1)}$. Logo, por 2.6 temos ainda que $\omega(x_{\sigma(p-1)}) = j_{\sigma(p-1)} - i_{\sigma(p-1)} = j'_{\sigma(p-1)} - i'_{\sigma(p-1)}$, de onde segue que $i_{\sigma(p-1)} = i'_{\sigma(p-1)}$. Continuando com este raciocínio, usando 2.6 e 2.7, concluímos que $\mathcal{S} = \mathcal{S}'$. Similarmente, se $\omega(m_\sigma^{[p,q]}) = n-1$, então $m_\sigma^{[p,q]}|_\mathcal{S} = E_{1n}$. Logo, $E_{i_{\sigma(p)}j_{\sigma(q)}} = E_{1n}$, isto é, $i_{\sigma(p)} = 1$ e $j_{\sigma(q)} = n$. Usando os argumentos expostos anteriormente, concluímos que os índices i_s e j_s, $s = 1, 2, \dots, k$ são determinados unicamente. ■

Para $i, j = 1, \dots, n$ e $\mathcal{S} \in SSt$, considere o conjunto

$$\Lambda(\mathcal{S}, i, j) = \{m_\sigma(x_1, x_2, \dots, x_k) \in \Lambda_0 \mid m_\sigma|_\mathcal{S} = E_{ij}\}.$$

Claramente, $\Lambda(\mathcal{S}, i, j) = \emptyset$, se $\omega(m_\sigma) \neq j - i$. Em virtude do Lema 2.3.6, os conjuntos $\Lambda(\mathcal{S}, i, j)$ são dois a dois disjuntos e a união coincide com Λ_0, ou seja,

$$\Lambda_0 = \bigcup_{(\mathcal{S},i,j)} \Lambda(\mathcal{S}, i, j), \tag{2.24}$$

onde $(\mathcal{S}, i, j)$ varia sobre todas as triplas ordenadas $(\mathcal{S}, i, j)$, com $\mathcal{S} \in SSt$ e $i, j = 1, \dots, n$. De fato, se $\Lambda(\mathcal{S}, i, j) \cap \Lambda(\mathcal{S}', i', j') \neq \emptyset$, então existe $m_\sigma \in \Lambda_0$ tal que $m_\sigma|_\mathcal{S} = E_{ij}$ e $m_\sigma|_{\mathcal{S}'} = E_{i'j'}$. Mas em virtude do Lema 2.3.6, $\mathcal{S} = \mathcal{S}'$ e consequentemente $(i, j) = (i', j')$. É imediato que

$$\bigcup_{(\mathcal{S},i,j)} \Lambda(\mathcal{S}, i, j) \subseteq \Lambda_0.$$

Seja $m_\sigma \in \Lambda_0$. Existe então uma única substituição $\mathcal{S}'$ tal que $m_\sigma|_{\mathcal{S}'} \neq 0$, ou seja, $m_\sigma|_{\mathcal{S}'} = E_{i'j'}$. Daí, $m_\sigma \in \Lambda(\mathcal{S}', i', j') \subseteq \bigcup_{(\mathcal{S},i,j)} \Lambda(\mathcal{S}, i, j)$.

Lema 2.3.7 *Se para uma permutação $\sigma \in S_k$, existir uma substituição Standard $\mathcal{S}$ tal que*

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

então

$$m_\sigma(x_1, x_2, \ldots, x_k) \equiv x_1 n(x_2, x_3, \ldots, x_k) \ (mod\ J_n),$$

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

Demonstração: Caso $\sigma(1) = 1$, a demonstração é trivial. Suponhamos que $\sigma(1) \neq 1$. Logo, $1 \neq \sigma^{-1}(1)$, e assim $1 = \sigma^{-1}(\sigma(1)) < \sigma^{-1}(1)$. Além disso, existe um inteiro positivo u tal que $\sigma(1) = 1 + u$. Daí, $1 = \sigma^{-1}(\sigma(1)) = \sigma^{-1}(1 + u) < \sigma^{-1}(1)$. Seja u_0 o menor inteiro positivo tal que $\sigma^{-1}(1 + u_0) < \sigma^{-1}(1)$. Obviamente,

$$1 \leq \sigma^{-1}(1 + u_0) < \sigma^{-1}(1) \leq \sigma^{-1}(u_0). \tag{2.25}$$

Desde que $m_\sigma|_{\mathcal{S}} = m|_{\mathcal{S}} \neq 0$, temos

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

e daí, $i_1 = i_{\sigma(1)}$, $j_t = i_{t+1}$, $t = 1, \ldots, k-1$ e, para $s > 1$, $j_{\sigma(s-1)} = i_{\sigma(s)}$. Considerando $p = \sigma^{-1}(u_0 + 1)$, $q = \sigma^{-1}(1)$ e $r = \sigma^{-1}(u_0)$, por 2.25 temos $1 \leq p < q \leq r$ com $j_{\sigma(q-1)} = i_{\sigma(q)} = i_{\sigma(1)}$, $j_{\sigma(r)} = i_{\sigma(p)}$ e, se $p > 1$, $j_{\sigma(p-1)} = i_{\sigma(p)}$. Vamos considerar inicialmente o caso $p > 1$. Das igualdades

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

temos que

$$j_{\sigma(p-1)} - i_{\sigma(1)} = i_{\sigma(p)} - j_{\sigma(q-1)} = j_{\sigma(r)} - i_{\sigma(q)} = \alpha_0$$

para algum $\alpha_o \in \mathbb{Z}$. Pelo Lema 2.3.2, temos

$$\omega(m_\sigma^{[1,p-1]}) = j_{\sigma(p-1)} - i_{\sigma(1)} = \alpha_0;$$

$$\omega(m_\sigma^{[p,q-1]}) = j_{\sigma(q-1)} - i_{\sigma(p)} = -\alpha_0;$$

$$\omega(m_\sigma^{[q,r]}) = j_{\sigma(r)} - i_{\sigma(q)} = \alpha_0.$$

Consequentemente, usando 2.16, segue que

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

$$\equiv m_\sigma^{[q,r]} m_\sigma^{[p,q-1]} m_\sigma^{[1,p-1]} m_\sigma^{[r+1,k]} = x_{\sigma(q)} x_{l_2} \ldots x_{l_k} = x_1 x_{l_2} \ldots x_{l_k} \ (mod\ J_n).$$

Consideremos agora $p = 1$. Neste caso, $j_{\sigma(q-1)} = i_{\sigma(q)} = i_{\sigma(1)} = j_{\sigma(r)}$, e pelo Lema 2.3.2

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

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

Portanto, por 2.15 segue que

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

$$\equiv m_\sigma^{[q,r]} m_\sigma^{[1,q-1]} m_\sigma^{[r+1,k]} = x_{\sigma(q)} x_{l_2} \ldots x_{l_k} = x_1 x_{l_2} \ldots x_{l_k} \ (mod\ J_n).$$

■

Corolário 2.3.8 *Se para duas permutações $\sigma, \tau \in S_k$, existir uma substituição Standard $\mathcal{S}$ tal que*

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

então $m_\sigma(x_1, x_2, \ldots, x_k) \equiv x_{\tau(1)} \mathtt{n}(x_{\tau(2)}, x_{\tau(3)}, \ldots, x_{\tau(k)})$ $(mod\ J_n)$, para algum $\mathtt{n}(y_2, y_3, \ldots, y_k) = y_{l_2} y_{l_3} \ldots y_{l_k}$.

Demonstração: Consideremos $x_1' = x_{\tau(1)}, x_2' = x_{\tau(2)}, \ldots, x_k' = x_{\tau(k)}$. Logo,

$$m_\tau(x_1, x_2, \ldots, x_k) = m(x_1', x_2', \ldots, x_k').$$

Tomemos agora $\mu = \tau^{-1} \circ \sigma$. Sendo assim,

$$m_\mu(x_1', x_2', \ldots, x_k') = m_\sigma(x_1, x_2, \ldots, x_k).$$

Por $m_\sigma|_{\mathcal{S}} = m_\tau|_{\mathcal{S}} \neq 0$, temos que $m_\mu(x_1', x_2', \ldots, x_k')|_{\mathcal{S}} = m(x_1', x_2', \ldots, x_k')|_{\mathcal{S}} \neq 0$. Do Lema 2.3.7 segue que

$$m_\mu(x_1', x_2', \ldots, x_k') \equiv x_1' x_{l_2}' \ldots x_{l_k}' \ (mod\ J_n),$$

onde $\{l_2, \ldots, l_k\} = \{2, \ldots, k\}$, ou seja,

$$m_\sigma(x_1, x_2, \ldots, x_k) \equiv x_{\tau(1)} x_{l_2}' \ldots x_{l_k}' \ (mod\ J_n),$$

o que nos dá

$$m_\sigma(x_1, x_2, \ldots, x_k) \equiv x_{\tau(1)} \mathtt{n}(x_{\tau(2)}, x_{\tau(3)}, \ldots, x_{\tau(k)}) \ (mod\ J_n),$$

para algum monômio $\mathtt{n}(y_2, y_3, \ldots, y_k) = y_{l_2} y_{l_3} \ldots y_{l_k}$. ■

A seguir apresentaremos o principal resultado desta seção.

Teorema 2.3.9 *Todas as identidades polinomiais da álgebra $\mathbb{Z}$-graduada $M_n(K)$ seguem de*

$$\begin{aligned} x = 0\ , &\qquad |\omega(x)| \geq n; \\ x_1x_2 - x_2x_1 = 0\ , &\qquad \omega(x_1) = \omega(x_2) = 0; \\ x_1x_2x_3 - x_3x_2x_1 = 0\ , &\qquad \omega(x_1) = \omega(x_3) = -\omega(x_2), \end{aligned}$$

isto é, $T_{\mathbb{Z}}(M_n(K)) = I_n$.

Demonstração: Para provar que $T_{\mathbb{Z}}(M_n(K)) = J_n$ nós usaremos indução sobre n. Seja $n = 1$. Neste caso, $M_1(K) = M_0 = K$. Em virtude de 2.14, nós precisamos considerar somente as identidades graduadas de $M_1(K)$ que são da forma $f(x_1, x_2, \ldots, x_k) = 0$, onde $\omega(x_1) = \omega(x_2) = \ldots = \omega(x_k) = 0$. De fato, pois do contrário existe $i \in \{1, 2, \ldots, k\}$ tal que $|\omega(x_i)| \geq 1$. Logo, $m_\sigma(x_1, x_2, \ldots, x_k) \in J_1$, para todo $\sigma \in S_k$ e consequentemente $f(x_1, x_2, \ldots, x_k) \in J_1$. As identidades $f(x_1, x_2, \ldots, x_k) = 0$, onde $\omega(x_1) = \omega(x_2) = \ldots = \omega(x_k) = 0$ são na verdade identidades polinomiais ordinárias de $M_0 = K$. Desde que todas as identidades de um corpo infinito seguem de $[x_1, x_2]$ (veja [13], página 45), concluímos que $T_{\mathbb{Z}}(M_1(K)) = J_1$.

Agora seja $n > 1$ e vamos supor que $T_{\mathbb{Z}}(M_{n-1}(K)) = J_{n-1}$. Desde que a característica do corpo base é zero, nós precisamos provar somente que cada identidade polinomial $\mathbb{Z}$-graduada multilinear de $M_n(K)$ está em J_n. Nós também usaremos indução sobre k assumindo que cada polinômio multilinear $g(y_1, y_2, \ldots, y_{k-1}) \in T_{\mathbb{Z}}(M_n(K))$ em $k-1$ variáveis está em J_n. Seja $f(x_1, x_2, \ldots, x_k)$ um polinômio $\mathbb{Z}$-graduado multilinear arbitrário em $T_{\mathbb{Z}}(M_n(K))$. Note que

$$\begin{aligned} \psi\ :\ M_{n-1}(K) &\longrightarrow \qquad M_n(K) \\ A \qquad &\longmapsto\ \psi(A) = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

é um mergulho natural $\mathbb{Z}$-graduado de $M_{n-1}(K)$ em $M_n(K)$. Desde que $f(x_1, x_2, \ldots, x_k) \in T_{\mathbb{Z}}(M_n(K))$ e ψ é um mergulho $\mathbb{Z}$-graduado, segue que $f(x_1, x_2, \ldots, x_k) \in T_{\mathbb{Z}}(M_{n-1}(K)) = J_{n-1}$. Logo, f é consequência de 2.14 a 2.16 e das identidades

$$x = 0,\ \text{para}\ |\omega(x)| = n - 1. \tag{2.26}$$

Então f pode ser escrito como

$$f = f_1 + f_2 + f_3,$$

para f_1, f_2, f_3 polinômios $\mathbb{Z}$-graduados multilineares, onde f_1 é consequência de 2.15, f_2 é consequência de 2.16 e f_3 é consequência de 2.14 e 2.26. É fácil ver que f_3 pode ser escrito da forma

$$f_3 = \sum_{\widehat{\omega}(m_\sigma) \geq n-1} a_\sigma m_\sigma(x_1, x_2, \ldots, x_k).$$

De fato, por f_3 ser consequência de 2.14 e 2.26, temos que $\sum a_\alpha g_1^\alpha g_2^\alpha g_3^\alpha$, onde $g_1^\alpha, g_3^\alpha \in K\langle X\rangle$ e g_2^α é tal que $|\omega(g_2^\alpha)| \geq n-1$. Por g_2^α ser homogêneo com respeito ao $\mathbb{Z}$-grau, podemos escrever f_3 da forma

$$f_3 = \sum a_\gamma m_1^\gamma m_2^\gamma m_3^\gamma,$$

onde $|\omega(m_2^\gamma)| \geq n-1$ e $m_1^\gamma, m_2^\gamma, m_3^\gamma$ são multilineares e sem termos $x_i's$ em comum. Como $|\omega(m_2^\gamma)| \geq n-1$, temos que $\widehat{\omega}(m_1^\gamma m_2^\gamma m_3^\gamma) \geq n-1$, para todo γ. Vamos considerar $m_1^\gamma m_2^\gamma m_3^\gamma = m_\sigma$. Fazendo γ variar, σ também varia. Logo, podemos escrever ainda f_3 da forma

$$f_3 = \sum_{\widehat{\omega}(m_\sigma) \geq n-1} a_\sigma m_\sigma(x_1, x_2, \ldots, x_k).$$

Desde que $m_\sigma(x_1, x_2, \ldots, x_k) \in J_n$ quando $\widehat{\omega}(m_\sigma) > n-1$, segue que

$$f \equiv f_3 \equiv \sum_{\widehat{\omega}(m_\sigma) = n-1} a_\sigma m_\sigma(x_1, x_2, \ldots, x_k) = \sum_{m_\sigma \in \Lambda_0} a_\sigma m_\sigma(x_1, x_2, \ldots, x_k) \ (mod\ J_n).$$

Então por 2.24

$$f \equiv \sum_{\mathcal{S} \in SSt} \sum_{i,j=1}^{n} \left(\sum_{m_\sigma \in \Lambda(\mathcal{S}, i, j)} a_\sigma m_\sigma(x_1, x_2, \ldots, x_k) \right) \ (mod\ J_n). \tag{2.27}$$

Se nós provarmos que cada polinômio graduado $\sum a_\sigma m_\sigma$ em 2.27 pertence a J_n, então a inclusão $T_{\mathbb{Z}}(M_n(K)) \subseteq J_n$ estará demonstrada. Observe que pelo Lema 2.3.6, para $\mathcal{S}_0, \mathcal{S} \in SSt$ e $i, j \in \{1, 2, \ldots, n\}$ nós temos que

$$\left(\sum_{m_\sigma \in \Lambda(\mathcal{S}, i, j)} a_\sigma m_\sigma \right) \Bigg|_{\mathcal{S}_0} = \begin{cases} 0, & se \quad \mathcal{S} \neq \mathcal{S}_0; \\ \left[\sum_{m_\sigma \in \Lambda(\mathcal{S}_0, i, j)} a_\sigma \right] E_{ij}, & se \quad \mathcal{S} = \mathcal{S}_0. \end{cases} \tag{2.28}$$

