C

Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Tese de Doutorado

Polinômios Centrais para Álgebras Graduadas

por

Antônio Pereira Brandão Júnior

Doutorado em Matemática - Campinas - SP

Orientador: Prof. Dr. Plamen Koshlukov

†Este trabalho contou com apoio financeiro da CAPES.

Polinômios Centrais para Álgebras Graduadas

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Antônio Pereira Brandão Júnior** e aprovada pela comissão julgadora.

Campinas, 15 de Setembro de 2006.

P Koshlukov

Prof. Dr. Plamen Koshlukov

Banca examinadora:

Prof. Dr. Plamen Koshlukov.

Prof. Dr. Alexei Nikolaevich Krassilnikov.

Prof. Dr. Vyacheslav Futorny.

Prof. Dr. Flávio Ulhoa Coelho.

Prof. Dr. Paulo Roberto Brumatti.

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

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Bibliotecária: Miriam Cristina Alves – CRB8a / 859

Brandão Júnior, Antônio Pereira

B733p Polinômios centrais para álgebras graduadas / Antônio Pereira Brandão Júnior -- Campinas, [S.P. :s.n.], 2006.

Orientador : Plamen Emilov Koshlukov

Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Álgebra não-comutativa. 2. PI-álgebras. 3. Álgebra. I. Koshlukov, Plamen Emilov. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Central polynomials for graded algebras

Palavras-chave em inglês (Keywords): 1.Noncommutative algebra. 2. PI-algebras. 3. Algebra.

Área de concentração: Álgebra

Titulação: Doutor em Matemática

Banca examinadora: Prof. Dr.Plamen Emilov Koshlukov (IMECC-UNICAMP)
Prof. Dr. Alexei Nikolaevich Krassilnikov (UnB)
Prof. Dr. Vyacheslav Futorny (IME-USP)
Prof. Dr. Flávio Ulhoa Coelho (IME-USP)
Prof. Dr. Paulo Roberto Brumatti (IMECC-UNICAMP)

Data da defesa: 15/09/2006

Programa de Pós-Graduação: Doutorado em Matemática

Tese de Doutorado defendida em 15 de setembro de 2006e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof. (a). Dr (a). PLAMEN EMILOV KOCHLOUKOV

Prof. (a). Dr (a). ALEXEI NIKOLAEVICH KRASSILNIKOV

Prof. (a). Dr (a). FLÁVIO ULHOA COELHO

Prof. (a). Dr (a). PAULO ROBERTO BRUMATTI

Prof. (a) Dr. (a) VYACHESLAV FUTORNY

Agradecimentos

Meus sinceros agradecimentos:

A Deus, pela vida, pela capacidade de pensar e aprender, pela matemática e pela música.

Aos meus pais, Antônio e Celene, e aos meus irmãos, Rosângela e José Roberto, pelo apoio, pelo incentivo e pelo maravilhoso ambiente familiar, no qual o amor, o respeito e o companheirismo sempre estiveram muito presentes.

À minha grande amiga e colega Marisa de Sales Monteiro, cuja satisfação em ensinar e aprender e cujas força interior e nobreza de alma são exemplos para todos.

Ao meu grande amigo, colega e "irmão acadêmico" Sérgio Mota Alves, pelo companheirismo, pelo incentivo e pelas discussões algébricas sempre muito proveitosas, e à sua esposa Maura.

Aos professores Ernesto Trajano e Francisco Júlio Sobreira, por tudo que me ensinaram, pela amizade, pelo apoio e por me encorajarem a estudar matemática através de ótimos cursos e conversas extremamente proveitosas. Ao professor Rudolf Maier, meu orientador de mestrado na Universidade de Brasília, pelo apoio dado ao meu ingresso no curso de doutorado através de uma carta de recomendação.

À Universidade Federal de Campina Grande (UFCG), da qual fui aluno e da qual sou professor com muito orgulho, e especialmente aos meus colegas, professores e funcionários, da Unidade Acadêmica de Matemática e Estatística, particularmente aos professores Rosângela, Florence, José Lindomberg, Claudianor, Marco Aurélio e Daniel Cordeiro, pelo apoio e incentivo. E também às minhas amigas Gracinha e Maria Aldano, professoras do Departamento de Administração e Contabilidade da UFCG.

Aos meus alunos da UFCG, com os quais a convivência foi sempre muito enriquecedora, humana e academicamente.

À toda comunidade do IMECC-UNICAMP, professores, funcionários e alunos da pós-graduação, especialmente ao meu amigo e "irmão acadêmico" José Antônio, pela sua inestimável ajuda nos problemas informáticos.

Ao meu orientador, professor Plamen Koshlukov, pela excelente orientação, pelos valorosos ensinamentos, pela amizade e por deixar um espaço aberto para futuras discussões algébricas que certamente serão imensamente proveitosas.

Ao meu amigo e colega Vânio Fragoso de Melo e à sua famíla, que me receberam em sua casa, dando-me um imenso apoio logo que cheguei em Campinas.

Ao Sr. Luis Antônio (in memoriam), à Dona Regina, ao Flávio, à Lourdes e à Zezinha, que foram para mim uma família aqui em Campinas.

Aos membros da banca examinadora, que avaliaram este trabalho e cujas sugestões ajudaram a melhorá-lo consideravelmente.

À CAPES, pelo apoio financeiro.

Resumo

Neste trabalho apresentamos um estudo sobre polinômios centrais graduados e polinômios centrais com involução para algumas álgebras importantes na PI-teoria sobre corpos infinitos. Mais precisamente, descrevemos os polinômios centrais $\mathbb{Z}_2$-graduados para as álgebras $M_2(K)$ (matrizes 2×2 sobre um corpo K), $M_{1,1}(S)$, onde S é uma álgebra supercomutativa (em particular, obtemos o caso $M_{1,1}(E)$), e $E \otimes E$. Para $M_{1,1}(S)$, apresentamos antes uma classificação em termos de identidades $\mathbb{Z}_2$-graduadas. Aqui E é a álgebra de Grassmann de dimensão infinita com unidade e $M_{1,1}(S)$ é a subálgebra de $M_2(S)$, cujos elementos são as matrizes que têm a diagonal principal com elementos de S_0, a componente par (central) de S, e a diagonal secundária com elementos de S_1, a componente ímpar (anticomutativa) de S. Descrevemos também os polinômios centrais graduados para as álgebras $M_n(K)$ (matrizes $n \times n$ sobre K), considerando suas graduações naturais pelos grupos cíclicos, e finalmente os polinômios centrais com involução para $M_2(K)$, considerando as involuções transposta e simplética.

Abstract

In this thesis we study graded central polynomials and central polynomials with involution for some important algebras in the theory of algebras with polynomial identities, over infinite fields. Namely we describe the $\mathbb{Z}_2$-graded central polynomials for the algebras $M_2(K)$ (the 2×2 matrices over the field K), $M_{1,1}(S)$, where S is an arbitrary supercommutative algebra. In particular we obtain the cases $M_{1,1}(E)$, and furthermore $E \otimes E$. For the case $M_{1,1}(S)$ we first give a classification in terms of $\mathbb{Z}_2$-graded identities. Here E stands for the infinite dimensional Grassmann algebra with 1. Also $M_{1,1}(S)$ is the subalgebra of $M_2(S)$ with elements the matrices whose main diagonal has entries from S_0, the even (central) component of S, and off-diagonal entries from S_1, the odd (anticommutative) component of S. We also describe the graded central polynomials for the algebras $M_n(K)$, the $n \times n$ matrices over K, considering their natural gradings by cyclic groups, and finally the central polynomials with involution for $M_2(K)$, considering the transpose and the symplectic involutions.

Sumário

Introdução

As álgebras são objetos de grande importância na teoria de anéis e dentre elas destacamos as álgebras com identidades polinomiais ou PI-álgebras. Uma identidade polinomial de uma álgebra A é um polinômio $f(x_1, \ldots, x_n)$ 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 (identidade polinomial não trivial), e como exemplos podemos citar as álgebras comutativas, as de dimensão finita e as nilpotentes. Tendo em vista que as identidades polinomiais dizem muito sobre a estrutura de uma álgebra, seu estudo é algo de grande interesse.

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 [24], [25], [37] e [16]), 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 [1], o qual afirma que a álgebra $M_n(K)$ das matrizes $n \times n$ sobre um corpo K satisfaz a identidade "standard" de grau $2n$. Este trabalho é baseado em argumentos combinatórios e, posteriormente, outras demonstrações foram dadas para este teorema usando-se técnicas diversas.

Uma questão central na PI-teoria é a descrição das identidades polinomiais de uma álgebra, ou seja, a determinação de um conjunto gerador do T-ideal (ideal das identidades), ou base das identidades. Em 1950, W. Specht colocou o problema da existência de base finita para as identidades de uma álgebra associativa sobre um corpo de característica zero, que é conhecido como problema de Specht. Kemer, em seu importante trabalho [27, 28] sobre a estrutura dos T-ideais em característica zero, apresentou uma solução positiva para este problema. Contudo, apesar de sua importância e profundidade, o trabalho de Kemer não mostra como determinar uma tal base finita e portanto não resolve o problema da descrição das identidades de uma álgebra, o qual continua em aberto até hoje, tendo sido resolvido apenas para algumas álgebras em particular.

O trabalho de Kemer também trata das importantes álgebras T-primas, que são álgebras cujos T-ideais são T-primos. Ele mostra 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 anti-comutativa de E. Também foi mostrado que em característica zero valem as igualdades $T(E \otimes E) = T(M_{1,1}(E))$, $T(M_{a,b}(E) \otimes E) = T(M_{a+b}(E))$ e $T(M_{a,b}(E) \otimes M_{c,d}(E)) = T(M_{ac+bd,ad+bc}(E))$ (onde $T(A)$ denota o T-ideal das identidades da álgebra A), sendo este resultado conhecido como Teorema do Produto Tensorial de Kemer e do qual segue que o produto tensorial de álgebras T-primas ainda é uma álgebra T-prima.

Ainda se sabe pouco sobre as descrições das identidades das algebras T-primas, apesar de nas últimas décadas terem surgido vários trabalhos neste sentido. As identidades da álgebra de Grassmann E foram descritas em característica zero por Latyshev [34] (o raciocínio usado neste artigo também funciona para corpos infinitos de qualquer característica maior que 2) e por Krakowski e Regev [33] (veja também o artigo [19] para as identidades de E sobre sobre corpos infinitos de característica diferente de 2). A descrição das identidades de $M_n(K)$ é conhecida apenas para $n = 2$ e foi dada por Razmyslov [40] e Drensky [13], em característica zero, e por Koshlukov [30], para corpos infinitos de característica diferente de 2. Em característica zero, geradores das identidades da álgebra $E \otimes E$, e consequentemente da álgebra $M_{1,1}(E)$, foram determinados por Popov [39]. É importante ressaltar 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. Vemos então que as identidades graduadas têm grande importância na PI-teoria e por esta razão se tornaram objetos de estudos independentes.