Logo, para qualquer $\mathcal{S} \in SSt$, por 2.27 e 2.28 teremos

$$f|_{\mathcal{S}} = \sum_{i,j=1}^{n} \left(\sum_{m_\sigma \in \Lambda(\mathcal{S}, i, j)} a_\sigma \right) E_{ij} = 0,$$

e portanto $\sum_{m_\sigma \in \Lambda(\mathcal{S},i,j)} a_\sigma = 0$, $i,j = 1,2,\ldots,n$. Por 2.28, temos que

$$\sum_{m_\sigma \in \Lambda(\mathcal{S},i,j)} a_\sigma m_\sigma(x_1, x_2, \ldots, x_k) \in T_{\mathbb{Z}}(M_n(K)),\ \mathcal{S} \in SSt,\ i,j = 1,2,\ldots,n.$$

Se $\Lambda(\mathcal{S},i,j) \neq \emptyset$, escolha uma permutação $\tau \in S_k$ de maneira que $m_\tau \in \Lambda(\mathcal{S},i,j)$. Pelo Corolário 2.3.8, para cada $m_\sigma \in \Lambda(\mathcal{S},i,j)$, existe um monômio $\mathtt{n}^{[\sigma]} = \mathtt{n}^{[\sigma]}(x_{\tau(2)}, x_{\tau(3)}, \ldots, x_{\tau(k)})$ tal que $m_\sigma \equiv x_{\tau(1)}\mathtt{n}^{[\sigma]}$ $(mod\ J_n)$. Notemos que $x_{\tau(1)}\mathtt{n}^{[\sigma]} \notin T_{\mathbb{Z}}(M_n(K))$, pois do contrário $m_\sigma \in T_{\mathbb{Z}}(M_n(K))$, o que contradiz o fato de $m_\sigma \in \Lambda(\mathcal{S},i,j)$. Logo, por $x_{\tau(1)}\mathtt{n}^{[\sigma]} \notin T_{\mathbb{Z}}(M_n(K))$ segue que $\widehat{\omega}(x_{\tau(1)}\mathtt{n}^{[\sigma]}) \leq n-1$. Considere $P = \{\sigma \in S_k \mid m_\sigma \in \Lambda(\mathcal{S},i,j)\}$. Sendo assim,

$$\sum_{m_\sigma \in \Lambda(\mathcal{S},i,j)} a_\sigma m_\sigma = \sum_{\sigma \in P} a_\sigma m_\sigma \equiv \sum_{\sigma \in P} a_\sigma x_{\tau(1)}\mathtt{n}^{[\sigma]} = x_{\tau(1)} \sum_{\sigma \in P} a_\sigma \mathtt{n}^{[\sigma]}\ (mod\ J_n). \tag{2.29}$$

Por $\sum_{m_\sigma \in \Lambda(\mathcal{S},i,j)} a_\sigma m_\sigma \in T_{\mathbb{Z}}(M_n(K))$ e 2.29, temos que $x_{\tau(1)} \sum_{\sigma \in P} a_\sigma \mathtt{n}^{[\sigma]} \in T_{\mathbb{Z}}(M_n(K))$. Logo, pelo Lema 2.3.4, $\sum_{\sigma \in P} a_\sigma \mathtt{n}^{[\sigma]} \in T_{\mathbb{Z}}(M_n(K))$ e por ser uma identidade graduada multilinear de $M_n(K)$ em $k-1$ variavéis, concluímos que $\sum_{\sigma \in P} a_\sigma \mathtt{n}^{[\sigma]} \in J_n$. Portanto, por 2.29 para quaiquer $\mathcal{S} \in SSt$ e $i,j = 1,2,\ldots,n$,

$$\sum_{m_\sigma \in \Lambda(\mathcal{S},i,j)} a_\sigma m_\sigma \equiv 0\ (mod\ J_n),$$

o que completa a demonstração. ■

2.4 Polinômios Centrais $\mathbb{Z}$-graduados

Apresentaremos nesta seção a descrição do espaço dos polinômios centrais $\mathbb{Z}$-graduados para a álgebra $M_n(K)$.

Sejam J_n o $T_{\mathbb{Z}}$-ideal gerado pelas identidades graduadas de 2.14 a 2.16 e $C_{\mathbb{Z}}(M_n(K))$ o $T_{\mathbb{Z}}$-espaço dos polinômios centrais $\mathbb{Z}$-graduados de $M_n(K)$. Claramente, temos $J_n \subseteq C_{\mathbb{Z}}(M_n(K))$.

Lema 2.4.1 *Seja $m(x_1, x_2, \ldots, x_k) = x_1 x_2 \ldots x_k$ um monômio multilinear de $K\langle X\rangle$ com $\omega(m) = 0$. Se uma substituição Standard $\mathcal{S}$*

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

é tal que $m|_{\mathcal{S}} \neq 0$, então $m_\sigma|_{\mathcal{S}} \neq 0$ para todo $\sigma \in H_k$.

Demonstração: Sendo $m|_{\mathcal{S}} \neq 0$, temos $j_1 = i_2$, $j_2 = i_3$, $\ldots$, $j_{k-1} = i_k$. Como $m|_{\mathcal{S}} = E_{i_1 j_k}$ e $\omega(m) = 0$, devemos ter $i_1 = j_k$. Observemos que $m_{\theta_k}|_{\mathcal{S}} = E_{i_2 j_k} E_{i_1 j_1} = E_{i_2 i_2} \neq 0$. O resultado segue então indutivamente. ∎

Proposição 2.4.2 *O polinômio multilinear*

$$f(x_1, x_2, \ldots, x_n) = \sum_{\sigma \in H_n} x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n)},$$

onde $\widehat{\omega}(x_1 x_2 \ldots x_k) \leq n - 1$ *e* $(\overline{\omega(x_1)}, \overline{\omega(x_2)}, \ldots, \overline{\omega(x_n)})$ *é uma sequência completa em* $\mathbb{Z}_n$*, é um polinômio central* $\mathbb{Z}$*-graduado, que não é identidade para a álgebra* $M_n(K)$*.*

Demonstração: Como f é multilinear, é suficiente mostrar que $f|_{\mathcal{S}} \in Z(M_n(K))$ para toda substituição Standard $\mathcal{S}$. Pelo Lema 2.4.1, se $m|_{\mathcal{S}} = 0$, então $m_\sigma|_{\mathcal{S}} = 0$ para todo $\sigma \in H_n$, e daí $f|_{\mathcal{S}} = 0$. Suponhamos então $\mathcal{S}$ uma substituição Standard

$$x_1 = E_{i_1 j_1},\ x_2 = E_{i_2 j_2},\ \ldots,\ x_n = E_{i_n j_n}$$

tal que $m|_{\mathcal{S}} \neq 0$. Observe que a existência de $\mathcal{S}$ é garantida pelo Corolário 2.3.5. Claramente devemos ter $j_1 = i_2$, $j_2 = i_3$, $\ldots$, $j_{n-1} = i_n$ e também $j_n = i_1$, pois $\omega(m) = \omega(x_1) + \omega(x_2) + \ldots + \omega(x_n) = 0$. Logo,

$$f|_{\mathcal{S}} = E_{i_1 i_1} + E_{i_2 i_2} + \ldots + E_{i_n i_n}.$$

Notando agora que

$$\omega(x_1) = i_2 - i_1,\ \omega(x_2) = i_3 - i_2,\ \ldots,\ \omega(x_{n-1}) = i_n - i_{n-1},\ \omega(x_n) = i_1 - i_n,$$

temos

$$\overline{\omega(x_1)} + \overline{\omega(x_2)} = \overline{i_3 - i_1},\ \ldots,\ \overline{\omega(x_1)} + \ldots + \overline{\omega(x_{n-1})} = \overline{i_n - i_1}.$$

Como $(\overline{\omega(x_1)}, \overline{\omega(x_2)}, \ldots, \overline{\omega(x_n)})$ é uma sequência completa, devemos ter $\overline{i_2 - i_1}, \overline{i_3 - i_1}, \ldots, \overline{i_n - i_1}$ não-nulos e dois a dois distintos, donde segue que $i_1, i_2, \ldots, i_n$ devem ser dois a dois incôgruos módulo n. Mas, $\{i_1, i_2, \ldots, i_n\} \subseteq \{1, 2, \ldots, n\}$. Logo, temos a igualdade destes dois conjuntos, e portanto $f|_{\mathcal{S}} = I_n \in Z(M_n(K))$. ∎

Lema 2.4.3 *Se para uma permutação* $\sigma \in S_k$*, existir uma substituição Standard* $\mathcal{S}$ *tal que*

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

então

$$m_\sigma(x_1, x_2, \ldots, x_k) \equiv m(x_1, x_2, \ldots, x_k)\ (mod\ J_n).$$

Demonstração: Pelo Lema 2.3.7, $m_\sigma(x_1, x_2, \ldots, x_k) \equiv x_1 n(x_2, x_3, \ldots, x_k)$ $(mod\ J_n)$. Seja r o maior inteiro positivo tal que

$$m_\sigma(x_1, x_2, \ldots, x_k) \equiv x_1 x_2 \ldots x_r n(x_{r+1}, \ldots, x_k)\ (mod\ J_n), \tag{2.30}$$

para algum monômio $n = n(x_{r+1}, \ldots, x_k)$. Mostraremos que $r = k$. Suponhamos por contradição que $r < k$. Então, obviamente $r \leq k-2$. Desde que $J_n = T_{\mathbb{Z}}(M_n(K))$, por 2.30 temos

$$x_1 x_2 \ldots x_r n(x_{r+1}, \ldots, x_k)|_{\mathcal{S}} = m_\sigma(x_1, x_2, \ldots, x_k)|_{\mathcal{S}} = m(x_1, x_2, \ldots, x_k)|_{\mathcal{S}} \neq 0.$$

Combinando a igualdade anterior com

$$x_1 x_2 \ldots x_r n|_{\mathcal{S}} = E_{i_1 j_1} E_{i_2 j_2} \ldots E_{i_r j_r} n|_{\mathcal{S}} = E_{i_1 j_r} n|_{\mathcal{S}}$$

e

$$m|_{\mathcal{S}} = E_{i_1 j_1} E_{i_2 j_2} \ldots E_{i_r j_r} \{x_{r+1} x_{r+2} \ldots x_k\}|_{\mathcal{S}},$$

temos que

$$n(x_{r+1}, \ldots, x_k)|_{\mathcal{S}} = x_{r+1} x_{r+2} \ldots x_k|_{\mathcal{S}} = E_{j_r j_k} \neq 0.$$

Pelo Lema 2.3.7, existe um monômio $n^{'}(x_{r+2}, \ldots, x_k)$ tal que

$$n(x_{r+1}, \ldots, x_k) \equiv x_{r+1} n^{'}(x_{r+2}, \ldots, x_k)\ (mod\ J_n).$$

Logo,

$$m_\sigma \equiv x_1 \ldots x_r n(x_{r+1}, x_{r+2} \ldots, x_k) \equiv x_1 \ldots x_r x_{r+1} n^{'}(x_{r+2}, \ldots, x_k)\ (mod\ J_n),$$

o que contradiz a escolha do número r. Portanto, $r = k$. ■

Corolário 2.4.4 *Se para duas permutações $\sigma, \tau \in S_k$, existir uma substituição Standard $\mathcal{S}$ tal que*

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

então $m_\sigma(x_1, x_2, \ldots, x_k) \equiv m_\tau(x_1, x_2, \ldots, x_k)$ $(mod\ I_n)$.

Demonstração: Consideremos $x_1^{'} = x_{\tau(1)}, x_2^{'} = x_{\tau(2)}, \ldots, x_k^{'} = x_{\tau(k)}$. Logo,

$$m_\tau(x_1, x_2, \ldots, x_k) = m(x_1^{'}, x_2^{'}, \ldots, x_k^{'}).$$

Tomemos agora $\mu = \tau^{-1} \circ \sigma$. Sendo assim,

$$m_\mu(x_1^{'}, x_2^{'}, \ldots, x_k^{'}) = m_\sigma(x_1, x_2, \ldots, x_k).$$

Por $m_\sigma|_{\mathcal{S}} = m_\tau|_{\mathcal{S}} \neq 0$, temos que $m_\mu(x_1^{'}, x_2^{'}, \ldots, x_k^{'})|_{\mathcal{S}} = m(x_1^{'}, x_2^{'}, \ldots, x_k^{'})|_{\mathcal{S}} \neq 0$. Pelo Lema 2.4.3, segue que

$$m_\mu(x_1^{'}, x_2^{'}, \ldots, x_k^{'}) \equiv m(x_1^{'}, x_2^{'}, \ldots, x_k^{'}) \ (mod\ J_n)$$

e portanto,

$$m_\sigma(x_1, x_2, \ldots, x_k) \equiv m_\tau(x_1, x_2, \ldots, x_k) \ (mod\ J_n).$$

■

Tomemos agora W como sendo o $T_{\mathbb{Z}}$-espaço gerado pelos polinômios

$$\begin{array}{rl} z_1 x z_2 \ , & |\omega(x)| \geq n; \\ z_1[x_1, x_2]z_2 \ , & \omega(x_1) = \omega(x_2) = 0; \\ z_1(x_1x_2x_3 - x_3x_2x_1)z_2 \ , & \omega(x_1) = \omega(x_3) = -\omega(x_2); \\ \sum\limits_{\sigma \in H_n} x_{\sigma(1)}x_{\sigma(2)} \ldots x_{\sigma(n)} \ , & (\overline{\omega(x_1)}, \overline{\omega(x_2)}, \ldots, \overline{\omega(x_n)}) \text{ sequência completa,} \end{array} \tag{2.31}$$

onde $\widehat{\omega}(x_1x_2 \ldots x_n) \leq n-1$ e z_1 e z_2 são variavéis em X.

Do fato de todos os polinômios em 2.31 serem centrais segue que $W \subseteq C_{\mathbb{Z}}(M_n(K))$. Observando agora que o $T_{\mathbb{Z}}$-espaço gerado pelos três primeiros polinômios em 2.31 é exatamente J_n, concluímos que $J_n \subset W$.

Lema 2.4.5 *Se o polinômio multilinear*

$$f(x_1, x_2, \ldots, x_k) = \lambda_1 m_1(x_1, x_2, \ldots, x_k) + \ldots + \lambda_n m_n(x_1, x_2, \ldots, x_k) \ (k \geq n)$$

é tal que existe uma substituição Standard $\mathcal{S}$ *tal que* $f|_{\mathcal{S}} = \lambda I_n$*, para agum* $0 \neq \lambda \in K$*, então* $f \in W$.

Demonstração: Como $f|_{\mathcal{S}} = \lambda I_n$, devemos ter $\lambda_1 = \lambda_2 = \ldots = \lambda_n = \lambda$ e $\omega(m_i) = 0$ para cada $i = 1, 2, \ldots, n$. Vamos supor que $m_1(x_1, x_2, \ldots, x_k) = x_1x_2 \ldots x_k$. Seja $\mathcal{S}$ uma substituição Standard

$$x_1 = E_{i_1j_1}, \ x_2 = E_{i_2j_2}, \ \ldots, \ x_k = E_{i_kj_k}$$

satisfazendo as hipóteses do Lema. Por $f|_{\mathcal{S}} = \lambda I_n$, para cada $i = 1, \ldots, n$ existe $j \in \{1, \ldots, n\}$ tal que $m_j|_{\mathcal{S}} = E_{ii}$. Logo, existem $1 = l_1 < l_2 < \ldots < l_n$ de modo que $\{i_{l_1}, i_{l_2}, \ldots, i_{l_n}\} = \{1, 2, \ldots, n\}$. Sendo assim,

$$m_1(x_1, x_2, \ldots, x_k) = \overbrace{x_{l_1} \ldots x_{l_2-1}}^{t_1} \overbrace{x_{l_2} \ldots x_{l_3-1}}^{t_2} \ldots \overbrace{x_{l_n} \ldots x_k}^{t_n}.$$

Logo,

$$\overline{\omega(t_1)} = \overline{i_{l_2} - i_1},\ \overline{\omega(t_2)} = \overline{i_{l_3} - i_{l_2}},\ \ldots,\ \overline{\omega(t_{n-1})} = \overline{i_{l_n} - i_{l_{n-1}}}\ e\ \overline{\omega(t_n)} = \overline{i_1 - i_{l_n}}.$$

A sequência $(\overline{\omega(t_1)}, \overline{\omega(t_2)}, \ldots, \overline{\omega(t_n)})$ é uma sequência completa em $\mathbb{Z}_n$, pois

$$\overline{\omega(t_1)} + \overline{\omega(t_2)} + \ldots + \overline{\omega(t_n)} = \overline{\omega(m_1)} = \overline{0} = \overline{i_{l_2} - i_1} + \overline{i_{l_3} - i_{l_2}} + \ldots + \overline{i_{l_n} - i_{l_n-1}} + \overline{i_1 - i_{l_n}}.$$

Além disso,

$$\overline{\omega(t_1)} = \overline{i_{l_2} - i_{l_1}},\ \overline{\omega(t_1)} + \overline{\omega(t_2)} = \overline{i_{l_3} - i_{l_1}},\ \ldots,\ \overline{\omega(t_1)} + \overline{\omega(t_2)} + \ldots + \overline{\omega(t_{n-1})} = \overline{i_{l_n} - i_{l_1}}.$$

Daí, sendo $\{i_{l_1}, i_{l_2}, \ldots, i_{l_n}\} = \{1, 2, \ldots, n\}$, devemos ter $\overline{i_{l_2} - i_{l_1}},\ \overline{i_{l_3} - i_{l_1}},\ \ldots,\ \overline{i_{l_n} - i_{l_1}}$ não-nulos e dois a dois distintos.

Consideremos agora o monômio

$$\overbrace{x_{l_2} \ldots x_{l_3-1}}^{t_2} \ldots \overbrace{x_{l_n} \ldots x_k}^{t_n} \overbrace{x_{l_1} \ldots x_{l_2-1}}^{t_1}$$

e observemos que $t_2 \ldots t_n t_1|_{\mathcal{S}} = E_{i_{l_2} i_{l_2}}$. Por $f|_{\mathcal{S}} = \lambda I_n$, existe algum $q \in \{1, 2, \ldots, n\}$ tal que $m_q|_{\mathcal{S}} = t_2 \ldots t_n t_1|_{\mathcal{S}} = E_{i_{l_2} i_{l_2}}$ e pelo Corolário 2.4.4, concluímos que $m_q \equiv t_2 \ldots t_n t_1$ $(mod\ J_n)$. Além disso, $\widehat{\omega}(t_1 t_2 \ldots t_n) \leq n - 1$. Como $\{t_{\sigma(1)} t_{\sigma(2)} \ldots t_{\sigma(n)}|_{\mathcal{S}};\ \sigma \in H_n\} = \{E_{11}, E_{22}, \ldots, E_{nn}\}$ continuamos com este raciocínio usando novamente o Corolário 2.4.4 e concluímos que

$$f(x_1, x_2, \ldots, x_k) = \lambda(m_1 + m_2 + \ldots + m_n) \equiv \lambda \sum_{\sigma \in H_n} t_{\sigma(1)} t_{\sigma(2)} \ldots t_{\sigma(n)}\ (mod\ J_n),$$

e daí

$$f(x_1, x_2, \ldots, x_k) \equiv \lambda \sum_{\sigma \in H_n} t_{\sigma(1)} t_{\sigma(2)} \ldots t_{\sigma(n)}\ (mod\ W)\ (pois\ J_n \subseteq W).$$

Além disso, $\sum_{\sigma \in H_n} t_{\sigma(1)} t_{\sigma(2)} \ldots t_{\sigma(n)} \in W$, donde segue que $f(x_1, x_2, \ldots, x_k) \in W$. ∎

Teorema 2.4.6 *Seja K um corpo de característica zero. Então $C_{\mathbb{Z}}(M_n(K)) = W$.*

Demonstração: Seja $f(x_1, x_2, \ldots, x_k) \in C_{\mathbb{Z}}(M_n(K))$. Podemos supor f multilinear. Suponhamos ainda que f não é identidade $\mathbb{Z}$-graduada para $M_n(K)$. Podemos escrever f na forma

$$f = \lambda_1 m_1 + \lambda_2 m_2 + \ldots + \lambda_l m_l,$$

onde $m_1, m_2, \ldots, m_l$ são monômios multilineares em $x_1, x_2, \ldots, x_k$. Por f não ser identidade $\mathbb{Z}$-graduada para $M_n(K)$, existe uma substituição Standard $\mathcal{S}$ tal que $f|_{\mathcal{S}} = \lambda I_n$, para algum $0 \neq \lambda \in K$. Logo, $l \geq n$. Observemos ainda que para cada $i = 1, 2, \ldots, l$, temos $m_i|_{\mathcal{S}} = 0$ ou $m_i|_{\mathcal{S}} = E_{jj}$. Temos também que para cada $i = 1, \ldots, n$, existe $j_i \in \{1, 2, \ldots, l\}$ tal que $m_{j_i}|_{\mathcal{S}} = E_{ii}$. Juntando os termos $m'_{j_i}s$ tais que $m_{j_i}|_{\mathcal{S}} = E_{ii}$ e usando o Corolário 2.4.4, concluímos que

$$f(x_1, x_2, \ldots, x_k) \equiv \alpha_1 m_{j_1} + \alpha_2 m_{j_2} + \ldots + \alpha_n m_{j_n} + \beta_1 m_{t_1} + \ldots + \beta_r m_{t_r} \ (mod\ W),$$

onde $r < l$ e $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_r \in K$. Pelo Lema 2.4.5, temos

$$\alpha_1 m_{j_1} + \alpha_2 m_{j_2} + \ldots + \alpha_n m_{j_n} \in W,$$

donde segue que

$$f(x_1, x_2, \ldots, x_k) \equiv \beta_1 m_{t_1} + \ldots + \beta_r m_{t_r} \ (mod\ W).$$

Por $f \in C_{\mathbb{Z}}(M_n(K))$, temos que $\beta_1 m_{t_1} + \ldots + \beta_r m_{t_r} \in C_{\mathbb{Z}}(M_n(K))$. Se $r < n$, então $\beta_1 m_{t_1} + \ldots + \beta_r m_{t_r} \in J_n \subseteq W$. Caso contrário, repetimos os mesmos argumentos usados anteriormente. ■

Capítulo 3

Polinômios Centrais para a Álgebra das matrizes de segunda ordem

Um dos principais problemas na PI-Teoria é determinar se para uma dada álgebra A o T-espaço dos polinômios centrais de A é finitamente gerado. Neste capítulo apresentaremos uma base finita construída por Okhitin [40] para o T-espaço dos polinômios centrais ordinários da álgebra $M_2(K)$, onde K denotará um corpo de característica zero. Colombo e Koshlukov [8] generalizaram esta descrição do T-espaço $C(M_2(K))$ para o caso de K ser infinito e de característica diferente de 2.

3.1 O T-espaço $C(M_2(K))$

Nesta seção denotaremos por $K\langle X\rangle$ a álgebra associativa livre, onde $X = \{x_0, x_1, \ldots\}$ é um conjunto não-vazio e enumerável (conforme Seção 1.2), $L = L(X) \subset K\langle X\rangle$ (veja Seção 1.4) uma álgebra de Lie livre com conjunto gerador X, $L_2 = L \cap T(M_2(K))$ e K denotará sempre um corpo de característica zero.

Consideremos os polinômios $H(x_1, x_2, x_3, x_4, x_5) = [h(x_1, x_2, x_3, x_4), x_5]$, onde $h(x_1, x_2, x_3, x_4) = [x_1, x_2] \circ [x_3, x_4]$ (polinômio de Hall) e $s_4(x_1, x_2, x_3, x_4)$ o polinômio Standard de grau 4 (veja Exemplo 1.2.7).

Lema 3.1.1 *São válidas as seguintes igualdades:*

(i) $H(x_1, x_2, x_3, x_4, x_5) = [x_1, x_2] \circ [x_3, x_4, x_5] + [x_1, x_2, x_5] \circ [x_3, x_4]$;

(ii) $s_4(x_1, x_2, x_3, x_4) = [x_1, x_2] \circ [x_3, x_4] - [x_1, x_3] \circ [x_2, x_4] + [x_1, x_4] \circ [x_2, x_3]$.

Demonstração: **(i)** Usando a igualdade em 1.1, temos

$$H(x_1,x_2,x_3,x_4,x_5) = [[x_1,x_2]\circ[x_3,x_4],x_5] = [[x_1,x_2][x_3,x_4]+[x_3,x_4][x_1,x_2],x_5] =$$

$$[[x_1,x_2],x_5][x_3,x_4]+[x_1,x_2][[x_3,x_4],x_5]+[[x_3,x_4],x_5][x_1,x_2]+[x_3,x_4][[x_1,x_2],x_5] =$$

$$[x_1,x_2,x_5][x_3,x_4]+[x_1,x_2][x_3,x_4,x_5]+[x_3,x_4,x_5][x_1,x_2]+[x_3,x_4][x_1,x_2,x_5] =$$

$$[x_1,x_2,x_5]\circ[x_3,x_4]+[x_1,x_2]\circ[x_3,x_4,x_5].$$

(ii) Temos também

$$s_4(x_1,x_2,x_3,x_4) = \sum_{\sigma\in S_4}(-1)^\sigma x_{\sigma(1)}x_{\sigma(2)}x_{\sigma(3)}x_{\sigma(4)} =$$

$$x_1x_2x_3x_4 - x_1x_2x_4x_3 - x_1x_3x_2x_4 + x_1x_3x_4x_2 + x_1x_4x_2x_3 - x_1x_4x_3x_2 -$$

$$x_2x_1x_3x_4 + x_2x_1x_4x_3 + x_2x_3x_1x_4 - x_2x_3x_4x_1 - x_2x_4x_1x_3 + x_2x_4x_3x_1 +$$

$$x_3x_1x_2x_4 - x_3x_1x_4x_2 - x_3x_2x_1x_4 + x_3x_2x_4x_1 + x_3x_4x_1x_2 - x_3x_4x_2x_1 -$$

$$x_4x_1x_2x_3 + x_4x_1x_3x_2 + x_4x_2x_1x_3 - x_4x_2x_3x_1 - x_4x_3x_1x_2 + x_4x_3x_2x_1 =$$

$$x_1x_2(x_3x_4-x_4x_3)+x_1x_3(x_4x_2-x_2x_4)+x_1x_4(x_2x_3-x_3x_2)-x_2x_1(x_3x_4-x_4x_3)+$$

$$x_2x_3(x_1x_4-x_4x_1)-x_2x_4(x_1x_3-x_3x_1)-x_3x_1(x_4x_2-x_2x_4)-x_3x_2(x_1x_4-x_4x_1)+$$

$$x_3x_4(x_1x_2-x_2x_1)-x_4x_1(x_2x_3-x_3x_2)+x_4x_2(x_1x_3-x_3x_1)-x_4x_3(x_1x_2-x_2x_1) =$$

$$(x_1x_2-x_2x_1)(x_3x_4-x_4x_3)+(x_3x_4-x_4x_3)(x_1x_2-x_2x_1)+(x_1x_3-x_3x_1)(x_4x_2-x_2x_4)+$$

$$(x_4x_2-x_2x_4)(x_1x_3-x_3x_1)+(x_1x_4-x_4x_1)(x_2x_3-x_3x_2)+(x_2x_3-x_3x_2)(x_1x_4-x_4x_1) =$$

$$[x_1,x_2]\circ[x_3,x_4]+[x_1,x_3]\circ[x_4,x_2]+[x_1,x_4]\circ[x_2,x_3] =$$

$$[x_1,x_2]\circ[x_3,x_4]-[x_1,x_3]\circ[x_2,x_4]+[x_1,x_4]\circ[x_2,x_3].$$

■

Uma base finita de identidades para a álgebra $M_2(K)$ foi construída inicialmente por Razmyslov [44]. Posteriormente, Drensky [10] mostrou que as identidades de $M_2(K)$ seguem dos polinômios $H(x_1,x_2,x_3,x_4,x_5)$ e $s_4(x_1,x_2,x_3,x_4)$.

Observemos que $x_0s_4 \notin V(h)$, onde $V(h)$ é o T-espaço gerado pelo polinômio $h(x_1,x_2,x_3,x_4)$. De fato, basta observarmos que $[h(x_1,x_2,x_3,x_4),x_5]$ é identidade para a álgebra exterior E, visto que $[x_1,x_2,x_3]$ é identidade para E (veja Exemplo 1.2.12). Logo, se $x_0s_4 \in V(h)$, então $[x_0s_4,x_5]$ seria identidade para E e portanto x_0s_4 seria um polinômio central para E. Sendo assim, para $x_1 = e_1$, $x_2 = e_2$, $x_3 = e_3$, $x_4 = e_4$ e $x_0 = e_5$, teríamos que $e_5 s_4(e_1, e_2, e_3, e_4) = 24 e_1 e_2 e_3 e_4 e_5 \in Z(E) = E_0$, o que é uma contradição. Além disso, $h \notin V(x_0 s_4)$, onde $V(x_0 s_4)$ é o T-espaço gerado pelo polinômio $x_0 s_4$. De fato, basta observarmos que $x_0 s_4 \in T(M_2(K))$ e $h \notin T(M_2(K))$.

Vamos denotar por $V = V(h, x_0 s_4)$ o T-espaço de $K\langle X\rangle$ gerado pelos polinômios h e $x_0 s_4$. Pelo que foi exposto anteriormente, V não pode ser gerado, como T-espaço, por apenas um desses polinômios. Ademais, por $h,\ x_0 s_4 \in C(M_2(K))$, concluímos que $V \subseteq C(M_2(K))$.