Por ser um trabalho mais fácil que a descrição das identidades ordinárias, a descrição das identidades graduadas das álgebras T-primas vai mais além. 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. No caso da álgebra E, a descrição das identidades $\mathbb{Z}_2$-graduadas é bem simples e pode ser encontrada no segundo capítulo deste trabalho. As identidades $\mathbb{Z}_2$-graduadas de $M_2(K)$ e de $M_{1,1}(E)$ foram descritas for Di Vincenzo [12], em característica zero, e por Koshlukov e Azevedo [31], para corpos infinitos de característica diferente de 2. Em [31] também foram descritas as identidades $\mathbb{Z}_2$-graduadas de $E \otimes E$. No caso das álgebras $M_n(K)$, ao contrário das identidades ordinárias, as graduadas são bem mais conhecidas. $M_n(K)$ possui graduações naturais pelos grupos $\mathbb{Z}$ e $\mathbb{Z}_n$ e suas identidades $\mathbb{Z}$-graduadas e $\mathbb{Z}_n$-graduadas foram descritas para n qualquer por Vasilovsky [48, 47], em característica zero, e por Azevedo [3, 4], para corpos infinitos.

As identidades com involução também aparecem como um importante tipo de generalização das identidades polinomiais ordinárias. Uma involução (do primeiro tipo) em uma álgebra A é um automorfismo de ordem 2 do espaço vetorial A que satisfaz $(ab)^* = b^*a^*$ para quaisquer a, $b \in A$. Quando se estuda o grupo de Brauer de um corpo K, observa-se que se uma K-álgebra central simples A possui uma involução, então sua classe no grupo de Brauer é o elemento neutro ou tem ordem 2. O problema da descrição das identidades com involução das álgebras T-primas ainda está longe de uma solução, tendo sido resolvido apenas para a álgebra E, por Anisimov [2] em característica zero, e para a álgebra $M_2(K)$ por Levchenko, para $\operatorname{char} K = 0$ [35] e para K finito [36], e por Colombo e Koshlukov [10], para K infinito com $\operatorname{char} K \neq 2$.

Um outro conceito que merece destaque na PI-teoria por sua estreita relação com o de identidade polinomial é o de polinômio central. Um polinômio $f(x_1, \ldots, x_n)$ é dito central para uma álgebra A se resulta em elemento do centro de A quando avaliado em quaisquer elementos desta álgebra. Observe que as identidades polinomiais aparecem como os exemplos mais simples, e são ditas polinômios centrais triviais. Em 1956, Kaplansky [26] apresentou uma lista de problemas em aberto que motivaram muitos pesquisadores nas décadas seguintes. Um destes problemas era sobre a existência de polinômio central não trivial para a álgebra de matrizes $M_n(K)$, com $n > 2$ (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 foi dada em 1972-1973 independentemente por Formanek [17] e Razmyslov [41] (veja também [43]), que provaram a existência de tais polinômios por construção direta. Mais tarde, outros polinômios centrais para $M_n(K)$ foram construídos, veja por exemplo [22], [14] e [20]. Razmyslov também construiu em [43] polinômios centrais para as álgebras $M_{a,b}(E)$ e Belov [6] provou que toda variedade T-prima de álgebras possui um polinômio central.

Assim como a descrição das identidades, a descrição dos polinômios centrais de uma álgebra é uma importante questão na PI-teoria. No entanto, muito pouco se conhece neste sentido. No caso das álgebras $M_n(K)$, geradores dos polinômios centrais são conhecidos apenas para o caso $n = 2$, e foram determinados por Okhitin [38], quando $\operatorname{char} K = 0$, e por Colombo e Koshlukov [9], quando K é infinito de característica diferente de 2. No caso da álgebra de Grassmann, uma descrição dos polinômios centrais em característica zero é apresentada no primeiro capítulo deste trabalho, onde também é apresentada uma demonstração de que os únicos polinômios centrais para $U_n(A)$, a álgebra das matrizes triangulares superiores com entradas numa álgebra associativa com unidade A, são as identidades.

Uma generalização natural dos conceitos de T-ideal e de polinômio central é o de *T-espaço*. Um T-espaço na álgebra associativa livre é um subespaço que é fechado sob os endomorfismos dessa álgebra. Os T-espaços estão sendo estudados por vários algebristas, pois providenciam um meio de estudar as propriedades dos T-ideais através de métodos provenientes da combinatória algébrica. Os estudos sobre T-espaços mostraram-se bastante eficientes nesse sentido. Ressaltamos que, usando-se T-espaços, pode ser obtida uma demonstração relativamente menos sofisticada do Teorema de Kemer sobre a geração finita dos T-ideais em característica 0. Ainda, os primeiros exemplos de T-ideais sem bases finitas de geradores, em característica positiva, foram obtidos estudando-se T-espaços. O leitor interessado pode procurar mais informações no artigo [21]. Aqui ressaltamos somente que, diferentemente das identidades polinomiais, nem todo T-espaço coincide com o conjunto dos polinômios centrais de alguma álgebra.

A importância das álgebras graduadas, das álgebras com involução e do conceito de polinômio central, e o fato de se saber pouco sobre as descrições dos polinômios centrais de álgebras importantes são motivações para o estudo de polinômios centrais graduados e com involução. O presente trabalho tem por objetivo este estudo para álgebras sobre corpos infinitos e está dividido em quatro capítulos. No primeiro são apresentados conceitos e resultados básicos necessários no seu desenvolvimento. No segundo são apresentadas as descrições dos polinômios centrais $\mathbb{Z}_2$-graduados para as álgebras $M_2(K)$, $M_{1,1}(S)$, onde S é uma álgebra supercomutativa, e $E \otimes E$. Também é demonstrado que $M_{1,1}(S)$ tem as mesmas identidades $\mathbb{Z}_2$-graduadas que $M_{1,1}(E)$ ou $M_{1,1}(E_n)$, onde E_n é a álgebra de Grassmann de dimensão 2^n.

O terceiro capítulo é destinado à descrição dos polinômios centrais graduados para $M_n(K)$. Nestas descrições são consideradas as $\mathbb{Z}_n$-graduação e $\mathbb{Z}$-graduação naturais desta álgebra e são usadas as matrizes genéricas graduadas definidas em [3] e [4]. Também é feito, através de métodos combinatórios, um estudo do número de geradores obtidos para os polinômios centrais.

Finalmente, no quarto capítulo é feito primeiramente um estudo sobre álgebras com involução, no qual são apresentados os conceitos de identidade e polinômios central com involução e também a classificação das involuções em álgebras centrais simples. Depois, são apresentadas as descrições dos polinômios centrais com involução para a álgebra $M_2(K)$, considerando as involuções transposta e simplética. Nestas descrições são usadas idéias e resultados de [9] e [10].

Em todas essas descrições de polinômios centrais, as identidades (graduadas ou com involução) das álgebras em questão são de fundamental importância, tanto na composição dos conjuntos geradores, quanto nas "reduções" feitas no sentido de mostrar que um dado polinômio central é realmente conseqüência desses geradores.

Esperamos que este trabalho contribua no sentido de ampliar um pouco o conhecimento acerca dos polinômios centrais das álgebras T-primas e melhorar a compreensão da forma concreta desses polinômios.

Capítulo 1

Conceitos Básicos

Neste capítulo vamos apresentar os conceitos e resultados básicos necessários para o desenvolvimento deste trabalho. Vamos começar falando sobre álgebras, que é o nosso objeto fundamental de estudo. Em todo este capítulo K será sempre um corpo e, a menos de alguma menção em contrário, todas as álgebras e espaços vetoriais serão sobre K.

1.1 Álgebras

Definição 1.1 *Uma K-álgebra é um par $(A, *)$, onde A é um espaço vetorial e $*$ é uma operação em A que é uma aplicação bilinear, ou seja, $* : A \times A \longrightarrow A$ satisfaz*

- $a * (b + c) = (a * b) + (a * c)$
- $(a + b) * c = (a * c) + (b * c)$
- $(\lambda a) * b = a * (\lambda b) = \lambda(a * b)$

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

Na definição acima, $*$ é chamada de produto ou multiplicação. Para simplificar a notação, vamos denotar a K-álgebra $(A, *)$ por A, ficando o produto subentendido, e $a*b$, para a, $b \in A$, vamos denotar simplesmente por ab. Também por simplicidade, vamos usar a expressão álgebra ao invés de K-álgebra. 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 $a_i \in A$. Dizemos que um subconjunto β é uma base da álgebra A se β é uma base de A como espaço vetorial e definimos a *dimensão de A* como sendo a dimensão de A como espaço vetorial.

Uma álgebra A é dita:

- *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, ou seja, se existe $1 \in A$

tal que $1a = a1 = a$ para todo $a \in A$.

- *álgebra de Lie* se $a^2 = aa = 0$ e $(ab)c + (bc)a + (ca)b = 0$ (identidade de Jacobi) para quaisquer a, b, $c \in A$.
- *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 $a_1a_2 \ldots a_na_{n+1} = 0$ 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.

De agora em diante, a menos que mencionemos o contrário, todas as álgebras serão associativas e com unidade. Em toda álgebra A, sendo 1 sua unidade e $\lambda \in K$, identificamos naturalmente $\lambda 1$ com λ e $\{\lambda 1 \mid \lambda \in K\}$ com K. Vejamos alguns exemplos importantes.

Exemplo 1.2 Para $n \in \mathbb{N}$, o espaço vetorial $M_n(K)$ de todas as matrizes $n \times n$ com entradas em K, munido do produto usual de matrizes, é uma álgebra associativa com unidade de dimensão n^2. 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 $M_n(K)$.

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 de matrizes em $M_n(A)$ é análogo ao produto de matrizes com entradas em K. Temos então uma estrutura de álgebra em $M_n(A)$.