Lema 3.1.2 *Existe um polinômio de Lie $l \in L$ tal que $c = x_0 h + l$ é um polinômio central para $M_2(K)$ e $c \in V$.*

Demonstração: Notemos inicialmente que na álgebra $K\langle X\rangle$ vale

$$x_0([x_1, x_2] \circ [x_3, x_4]) + x_1([x_0, x_2] \circ [x_3, x_4]) = c_1 + l_1, \tag{3.1}$$

onde

$$c_1 = [x_0 x_1, x_2] \circ [x_3, x_4] - [x_0, x_2, x_1] \circ [x_3, x_4] - \frac{1}{2}([x_3, x_4, x_0] \circ [x_1, x_2] + [x_3, x_4, x_1] \circ [x_0, x_2]),$$

$$l_1 = \frac{1}{2}([[x_1, x_2], [x_3, x_4, x_0]] + [[x_0, x_2], [x_3, x_4, x_1]]) \in L.$$

Observe que pela expressão de c_1, podemos concluir que $c_1 \in V(h)$. De fato, a igualdade em 3.1 é verdadeira, pois por 1.1 temos que

$$\begin{gathered}
c_1 + l_1 = ([x_0, x_2]x_1 + x_0[x_1, x_2]) \circ [x_3, x_4] - [x_0, x_2, x_1] \circ [x_3, x_4] - \\
\frac{1}{2}[x_3, x_4, x_0] \circ [x_1, x_2] - \frac{1}{2}[x_3, x_4, x_1] \circ [x_0, x_2] + \frac{1}{2}[x_1, x_2][x_3, x_4, x_0] - \\
\frac{1}{2}[x_3, x_4, x_0][x_1, x_2] + \frac{1}{2}[x_0, x_2][x_3, x_4, x_1] - \frac{1}{2}[x_3, x_4, x_1][x_0, x_2] = \\
([x_0, x_2]x_1 + x_0[x_1, x_2]) \circ [x_3, x_4] - [x_0, x_2, x_1] \circ [x_3, x_4] - \\
[x_3, x_4, x_0][x_1, x_2] - [x_3, x_4, x_1][x_0, x_2] = \\
[x_0, x_2]x_1[x_3, x_4] + [x_3, x_4][x_0, x_2]x_1 + x_0[x_1, x_2][x_3, x_4] + [x_3, x_4]x_0[x_1, x_2] - \\
[x_0, x_2, x_1][x_3, x_4] - [x_3, x_4][x_0, x_2, x_1] - [x_3, x_4, x_0][x_1, x_2] - [x_3, x_4, x_1][x_0, x_2] = \\
(x_1[x_0, x_2] + [x_0, x_2, x_1])[x_3, x_4] + [x_3, x_4](x_1[x_0, x_2] + [x_0, x_2, x_1]) +
\end{gathered}$$

$$x_0[x_1,x_2][x_3,x_4] + (x_0[x_3,x_4] + [x_3,x_4,x_0])[x_1,x_2] - [x_0,x_2,x_1][x_3,x_4] -$$

$$[x_3,x_4][x_0,x_2,x_1] - [x_3,x_4,x_0][x_1,x_2] - [x_3,x_4,x_1][x_0,x_2] =$$

$$x_1[x_0,x_2][x_3,x_4] + [x_0,x_2,x_1][x_3,x_4] + [x_3,x_4]x_1[x_0,x_2] + [x_3,x_4][x_0,x_2,x_1] +$$

$$x_0[x_1,x_2][x_3,x_4] + x_0[x_3,x_4][x_1,x_2] + [x_3,x_4,x_0][x_1,x_2] - [x_0,x_2,x_1][x_3,x_4] -$$

$$[x_3,x_4][x_0,x_2,x_1] - [x_3,x_4,x_0][x_1,x_2] - [x_3,x_4,x_1][x_0,x_2] =$$

$$x_1[x_0,x_2][x_3,x_4] + (x_1[x_3,x_4] + [x_3,x_4,x_1])[x_0,x_2] +$$

$$x_0[x_1,x_2][x_3,x_4] + x_0[x_3,x_4][x_1,x_2] - [x_3,x_4,x_1][x_0,x_2] =$$

$$x_1[x_0,x_2][x_3,x_4] + x_1[x_3,x_4][x_0,x_2] + x_0[x_1,x_2][x_3,x_4] + x_0[x_3,x_4][x_1,x_2] =$$

$$x_1([x_0,x_2] \circ [x_3,x_4]) + x_0([x_1,x_2] \circ [x_3,x_4]).$$

Por 3.1, existem $c_2, c_3 \in V(h)$ e $l_2, l_3 \in L$ tais que

$$x_0h - x_0([x_1,x_3] \circ [x_2,x_4]) = c_2 + l_2; \tag{3.2}$$

$$x_0h - x_0([x_1,x_4] \circ [x_2,x_3]) = c_3 + l_3. \tag{3.3}$$

Como $x_0h = x_0([x_1,x_2] \circ [x_3,x_4])$, subtraimos 3.2 de 3.3 e obtemos

$$x_0h - x_0([x_1,x_2]\circ[x_3,x_4]) - x_0([x_1,x_4]\circ[x_2,x_3]) + x_0([x_1,x_3]\circ[x_2,x_4]) = (c_3-c_2)+(l_3-l_2)$$

o que nos dá

$$x_0h - x_0s_4 = (c_3 - c_2) + (l_3 - l_2) \text{ e daí } x_0h + (l_2 - l_3) = (c_3 - c_2) + x_0s_4,$$

ou seja,

$$x_0h + l = c \in V,$$

onde $l = l_2 - l_3 \in L$ e $c = c_3 - c_2 + x_0s_4 \in V$. ■

Lema 3.1.3 $T(M_2(K)) \subset V$.

Demonstração: Primeiramente vamos mostrar que $s_4, x_0s_4, H, x_0H \in V$. Claramente, s_4, x_0s_4 *e* $H \in V$, pois pelo Lema 3.1.1, s_4 e H pertencem a $V(h) \subset V$. Em [44] foi provado que $L_2 \subset V$. Do Lema 3.1.2, existe um polinômio de Lie l tal que $x_0H + l \in V$. De fato, existem $l_1, l_2 \in L$, tais que

$$x_0([x_1,x_2] \circ [x_3,x_4,x_5]) + l_1 \in V, \tag{3.4}$$

$$x_0([x_1,x_2,x_5] \circ [x_3,x_4]) + l_2 \in V. \tag{3.5}$$

Somando as igualdades 3.4 e 3.5, obtemos que $x_0H + l \in V$, onde $l = l_1 + l_2$. Sendo assim, $x_0H+l = f \in V$. Por x_0H ser identidade para $M_2(K)$, segue que $l \in C(M_2(K))$. Por outro lado, l é um polinômio de Lie, logo tem traço zero em qualquer substituição e por 1.6.11 concluímos que l é identidade para $M_2(K)$. Logo, $l \in T(M_2(K)) \cap L = L_2 \subset V$. Portanto, $x_0H = f - l \in V$. Observe que $[x_0s_4, x_5] = x_0s_4x_5 - x_5x_0s_4$. Por outro lado, usando 1.1, segue que $[x_0s_4, x_5] = [x_0, x_5]s_4 + x_0[s_4, x_5]$. Dessa forma,

$$x_0s_4x_5 - x_5x_0s_4 = [x_0, x_5]s_4 + x_0[s_4, x_5].$$

Notemos que

$$x_0[s_4, x_5] = x_0[[x_1, x_2]\circ[x_3, x_4], x_5] - x_0[[x_1, x_3]\circ[x_2, x_4], x_5] + x_0[[x_1, x_4]\circ[x_2, x_3], x_5] \in V,$$

pois é uma consequência de x_0H. Daí, como $x_5x_0s_4, [x_0, x_5]s_4, x_0[s_4, x_5] \in V$, concluímos que $x_0s_4x_5 \in V$. Analogamente, mostra-se que $x_0Hx_6 \in V$. Portanto, $T(M_2(K)) \subset V$. ■

Sejam A uma álgebra associativa e $a, b, c \in A$. Apartir de um cálculo direto, podemos mostrar que

$$[a \circ b, c] = a \circ [b, c] + b \circ [a, c], \tag{3.6}$$

$$(b \circ c) \circ a - b \circ (c \circ a) = [a, b, c]. \tag{3.7}$$

Lema 3.1.4 *Se $A_1, A_2, A_3, A_4 \in Sl_2(K)$ (conjunto das matrizes de traço zero em $M_2(K)$), então*

$$4[A_1, A_2](A_3 \circ A_4) = [A_1, A_3, A_4, A_2] + [A_1, A_4, A_3, A_2] - [A_2, A_3, A_1, A_4] - [A_2, A_4, A_1, A_3].$$

Consequentemente, se u e v são comutadores em $K\langle X\rangle$, então

$$4[x, y](u \circ v) \equiv [x, u, v, y] + [x, v, u, y] - [y, u, x, v] - [y, v, x, u] \ (mod\ T(M_2(K)).$$

Demonstração: Observemos inicialmente que $A \circ B \in Z(M_2(K))$, para A, $B \in Sl_2(K)$. Logo, usando as igualdades 3.6 e 3.7, temos que

$$[A_1, A_3, A_4, A_2] + [A_1, A_4, A_3, A_2] - [A_2, A_3, A_1, A_4] - [A_2, A_4, A_1, A_3] =$$

$$[[A_1, A_3, A_4], A_2] + [[A_1, A_4, A_3], A_2] - [[A_2, A_3, A_1], A_4] - [[A_2, A_4, A_1], A_3] =$$

$$[(A_3 \circ A_4) \circ A_1 - A_3 \circ (A_4 \circ A_1), A_2] + [(A_4 \circ A_3) \circ A_1 - A_4 \circ (A_3 \circ A_1), A_2] -$$

$$[(A_3 \circ A_1) \circ A_2 - A_3 \circ (A_1 \circ A_2), A_4] - [(A_4 \circ A_1) \circ A_2 - A_4 \circ (A_1 \circ A_2), A_3] =$$

$$[(A_3 \circ A_4) \circ A_1, A_2] - [A_3 \circ (A_4 \circ A_1), A_2] + [(A_4 \circ A_3) \circ A_1, A_2] - [A_4 \circ (A_3 \circ A_1), A_2] -$$

$$[(A_3 \circ A_1) \circ A_2, A_4] + [A_3 \circ (A_1 \circ A_2), A_4] - [(A_4 \circ A_1) \circ A_2, A_3] + [A_4 \circ (A_1 \circ A_2), A_3] =$$

$$(A_3 \circ A_4) \circ [A_1, A_2] + A_1 \circ [A_3 \circ A_4, A_2] - A_3 \circ [A_4 \circ A_1, A_2] - (A_4 \circ A_1) \circ [A_3, A_2] +$$

$$(A_4 \circ A_3) \circ [A_1, A_2] + A_1 \circ [A_4 \circ A_3, A_2] - A_4 \circ [A_3 \circ A_1, A_2] - (A_3 \circ A_1) \circ [A_4, A_2] -$$

$$(A_3 \circ A_1) \circ [A_2, A_4] - A_2 \circ [A_3 \circ A_1, A_4] + A_3 \circ [A_1 \circ A_2, A_4] + (A_1 \circ A_2) \circ [A_3, A_4] -$$

$$(A_4 \circ A_1) \circ [A_2, A_3] - A_2 \circ [A_4 \circ A_1, A_3] + A_4 \circ [A_1 \circ A_2, A_3] + (A_1 \circ A_2) \circ [A_4, A_3] =$$

$$(A_3 \circ A_4) \circ [A_1, A_2] - (A_4 \circ A_1) \circ [A_3, A_2] + (A_4 \circ A_3) \circ [A_1, A_2] - (A_3 \circ A_1) \circ [A_4, A_2] -$$

$$(A_3 \circ A_1) \circ [A_2, A_4] + (A_1 \circ A_2) \circ [A_3, A_4] - (A_4 \circ A_1) \circ [A_2, A_3] + (A_1 \circ A_2) \circ [A_4, A_3] =$$

$$(A_3 \circ A_4) \circ [A_1, A_2] + (A_4 \circ A_3) \circ [A_1, A_2] = 2(A_3 \circ A_4)[A_1, A_2] + 2(A_3 \circ A_4)[A_1, A_2] =$$

$$4[A_1, A_2](A_3 \circ A_4).$$

Para mostrarmos a segunda afirmação basta observarmos que

$$M_2(K) = Sl_2(K) \oplus D,$$

onde $D = \{\lambda I_2 \mid \lambda \in K\} = Z(M_2(K))$ e que qualquer comutador resulta em uma matriz de traço zero em $M_2(K)$. ■

A primeira afirmação do Lema 3.1.4 nos diz que o polinômio $g(x_1, x_2, x_3, x_4) = 4[x_1, x_2](x_3 \circ x_4) - [x_1, x_3, x_4, x_2] - [x_1, x_4, x_3, x_2] + [x_2, x_3, x_1, x_4] + [x_2, x_4, x_1, x_3]$ é uma identidade fraca para $M_2(K)$ (veja Seção 4.3).

A próxima definição será de grande importância na demonstração do principal resultado desta seção.

Definição 3.1.5 *Seja $f(x_1, x_2, \ldots, x_k) \in K\langle X\rangle$ um polinômio multilinear. Dizemos que o **posto** de f é igual a n e denotamos por $r(f) = n \geq 0$, se existem n variavéis no polinômio f tal que $f|_{x_{i_1} = \ldots = x_{i_n} = 1} \neq 0$ e n é o maior número que satisfaz tal propriedade.*

Se $f(x_1, x_2, \ldots, x_k)$ é um polinômio central multilinear, então por 1.4 podemos expressá-lo da forma

$$f(x_1, x_2, \ldots, x_k) = \sum_a x_1^{a_1} x_2^{a_2} \ldots x_k^{a_k} w_a, \tag{3.8}$$

onde $w_a \in B(X)$, $x_1^{a_1}x_2^{a_2}\dots x_k^{a_k}w_a$ é multilinear e $a = (a_1, a_2, \dots, a_k)$. Por $x_1^{a_1}x_2^{a_2}\dots x_k^{a_k}w_a$ ser multilinear temos $0 \leq a_i \leq 1$. Mostraremos que esta forma de representar f é única. Suponhamos que

$$f(x_1, x_2, \dots, x_k) = \sum_a x_1^{a_1}x_2^{a_2}\dots x_k^{a_k}w'_a, \tag{3.9}$$

onde $w'_a \in B(X)$, $a = (a_1, a_2, \dots, a_k)$ e $0 \leq a_i \leq 1$. Para cada a consideremos $M_a = \sum_{i=1}^k a_i$ e $\Gamma = \{M_a \mid a = (a_1, a_2, \dots, a_k)\}$. Tomemos $M_b = \max\Gamma$. Substituindo em 3.8 e 3.9 as variáveis x_i por 1, onde $b_i \neq 0$, temos que $w_b = w'_b$. Logo, por 3.8 e 3.9 segue que

$$\sum_{\substack{a\\a\neq b}} x_1^{a_1}x_2^{a_2}\dots x_k^{a_k}w_a = \sum_{\substack{a\\a\neq b}} x_1^{a_1}x_2^{a_2}\dots x_k^{a_k}w'_a.$$

Continuando com este raciocínio, concluímos que $w_a = w'_a$ para todo a e portanto temos a unicidade da representação de f em 3.8. Dessa forma, o posto do polinômio f pode ser entendido como sendo o máximo do conjunto Γ, ou seja, $r(f) = \max\Gamma$.

Lema 3.1.6 *Seja f um polinômio central multilinear de $M_2(K)$, onde $r(f) = 0$. Neste caso, $f = c + g$, onde $c = \sum l_1^i \circ l_2^i$, $l_1^i, l_2^i \in L$ e $g \in T(M_2(K))$.*

Demonstração: Para provar o Lema é suficiente representarmos f como uma combinação linear de um produto de comutadores e aplicar o número de vezes necessário a igualdade

$$2uv = u \circ v + [u, v] \tag{3.10}$$

e a identidade da álgebra $M_2(K)$ do Lema 3.1.4. Notemos que se u_1 e u_2 são comutadores, então por 3.10, $u_1u_2 = \frac{1}{2}(u_1 \circ u_2) + \frac{1}{2}[u_1, u_2]$. Por $u_1, u_2 \in L$ e L ser uma subálgebra de $K\langle X\rangle^{(-)}$, segue que $[u_1, u_2] \in L$. Suponhamos que

$$u_1u_2\dots u_n \equiv \sum l_1^i \circ l_2^i + l \ (mod\ T(M_2(K))),\ onde\ l_1^i, l_2^i\ e\ l \in L. \tag{3.11}$$

Observe que estamos indução sobre n. Para $n = 2$ a afirmação é verdadeira. Supondo 3.11 temos

$$u_1u_2\dots u_nu_{n+1} \equiv \left(\sum l_1^i \circ l_2^i\right) u_{n+1} + lu_{n+1}\ (mod\ T(M_2(K))).$$

Além disso por 3.10, $lu_{n+1} = \frac{1}{2}(l \circ u_{n+1}) + \frac{1}{2}[l, u_{n+1}]$ está na forma $\sum l_1^i \circ l_2^i + l$. Analisaremos agora o termo $(\sum l_1^i \circ l_2^i)u_{n+1}$. Notemos que

$$(l_1^i \circ l_2^i)u_{n+1} = u_{n+1}(l_1^i \circ l_2^i) + [l_1^i \circ l_2^i, u_{n+1}].$$

Usando a identidade do Lema 3.1.4, com $x = [y_1, \ldots, y_{m-1}]$ e $y = y_m$, onde $u_{n+1} = [y_1, y_2 \ldots, y_m]$ e $y_i \in X$, concluímos que *mod* $T(M_2(K))$, $u_{n+1}(l_1^i \circ l_2^i)$ está na forma $\sum l_1^i \circ l_2^i + l$. Por 3.6, temos que

$$[l_1^i \circ l_2^i, u_{n+1}] = l_1^i \circ [l_2^i, u_{n+1}] + l_2^i \circ [l_1^i, u_{n+1}].$$

Como $[l_2^i, u_{n+1}], [l_1^i, u_{n+1}] \in L$, segue que $l_1^i \circ [l_2^i, u_{n+1}]$ e $l_2^i \circ [l_1^i, u_{n+1}]$ estão na forma $l_1^i \circ l_2^i$, com $l_1^i, l_2^i \in L$. Portanto, $u_1 u_2 \ldots u_n u_{n+1} \equiv \sum l_1^i \circ l_2^i + l$ (*mod* $T(M_2(K))$, onde l_1^i, l_2^i *e* $l \in L$. Logo, $f \equiv \sum l_1^i \circ l_2^i + l'$, onde $l' \in L$. Desde que f e $l_1^i \circ l_2^i$ são centrais, segue que $l' \in C(M_2(K))$. Mas l' é de Lie, logo resulta em uma matriz de traço zero, donde $l' \in T(M_2(K))$. Sendo assim, $f = \sum l_1^i \circ l_2^i + g$, onde $g \in T(M_2(K))$. ■

A seguir apresentaremos a descrição do espaço dos polinômios centrais da álgebra $M_2(K)$.

Teorema 3.1.7 $C(M_2(K)) = V$.

Demonstração: Como $V \subseteq C(M_2(K))$, basta mostrarmos a inclusão contrária. A demonstração será feita por indução com respeito ao posto do polinômio central f. Seja $f \in C(M_2(K))$ um polinômio multilinear ($char K = 0$) e suponhamos que $r(f) = 0$. Pelo Lema 3.1.6, $f = \sum l_1^i \circ l_2^i + g$, onde $l_1^i, l_2^i \in L$ e $g \in T(M_2(K))$. Além disso, $l_1^i \circ l_2^i \in V(h) \subset V$ e pelo Lema 3.1.3 $g \in T(M_2(K)) \subset V$. Portanto, $f \in V$. Suponhamos que se f é um polinômio central multilinear de posto menor que n, então $f \in V$. Seja f um polinômio central multilinear de posto $n \geq 1$. Por 3.8, f pode ser representado como uma combinação linear de expressões multilineares do tipo

$$x_{i_1} \ldots x_{i_k} u_{j_1} \ldots u_{j_l},$$

onde $i_1 < \ldots < i_k$ e os u_{j_m}'s são comutadores. Nós podemos assumir que

$$f = x_1 \ldots x_n \varphi + \sum x_{i_1} \ldots x_{i_n} \varphi_i + f', \tag{3.12}$$

onde $\varphi \neq 0$, $r(\varphi) = r(\varphi_i) = 0$ e $r(f') < n$. Observe que $\varphi = f|_{x_1 = \ldots = x_n = 1}$, pois $\varphi_i|_{x_1 = \ldots = x_n = 1} = 0$, uma vez que $\{1, \ldots, n\} \neq \{i_1, \ldots, i_n\}$. Daí, φ é um polinômio central. Analogamente, cada φ_i é um polinômio central, pois $\varphi_i = f|_{x_{i_1} = \ldots = x_{i_n} = 1}$. Analisaremos agora o termo $x_1 \ldots x_n \varphi$. O termo $\sum x_{i_1} \ldots x_{i_n} \varphi_i$ é análogo. Em virtude do Lema 3.1.6, por φ ser um polinômio central de posto zero, temos que $\varphi = c + g$, onde $g \in T(M_2(K))$ e $c = \sum l_1^i \circ l_2^i \in V(h)$, com $l_1^i, l_2^i \in L$. Logo,

$$x_1 \ldots x_n \varphi = x_1 \ldots x_n c + x_1 \ldots x_n g.$$

Por $x_1 \ldots x_n g \in T(M_2(K)) \subset V$, temos que

$$x_1 \ldots x_n \varphi \equiv x_1 \ldots x_n c \ (mod\ V). \tag{3.13}$$

Pelo Lema 3.1.2, para cada polinômio $y(l_1^i \circ l_2^i)$, onde y é uma variável, existe um polinômio de Lie $l^i \in L$ tal que

$$c_i = y(l_1^i \circ l_2^i) + l^i, \tag{3.14}$$

onde c_i é um polinômio central de V. Logo, substituindo y por $x_1 x_2 \ldots x_n$ em 3.14 temos

$$x_1 \ldots x_n c = x_1 \ldots x_n \sum l_1^i \circ l_2^i = \sum c_i|_{y=x_1x_2\ldots x_n} - \sum l_i|_{y=x_1x_2\ldots x_n}, \tag{3.15}$$

para algum $l_i \in L$ e $c_i \in V$. Como $c_i|_{y=x_1x_2\ldots x_n} \in V$, temos

$$x_1 \ldots x_n c \equiv -\sum l_i|_{y=x_1x_2\ldots x_n} \ (mod\ V).$$

Usando a igualdade 1.2 (p.7) sabe-se que $r(l_i|_{y=x_1x_2\ldots x_n}) < n$. Logo,

$$x_1 \ldots x_n c \equiv t \ (mod\ V),$$

onde t é um polinômio de posto menor que n. Usando o mesmo raciocínio para todos os $\varphi_i's$, temos que $f \equiv F \ (mod\ V)$, com $r(F) < n$. Por f ser um polinômio central e $V \subset C(M_2(K))$, segue que F também é um polinômio central e tem posto menor que n. Logo, por hipótese de indução $F \in V$, e por conseguinte $f \in V$.

■

Capítulo 4

Construções de Polinômios Centrais para a Álgebra $M_n(K)$

Em 1956, Kaplansky [28] apresentou uma lista de problemas em aberto na Teoria de Anéis, em particular na PI-Teoria, que motivaram muitos pesquisadores nas décadas seguintes. Um destes problemas era sobre a existência de polinômio central não-trivial para a álgebra $M_n(K)$, com $n > 2$ (no caso $n = 2$ o polinômio de Hall $[x_1, x_2] \circ [x_3, x_4]$ já era conhecido). A solução para este problema foi dada em 1972-1973 independentemente por Formanek [15] e Razmyslov [45] que provaram a existência de tais polinômios por construção direta. Neste Capítulo apresentaremos as contruções de polinômios centrais feitas por Formanek e Razmyslov. Já na última seção, trataremos da construção por Latyshev e Shmelkin (veja [36]) de um polinômio central em uma variável para a álgebra $M_n(K)$, onde K será um corpo finito.

4.1 Matrizes Genéricas

Nesta seção vamos assumir K um corpo e, para um inteiro $n \geq 2$, fixaremos a notação Ω_n para a K-álgebra dos polinômios em variáveis comutativas

$$\Omega_n = K[y_{pq}^{(i)} \mid p, q = 1, \ldots, n,\ i = 1, 2, \ldots].$$

Definição 4.1.1 *As matrizes de $M_n(\Omega_n)$*

$$y_i = \sum_{p,q=1}^{n} y_{pq}^{(i)} E_{pq},\ i = 1, 2, \ldots$$

são chamadas matrizes genéricas $n \times n$. A álgebra gerada pelas matrizes genéricas y_i, $i = 1, 2, \ldots$, denotada por R_n, é chamada de álgebra das matrizes genéricas de ordem *n. Nós denotaremos por $R_{n,m}$ a subálgebra de R_n gerada pelas m primeiras matrizes genéricas $y_1, y_2, \ldots, y_m$.*

Exemplo 4.1.2 *Para $n = m = 2$, trocando a notação e assumindo que $y_{pq}^{(1)} = x_{pq}$ e $y_{pq}^{(2)} = y_{pq}$, a álgebra $R_{2,2}$ é gerada por*

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

Sendo C uma K-álgebra comutativa, as matrizes $n \times n$ com entradas em C podem ser obtidas por especializações das matrizes genéricas, isto é, $\alpha = \sum_{p,q=1}^{n} \gamma_{pq} E_{pq}$, $\gamma_{pq} \in C$ é obtida de $y_1 = \sum_{p,q=1}^{n} y_{pq}^{(1)} E_{pq}$ trocando as variáveis $y_{pq}^{(1)}$ por γ_{pq}.

Os resultados enunciados a seguir serão de grande valia na demonstração do Teorema 4.2.1 que será tratado na próxima seção.

Lema 4.1.3 *Os autovalores da matriz genérica y_1 são dois a dois distintos.*

Demonstração: Consideremos y_1 uma matriz com entradas no corpo de frações da álgebra polinomial Ω_n. Seja $f(\lambda)$ o polinômio característico de y_1. Suponhamos que $f(\lambda)$ tem zeros múltiplos. Então o discriminante de $f(\lambda)$ é igual a zero. Desde que cada matriz A de ordem $n \times n$ com entradas em K pode ser obtida por uma especialização de y_1, o discriminante do polinômio característico $f_A(\lambda)$ também é igual a zero e isto significa que $A \in M_n(K)$ tem autovalores múltiplos. Para mostrar o Lema é suficiente encontrarmos uma matriz $A \in M_n(K)$ que não possua autovalores múltiplos. Se K é um corpo infinito, então podemos considerar uma matriz diagonal cujos elementos da diagonal são todos distintos. Se $K = F_q$ é um corpo de q elementos, então existe um polinômio irredutível sobre F_q de grau n e dessa forma podemos construir uma matriz $A \in M_n(F_q)$ que tem como polinômio característico este polinômio irredutível (basta tomar a matriz associada ou companheira do polinômio). Portanto, a matriz A não tem autovalores múltiplos em nenhuma extensão de F_q. ■

Corolário 4.1.4 *Sejam*

$$y_1' = \sum_{p,q=1}^{n} y_{pp}^{(1)} E_{pp}, \; y_i' = y_i, \; i > 1$$

matrizes genéricas. A álgebra R_n' gerada por $y_1', y_2', \ldots$ é isomorfa a álgebra genérica R_n.

Demonstração: Seja Ξ o fecho algébrico do corpo de frações da álgebra polinomial Ω_n. Pelo Lema 4.1.3, a matriz genérica y_1 não tem autovalores múltiplos. Logo, existe uma matriz z com entradas em Ξ tal que $u_1 = z^{-1}y_1z$ é diagonal. Seja

$$u_i = z^{-1}y_iz, \ i = 1, 2, \dots$$

Denotemos por U_n a K-subálgebra de $M_n(\Xi)$ gerada por $u_1, u_2, \dots$. As álgebras U_n e R_n são isomorfas. De fato, consideremos o homomorfismo

$$\begin{array}{rcl} \varphi : R_n & \longrightarrow & U_n \\ y_i & \longmapsto & \varphi(y_i) = u_i. \end{array}$$

Não é difícil ver que φ é um isomorfismo. Sejam $\phi : R_n \longrightarrow R'_n$ e $\psi : R'_n \longrightarrow U_n$ os homomorfismos de álgebras satisfazendo $\phi(y_i) = y'_i$ e $\psi(y'_i) = u_i$, $i = 1, 2, \dots$. A composição

$$\begin{array}{rcl} \psi\phi : R_n & \longrightarrow & U_n \\ y_i & \longmapsto & (\psi\phi)(y_i) = u_i. \end{array}$$

é um isomorfismo, de onde segue que $Ker\phi = \{0\}$. Além disso, ϕ é sobrejetora, logo ϕ é um isomorfismo. ■

4.2 Construção de Formanek

Nesta seção vamos considerar $M_n(K)$ a álgebra das matrizes com entradas em K, onde K será um corpo qualquer.

Sejam $x_1, \dots, x_{n+1}$ variáveis comutativas e $X, Y_1, \dots, Y_n$ variáveis não-comutativas. Consideremos a aplicação de $K[x_1, \dots, x_{n+1}]$ em $K\langle X, Y_1, \dots, Y_n\rangle$ definida por

$$\theta : K[x_1, \dots, x_{n+1}] \longrightarrow K\langle X, Y_1, \dots, Y_n\rangle$$
$$g(x_1, \dots, x_{n+1}) \longrightarrow \theta(g(x_1, \dots, x_{n+1})) = G(X, Y_1, \dots, Y_n),$$

onde

$$g(x_1, \dots, x_{n+1}) = \sum \alpha_a x_1^{\alpha_1} \dots x_{n+1}^{\alpha_{n+1}} \text{ e}$$
$$G(X, Y_1, \dots, Y_n) = \sum \alpha_a X^{\alpha_1} Y_1 X^{\alpha_2} Y_2 \dots X^{\alpha_n} Y_n X^{\alpha_{n+1}}.$$

Dados $\overline{x} = \sum_{p=1}^n x_p E_{pp}$, $\overline{y_q} = E_{i_q j_q} \in M_n(K)$, onde $x_p \in K$ e $q = 1, \dots, n$ é fácil ver que

$$G(\overline{x}, \overline{y_1}, \dots, \overline{y_n}) = g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) E_{i_1 j_1} \dots E_{i_n j_n}. \tag{4.1}$$

Basta notarmos que $\overline{x}E_{ij} = x_iE_{ij}$ e $E_{ij}\overline{x} = x_jE_{ij}$.

O próximo resultado garante a existência de um polinômio central não trivial para álgebra das matrizes $M_n(K)$.

Teorema 4.2.1 *Seja*

$$g(x_1, \ldots, x_{n+1}) = \prod_{2\leq i\leq n}(x_1 - x_i)(x_{n+1} - x_i)\prod_{2\leq j<k\leq n}(x_j - x_k)^2$$

um polinômio em $K[x_1, \ldots, x_{n+1}]$. *O polinômio em* $K\langle X, Y_1, \ldots, Y_n\rangle$ *dado por*

$$F(X, Y_1, \ldots, Y_n) = G(X, Y_1, \ldots, Y_n)+G(X, Y_2, \ldots, Y_n, Y_1)+\ldots+G(X, Y_n, Y_1, \ldots, Y_{n-1}),$$

onde $G(X, Y_1, \ldots, Y_n) = \theta(g(x_1, \ldots, x_{n+1}))$, *é um polinômio central não trivial para a álgebra* $M_n(K)$.