Exemplo 1.3 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 $E(V)$ (ou simplesmente 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 $e_i^2 = 0$ e $e_ie_j = -e_je_i$ para quaisquer i, $j \in \mathbb{N}$. Destacamos em E os subespaços vetoriais E_0, gerado pelo conjunto $\{1,\ e_{i_1}e_{i_2}\ldots e_{i_m} \mid m \text{ par}\}$, e E_1, gerado pelo conjunto $\{\ e_{i_1}e_{i_2}\ldots e_{i_k} \mid k \text{ ímpar}\}$. Claramente, $E = E_0 \oplus E_1$ como espaço vetorial. De $e_ie_j = -e_je_i$ segue que $(e_{i_1}\ldots e_{i_m})(e_{j_1}\ldots e_{j_k}) = (-1)^{mk}(e_{j_1}\ldots e_{j_k})(e_{i_1}\ldots e_{i_m})$ para quaisquer 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 $\operatorname{char} K = 2$, então E é uma álgebra comutativa.

Tomando agora E' como sendo 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*.

Exemplo 1.4 Seja A uma álgebra e consideremos o espaço vetorial

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

Definindo em $K \oplus A$ o produto $(\lambda_1, a_1)(\lambda_2, a_2) = (\lambda_1\lambda_2, \lambda_1a_2 + \lambda_2a_1 + a_1a_2)$, temos que $K \oplus A$ é uma álgebra associativa com unidade (que é o elemento $(1, 0)$). Esta construção é chamada de *adjunção formal da unidade a* A.

Observação 1.5 Se A é um espaço vetorial, β é uma base de A e $f : \beta \times \beta \longrightarrow A$ é uma aplicação qualquer, então existe uma única aplicação bilinear $F : A \times A \longrightarrow A$ estendendo f. 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, $(v_1v_2)v_3 = v_1(v_2v_3)$ para quaisquer v_1, v_2, $v_3 \in \beta$. Isto se deve ao fato de que a aplicação $g : A \times A \times A \longrightarrow A$, definida por $g(a, b, c) = (ab)c - a(bc)$, sendo trilinear, é nula se, e somente se, é nula em $\beta \times \beta \times \beta$.

Exemplo 1.6 Produto tensorial de álgebras. Sejam A e B duas álgebras. Recordamos que o produto tensorial dos espaços vetoriais A e B, denotado por $A \otimes B$, é o espaço vetorial que consiste dos elementos da forma $\sum u_i \otimes v_i$ para $u_i \in A$ e $v_i \in B$. Os elementos $a \otimes c$ (tensores) satisfazem $(a + c) \otimes b = (a \otimes b) + (c \otimes b)$, $a \otimes (b + d) = (a \otimes b) + (a \otimes d)$ e $\lambda a \otimes b = a \otimes \lambda b = \lambda(a \otimes b)$ para quaisquer a, $b \in A$, c, $d \in B$ e $\lambda \in K$. É um fato bem conhecido que se β_1 e β_2 são bases de A e B, respectivamente, então o conjunto $\beta = \{u \otimes v \mid u \in \beta_1,\ v \in \beta_2\}$ é uma base de $A \otimes B$. Se V é um espaço vetorial e $f : A \times B \longrightarrow V$ é uma aplicação bilinear, então existe uma única transformação linear $\varphi : A \otimes B \longrightarrow V$ satisfazendo $\varphi(a \otimes b) = f(a, b)$ (propriedade universal do produto tensorial). Para maiores detalhes, veja [11], Capítulo II, §12.

Para definir uma estrutura de álgebra em $A \otimes B$, fixemos duas bases β_1 e β_2 de A e B, respectivamente, e definimos $(u_1 \otimes v_1)(u_2 \otimes v_2) = u_1u_2 \otimes v_1v_2$. Temos que $A \otimes B$, munido deste produto, é uma álgebra associativa, o que é fácil ver pela Observação 1.5. Ademais, o elemento $1_A \otimes 1_B$ é a unidade desta álgebra.

Tomando agora a_1, $a_2 \in A$ e b_1, $b_2 \in B$ elementos quaisquer e escrevendo-os como combinações lineares dos elementos de β_1 e β_2, respectivamente, podemos ver facilmente que $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2$. Temos então que a definição do produto independe da escolha das bases.

Se A é uma álgebra associativa e a, $b \in A$, definimos o *comutador* $[a, b] = ab - ba$ e, se $\operatorname{char} K \neq 2$, o *produto de Jordan* $a \circ b = \frac{1}{2}(ab + ba)$. Definimos também *o comutador de comprimento* n como sendo $[a_1, \ldots, a_{n-1}, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$ para $a_i \in A$. Através de um cálculo simples, podemos mostrar que para quaisquer a, b, $c \in A$ vale

$$[ab, c] = a[b, c] + [a, c]b. \tag{1.1}$$

Ademais, usando indução e (1.1), é possível mostrar que

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

Definição 1.7 *Seja A uma álgebra. Dizemos que um subespaço vetorial B de A é uma subálgebra de A se $BB \subseteq B$ e $1 \in B$. Dizemos que um subespaço vetorial I de A é um ideal de A se $AI \subseteq I$ e $IA \subseteq I$.*

Exemplo 1.8 Considere a álgebra exterior E (Exemplo 1.3). Dado $n \in \mathbb{N}$, tomemos o subespaço E_n de E gerado pelo conjunto $\{1,\ e_{i_1}e_{i_2}\dots e_{i_k} \mid i_1 < i_2 < \dots < i_k \leq n\}$. Temos que 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 1.9 Centro de uma álgebra. Sendo A uma álgebra, o conjunto

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

é uma importante subálgebra de A, chamada de *centro de A*. É um fato bem conhecido que para todo $n \in \mathbb{N}$ vale $Z(M_n(K)) = \{\lambda I_{n\times n} \mid \lambda \in K\}$ (matrizes escalares). Quanto à álgebra de Grassmann, observando o Exemplo 1.3 podemos concluir que $Z(E) = E_0$ ($\operatorname{char} K \neq 2$).

Exemplo 1.10 Subálgebra gerada. Sejam A uma álgebra de $S \subseteq A$. Consideremos o subespaço B_S de A gerado pelo conjunto $\{1,\ s_1s_2\dots s_k \mid k \in \mathbb{N},\ s_i \in S\}$. Temos que B_S é multiplicativamente fechado e que $1 \in B_S$. Logo, B_S é uma subálgebra de A, chamada de *subálgebra gerada por S*. Observe que toda subálgebra de A que contém S deve conter B_S e assim B_S é a *menor subálgebra de A contendo S*.

Definição 1.11 *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 $\varphi(1_A) = 1_B$.*

Se φ é um homomorfismo de álgebras, dizemos que é um *mergulho* (ou *monomorfismo*) se é injetivo, e que é um *isomorfismo* se é bijetivo. Um *endomorfismo* de uma álgebra A é um homomorfismo de A em A e um *automorfismo* é um endomorfismo bijetivo (endomorfismo e isomorfismo ao mesmo tempo). Denotamos por *End A* e *Aut A* os conjuntos dos endomorfismos e automorfismos, respectivamente, da álgebra A. Quando existe um isomorfismo $\varphi : A \longrightarrow B$, dizemos que as álgebras A e B são *isomorfas* e denotamos $A \simeq B$. Como exemplo, observamos que as álgebras E e $K \oplus E'$ (Exemplo 1.4) são isomorfas, sendo $\psi : K \oplus E' \longrightarrow E$, definida por $\psi(\lambda, x) = \lambda + x$, um isomorfismo.

Se $\varphi : A \longrightarrow B$ é um homomorfismo de álgebras, o conjunto $\ker \varphi = \{a \in A \mid \varphi(a) = 0\}$, *núcleo de φ*, é um ideal de A, e o conjunto $Im\varphi = \{\varphi(a) \mid a \in A\}$, *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 faz de A/I uma álgebra, chamada de *álgebra quociente de A por I.* Vamos denotar $a + I$ por $\overline{a}$. A aplicação $\pi : A \longrightarrow A/I$, definida por $\pi(a) = \overline{a}$, é um homomorfismo chamado de *projeção canônica.*

É um fato bem conhecido que se $\varphi : A \longrightarrow B$ é um homomorfismo de álgebras, então $A/\ker\varphi \simeq Im\varphi$.

Definição 1.12 *Seja A uma álgebra. Dizemos que A é simples se $\{0\}$ e A são seus únicos ideais. Dizemos que A é central simples se A é simples e $Z(A) = K$.*

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

Proposição 1.13 *Se A é uma álgebra central simples de dimensão finita, então todo automorfismo de A é interno.*

Este resultado é uma conseqüência imediata do Teorema de Skolem-Noether, cuja demonstração pode ser encontrada em [23], página 99.

1.2 Identidades polinomiais

Seja $X = \{x_1, x_2, x_3, \ldots\}$ um conjunto enumerável, cujos elementos vamos chamar de *variáveis*. Uma *palavra* em X é uma seqüência $x_{i_1}x_{i_2}\ldots x_{i_n}$ onde $n \in \mathbb{N}$ e $x_{i_j} \in X$. Vamos também considerar a palavra vazia, que denotaremos por 1. Tomemos $K\langle X\rangle$ como sendo o espaço vetorial que tem como base o conjunto de todas as palavras em X. Assim, 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 agora em $K\langle X\rangle$ a multiplicação definida por

$$(x_{i_1}x_{i_2}\ldots x_{i_n})(x_{j_1}x_{j_2}\ldots x_{j_m}) = x_{i_1}x_{i_2}\ldots x_{i_n}x_{j_1}x_{j_2}\ldots x_{j_m}.$$

Munido deste produto, $K\langle X\rangle$ é uma álgebra associativa (veja a Observação 1.5) com unidade, que é a palavra vazia 1.

Sejam A uma álgebra e $h : X \longrightarrow A$ uma aplicação qualquer, com $h(x_i) = a_i$ para $i \in \mathbb{N}$. Consideremos agora a aplicação linear $\varphi_h : K\langle X\rangle \longrightarrow A$ tal que $\varphi(1) = 1_A$ e $\varphi(x_{i_1}x_{i_2}\ldots x_{i_n}) = a_{i_1}a_{i_2}\ldots a_{i_n}$. Temos que φ_h é um homomorfismo de álgebras e é o único satisfazendo $\varphi_h|_X = h$. Dizemos então que $K\langle X\rangle$ é a *álgebra associativa livre unitária, livremente gerada por X.* Sendo $f = f(x_1, \ldots, x_n) \in K\langle X\rangle$, vamos denotar por $f(a_1, \ldots, a_n)$

a imagem de f por φ_h. Observe que $f(a_1, \ldots, a_n)$ é o elemento de A obtido substituindo-se x_i por a_i em f.

Definição 1.14 *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 de A se $f(a_1, \ldots, a_n) = 0$ para quaisquer $a_1, \ldots, a_n \in A$.*

Observemos então que $f = f(x_1, \ldots, x_n)$ é uma identidade 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* se $T(A) \neq \{0\}$. Se A_1 e A_2 são álgebras, dizemos que A_1 e A_2 são *PI-equivalentes* se $T(A_1) = T(A_2)$.

Exemplo 1.15 Se A é uma álgebra comutativa, então o polinômio $f(x_1, x_2) = [x_1, x_2] = x_1x_2 - x_2x_1$ é uma identidade de A.

Exemplo 1.16 O polinômio $[x_1, x_2, x_3]$ é uma identidade polinomial da álgebra de Grassmann E. Para ver isto, basta observar que $[a, b] \in E_0 = Z(E)$ para quaisquer a, $b \in E$.

Exemplo 1.17 Considere o polinômio

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

onde S_n é o grupo simétrico sobre n elementos, $\varepsilon_\sigma = 1$ se σ é par, e $\varepsilon_\sigma = -1$ se σ é ímpar, é chamado de *polinômio standard de grau n*. Em [1] foi provado que $s_{2n}(x_1, \ldots, x_{2n}) \in T(M_n(K))$, fato conhecido como Teorema de Amitsur-Levitzki. Posteriormente, foram apresentadas outras demonstrações deste teorema (veja [32], [46], [42] e [44]).

O conceito que apresentaremos agora e suas propriedades são de extrema importância na PI-teoria.

Definição 1.18 *Dizemos que um ideal I de $K\langle X\rangle$ é um T-ideal se $\varphi(I) \subseteq I$ para todo $\varphi \in End\ K\langle X\rangle$, 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 1.19 *Se A é uma álgebra, então $T(A)$ 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 $T(B) = I$.*

Demonstração. Primeiramente, é fácil ver que $T(A)$ é um ideal de $K\langle X\rangle$. Agora, sejam $f = f(x_1, \ldots, x_n) \in T(A)$ e $\varphi \in End\ K\langle X\rangle$, arbitrários. Provemos que $\varphi(f) \in T(A)$. De fato, se $\psi : K\langle X\rangle \longrightarrow A$ é um homomorfismo qualquer de álgebras, então $\psi(\varphi(f)) = (\psi \circ \varphi)(f) = 0$ pois $\psi \circ \varphi : K\langle X\rangle \longrightarrow A$ é um homomorfismo de álgebras e $f \in T(A)$. Assim, $\varphi(f) \in \ker \psi$ e daí $\varphi(f) \in T(A)$.

Sendo 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 deve pertencer a $\ker \pi$. Como $\ker \pi = I$, devemos ter $T(B) \subseteq I$. 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, $f(g_1, \ldots, g_n) \in T(B)$, o que conclui a demonstração. □

Não é difícil ver que a interseção de uma família qualquer de T-ideais é ainda um T-ideal. Logo, dado um subconjunto S qualquer de $K\langle X\rangle$, podemos definir 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 contêm S. Assim, $\langle S\rangle^T$ é o *menor* T-ideal de $K\langle X\rangle$ 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 existe S finito nestas condições, dizemos que A possui a *propriedade da base finita* ou *propriedade de Specht* (W. Specht). A questão da existência de base finita para as identidades das álgebras associativas sobre corpos de característica zero é conhecida como *problema de Specht* e, em [28], Kemer deu uma solução positiva para este problema. Vejamos agora alguns exemplos de bases de identidades de algumas álgebras importantes.

Exemplo 1.20 Se A é uma álgebra comutativa qualquer e K é um corpo infinito, então é um fato bem conhecido que $T(A) = \langle [x_1, x_2]\rangle^T$. Dizemos então que todas as identidades de A seguem (ou são conseqüências) do polinômio $[x_1, x_2]$.

Exemplo 1.21 Se K é um corpo infinito de característica diferente de 2, então $T(E) = \langle [x_1, x_2, x_3]\rangle^T$ (veja [33] e [19]).

Exemplo 1.22 Em 1973 Razmyslov [40] provou que $T(M_2(K))$ é finitamente gerado para $\operatorname{char} K = 0$, determinando uma base com 9 identidades. Posteriormente, Drensky [13] 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 para $\operatorname{char} K = 0$. Em 2001 Koshlukov [30] generalizou este resultado de Drensky para K infinito de característica diferente de 2 e 3. Quando $\operatorname{char} K = 3$, uma terceira identidade é necessária para gerar o T-ideal (veja [9]). Para $\operatorname{char} K = 2$, o problema da descrição de $T(M_2(K))$ ainda está em aberto.

1.3 Variedades e álgebras livres

Definição 1.23 *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.*

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 1.24 (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 [15], página 24. □

Seja $\mathcal{V}$ uma variedade de álgebras. Dizemos que uma álgebra $F \in \mathcal{V}$ é uma *álgebra relativamente livre de* $\mathcal{V}$ (de posto enumerável) se existe um subconjunto Y (enumerável) gerador de F tal que para toda álgebra $A \in \mathcal{V}$ e toda aplicação $h : Y \longrightarrow A$ existe um homomorfismo de álgebras $\varphi : F \longrightarrow A$ estendendo h. F é então dita ser *livremente gerada por* Y.

Teorema 1.25 *Toda variedade $\mathcal{V}$ possui alguma álgebra relativamente livre. Ademais, duas álgebras relativamente livres de $\mathcal{V}$ são isomorfas.*

Demonstração. Seja $I = \bigcap_{R\in\mathcal{V}} T(R)$ e considere a álgebra quociente $F = K\langle X\rangle/I$. Tomando $Y = \{\overline{x} \mid x \in X\}$, temos que F é gerada por Y e que Y é enumerável (para $i \neq j$ temos $x_i - x_j \notin I$). Tomando agora uma álgebra $A \in \mathcal{V}$ e uma aplicação $h : Y \longrightarrow A$, consideremos $\psi : K\langle X\rangle \longrightarrow A$ o homomorfismo de álgebras que satisfaz $\psi(x) = h(\overline{x})$ para todo $x \in X$. Como $I \subseteq T(A)$, temos que $I \subseteq \ker\psi$ e assim a aplicação $\varphi : F \longrightarrow A$, dada por $\varphi(\overline{f}) = \psi(f)$, é bem definida. Além disso, φ é um homomorfismo de álgebras que estende h.

Suponhamos agora F_1 e F_2 álgebras relativamente livres de $\mathcal{V}$. 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 maiores detalhes, veja [15], Seções 1.2, 2.2 e 2.3.

1.4 Álgebras envolventes

Seja A uma álgebra associativa e considere em A o novo produto $[a,b]=ab-ba$ para a, $b\in A$. Com este produto temos uma nova estrutura de álgebra em A, que vamos denotar por $A^{(-)}$. Como $[a,a]=0$ e $[a,b,c]+[b,c,a]+[c,a,b]=0$ (identidade de Jacobi) para quaisquer a, b, $c\in A$, temos 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 1.26 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 de Lie.

Seja L uma álgebra de Lie. Dizemos que uma álgebra associativa U é uma *álgebra universal envolvente de* L se L é uma subálgebra de $U^{(-)}$ e para toda álgebra associativa A e todo homomorfismo $\phi:L\longrightarrow A^{(-)}$ de álgebras de Lie, existe um único homomorfismo de álgebras associativas $\psi:U\longrightarrow A$ tal que $\psi|_L=\phi$.

Teorema 1.27 (Poincaré, Birkhoff, Witt) *Toda álgebra de Lie L possui uma única (a menos de isomorfismo) álgebra universal envolvente $U(L)$. Se L possui uma base $\{e_i\mid i\in I\}$, sendo I totalmente ordenado, então $U(L)$ possui uma base formada pelos elementos*

$$e_{i_1}e_{i_2}\dots e_{i_p}\quad,\quad \textit{com } i_1\leq i_2\leq\dots\leq i_p\ ,\ i_k\in I \textit{ e } p=0,1,2,\dots$$

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

Demonstração. Veja [15], página 11. □

Sendo $X=\{x_1,x_2,x_3,\dots\}$, tomemos $ComX=\{[x_{i_1},x_{i_2},\dots,x_{i_k}]\mid k\geq 2\ ,\ x_{i_j}\in X\}$. Sejam $B(X)$ a subálgebra (com 1) 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 $K\langle X\rangle^{(-)}$. Usando a identidade de Jacobi é possível mostrar que se u, $v\in X\cup ComX$, então $[u,v]\in L(X)$. Logo, $L(X)$ é uma subálgebra de Lie de $K\langle X\rangle^{(-)}$.

Teorema 1.28 (Witt) $U(L(X))=K\langle X\rangle$.

Demonstração. Veja [15], página 14, Teorema 1.3.5. □

Se L é uma álgebra de Lie e $h : X \longrightarrow L$ é uma aplicação qualquer, tomemos o homomorfismo de álgebras $\varphi : K\langle X\rangle \longrightarrow U(L)$ que estende 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 $\varphi(L(X)) \subseteq L$. Ademais, é fácil 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 estendendo h e assim chamamos $L(X)$ de *álgebra de Lie livre, livremente gerada por* X.

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

$$x_1,\ x_2,\ x_3,\ \ldots,\ x_n,\ \ldots, u_1,\ u_2,\ u_3,\ \ldots,\ u_m,\ \ldots$$

onde $\{u_1, u_2, u_3, \ldots\} \subseteq ComX$ é uma base de $[L(X), L(X)]$, o subespaço vetorial de $L(X)$ gerado por $ComX$. Segue dos Teoremas 1.27 e 1.28 que $K\langle X\rangle$ possui uma base formada pelos elementos

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

onde $i_1 < i_2 < \ldots < i_k$, $j_1 \leq j_2 \leq \ldots \leq j_q$. Observe 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

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

onde $a = (a_1, a_2, \ldots, a_n)$, $a_i \geq 0$, $\alpha_a \in K$ e $g_a \in B(X)$. Ademais, pela independência linear dos elementos em (1.3), temos que f possui uma única expressão nesta forma.

1.5 Polinômios multi-homogêneos e multilineares

Definição 1.29 *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.*

Se $m = m(x_1, x_2, \ldots, x_k)$ é um monômio de $K\langle X\rangle$, definimos o *multigrau* de m como sendo a k-upla $(a_1, a_2, \ldots, a_k)$ onde $a_i = \deg_{x_i} m$. Se $f \in K\langle X\rangle$, a soma de todos os monômios de f com um dado multigrau é dita ser uma *componente multi-homogênea* de f. Observe então que f é multi-homogêneo se, e somente se, possui uma única componente multi-homogênea.

O próximo resultado nos dá uma importante ferramenta no trabalho de determinar geradores para T-ideais quando K é infinito.