Demonstração: Para mostrar que $F(X, Y_1, \ldots, Y_n)$ é um polinômio central para $M_n(K)$ é suficiente mostrarmos que $F(\overline{X}, \overline{Y_1}, \ldots, \overline{Y_n})$ é central quando $\overline{X}, \overline{Y_1}, \ldots, \overline{Y_n}$ são matrizes genéricas. De fato, consideremos a aplicação

$$\begin{aligned} h : \{y_{pq}^{(i)} \mid p, q = 1, \ldots, n,\ i = 1, 2, \ldots\} &\longrightarrow K \\ h(y_{pq}^{(1)}) = 1, \quad \text{se} \quad (p, q) &= (1, 1); \\ h(y_{pq}^{(1)}) = 0, \quad \text{se} \quad (p, q) &\neq (1, 1); \\ h(y_{pq}^{(2)}) = 1, \quad \text{se} \quad (p, q) &= (1, 2); \\ h(y_{pq}^{(2)}) = 0, \quad \text{se} \quad (p, q) &\neq (1, 2); \\ &\vdots \\ h(y_{pq}^{(n^2)}) = 1, \quad \text{se} \quad (p, q) &= (n, n); \\ h(y_{pq}^{(n^2)}) = 0, \quad \text{se} \quad (p, q) &\neq (n, n). \end{aligned}$$

Por Ω_n ser uma álgebra associativa e comutativa livre gerada por

$$\{y_{pq}^{(i)} \mid p, q = 1, \ldots, n,\ i = 1, 2, \ldots\},$$

concluímos que a aplicação h se estende a um único homomorfismo

$$\psi : \Omega_n \longrightarrow K.$$

O homomorfismo ψ induz um homomorfismo de $M_n(\Omega_n)$ em $M_n(K)$ dado por

$$\begin{array}{rcl} \Gamma \ :\ M_n(\Omega_n) & \longrightarrow & M_n(K) \\ (f_{ij})_{n\times n} & \longmapsto & \Gamma((f_{ij})) = (\psi(f_{ij}))_{n\times n}. \end{array}$$

Além disso, $\varphi = \Gamma|_{R_n} : R_n \longrightarrow M_n(K)$ é um homomorfismo que satisfaz $\varphi(y_1) = E_{11}$, $\varphi(y_2) = E_{12}, \ \ldots, \ \varphi(y_{n^2}) = E_{nn}$ e portanto sobrejetivo. Logo, dados

$$X, Y_1, \ldots, Y_n \in M_n(K),$$

existem $\overline{X}, \overline{Y_1}, \ldots, \overline{Y_n} \in R_n$ tais que $\varphi(\overline{X}) = X, \ \varphi(\overline{Y_1}) = Y_1, \ \ldots, \ \varphi(\overline{Y_n}) = Y_n$. Logo,

$$F(X, Y_1, \ldots, Y_n) = F(\varphi(\overline{X}), \varphi(\overline{Y_1}), \ldots, \varphi(\overline{Y_n})) = \varphi(F(\overline{X}, \overline{Y_1}, \ldots, \overline{Y_n})) \in Z(M_n(K)),$$

pois estamos supondo $F(\overline{X}, \overline{Y_1}, \ldots, \overline{Y_n})$ central para as matrizes genéricas $\overline{X}, \overline{Y_1}, \ldots, \overline{Y_n}$.

Por $R_n \simeq R'_n$ (veja Corolário 4.1.4) podemos supor $\overline{X}$ diagonal, ou seja, $\overline{X} = \sum_{i=1}^{n} x_i E_{ii}$, onde os $x_i's$ são variáveis comutativas. Verificaremos esta afirmação. Sejam $X, Y_1, \ldots, Y_n$ matrizes genéricas em R_n. Usando o fato de $R_n \simeq R'_n$, tomemos $\overline{X}, \overline{Y_1}, \ldots, \overline{Y_n} \in R'_n$, onde $\overline{X}$ é diagonal, e um isomorfismo $\phi : R'_n \longrightarrow R_n$ tais que $\phi(\overline{X}) = X, \ \phi(\overline{Y_1}) = Y_1, \ \ldots, \ \phi(\overline{Y_n}) = Y_n$. Daí,

$$F(X, Y_1, \ldots, Y_n) = F(\phi(\overline{X}), \phi(\overline{Y_1}), \ldots, \phi(\overline{Y_n})) = \phi(F(\overline{X}, \overline{Y_1}, \ldots, \overline{Y_n})) \in Z(R_n),$$

se $F(\overline{X}, \overline{Y_1}, \ldots, \overline{Y_n}) \in Z(R'_n)$. Sendo assim, podemos supor $\overline{X}$ uma matriz genérica diagonal. Desde que $F(X, Y_1, \ldots, Y_n)$ é um polinômio multilinear em $Y_1, \ldots, Y_n$ basta mostrarmos que é central para as matrizes $\overline{Y_1}, \ldots, \overline{Y_n}$ unitárias. Observe que por 4.1

$$G(\overline{X}, E_{i_1 j_1}, \ldots, E_{i_n j_n}) = g(x_{i_1}, \ldots, x_{i_n}, x_{j_n}) E_{i_1 j_1} \ldots E_{i_n j_n}.$$

Mostraremos que $g(x_{i_1}, \ldots, x_{i_n}, x_{j_n})$ é não-nulo somente quando $\{i_1, \ldots, i_n\}$ é uma permutação de $\{1, \ldots, n\}$ e $i_1 = j_n$. De fato,

$$g(x_{i_1}, \ldots, x_{i_n}, x_{j_n}) = \prod_{i \in \{i_2, \ldots, i_n\}} (x_{i_1} - x_i)(x_{j_n} - x_i) \prod_{\substack{j<k \\ j,k \in \{i_2, \ldots, i_n\}}} (x_j - x_k)^2. \qquad (4.2)$$

Se $\{i_1, \ldots, i_n\}$ não é uma permutação de $\{1, \ldots, n\}$, então haverá repetição entre os $i'_j s$. Logo, por 4.2 segue que $g(x_{i_1}, \ldots, x_{i_n}, x_{j_n}) \equiv 0$. Caso $j_n \neq i_1$, e $\{i_1, i_2, \ldots, i_n\}$ é uma permutação de $\{1, 2, \ldots, n\}$ temos $j_n \in \{i_2, \ldots, i_n\}$ e por 4.2 também concluímos que $g(x_{i_1}, \ldots, x_{i_n}, x_{j_n}) \equiv 0$. Daí, quando $\{i_1, \ldots, i_n\}$ é uma permutação de $\{1, \ldots, n\}$ e $i_1 = j_n$, obtemos que

$$g(x_{i_1}, \ldots, x_{i_n}, x_{j_n}) = \prod_{1 \le i < j \le n} (x_i - x_j)^2 = D.$$

Claramente $E_{i_1j_1}E_{i_2j_2}\dots E_{i_nj_n} \neq 0$ somente se $j_1 = i_2,\ j_2 = i_3,\ \dots,\ j_{n-1} = i_n$. Diremos que $E_{i_1j_1}, E_{i_2j_2}, \dots, E_{i_nj_n}$ formam um *ciclo de matrizes unitárias* se $\{i_1, \dots, i_n\}$ é uma permutação de $\{1, \dots, n\}$ e $j_1 = i_2,\ j_2 = i_3,\ \dots,\ j_{n-1} = i_n\ e\ j_n = i_1$. Sendo assim,

$$G(\overline{X}, E_{i_1j_1}, \dots, E_{i_nj_n}) = \begin{cases} DE_{i_1i_1}, & \text{se as matrizes unitárias formam um ciclo;} \\ 0, & \text{caso contrário,} \end{cases}$$

onde $D = \prod_{1 \leq i < j \leq n}(x_i - x_j)^2$. Analogamente, mostra-se que

$$G(\overline{X}, E_{i_2j_2}, \dots, E_{i_nj_n}, E_{i_1j_1}) = \begin{cases} DE_{i_2i_2}, & \text{se as matrizes unitárias formam um ciclo;} \\ 0, & \text{caso contrário.} \end{cases}$$

Continuando com este raciocínio, concluímos que

$$F(\overline{X}, E_{i_2j_2}, \dots, E_{i_nj_n}, E_{i_1j_1}) = \begin{cases} DI_n, & \text{se as matrizes unitárias formam um ciclo;} \\ 0, & \text{caso contrário.} \end{cases}$$

Portanto, $F(X, Y_1, \dots, Y_n) \in Z(M_n(K))$ para qualquer substituição em $X, Y_1, \dots, Y_n$. Para concluir a demonstração resta-nos provar que $F(X, Y_1, \dots, Y_n)$ não é identidade polinomial para $M_n(K)$. Se K é um corpo infinito e $X \in M_n(K)$ é uma matriz diagonal com autovalores distintos $\rho_1, \dots, \rho_n$, então

$$F(X, E_{12}, \dots, E_{k-1,k}, E_{k1}) = \prod_{1 \leq p < q \leq n} (\rho_p - \rho_q)^2 I_n \neq 0. \tag{4.3}$$

que é uma matriz não-nula em $M_n(K)$.

Suponhamos $K = F_q$ um corpo finito de ordem q. Dado $n \in \mathbb{N}$, existe um polinômio $l(x)$ mônico, irredutível e de grau n em $F_q[x]$. Sendo F_{q^m} o corpo de raízes de $l(x)$, temos que as n raízes de $l(x)$ em F_{q^m} são distintas. Consideremos então $\overline{X} \in M_n(F_q)$ que tem por polinômio característico $l(x)$. Dessa forma, existe uma matriz $Z \in M_n(F_{q^m})$ tal que $Z^{-1}\overline{X}Z$ é diagonal. Portanto, por 4.3 segue que

$$F(Z^{-1}\overline{X}Z, E_{12}, E_{23}, \dots, E_{n1}) \neq 0, \text{ ou seja, } ZF(Z^{-1}\overline{X}Z, E_{12}, E_{23}, \dots, E_{n1})Z^{-1} \neq 0,$$

e daí

$$F(Z(Z^{-1}\overline{X}Z)Z^{-1}, ZE_{12}Z^{-1}, ZE_{23}Z^{-1}, \dots, ZE_{n1}Z^{-1}) \neq 0, \text{ isto é,}$$

$$F(\overline{X}, ZE_{12}Z^{-1}, ZE_{23}Z^{-1}, \dots, ZE_{n1}Z^{-1}) \neq 0 \text{ em } M_n(F_{q^m}).$$

Notemos que $F(\overline{X}, ZE_{12}Z^{-1}, ZE_{23}Z^{-1}, \ldots, ZE_{n1}Z^{-1})$ é uma combinação linear dos termos $F(\overline{X}, E_{i_1j_1}, E_{i_2j_2}, \ldots, E_{i_nj_n})$, onde os coeficientes pertencem a F_{q^m}. Logo, por $F(\overline{X}, ZE_{12}Z^{-1}, ZE_{23}Z^{-1}, \ldots, ZE_{n1}Z^{-1}) \neq 0$, concluímos que algum

$$F(\overline{X}, E_{i_1j_1}, E_{i_2j_2}, \ldots, E_{i_nj_n}) \neq 0.$$

Além disso, $F(\overline{X}, E_{i_1j_1}, E_{i_2j_2}, \ldots, E_{i_nj_n}) \in M_n(F_q)$, o que completa a demonstração. ∎

4.3 Construção de Razmyslov

Nesta seção apresentaremos a construção dada por Razmyslov [45] de um polinômio central para a álgebra $M_n(K)$, onde K denota um corpo. Vamos introduzir o conceito de identidade polinomial fraca que será de grande valia no desenvolvimento das idéias desta construção.

Definição 4.3.1 *O polinômio $f(x_1, \ldots, x_k) \in K\langle X\rangle$ será dito uma **identidade polinomial fraca** para a álgebra $M_n(K)$, se $f(a_1, \ldots, a_k) = 0$ para quaisquer $a_1, \ldots, a_k$ matrizes de traço zero em $M_n(K)$, ou seja, para quaisquer $a_1, \ldots, a_k \in Sl_n(K)$. Uma identidade polinomial fraca é dita ser **essencialmente fraca** se não é identidade para $M_n(K)$.*

Exemplo 4.3.2 *O polinômio $[x_1^2, x_2]$ é uma identidade essencialmente fraca para $M_2(K)$. De fato, sejam $A_1, A_2 \in Sl_2(K)$. Pelo Teorema de Cayley-Hamilton o polinômio característico de A_1 é $x^2 - (tr\ A_1)x + det(A_1)$. Logo, $A_1^2 = -det(A_1)I_2$, de onde segue que $[A_1^2, A_2] = 0$. Por outro lado, $[x_1^2, x_2]$ não é identidade para $M_2(K)$, basta considerarmos $x_1 = E_{11}$ e $x_2 = E_{12}$.*

Lema 4.3.3 *Considerando o polinômio de Capelli*

$$d_n(x_1, \ldots, x_n; y_1, \ldots, y_n, y_{n+1}) = \sum_{\sigma \in S_n} (-1)^\sigma y_1 x_{\sigma(1)} y_2 \ldots y_n x_{\sigma(n)} y_{n+1},$$

o polinômio $d_{n^2}(x_1, \ldots, x_{n^2}; y_1, \ldots, y_{n^2}, y_{n^2+1})$ é uma identidade essencialmente fraca para $M_n(K)$, o qual se anula quando os $x's$ são substituídos por elementos de $Sl_n(K)$ e os $y's$ são matrizes arbitrárias de $M_n(K)$.

Demonstração: Como d_{n^2} é um polinômio multilinear nas variavéis $x's$ basta mostrarmos a afirmação para uma base de $Sl_n(K)$. Desde que $\dim Sl_n(K) = n^2 - 1$, dados $A_1, \ldots, A_{n^2} \in \beta$, onde β é uma base de $Sl_n(K)$, existem $i_0, j_0 \in \{1, \ldots, n^2\}$ tais que $A_{i_0} = A_{j_0}$, $i_0 \neq j_0$. Tome $\theta = (i_0\ j_0) \in S_{n^2}$. Observemos que $S_{n^2} = A_{n^2} \cup \theta A_{n^2}$, uma vez que $\theta \in S_{n^2} - A_{n^2}$. Sejam $\sigma \in A_{n^2}$ e $B_1, \ldots, B_{n^2}, B_{n^2+1} \in M_n(K)$. Daí, por

$$B_1 A_{\sigma(1)} B_2 A_{\sigma(2)} B_3 \ldots B_{n^2} A_{\sigma(n^2)} B_{n^2+1} = B_1 A_{(\theta\sigma)(1)} B_2 A_{(\theta\sigma)(2)} B_3 \ldots B_{n^2} A_{(\theta\sigma)(n^2)} B_{n^2+1},$$

temos

$$d_{n^2}(A_1, \ldots, A_{n^2}; B_1, \ldots, B_{n^2}, B_{n^2+1}) = \sum_{\sigma \in A_{n^2}} B_1 A_{\sigma(1)} B_2 A_{\sigma(2)} B_3 \ldots B_{n^2} A_{\sigma(n^2)} B_{n^2+1} +$$

$$\sum_{\sigma \in A_{n^2}} (-1) B_1 A_{(\theta\sigma)(1)} B_2 A_{(\theta\sigma)(2)} B_3 \ldots B_{n^2} A_{(\theta\sigma)(n^2)} B_{n^2+1} = 0,$$

e assim d_{n^2} é uma identidade polinomial fraca para $M_n(K)$. Resta mostrarmos que d_{n^2} não é identidade para $M_n(K)$.