Proposição 1.30 *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 $i = 0, 1, \ldots, n$, tomemos $f_i(x_1, x_2, \ldots, x_k)$ 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 $f = f_0 + f_1 + \ldots + f_n$. Como K é infinito, podemos escolher $\lambda_0, \lambda_1, \ldots, \lambda_n \in K$ todos distintos. Para cada $j = 0, 1, \ldots, m$, temos $g_j = f(\lambda_j x_1, x_2, \ldots, x_k) = f_0 + \lambda_j f_1 + \ldots + \lambda_j^n f_n$ e assim

$$\begin{pmatrix} 1 & \lambda_0 & \cdots & \lambda_0^n \\ 1 & \lambda_1 & \cdots & \lambda_1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^n \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_n \end{pmatrix}$$

Observe que $g_0, g_1, \ldots, g_n \in I$, pois I é T-ideal. Ademais, a primeira matriz na igualdade acima é uma matriz de Vandermonde invertível. Logo, devemos ter $f_0, f_1, \ldots, f_m \in I$.

Agora, para cada $i = 0, 1, \ldots, n$ e cada $t = 0, 1, 2, \ldots$, tomemos f_{it} como sendo a componente homogênea em f_i de grau t em x_2. Usando então os mesmos argumentos acima, concluímos que $f_{it} \in I$ 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. □

Dizemos que um polinômio $f(x_1, x_2, \ldots, x_k) \in K\langle X\rangle$ é *multilinear* se é multi-homogêneo com multigrau $(1, 1, \ldots, 1)$, ou seja, se em cada monômio cada variável tem grau exatamente 1. Neste caso, f tem a forma

$$\sum_{\sigma \in S_k} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(k)} \quad , \text{ com } \alpha_\sigma \in K.$$

Suponhamos $f(x_1, x_2, \ldots, x_k) \in K\langle X\rangle$ multi-homogêneo de grau n em x_1. Tomando y_1 e y_2 variáveis de X distintas de $x_1, x_2, \ldots, x_k$, consideremos o polinômio $h(y_1, y_2, x_2, \ldots, x_k) = f(y_1+y_2, x_2, \ldots, x_k)$. Tomando $h_1(y_1, y_2, x_2, \ldots, x_k)$ como sendo a componente homogênea de grau 1 em y_1 de $h(y_1, y_2, x_2, \ldots, x_k)$, temos que $\deg_{y_2} h_1 = n-1$ e que $h_1(x_1, x_1, x_2, \ldots, x_k) = nf(x_1, x_2, \ldots, x_k)$.

De posse dessas idéias, vamos agora provar o seguinte resultado.

Proposição 1.31 *Se I é um T-ideal de $K\langle X\rangle$ e $\operatorname{char} K = 0$, então I é gerado por seus polinômios multilineares.*

Demonstração. Como $\operatorname{char} K = 0$, temos que K é infinito e portanto I é gerado por seus polinômios multi-homogêneos. Seja então $f(x_1, x_2, \ldots, x_k) \in I$ multi-homogêneo. Como I é T-ideal, temos $h(y_1, y_2, x_2, \ldots, x_k) = f(y_1 + y_2, x_2, \ldots, x_k) \in I$ e daí, como K é infinito, $h_1(y_1, y_2, x_2, \ldots, x_k) \in I$. Da igualdade $h(x_1, x_1, x_2, \ldots, x_k) = nf(x_1, x_2, \ldots, x_k)$ e da hipótese de $\operatorname{char} K = 0$ segue que f é conseqüência de $h_1(y_1, y_2, x_2, \ldots, x_k)$. Tomemos agora $h_2(y_1, y_2, y_3, y_4, x_3, \ldots, x_k)$ como sendo a componente de grau 1 em y_3 de $h_1(y_1, y_2, y_3 + y_4, x_3, \ldots, x_k)$. Usando as mesmas idéias, concluímos que $\deg_{y_4} h_2 = \deg_{x_2} h_1 - 1$, $h_2 \in I$ e h_1 é conseqüência de h_2. Continuando com este processo (chamado de *processo de linearização*), concluímos que f é conseqüência de algum polinômio multilinear de I e assim o resultado está demonstrado. $\square$

1.6 T-espaços e polinômios centrais

Definição 1.32 *Sejam A uma álgebra e $f(x_1, \ldots, x_n) \in K\langle X \rangle$. Dizemos que f é um polinômio central para A se f tem termo constante nulo e $f(a_1, \ldots, a_n) \in Z(A)$ para quaisquer $a_1, \ldots, a_n \in A$.*

De acordo com esta definição, dizer que f é um polinômio central para A significa dizer que $[f, g]$ é uma identidade de A para todo polinômio $g \in K\langle X \rangle$. Segue então que se duas álgebras são PI-equivalentes, então elas têm exatamente os mesmos polinômios centrais. Vejamos agora alguns exemplos.

Exemplo 1.33 Sendo A uma álgebra, toda identidade de A é um polinômio central para A. As identidades são ditas polinômios centrais triviais. Conforme veremos mais adiante, a álgebra $U_n(A)$ $(n \geq 2)$ das matrizes triangulares superiores com entradas em A não possui polinômios centrais além dos triviais.

Exemplo 1.34 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 $M_2(K)$. Okhitin [38] descreveu os polinômios centrais para a álgebra $M_2(K)$, no caso de $\operatorname{char} K = 0$, e Colombo e Koshlukov [9] generalizaram esta descrição para o caso de K ser um corpo infinito de característica diferente de 2.

Exemplo 1.35 Sejam K um corpo qualquer e E a álgebra exterior sobre K. Temos que $f(x_1, x_2) = [x_1, x_2]$ é um exemplo de polinômio central para E. No caso de $\operatorname{char} K = p > 0$, temos que $g(x) = x^p$ é um polinômio central para E. Mais adiante, apresentaremos a descrição dos polinômios centrais para E quando $\operatorname{char} K = 0$.

Definição 1.36 *Um subespaço V de $K\langle X \rangle$ é dito ser um T-espaço se $\varphi(V) \subseteq V$ para todo $\varphi \in End\ K\langle X \rangle$.*

Sabemos que dado um subconjunto $\{f_i \mid i \in \mathbb{N}\}$ de $K\langle X\rangle$, existe um único endomorfismo φ de $K\langle X\rangle$ tal que $\varphi(x_i) = f_i$ para todo $i \in \mathbb{N}$. Assim, dizer que que V é um T-espaço de $K\langle X\rangle$ significa dizer que V é um subespaço tal que $f(g_1, \ldots, g_n) \in V$ para quaisquer $f(x_1, \ldots, x_n) \in V$ e $g_1, \ldots, g_n \in K\langle X\rangle$. Vejamos agora alguns exemplos de T-espaços importantes.

Exemplo 1.37 Todo T-ideal de $K\langle X\rangle$ é um T-espaço. O subespaço $K = \{\alpha 1 \mid \alpha \in K\}$ é também um exemplo de T-espaço de $K\langle X\rangle$.

Exemplo 1.38 Sejam A uma K-álgebra e W um subespaço de A. O conjunto

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

é um T-espaço de $K\langle X\rangle$.

No exemplo anterior, destacamos o caso particular $W = Z(A)$, no qual temos nosso maior interesse. Neste caso 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 chamado de *espaço dos polinômios centrais* de A e é normalmente denotado por $C(A)$. Como $Z(A)$ é uma subálgebra de A, temos que $C(A)$ é multiplicativamente fechado, condição que nem todo T-espaço satisfaz, como veremos mais adiante.

Observação 1.39 É importante observar que os elementos de $C(A)$ são na verdade da forma $g+C$, onde g é um polinômio central (de acordo com a Definição 1.32), e C é uma constante. É também importante observar que o conjunto dos polinômios centrais propriamente ditos de alguma álgebra pode não ser um T-espaço. No Exemplo 1.35, considerando $\operatorname{char} K = p$, vimos que $g(x) = x^p$ é um polinômio central para E. No entanto, $g(x+1) = x^p + 1$ possui termo constante não nulo.

É fácil ver que a interseção e a soma de uma família qualquer de T-espaços ainda são T-espaços. Dado então um subconjunto S de $K\langle X\rangle$, podemos definir o *T-espaço gerado por S* como sendo a interseção de todos os T-espaços que contêm S. Em outras palavras, estamos tomando o *menor T-espaço* de $K\langle X\rangle$ que contém S. A próxima proposição nos dá uma caracterização (mais interessante do ponto de vista prático) do T-espaço gerado por um conjunto.

Proposição 1.40 *Se $S \subseteq K\langle X\rangle$ e V é o T-espaço de $K\langle X\rangle$ gerado por S, então V é exatamente 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. Comecemos observando que este conjunto é exatamente igual a

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

Tomemos 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 $\varphi(f) \in V$ para quaisquer $f \in S$ e $\varphi \in End\ K\langle X\rangle$, ou seja, $(End\ K\langle X\rangle)S \subseteq V$. Logo, $V_1 \subseteq V$.

Observando agora que $\psi(g) \in (End\ K\langle X\rangle)S$ para quaisquer $\psi \in End\ K\langle X\rangle$ e $g \in (End\ K\langle X\rangle)S$, concluímos que V_1 é um T-espaço de $K\langle X\rangle$. Ademais, temos $S \subseteq V_1$. Logo, $V \subseteq V_1$, o que conclui a demonstração. □

Exemplo 1.41 Sejam $S \subseteq K\langle X\rangle$ e J o T-ideal gerado por S. Tomando

$$S_1 = \{x_{n+1}f(x_1, \ldots, x_n)x_{n+2} \mid f \in S\}$$

temos que J é exatamente o T-espaço de $K\langle X\rangle$ gerado por S_1. Assim, a partir de uma base de um T-ideal é possível construir um conjunto capaz de gerá-lo *como T-espaço*.

Observação 1.42 Sabemos que todo T-ideal é gerado por seus polinômios multilineares quando o corpo base tem característica zero, e por seus polinômios multi-homogêneos quando o corpo base é infinito. Essas técnicas de redução são extremamente importantes quando trabalhamos com identidades polinomiais e, conforme veremos, também no estudo de polinômios centrais. Através dos mesmos processos usados para T-ideais é possível mostrar que todo T-espaço é gerado por seus polinômios multilineares no caso de característica zero, e por seus polinômios multi-homogêneos no caso de corpo base infinito.

Nos próximos exemplos vamos ver as descrições de alguns T-espaços interessantes.

Exemplo 1.43 Seja K um corpo e consideremos a álgebra $M_n(K)$, com $n \geq 2$. Sejam I o T-ideal das identidades de $M_n(K)$ e

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

Temos que V é um T-espaço de $K\langle X\rangle$ e que $I \subseteq V$. Ademais, $[x_1, x_2] \in V$ e daí $I + V_1 \subseteq V$, onde V_1 é o T-espaço gerado pelo polinômio $[x_1, x_2]$. Mostremos agora que quando char $K = 0$ temos $V = I + V_1$. De fato, tomemos

$$f(x_1, \ldots, x_m) = \sum_{\sigma \in S_m} \alpha_\sigma x_{\sigma(1)} \ldots x_{\sigma(m)} \in V$$

lembrando que V é gerado por seus polinômios multilineares. Observemos que, para todo $\sigma \in S_m$,

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

onde $\sigma(i) = 1$. Logo, $f(x_1, \ldots, x_m) \equiv x_1 g(x_2, \ldots, x_m) \pmod{V_1}$, onde g é um polinômio multilinear. Como $V_1 \subseteq V$ e $f \in V$, devemos ter $x_1 g(x_2, \ldots, x_m) \in V$, o que significa $tr(A_1 g(A_2, \ldots, A_m)) = 0$ para quaisquer A_1, A_2, $\ldots$, $A_m \in M_n(K)$. Mas, isto só é possível se $g(A_2, \ldots, A_m) = 0$ para quaisquer A_2, $\ldots$, $A_m \in M_n(K)$. Logo, $x_1 g(x_2, \ldots, x_m)$ deve ser identidade de $M_n(K)$ e portanto $f \in I + V_1$.

No caso $n = 2$, temos uma descrição completa de V, uma vez que se conhece uma base finita do T-ideal I. Observando o Exemplo 1.22, podemos concluir que os polinômios

$$x_5 s_4(x_1, x_2, x_3, x_4) x_6 \quad , \quad x_4[[x_1, x_2]^2, x_3] x_5 \quad , \quad [x_1, x_2]$$

geram V como T-espaço.

É fácil ver que V não é multiplicativamente fechado. Basta observar que $[x_1, x_2]^2 \notin V$, fato que se verifica facilmente tomando $x_1 = E_{12} - E_{21}$ e $x_2 = E_{22}$.

Exemplo 1.44 Sejam $n \geq 2$ e A uma álgebra qualquer. No Exemplo 1.33, mencionamos que os únicos polinômios centrais para a álgebra $U_n(A)$ são as identidades. Para demonstrar este fato, comecemos considerando os subespaços $\mathcal{D}$ (matrizes diagonais) e $\mathcal{N}$ (matrizes com diagonal nula) de $U_n(A)$. Temos que $\mathcal{D}$ é uma subálgebra e $\mathcal{N}$ é um ideal de $U_n(A)$. Ademais, $U_n(A) = \mathcal{D} \oplus \mathcal{N}$ como espaço vetorial. Temos também que o centro de $U_n(A)$ é exatamente o conjunto das matrizes da forma $aI_{n\times n}$, onde $a \in Z(A)$.

Tomemos $f(x_1, \ldots, x_m) \in K\langle X \rangle$ um polinômio central para $U_n(A)$. Primeiramente, vejamos que f é uma identidade de $\mathcal{D}$. De fato, dados a_1, $\ldots$, $a_m \in A$, temos que $f(a_1 E_{11}, \ldots, a_m E_{11}) = f(a_1, \ldots, a_m) E_{11}$. Mas, como f é central para $U_n(A)$, devemos ter $f(a_1, \ldots, a_m) E_{11} = aI_{n\times n}$ para algum $a \in Z(A)$. Logo, a deve ser nulo e portanto $f(a_1, \ldots, a_m) = 0$. Segue então que $f \in T(A)$ e daí é imediato que $f \in T(\mathcal{D})$. Tomando agora $X_1, \ldots, X_m \in U_n(A)$, temos $X_i = D_i + N_i$, com $D_i \in \mathcal{D}$ e $N_i \in \mathcal{N}$, e assim $f(X_1, \ldots, X_m) = f(D_1, \ldots, D_m) + C = C$, onde $C \in \mathcal{N}$. Como $f(X_1, \ldots, X_m)$ é diagonal, devemos ter $C = 0$ e assim f é uma identidade de $U_n(A)$.

Exemplo 1.45 Seja V o T-espaço de $K\langle X \rangle$ gerado pelos polinômios $[x_1, x_2]$ 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

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

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

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

Logo, $x_3[x_1,x_2,x_4]x_5 \in V$ e portanto o T-ideal $\langle [x_1,x_2,x_3] \rangle^T$ está contido em V. Usando agora a igualdade (1.2), podemos concluir que

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

para todo $n \geq 3$, e assim, como

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

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

Vamos agora mostrar que, quando $\operatorname{char} K = 0$, $C(E) = V$ (sendo E a álgebra exterior). Como $[x_1,x_2]$ e $[x_1,x_2][x_3,x_4]$ são polinômios centrais para E, temos $V \subseteq C(E)$. Ademais, $T(E) \subseteq V$, uma vez que $T(E)$ é exatamente o T-ideal de $K\langle X\rangle$ gerado por $[x_1,x_2,x_3]$. Tomando agora $f(x_1,\dots,x_n) \in C(E)$ multilinear e usando a mesma idéia do Exemplo 1.43, podemos concluir que $f(x_1,\dots,x_n) \equiv x_1 g(x_2,\dots,x_n) \pmod V$, onde g é multilinear. Segue então que $x_1 g(x_2,\dots,x_n) \in C(E)$ e daí $g(x_2,\dots,x_n) \in C(E)$ (faça $x_1 = 1$). Mas, g e $x_1 g$ pertencentes a $C(E)$ só é possível se g for identidade de E. Logo, $x_1 g \in T(E)$ e assim devemos ter $f(x_1,\dots,x_n) \in V$.

Observação 1.46 No caso de $\operatorname{char} K = p > 0$ temos $V \neq C(E)$. De fato, consideremos a álgebra $U_2(K)$ (matrizes 2×2 triangulares superiores) e o T-espaço

$$W = \{f(x_1,\dots,x_n) \in K\langle X\rangle \mid f(A_1,\dots,A_n) \text{ tem diagonal nula para } A_1,\dots,A_n \in U_2(K)\}.$$

É fácil ver que $[x_1,x_2]$ e $[x_1,x_2][x_3,x_4]$ então em W, donde $V \subseteq W$. tomando agora o polinômio $g(x_1) = x_1^p$ de $C(E)$, verificamos facilmente que não pertence a W (basta fazer $x_1 = E_{11}$). Logo, $g(x_1) \in C(E) - V$.

No estudo que fizemos até agora de T-espaços e polinômios centrais, vimos que o conjunto $C(A)$ é sempre um T-espaço de $K\langle X\rangle$ para toda álgebra A. Quando falamos em descrever os polinômios centrais de A, estamos falando em determinar um subconjunto de $C(A)$ que possa gerá-lo como T-espaço. Assim, observa-se uma ampla ligação entre os conceitos de polinômio central e T-espaço, embora este último seja mais abrangente. Existem T-espaços que não são multiplicativamente fechados (observe o Exemplo 1.43) e também T-espaços multiplicativamente fechados que não são espaços de polinômios centrais para nenhuma álgebra. O T-espaço V do Exemplo 1.45 satisfaz estas condições em característica positiva, conforme veremos a seguir.

Proposição 1.47 *Se $\operatorname{char} K = p > 2$, então não existe álgebra A tal que $C(A) = V$.*

Demonstração. Suponha, por contradição, que $C(A) = V$ para alguma álgebra associativa A. Então, $[x_1, x_2] \in C(A)$ e daí $[x_1, x_2, x_3] \in T(A)$. 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 $[y, x, \ldots, x] = yx^p - x^p y = [y, x^p]$. Assim, concluímos que $[x_2, x_1^p] \in T(A)$ e daí $x_1^p \in C(A)$, o que contradiz a hipótese de que $C(A) = V$ (veja a observação anterior). □

1.7 Identidades e polinômios centrais graduados

Nesta seção vamos apresentar os conceitos de identidades e polinômios centrais para álgebras graduadas. As idéias apresentadas aqui serão fundamentais nos próximos dois capítulos. Alguns resultados têm demonstrações análogas às daqueles relacionados a identidades e polinômios centrais ordinários e assim faremos apenas breves comentários a respeito deles. Comecemos com a definição de álgebra G-graduada. Em toda esta seção, G denotará um grupo abeliano com notação aditiva.

Definição 1.48 *Dizemos que uma álgebra A é G-graduada se existe uma família de subespaços $\{A_g \mid g \in G\}$ de A tais que*

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

para quaisquer $g, h \in G$.

Na definição acima, dizemos que a família $\{A_g \mid g \in G\}$ é uma *G-graduação em A* e que os elementos de A_g são *homogêneos de grau g*.

Exemplo 1.49 Toda álgebra A admite uma G-graduação. Basta tomar $A_0 = A$ e $A_g = \{0\}$ para todo $g \in G - \{0\}$. Esta graduação é chamada de trivial.

Exemplo 1.50 A álgebra exterior E possui uma $\mathbb{Z}_2$-graduação natural: $E = E_0 \oplus E_1$, onde E_0 é o subespaço dos elementos pares e E_1 dos elementos ímpares. Considerando agora a álgebra exterior E_n de dimensão 2^n (veja o Exemplo 1.8) e tomando $(E_n)_0 = E_n \cap E_0$ e $(E_n)_1 = E_n \cap E_1$, temos $E_n = (E_n)_0 \oplus (E_n)_1$ e esta decomposição define uma $\mathbb{Z}_2$-graduação em E_n.

Exemplo 1.51 Considere n um inteiro positivo e $M = M_n(K)$. Para cada $\gamma \in \mathbb{Z}_n$, tomemos o subespaço $M_\gamma = \langle E_{ij} \mid \overline{j-i} = \gamma \rangle$. Para cada $k \in \mathbb{Z}$, tomemos

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

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

$$M = \bigoplus_{\gamma \in \mathbb{Z}_n} M_\gamma \qquad \text{e} \qquad M = \bigoplus_{k \in \mathbb{Z}} M_k$$

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

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

donde temos $M_{\gamma_1}M_{\gamma_2} \subseteq M_{\gamma_1+\gamma_2}$ para γ_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 1.52 *Se A é uma álgebra G-graduada, então $1 \in A_0$.*

Demonstração. Temos que existem $g_1, \ldots, g_n \in G$ 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

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

Observando 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, podemos concluir que $a_h a_{g_i} = 0$ para $i = 1, \ldots, n$, donde $a_h a_0 = a_h$. De modo totalmente análogo mostramos que $a_0 a_h = a_h$ e assim concluímos que $a_0 = 1$. □

Definição 1.53 *Sejam A e B álgebras G-graduadas com componentes homogêneas A_g e B_g, respectivamente. Dizemos que um homomorfismo de álgebras $\varphi : A \longrightarrow B$ é G-graduado se $\varphi(A_g) \subseteq B_g$ para todo $g \in G$.*

Vamos agora tratar de identidades e polinômios centrais G-graduados. Para isso, precisamos do conceito de álgebra associativa livre G-graduada. Para definí-lo, comecemos considerando para cada $g \in G$ um conjunto enumerável X_g, e suponhamos que X_{g_1} e X_{g_2}

são disjuntos para $g_1 \neq g_2$. Tomemos então $X = \bigcup_{g \in G} X_g$ e consideremos a álgebra associativa livre unitária $K\langle X \rangle$. Definimos agora

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

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

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

temos

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

para quaisquer $g, h \in G$, assim $K\langle X \rangle$ é chamada de 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 $\alpha(f) = g$.