Considere $E_{p_1 q_1}, E_{p_2 q_2}, \ldots, E_{p_{n^2} q_{n^2}}$ as distintas matrizes unitárias de $M_n(K)$. Notemos que

$$d_{n^2}(E_{p_1 q_1}, E_{p_2 q_2}, \ldots, E_{p_{n^2} q_{n^2}}; E_{1 p_1}, E_{q_1 p_2}, \ldots, E_{q_{n^2-2} p_{n^2-1}}, E_{q_{n^2-1} p_{n^2}}, E_{q_{n^2} 1}) =$$

$$\sum_{\sigma \in S_{n^2}} (-1)^{\sigma} E_{1 p_1} E_{p_{\sigma(1)} q_{\sigma(1)}} E_{q_1 p_2} E_{p_{\sigma(2)} q_{\sigma(2)}} \ldots E_{q_{n^2-1} p_{n^2}} E_{p_{\sigma(n^2)} q_{\sigma(n^2)}} E_{q_{n^2} 1}.$$

Além disso, $E_{1 p_1} E_{p_{\sigma(1)} q_{\sigma(1)}} E_{q_1 p_2} E_{p_{\sigma(2)} q_{\sigma(2)}} \ldots E_{q_{n^2-1} p_{n^2}} E_{p_{\sigma(n^2)} q_{\sigma(n^2)}} E_{q_{n^2} 1}$ é igual a zero a menos que

$$\begin{array}{ccccc}
p_1 = p_{\sigma(1)} & e & q_{\sigma(1)} = q_1, & \text{ou seja,} & \sigma(1) = 1; \\
p_2 = p_{\sigma(2)} & e & q_{\sigma(2)} = q_2, & \text{ou seja,} & \sigma(2) = 2; \\
\vdots & & \vdots & & \vdots \\
p_{n^2-1} = p_{\sigma(n^2-1)} & e & q_{\sigma(n^2-1)} = q_{n^2-1}, & \text{ou seja,} & \sigma(n^2-1) = n^2-1; \\
p_{n^2} = p_{\sigma(n^2)} & e & q_{\sigma(n^2)} = q_{n^2}, & \text{ou seja,} & \sigma(n^2) = n^2.
\end{array}$$

Logo, este produto é igual a zero a menos que σ seja a permutação identidade. Portanto,

$$d_{n^2}(E_{p_1 q_1}, E_{p_2 q_2}, \ldots, E_{p_{n^2} q_{n^2}}; E_{1 p_1}, E_{q_1 p_2}, \ldots, E_{p_1 q_1}, E_{q_{n^2-1} p_{n^2}}, E_{q_{n^2} 1}) =$$

$$E_{1 p_1} E_{p_1 q_1} E_{q_1 p_2} E_{p_2 q_2} \ldots E_{q_{n^2-1} p_{n^2}} E_{p_{n^2} q_{n^2}} E_{q_{n^2} 1} = E_{11} \neq 0.$$

■

A seguir apresentaremos o conceito da transformada de Razmyslov, cuja importância está no fato da construção de Razmyslov está baseada neste conceito.

Definição 4.3.4 *Seja* $f(x, y_1, \ldots, y_m) \in K\langle x, y_1, \ldots, y_m\rangle$ *um polinômio linear (homogêneo e de grau 1) na variavél* x. *Escrevendo* f *sob a forma* $f = \sum_{i=1}^{k} g_i x h_i$, *onde* $g_i, h_i \in K\langle y_1, \ldots, y_m\rangle$, *a transformada de Razmyslov de* f *é o polinômio*

$$f^*(x, y_1, \ldots, y_m) = \sum_{i=1}^{k} h_i x g_i.$$

Lema 4.3.5 *Sejam* $a_i, b_i \in M_n(K)$, $i = 1, \ldots, m$, $f(u) = \sum_{i=1}^{m} a_i u b_i$ *e* $f^*(u) = \sum_{i=1}^{m} b_i u a_i$, *para* $u \in M_n(K)$. *Se* $f(u) = 0$ *para todo* $u \in M_n(K)$, *então* $f^*(u) = 0$ *para todo* $u \in M_n(K)$.

Demonstração: Consideremos a forma bilinear em $V = M_n(K)$ dada por $\langle A, B\rangle = tr(AB)$. Notemos que esta forma bilinear é não-degenerada, ou seja, se $\langle u, V\rangle = 0$, então $u = 0$. Logo, dados $u, v \in M_n(K)$, visto que $f(u) = 0$, temos que $tr(f(u)) = 0$ e daí

$$0 = tr\left(\left(\sum_{i=1}^{m} a_i u b_i\right) v\right) = tr\left(\sum_{i=1}^{m} a_i u b_i v\right) = \sum_{i=1}^{m} tr[(a_i u)(b_i v)] =$$

$$\sum_{i=1}^{m} tr[(b_i v)(a_i u)] = \sum_{i=1}^{m} tr(b_i v a_i u) = tr\left[\left(\sum_{i=1}^{m} b_i v a_i\right) u\right] = tr(f^*(v)u),$$

e assim $\langle f^*(v), u\rangle = 0$. Como u foi tomado arbitrariarmente, concluímos que $\langle f^*(v), V\rangle = 0$, e portanto $f^*(v) = 0$. Mas v também foi tomado arbitrariarmente, de onde segue que $f^*(v) = 0$, $\forall v \in M_n(K)$. ■

Lema 4.3.6 *Toda matriz de traço zero em* $M_n(K)$ *é uma combinação linear de comutadores.*

Demonstração: Seja $A \in Sl_n(K)$. Então $A = \sum_{p,q=1}^{n} \alpha_{pq} E_{pq}$, onde $\alpha_{11} + \ldots + \alpha_{nn} = 0$. Logo,

$$A = \sum_{\substack{p,q=1 \\ p \neq q}}^{n} \alpha_{pq} E_{pq} + \sum_{p=1}^{n} \alpha_{pp} E_{pp} = \sum_{\substack{p,q=1 \\ p \neq q}}^{n} \alpha_{pq} E_{pq} + \alpha_{11} E_{11} + \sum_{p=2}^{n} \alpha_{pp} E_{pp} =$$

$$\sum_{\substack{p,q=1 \\ p \neq q}}^{n} \alpha_{pq} E_{pq} + \sum_{p=2}^{n} -\alpha_{pp} E_{11} + \sum_{p=2}^{n} \alpha_{pp} E_{pp} = \sum_{\substack{p,q=1 \\ p \neq q}}^{n} \alpha_{pq} E_{pq} + \sum_{p=2}^{n} -\alpha_{pp}(E_{11} - E_{pp}).$$

Portanto, os elementos E_{ij}, $i \neq j$ e $E_{11} - E_{ii}$, $i = 2, \ldots, n$ formam uma base para $Sl_n(K)$. Além disso, $E_{ij} = [E_{ij}, E_{jj}]$ para $i \neq j$ e $E_{11} - E_{ii} = [E_{1i}, E_{i1}]$ para $i = 2, \ldots, n$. ■

Lema 4.3.7 ***(Lema de Razmyslov)*** *Sejam $f(x, y_1, \ldots, y_m) \in K\langle x, y_1, \ldots, y_m\rangle$ um polinômio linear em x e $f^*(x, y_1, \ldots, y_m)$ o polinômio dado pela transformada de Razmyslov de f. Então*

(i) $f(x, y_1, \ldots, y_m)$ é uma identidade polinomial para a álgebra $M_n(K)$ se, e somente se, $f^*(x, y_1, \ldots, y_m)$ é uma identidade polinomial para $M_n(K)$.

(ii) $f^*(x, y_1, \ldots, y_m)$ é um polinômio central não trivial para a álgebra $M_n(K)$ se, e somente se, $f(x, y_1, \ldots, y_m)$ é uma identidade essencialmente fraca e $f([x, y_0], y_1, \ldots, y_m)$ é uma identidade polinomial para $M_n(K)$.

Demonstração:

(i) Seja

$$f(x, y_1, \ldots, y_m) = \sum_{i=1}^{k} a_i(y_1, \ldots, y_m)xb_i(y_1, \ldots, y_m)$$

e para $r_1, \ldots, r_m \in M_n(K)$ considere

$$f(u) = f(u, r_1, \ldots, r_m) = \sum_{i=1}^{k} a_i(r_1, \ldots, r_m)ub_i(r_1, \ldots, r_m).$$

Pelo Lema 4.3.5, $f(u) = 0$ para todo $u \in M_n(K)$ se, e somente se, $f^*(u) = 0$ para todo $u \in M_n(K)$. Observe que $f^*(u) = f^*(u, r_1, \ldots, r_m)$. Como $r_1, \ldots, r_m$ foram tomados arbitrariarmente, concluímos a demonstração.

(ii) Considere

$$f(x, y_1, \ldots, y_m) = \sum_{i=1}^{k} a_i(y_1, \ldots, y_m)xb_i(y_1, \ldots, y_m).$$

Aplicando a transformada de Razmyslov a

$$g(x, y_0, y_1, \ldots, y_m) = f([x, y_0], y_1, \ldots, y_m) = \sum_{i=1}^{k} a_i(xy_0 - y_0x)b_i,$$

obtemos

$$g^*(x, y_0, y_1, \ldots, y_m) = \sum_{i=1}^{k}(y_0b_ixa_i - b_ixa_iy_0) = \left[y_0, \sum_{i=1}^{k} b_ixa_i\right] = [y_0, f^*(x, y_1, \ldots, y_m)].$$

Claramente, $f^*(x, y_1, \ldots, y_m)$ é um polinômio central para $M_n(K)$ se, e somente se, $g^*(x, y_0, y_1, \ldots, y_m)$ é uma identidade polinomial para $M_n(K)$ e pela primeira parte do Lema, se, e somente se, $g(x, y_0, y_1, \ldots, y_m)$ é uma identidade polinomial para $M_n(K)$. Obviamente, $f^*(x, y_1, \ldots, y_m)$ não se anula sobre $M_n(K)$ se, e somente se, $f(x, y_1, \ldots, y_m)$ não é identidade polinomial para $M_n(K)$. Além disso, dados $A, B_1, \ldots, B_m \in Sl_n(K)$, pelo Lema 4.3.6, existem $C_i, D_i \in M_n(K)$ tais que $A = \sum_{i=1}^{t} \alpha_i [C_i, D_i]$. Logo,

$$f(A, B_1, \ldots, B_m) = f\left(\sum_{i=1}^{t} \alpha_i [C_i, D_i], B_1, \ldots, B_m\right) = \sum_{i=1}^{t} \alpha_i f([C_i, D_i], B_1, \ldots, B_m) = 0,$$

pois $f([x, y_0], y_1, \ldots, y_m)$ é uma identidade polinomial para $M_n(K)$. ■

Teorema 4.3.8 *Considere o polinômio*

$$f(x, z_1, \ldots, z_{2n^2-2}, y_1, \ldots, y_{n^2-1}) = d_{n^2}(x, [z_1, z_2], \ldots, [z_{2n^2-3}, z_{2n^2-2}]; 1, y_1, \ldots, y_{n^2-1}, 1),$$

onde $d_n(x_1, \ldots, x_n; y_1, \ldots, y_n, y_{n+1})$ *é o polinômio de Capelli. A transformada de Razmyslov aplicada a* f *nos dá um polinômio central nao trivial para a álgebra* $M_n(K)$.

Demonstração: Do lema 4.3.3 temos que $f(x, z_1, \ldots, z_{2n^2-2}, y_1, \ldots, y_{n^2-1})$ é uma identidade polinomial fraca para $M_n(K)$. É também claro que a substituição de x por um comutador nos dá uma identidade polinomial (veja Lema 4.3.3). Logo, $f([x, y_0], z_1, \ldots, y_{n^2-1})$ é uma identidade polinomial para $M_n(K)$. Pelo lema de Razmyslov 4.3.7 é suficiente mostrar que $f(x, z_1, \ldots, y_{n^2-1})$ não é identidade polinomial para $M_n(K)$. Podemos escolher $2n^2 - 2$ matrizes de traço zero $\overline{z_i} \in Sl_n(K)$ tais que o conjunto de comutadores $[\overline{z_{2i-1}}, \overline{z_{2i}}]$, $i = 1, \ldots, n^2 - 1$ coincida com a base de $Sl_n(K)$ dada no Lema 4.3.6. Para isso, basta notarmos que $E_{11} - E_{ii} = [E_{1i}, E_{i1}]$, onde $i = 2, \ldots, n$ e para $i \neq j$ e $l \neq i, j$, $E_{ij} = [E_{ij}, E_{jj} - E_{ll}]$. Substituindo x por $\overline{x} = E_{11}$ e usando a anti-simetria da identidade de Capelli nas variáveis $x_i's$ temos que

$$f(\overline{x}, \overline{z_1}, \ldots, \overline{z_{2n^2-3}}, \overline{z_{2n^2-2}}, y_1, \ldots, y_{n^2-1}) = \pm d_{n^2}(E_{ij}; 1, y_1, \ldots, y_{n^2-1}, 1),$$

onde $d_{n^2}(E_{ij}; 1, y_1, \ldots, y_{n^2-1}, 1)$ significa que estamos substituindo as variavéis anti-simétricas por n^2 matrizes unitárias distintas. Além disso, usando a idéia da demonstração do Lema 4.3.3, não é difícil ver que

$$d_{n^2}(E_{p_1q_1}, E_{p_2q_2}, \ldots, E_{p_{n^2}q_{n^2}}; 1, E_{q_1p_2}, \ldots, E_{q_{n^2-1}p_{n^2}}, 1) = E_{p_1q_{n^2}} \neq 0.$$

Portanto, pelo lema de Razmyslov, concluímos que f^* é um polinômio central não trivial para $M_n(K)$. ■

4.4 Construção de Latyshev e Shmelkin

Nesta seção apresentaremos a construção dada por Latyshev e Shmelkin [36] de um polinômio central em uma variável para a álgebra $M_n(K)$, onde K denotará um corpo finito. Começaremos com alguns resultados necessários para a demonstração do resultado central desta seção.

Lema 4.4.1 *Sejam $n \in \mathbb{N}$, K um corpo finito de ordem q e L uma extensão algebricamente fechada de K. Então L possui um único subcorpo de ordem q^n.*

Demonstração: Considere $f(x) = x^{q^n} - x \in L[x]$. Por $f'(x) = q^n x^{q^n-1} - 1 = -1$, temos que $f(x)$ possui em L q^n raízes distintas. Estas raízes são exatamente os elementos do conjunto $F = \{a \in L \mid a^{q^n} = a\}$ que é um subcorpo de L. Assim, $|F| = q^n$. Suponhamos que existam dois subcorpos distintos F_1 e F_2 de L, ambos com ordem q^n. Logo, $a^{q^n} = a$ para todo $a \in F_1 \cup F_2$. Sendo assim, todo elemento de $F_1 \cup F_2$ é raíz de $f(x) = x^{q^n} - x$, o que é um absurdo, pois $F_1 \cup F_2$ tem mais que q^n elementos.
■

Lema 4.4.2 *Sejam $f(x) \in K[x]$, $\lambda \in K$ e* $N = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in M_n(K)$.

Então $f(\lambda I_n + N) = f(\lambda)I_n + N_1$, onde $N_1^n = 0$.

Demonstração: Basta usar o Binômio de Newton e o fato de N ser nilpotente de índice n. ■

Teorema 4.4.3 *Sejam $K = F_q$ um corpo finito de q elementos e $p(x)$ um polinômio irredutível de grau n em $F_q[x]$. O polinômio em uma variavél*

$$c(x) = \left(\frac{x^{q^n} - x}{p(x)}\right)^{(q^n-1)n} \prod_{m=1}^{n-1} (x^{q^m} - x)^{(q^n-1)n}$$

é central para $M_n(F_q)$.

Demonstração:

Mostraremos inicialmente que $p(x)$ divide $x^{q^n} - x$. Sejam L uma extensão algebricamente fechada de F_q e $a \in L$ tal que $p(a) = 0$. Consideremos o ideal $I = \{h(x) \in F_q[x] \mid h(a) = 0\}$ de $F_q[x]$ e $m_{a,K}(x)$ o polinômio minimal de a sobre K. Sabe-se que o ideal I é gerado por $m_{a,K}(x)$, isto é, $I = \langle m_{a,F_q}(x)\rangle$ e $m_{a,F_q}(x)$ é irredutível sobre F_q. Além disso, por $p(x) \in I$ existe $s(x) \in K[x]$ tal que $p(x) = m_{a,K}(x)s(x)$. Como $p(x)$ é irredutível em $F_q[x]$, concluímos que $\partial m_{a,F_q}(x) = \partial p(x) = n$. Sendo assim, $[F_q(a) : K] = \partial m_{a,F_q}(x) = n$ e consequentemente $|F_q(a)| = q^n$. Consideremos agora $f(x) = x^{q^n} - x$. Dividindo $f(x)$ por $p(x)$ em $F_q[x]$ obtemos $q(x), r(x) \in F_q[x]$ tais que $f(x) = p(x)q(x)+r(x)$, onde $r(x) \equiv 0$ ou $\partial r(x) < \partial p(x)$. Logo, $f(a) = p(a)q(a)+r(a) = r(a)$. Além disso, por $F_q(a)^* = F_q(a) - \{0\}$ ser um grupo multiplicativo de ordem $q^n - 1$, segue que $a^{q^n-1} = 1$ e portanto $a^{q^n} = a$. Logo, $r(a) = 0$. Como $r(a) = 0$ e $\partial p(x) = \partial m_{a,K}(x) = n$ segue que $r(x) \equiv 0$. Portanto, $p(x)$ divide $f(x)$.