Agora estamos prontos para definir identidade e polinômio central G-graduados.

Definição 1.54 *Seja $A = \bigoplus_{g \in G} A_g$ uma álgebra G-graduada. Dizemos que um polinômio $f(x_1, \dots, x_n) \in K\langle X \rangle$ é:*
a) *uma identidade G-graduada de A se $f(a_1, \dots, a_n) = 0$ para quaisquer $a_i \in A_{\alpha(x_i)}$ com $i = 1, \dots, n$.*
b) *um polinômio central G-graduado para A se $f(a_1, \dots, a_n) \in Z(A)$ para quaisquer $a_i \in A_{\alpha(x_i)}$ com $i = 1, \dots, n$.*

No estudo das identidades e polinômios centrais ordinários, os conceitos de T-ideal e T-espaço têm importância fundamental, como foi visto nas seções anteriores. Para o caso de identidades e polinômios centrais G-graduados temos conceitos análogos, a saber, os de T_G-ideal e T_G-espaço, que definiremos a seguir.

Definição 1.55 *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 $K\langle X \rangle$.*

De acordo com esta definição, dizer que I é um T_G-ideal equivale a dizer que $f(g_1, \dots, g_n) \in I$ para quaisquer $f(x_1, \dots, x_n) \in I$ e $g_i \in K\langle X \rangle_{\alpha(x_i)}$ com $i = 1, \dots, n$. Analogamente, para T_G-espaços. As idéias de T_G-ideal e T_G-espaço gerados por um subconjunto S de $K\langle X \rangle$ são análogas às idéias de T-ideal e T-espaço gerados. Denotamos por $\langle S \rangle^{T_G}$ o T_G-ideal gerado por S.

Sendo A uma álgebra G-graduada, temos que o conjunto $T_G(A)$ das identidades G-graduadas de A é um T_G-ideal de $K\langle X\rangle$ e que o conjunto $C_G(A)$ dos polinômios centrais G-graduados para A é um T_G-espaço de $K\langle X\rangle$.

É importante observar que todo T_G-ideal e todo T_G-espaço é gerado por seus polinômios multi-homogêneos no caso do corpo base ser infinito, e por seus polinômios multilineares no caso do corpo base ter característica zero (as demonstrações são as mesmas feitas para T-ideais).

Exemplo 1.56 Consideremos a álgebra exterior E com sua $\mathbb{Z}_2$-graduação natural (Exemplo 1.50). Sendo $K\langle X\rangle$ a álgebra livre $\mathbb{Z}_2$-graduada, temos $X = X_0 \cup X_1$. Como $ab = -ba$ para quaisquer $a, b \in E_1$, temos que $f(x_1, x_2) = x_1 \circ x_2$, com $\alpha(x_1) = \alpha(x_2) = 1$, é identidade $\mathbb{Z}_2$-graduada de E. Como $E_0 = Z(E)$, temos que todo polinômio $f \in K\langle X\rangle_0$ é um polinômio central $\mathbb{Z}_2$-graduado para E.

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

Proposição 1.57 *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 $b_{ig} \in B_g$, para $i = 1, \ldots, n$ e $g \in G$, tais que $b_i = \sum_{g\in G} b_{ig}$. Para cada $b_{ig} \neq 0$, tomemos $x_{ig} \in X_g$ e consideremos o polinômio $f_1 = f(\sum_{g\in G} x_{ig}, \ldots, \sum_{g\in G} x_{ng}) \in K\langle X\rangle$. Como $f \in T(A)$, temos $f_1 \in T_G(A)$ e daí $f_1 \in T_G(B)$. Fazendo então as substituições $x_{ig} = b_{ig}$, para $i = 1, \ldots, n$ e $g \in G$, temos

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

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. Para ver isto tomemos n par e as álgebras E_n e E_{n+1} (sendo o corpo K infinito de característica diferente de 2) com suas $\mathbb{Z}_2$-graduações naturais (Exemplo 1.50). Temos que $T(E_n) = T(E_{n+1})$ (veja [15], página 52), mas $T_{\mathbb{Z}_2}(E_n) \neq T_{\mathbb{Z}_2}(E_{n+1})$, pois o polinômio $f(x_1, x_2, \ldots, x_{n+1}) = x_1x_2 \ldots x_{n+1}$, com $\alpha(x_1) = \alpha(x_2) = \ldots = \alpha(x_{n+1}) = 1$, é identidade $\mathbb{Z}_2$-graduada para E_n, mas não é para E_{n+1}.

Capítulo 2

Identidades e Polinômios Centrais para Álgebras $\mathbb{Z}_2$-graduadas

As identidades graduadas apareceram como uma forte ferramenta no trabalho de Kemer [27, 28] (veja também [29]) sobre a estrutura dos T-ideais em característica zero e, por sua importância, se tornaram objetos de estudos independentes. Neste trabalho de Kemer foi feita, entre outras coisas, a classificação das álgebras associativas T-primas sobre um corpo de característica zero. Como exemplos deste importante tipo de álgebra podemos citar as álgebras comutativas, a álgebra de Grassmann E, as álgebras $M_2(K)$, $M_{1,1}(E)$ e $E \otimes E$. Essas três últimas possuem $\mathbb{Z}_2$-graduações naturais e as identidades $\mathbb{Z}_2$-graduadas de $M_2(K)$ e de $M_{1,1}(E)$ foram descritas por Di Vincenzo [12] em característica zero. Mais tarde, Koshlukov e Azevedo [31] generalizaram estas descrições para corpos infinitos de característica diferente de 2, e também descreveram as identidades $\mathbb{Z}_2$-graduadas de $E \otimes E$. No decorrer deste capítulo, estes resultados serão oportunamente enunciados.

Nas primeira e quarta seções deste capítulo apresentaremos as descrições dos polinômios centrais $\mathbb{Z}_2$-graduados para $M_2(K)$ e $E \otimes E$ que foram feitas em [8]. Nas outras duas seções, serão estudadas as álgebras supercomutativas e as álgebras $M_{1,1}(S)$, onde S é supercomutativa. Este estudo consiste na classificação destas álgebras do ponto de vista da PI-teoria e na descrição dos polinômios centrais $\mathbb{Z}_2$-graduados para $M_{1,1}(S)$, a qual é uma generalização da descrição dos polinômios centrais $\mathbb{Z}_2$-graduados para $M_{1,1}(E)$, também feita em [8].

A álgebra associativa livre $\mathbb{Z}_2$-graduada, que tem fundamental importância neste capítulo, será denotada por $K\langle X \cup Y\rangle$, onde $X = \{x_1, x_2, x_3, \ldots\}$ é o conjunto das variáveis de grau 0 e $Y = \{y_1, y_2, y_3, \ldots\}$ é o conjunto das variáveis de grau 1. A construção de $K\langle X \cup Y\rangle$, assim como os conceitos e notações relacionados com ela, podem ser vistos na Seção 1.7, fazendo $G = \mathbb{Z}_2$. Para simplificar a notação, vamos denotar $T_{\mathbb{Z}_2}$ e $C_{\mathbb{Z}_2}$ por T_2 e C_2, respectivamente.

Em todo este capítulo K será sempre um corpo infinito de característica diferente de 2.

2.1 Polinômios centrais $\mathbb{Z}_2$-graduados para $M_2(K)$

A álgebra $M_2(K)$ possui uma $\mathbb{Z}_2$-graduação natural, a qual definiremos agora. Tomando

$$A_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| \, a, d \in K \right\} \qquad \text{e} \qquad A_1 = \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \middle| \, b, c \in K \right\}$$

temos que $M_2(K) = A_0 \oplus A_1$ (como espaço vetorial) e também que $A_iA_j \subseteq A_{i+j}$ para quaisquer i, $j \in \mathbb{Z}_2$. Observe que este é o caso particular $n = 2$ no Exemplo 1.51.

A descrição das identidades $\mathbb{Z}_2$-graduadas de $M_2(K)$, feita primeiramente para $\operatorname{char} K = 0$ e depois generalizada para K infinito com $\operatorname{char} K \neq 2$, é dada pelo seguinte teorema.

Teorema 2.1 ([12, 31]) *O T_2-ideal das identidades $\mathbb{Z}_2$-graduadas de $M_2(K)$ é gerado pelos polinômios $[x_1, x_2]$ e $y_1y_2y_3 - y_3y_2y_1$.*

Vamos começar nosso estudo dos polinômios centrais $\mathbb{Z}_2$-graduados para $M_2(K)$ observando que

$$\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}^2 = \begin{pmatrix} bc & 0 \\ 0 & bc \end{pmatrix} \in Z(M_2(K))$$

para b, $c \in K$. Daí concluímos que $y_1^2 \in C_2(M_2(K))$. Consideremos então o T_2-espaço V de $K\langle X \cup Y \rangle$ gerado pelos polinômios

$$z_1[x_1, x_2]z_2 \quad , \quad z_1(y_1y_2y_3 - y_3y_2y_1)z_2 \quad , \quad y_1^2$$

onde z_1 e z_2 são variáveis em $X \cup Y$. Nosso objetivo nesta seção é mostrar que $C_2(M_2(K))$ é igual a V. Tendo em vista que os três polinômios acima são centrais, concluímos que $V \subseteq C_2(M_2(K))$. Pelo Teorema 2.1 temos $T_2(M_2(K)) \subset V$.

Lema 2.2 *Os polinômios $y_1 \circ y_2$, $y_1^2y_2^2$ e $[y_1, y_2][y_3, y_4]$ pertencem a V. Ademais, V é multiplicativamente fechado.*

Demonstração. Como $y_1 + y_2 \in K\langle X \cup Y \rangle_1$, temos que $(y_1 + y_2)^2 \in V$. Mas, $(y_1 + y_2)^2 = y_1^2 + y_2^2 + 2(y_1 \circ y_2)$. Logo, $y_1 \circ y_2 \in V$.