Sejam $A \in M_n(F_q)$ e $p_A(x) \in F_q[x]$ o polinômio característico de A. Considere $\alpha \in L$ um autovalor de A. Como $p_A(\alpha) = 0$ e $\partial p_A(x) = n$, temos que $[K(\alpha) : K] = m \leq n$, ou seja, cada autovalor de A pertence a alguma extensão F_{q^m} de F_q com $m \leq n$. Existe uma extensão de F_q, por exemplo o corpo de raízes de $p_A(x)$, onde A é semelhante a uma matriz N na forma Canônica de Jordan. Se mostrarmos que c(N)=0, segue claramente que $c(A) = 0$, pois existe uma matriz inversível $B \in M_n(F)$, onde F é tal extensão, de modo que $B^{-1}AB = N$. Logo, $c(A) = c(BNB^{-1}) = Bc(N)B^{-1} = 0$. Podemos escrever N na forma

$$N = \begin{pmatrix} N_{\lambda_1} & 0 & \cdots & 0 \\ 0 & N_{\lambda_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & N_{\lambda_r} \end{pmatrix},$$

onde $\lambda_1, \lambda_2, \cdots, \lambda_r$ são os autovalores de A, $N_{\lambda_i} = \lambda_i I_{s_i} + B_{s_i}$,

$$B_{s_i} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

e s_i é a multiplicidade do autovalor λ_i. Logo,

$$c(N) = \begin{pmatrix} c(N_{\lambda_1}) & 0 & \cdots & 0 \\ 0 & c(N_{\lambda_2}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & c(N_{\lambda_r}) \end{pmatrix}$$

Mostraremos que se os autovalores de A não são zeros de $p(x)$, então $c(N) = 0$. Suponhamos que λ_1 está em alguma extensão $F_{q^{m_0}}$ para algum $m_0 \in \{1, \cdots, n-1\}$. Consideremos $h(x) = \frac{x^{q^n}-x}{p(x)}$ e $l(x) = x^{q^{m_0}} - x$. Por $\lambda_1 \in F_{q^{m_0}}$, temos que $l(\lambda_1) = 0$. Daí, usando o fato da matriz B_{s_1} ser nilpotente de índice s_1 e o Lema 4.4.2, concluímos que

$$c(N_{\lambda_1}) = h(N_{\lambda_1})^{(q^n-1)n} l(N_{\lambda_1})^{(q^n-1)n} \prod_{\substack{m=1 \\ m \neq m_0}}^{n-1} (N_{\lambda_1}^{q^m} - N_{\lambda_1})^{(q^n-1)n} =$$

$$h(N_{\lambda_1})^{(q^n-1)n} (l(\lambda_1) I_{s_1} + B_{s_1})^{(q^n-1)n} \prod_{\substack{m=1 \\ m \neq m_0}}^{n-1} (N_{\lambda_1}^{q^m} - N_{\lambda_1})^{(q^n-1)n} =$$

$$h(N_{\lambda_1})^{(q^n-1)n} (B_{s_1}^n)^{(q^n-1)} \prod_{\substack{m=1 \\ m \neq m_0}}^{n-1} (N_{\lambda_1}^{q^m} - N_{\lambda_1})^{(q^n-1)n} = 0.$$

Suponhamos agora que λ_1 está em alguma extensão F_{q^n} de F_q e λ_1 não é zero de $p(x)$. Logo, $(x - \lambda_1)$ está entre os fatores de $h(x)$. Daí,

$$c(N_{\lambda_1}) = h(N_{\lambda_1})^{(q^n-1)n} \prod_{m=1}^{n-1} (N_{\lambda_1}^{q^m} - N_{\lambda_1})^{(q^n-1)n} =$$

$$(h(\lambda_1) I_{s_1} + B_{s_1})^{(q^n-1)n} \prod_{m=1}^{n-1} (N_{\lambda_1}^{q^m} - N_{\lambda_1})^{(q^n-1)n} = (B_{s_1}^n)^{(q^n-1)} \prod_{m=1}^{n-1} (N_{\lambda_1}^{q^m} - N_{\lambda_1})^{(q^n-1)n} = 0.$$

Analogamente, mostramos que $c(N_{\lambda_i}) = 0$ para $i = 2, \cdots, r$ e portanto $c(N) = 0$.

Consideremos agora $A \in M_n(F_q)$ que tem um autovalor sendo zero de $p(x)$. Seja λ este autovalor. Consideremos o ideal $J = \{h(x) \in F_q[x] \mid h(\lambda) = 0\}$ e $m_{\lambda,F_q}(x)$ o polinômio minimal de λ sobre F_q. Não é difícil provar que $J = \langle m_{\lambda,F_q}(x) \rangle$. Por $p(x) \in J$, existe $g(x) \in F_q[x]$ tal que $p(x) = m_{\lambda,F_q}(x) g(x)$. Mas $p(x)$ é irredutível, de onde segue que $J = \langle p(x) \rangle$. Como $p_A(x) \in J$, concluímos que $p_A(x)$ é divisível por $p(x)$ e por $\partial p_A(x) = \partial p(x)$, temos que $p_A(x) = \gamma p(x)$ para algum $\gamma \in F_q$ e daí os autovalores de A são exatamente os zeros de $p(x)$. A matriz A não tem autovalores múltiplos em F_{q^n}, pois polinômios irredutíveis sobre corpos finitos não tem zeros múltiplos em nenhuma extensão. Sendo assim, a forma canônica de Jordan de A em $M_n(F_{q^n})$, onde F_{q^n} é uma extensão de grau n de F_q (F_{q^n} é o corpo de raízes do polinômio $p(x)$), é uma matriz diagonal que chamaremos de N. Logo,

$$c(N) = \left(h(N)^n \prod_{m=1}^{n-1} (N^{q^m} - N)^n \right)^{q^n-1} = g(N)^{q^n-1},$$

onde $h(x) = \frac{x^{q^n}-x}{p(x)}$ e $g(x) = h(x)^n \prod_{m=1}^{n-1}(x^{q^m} - x)^n$. Mostraremos que $g(N)$ é uma matriz diagonal, cujos autovalores são não-nulos em F_{q^n}. A matriz N tem a forma

$$N = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

onde $\lambda_1, \lambda_2, \cdots, \lambda_n$ são os autovalores de A. Notemos que:

(i) λ_i não é raíz do polinômio $x^{q^m} - x$ para $m \in \{1, \cdots, n-1\}$. Suponhamos, por contradição, que λ_i é raíz do polinômio $x^{q^m} - x$ para algum $m = 1, \cdots, n-1$. Consideremos o subcorpo $F_{q^m} = \{a \in L \mid a^{q^m} - a = 0\}$ de L. Pelo Lema 4.4.1, concluímos que $|F_{q^m}| = q^m$. É possível mostrar, usando um raciocínio análogo ao que foi feito no início da demonstração deste teorema, que $[F_q(\lambda_i) : K] = n$, ou seja, $|F_q(\lambda_i)| = q^n$. Por outo lado, por $\lambda_i \in F_{q^m}$, temos que $F_q(\lambda_i) \subseteq F_{q^m}$, o que é um absurdo visto que $m < n$.

(ii) λ_i não pode anular $h(x)$, pois λ_i é zero de $p(x)$ e sendo assim $(x - \lambda_i)$ não aparece na fatoração de $h(x)$.

Sendo assim,

$$g(N) = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n \end{pmatrix} \text{ e daí } g(N)^{q^n-1} = \begin{pmatrix} \alpha_1^{q^n-1} & 0 & \cdots & 0 \\ 0 & \alpha_2^{q^n-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n^{q^n-1} \end{pmatrix},$$

onde $\alpha_1, \alpha_2, \cdots, \alpha_n$ são todos não-nulos. Como $F_{q^n} - \{0\}$ é um grupo multiplicativo de ordem $q^n - 1$, segue que $\alpha_i^{q^n-1} = 1$ para todo $i = 1, \cdots, n$. Logo,

$$c(N) = g(N)^{q^n-1} = \begin{pmatrix} \alpha_1^{q^n-1} & 0 & \cdots & 0 \\ 0 & \alpha_2^{q^n-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n^{q^n-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = I_n.$$

Por A ser semelhante a N, existe $B \in M_n(F_{q^n})$ tal que $B^{-1}AB = N$. Daí, $c(A) = c(BNB^{-1}) = Bc(N)B^{-1} = BI_nB^{-1} = I_n \in Z(M_n(F_q))$. ■

Como no caso de identidades polinomiais pode-se perguntar qual o grau mínimo de um polinômio central para $M_n(K)$, quando $char K = 0$. O polinômio central de Formanek (Seção 4.2) é de grau n^2. Do polinômio de Razmyslov (Seção 4.3), cujo grau é maior, Halpin [22] deduziu um novo polinômio central de grau n^2. Acreditou-se por algum tempo que n^2 fosse a resposta para este problema no caso de $n \geq 3$. Entretanto, Drensky e Kasparian [11] construíram um novo polinômio central de grau 8 para a álgebra das matrizes de ordem 3 e provaram que 8 é o grau mínimo. Em [17] Formanek conjecturou que quando $char K = 0$ o grau mínimo de um polinômio central de $M_n(K)$ é $\frac{1}{2}(n^2+3n-2)$ se $n \geq 3$. Notou-se que esta é a única função quadrática que assumia os valores 1, 4 e 8 para $n = 1, 2$ e 3, respectivamente. Drensky [12] construiu polinômios centrais de grau $(n-1)^2 + 1$ para $n \geq 3$ e estes são os polinômios de menor grau até então construídos.

Referências Bibliográficas

[1] E. Alves, A. Brandão, P. Koshlukov, A. Krasilnikov, *The central polynomials for the Grassmann algebra*, Israel J. Math. a aparecer.

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

[3] S. A. Amitsur, *A note on Pi-rings*, Israel J. Math. **10**, 210-211 (1971).

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

[5] S. S. Azevedo, *A basis for $\mathbb{Z}$-graded identities of matrices over infinite fields*, Serdica Math. Journal **29 (2)**, 149-158 (2003).

[6] A. Brandão, *Graded central polynomials for the algebra $M_n(K)$*, Rendiconti del Circolo Matematico di Palermo. **57**, 265-278 (2008).

[7] P. Zh. Chiripov, P. N. Siderov, *On bases for identities of some varieties of associative algebras*, Pliska Studia Mathematica Bulgarica **2**, 103-115 (1981).

[8] J. Colombo, P. Koshlukov, *Central polynomials in the matrix algebra of order two*, Linear Algebra Appl. **377**, 53-67 (2004).

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

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

[11] V. Drensky, A. Kasparian, *A new central polynomial for* 3×3 *matrices*, Comm. Algebra **13**, 745-752 (1985).

[12] V. Drensky, *New Central polynomials for the matrix algebra*, Israel J. Math. **92**, 235-248 (1995).

[13] V. Drensky, *Free algebras and PI algebras*, Graduate Course in Algebra, Springer-Verlag PTE.LTD, 1999.

[14] J. Dubnov, V. Ivanov, *Sur l'abaissement du degré des polynômes en affineurs*, C. R. (Doklady) Acad. Sci. USSR **41**, 96-98 (1943).

[15] E. Formanek, *Central polynomials for matrix rings*, J. Algebra **23**, 129-132 (1972).

[16] E. Formanek, *Invariants and the ring of generic matrices*, J. Algebra **89**, 178-223 (1984).

[17] E. Formanek, *The polynomial identities and invariants of $n \times n$ matrices*, CBMS Regional Conference Series in Mathematics **78**, American Mathematical Society, Providence, RI (1991).

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

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

[20] A. Giambruno, P. Koshlukov, *On the identities of the Grassmann algebras in characteristic p>0*, Israel J. Math. **122**, 305-316 (2001).

[21] A. Giambruno, A. Valenti, *Central polynomials and matrix invariants*, Israel J. Math. **96**, 281-297 (1996).

[22] P. Halpin, *Central and weak identities for matrices*, Commun. Algebra **11 (19)**, 2237-2248 (1983).

[23] I. N. Herstein, *Noncommutative Rings*, Carus Math. Monographs **15**, Wiley and Sons, Inc., New York (1968).

[24] I. N. Herstein, *Notes from a Ring Theory Conference*, CBMS Regional Conference Series in Math. Amer. Math. Soc. **9** (1971).

[25] G. Higman, *On a conjecture of Nagata*, Proc. Camb. Philos. Soc. **52**, 1-4 (1956).

[26] N. Jacobson, *Structure theory of algebraic algebras of bounded degree*, Annals of Math. **46**, 695-707 (1945).

[27] I. Kaplansky, *Rings with a polynomial identity*, Bull. Amer. Math. Soc. **54**, 575-580 (1948).

[28] I. Kaplansky, *Problems in the theory of rings*, Report of a Conference on Linear Algebras, June, 1956, in National Acad. of Sci. - National Research Council, Washington, Publ. **502**, 1-3 (1957).

[29] A. Kemer, *Varieties and $\mathbb{Z}_2$-graded algebras*, Math. USSR, Izv. **25**, 359-374 (1985).

[30] A. Kemer, *Finite basis property of identities os associative algebas*, Algebra and Logic. **26**, 362-397 (1987).

[31] 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).

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

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

[34] D. Krakowski, A. Regev, *The polinomial identities of the Grassmann algebra*, Transactions of the American mathematical Society **181**, 429-438 (1973).

[35] V. N. Latyshev, *On the choice of basis in a T-ideal* (Russo), Sibirskii Matematicheskii Zhurnal **4 (5)**, 1122-1126 (1962).

[36] V. N. Latyshev, A. L. Shmelkin, *A certain problem of Kaplansky*, Algebra and Logic **8**, 257 (1969).

[37] J. Levitski, *On a problem of A. Kurosch*, Bull. Amer. Math. Soc. **52**, 1033-1035 (1946).

[38] 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**, 17-21 (1978).

[39] M. Nagata, *On the nilpotency of nil algebras*, J. Math. Soc. Japan **4**, 296-301 (1953).

[40] S. Okhitin, *Central polynomials of the algebra of second order matrices*, Moscow Univ. Math. Bull. **43 (4)**, 49-51 (1988).

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

[42] E. C. Posner, *Prime rings satisfying a polinomial identity*, Proc. Amer. Math. Soc. **11**, 180-183 (1960).

[43] C. Procesi, *Rings with polynomial identities*, Marcel Dekker, New York (1973).

[44] Yu. P. Rasmyslov, *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).

[45] Yu. P. Rasmyslov, *On a problem of Kaplansky*, Math. USSR, Izv. **7**, 479-496 (1973).

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

[47] Yu. P. Razmyslov, *Identities of algebras and their representations*, Translations Math. Monographs, **138**, AMS, Providence, RI, 1994.

[48] S. Rosset, *A new proof of the Amitsur-Levitski identity*, Israel J. Math. **23**, 187-188 (1976).

[49] L. H. Rowen, *Some results on the center of a ring with polynomial identity*, Bull. Amer. Math. Soc. **79**, 219-223 (1973).

[50] L. H. Rowen, *Polynomial identities of ring theory*, Acad. Press (1980).

[51] A. I. Shirshov, *On rings with identity relations (Russian)*, Mat. Sb. **41**, 277-283 (1957).

[52] A. H. Stojanova-Venkova, *Bases of identities of Grassmann algebras*, Serdica **6**, 63-72 (1980).

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

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

[55] 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).