Observando agora que $y_1 + y_1y_2^2 \in K\langle X \cup Y \rangle_1$, temos

$$y_1^2 + y_1^2y_2^2 + y_1y_2^2y_1 + (y_1y_2^2)^2 = (y_1 + y_1y_2^2)^2 \in V.$$

Logo, $y_1^2y_2^2 + y_1y_2^2y_1 \in V$. Mas, como $[y_2^2, y_1] \in T_2(M_2(K))$, devemos ter $y_1^2y_2^2 + y_1y_2^2y_1 \equiv 2y_1^2y_2^2 \pmod{T_2(M_2(K))}$ e assim $y_1^2y_2^2 \in V$ (lembre que $T_2(M_2(K)) \subset V$).

Para mostrar que $[y_1, y_2][y_3, y_4] \in V$, observemos primeiramente que $y_2y_3y_4 - y_4y_3y_2$ é uma identidade $\mathbb{Z}_2$-graduada de $M_2(K)$ e consequentemente $y_1y_2y_3y_4 - y_1y_4y_3y_2$ também é.

Logo, $y_1y_2y_3y_4 - y_1y_4y_3y_2 \in V$. Como a igualdade $-ab = ba - 2a \circ b$ vale em toda álgebra associativa, temos

$$-y_1y_4y_3y_2 = y_2y_1y_4y_3 - 2((y_1y_4y_3) \circ y_2)$$

e daí segue que $y_1y_2y_3y_4 + y_2y_1y_4y_3 \in V$, pois $(y_1y_4y_3) \circ y_2 \in V$. De modo análogo mostramos que $y_2y_1y_3y_4 + y_1y_2y_4y_3 \in V$ e assim concluímos que $[y_1, y_2][y_3, y_4] \in V$.

Para mostrar que V é multiplicativamente fechado, observemos que todos os seus elementos têm a forma

$$\alpha_1 f_1^2 + \ldots + \alpha_n f_n^2 + g$$

onde $\alpha_i \in K$, $f_i \in K\langle X \cup Y\rangle_1$ e $g \in T_2(M_2(K))$. Logo, o produto de dois elementos de V é a soma de uma identidade com uma combinação linear de elementos da forma $f_i^2 f_j^2$, os quais pertencem a V, de acordo com a afirmação anterior. Assim, temos o resultado. □

Provemos agora o principal resultado desta seção.

Teorema 2.3 $C_2(M_2(K)) = V$.

Demonstração. Como já sabemos que $V \subseteq C_2(M_2(K))$, basta mostrar a inclusão contrária. Seja $f \in C_2(M_2(K))$ multi-homogêneo (lembre que o corpo K é infinito). Suponhamos primeiramente que f depende somente de variáveis de grau 0, digamos $f = f(x_1, \ldots, x_n)$. Usando então o fato de que $[x_i, x_j] \in T_2(M_2(K))$, concluímos que $f = \alpha x_1^{l_1} \ldots x_n^{l_n} + g$, onde $g \in T_2(M_2(K))$. Logo, $f(E_{11}, \ldots, E_{11}) = \alpha E_{11}$ e daí devemos ter $\alpha = 0$, o que nos dá $f \in T_2(M_2(K))$. Assim, podemos supor que f depende também de variáveis de grau 1.

Sendo f multi-homogêneo, temos que todos os seus termos têm as mesmas variáveis com os mesmos graus. Logo, todos os termos de f têm o mesmo $\mathbb{Z}_2$-grau e portanto f é homogêneo com respeito à $\mathbb{Z}_2$-graduação de $K\langle X \cup Y\rangle$. Supondo $\alpha(f) = 1$, temos que todo valor que f assume em $M_2(K)$ é uma matriz de diagonal nula. Daí, sendo central, f deve ser uma identidade.

Suponhamos agora que $\alpha(f) = 0$, o que significa que em cada termo de f o número de variáveis de grau 1 (contando com repetições) é par. Concluímos então que f é uma combinação linear de termos da forma $u_1u_2 \ldots u_n$, u_i é um monômio de $\mathbb{Z}_2$-grau 1 e n é par. Observando agora que $u_iu_{i+1} = (u_i \circ u_{i+1}) + \frac{1}{2}[u_i, u_{i+1}]$, podemos concluir que, módulo $T_2(M_2(K))$, f é uma combinação linear de termos da forma

$$h_1 \ldots h_m v_1 \ldots v_l \qquad m, l \geq 0$$

onde cada h_i é da forma $(u_i \circ u_{i+1})$ e cada v_i é da forma $[u_i, u_{i+1}]$. É importante observar que a ordenação pode ser feita, pois os h_i's e os v_i's têm $\mathbb{Z}_2$-grau 0 e portanto comutam módulo

$T_2(M_2(K))$. Assim, $f \equiv f_1 + f_2 \pmod{T_2(M_2(K))}$, onde f_1 é uma combinação linear de termos com l par e f_2 é uma combinação linear de termos com l ímpar. Pelo lema anterior, temos $f_1 \in V$ e daí segue que f_2 é central. Mas, cada termo $h_1 \dots h_m v_1 \dots v_l$ com l ímpar resulta em matriz de traço 0, pois $h_1 \dots h_m v_1 \dots v_{l-1}$ é central e v_l é um comutador. Logo, f_2 é central e resulta em matriz de traço 0, donde $f_2 \in T_2(M_2(K))$. Segue então que $f \in V$, o que conclui a demonstração. □

2.2 Álgebras supercomutativas

Nesta seção vamos fazer um breve estudo das álgebras supercomutativas, observando que elas estão fortemente relacionadas com as álgebras exteriores. Comecemos com a definição de álgebra supercomutativa e alguns exemplos.

Definição 2.4 *Dizemos que uma álgebra $\mathbb{Z}_2$-graduada $S = S_0 \oplus S_1$ é supercomutativa se $ab = (-1)^{ij} ba$ para quaisquer $a \in S_i$ e $b \in S_j$.*

De acordo com esta definição, dizer que S é álgebra supercomutativa equivale a dizer que $S_0 \subseteq Z(S)$ e $ab = -ba$ para quaisquer $a, b \in S_1$.

Exemplo 2.5 A álgebra exterior E, com sua $\mathbb{Z}_2$-graduação natural $E = E_0 \oplus E_1$, é um exemplo de álgebra supercomutativa. A álgebra exterior E_n de dimensão 2^n, com sua $\mathbb{Z}_2$-graduação natural $E_n = (E_n)_0 \oplus (E_n)_1$ (veja o Exemplo 1.50), também é um exemplo de álgebra supercomutativa.

Exemplo 2.6 Seja L uma álgebra de Lie nilpotente de classe 2 e seja L_1 um subespaço tal que $L = Z(L) \oplus L_1$ (como espaço vetorial), onde $Z(L) = \{x \in L \mid xa = 0 \text{ para todo } a \in L\}$ (centro de L). Consideremos a álgebra $H_L = K \oplus L$ (veja o Exemplo 1.4), cujo produto é dado por $(\lambda_1, x)(\lambda_2, y) = (\lambda_1\lambda_2, \lambda_1 y + \lambda_2 x + xy)$. Como $(xy)z = x(yz) = 0$ para quaisquer x, y, $z \in L$, temos que H_L é associativa.

Tomando agora $V_0 = \{(\lambda, x) \mid \lambda \in K \ , \ x \in Z(L)\}$ e $V_1 = \{(0, y) \mid y \in L_1\}$, observamos que $H_L = V_0 \oplus V_1$ e que esta decomposição define uma $\mathbb{Z}_2$-graduação em H_L. Ademais, $V_0 = Z(H_L)$ e $uv = -vu$ para quaisquer u, $v \in V_1$. Logo, H_L é supercomutativa.

Exemplo 2.7 Se $S = S_0 \oplus S_1$ é uma álgebra supercomutativa e A é uma álgebra comutativa qualquer, então $A \otimes S$ é uma álgebra supercomutativa. Para ver isto basta observar que a decomposição $A \otimes S = (A \otimes S_0) \oplus (A \otimes S_1)$ define uma $\mathbb{Z}_2$-graduação em $A \otimes S$ e que $A \otimes S_0 \subseteq Z(A \otimes S)$ e $xy = -yx$ para quaisquer x, $y \in A \otimes S_1$.

Proposição 2.8 *Seja $S = S_0 \oplus S_1$ uma álgebra supercomutativa. Então $T_2(S) = T_2(E)$ ou $T_2(S) = T_2(E_n)$ para algum $n \in \mathbb{N}$.*

Demonstração. Segue imediatamente da definição de álgebra supercomutativa que os polinômios $[x_1, x_2]$, $[x_1, y_1]$ e y_1^2 são identidades $\mathbb{Z}_2$-graduadas de S. Se $I = \langle [x_1, x_2], [x_1, y_1], y_1^2 \rangle^{T_2}$, temos $I \subseteq T_2(S)$. Seja $f(x_1, \ldots, x_m, y_1, \ldots, y_q) \in T_2(S)$ um polinômio multi-homogêneo. Como $[x_1, x_2]$, $[x_1, y_1]$, $y_1 \circ y_2 \in I$, temos

$$f \equiv \alpha x_1^{l_1} \ldots x_m^{l_m} y_1^{k_1} \ldots y_q^{k_q} \pmod{I}$$

onde $\alpha \in K$, $l_i = \deg_{x_i} f$ e $k_j = \deg_{y_j} f$. Se $f \notin I$, devemos ter $k_1 = \ldots = k_q = 1$ e $\alpha \neq 0$. Daí, fazendo $x_i = 1$ para $i = 1, \ldots, m$, concluímos que $y_1 y_2 \ldots y_q \in T_2(S)$. Logo, se $y_1 y_2 \ldots y_t \notin T_2(S)$ para todo $t \in \mathbb{N}$, devemos ter $T_2(S) = I$. Particularmente, $T_2(E) = I$.

Supondo agora que $y_1 y_2 \ldots y_t \in T_2(S)$ para algum $t \in \mathbb{N}$, tomemos $t_0 = \min\{t \in \mathbb{N} \mid y_1 y_2 \ldots y_t \in T_2(S)\}$. Daí, $I_1 = \langle [x_1, x_2], [x_1, y_1], y_1^2, y_1 y_2 \ldots y_{t_0} \rangle^{T_2} \subseteq T_2(S)$. Usando os argumentos acima, concluímos que se $f \notin I$, então $q \geq t_0$ e daí f é congruente módulo I a uma consequência de $y_1 y_2 \ldots y_{t_0}$. Logo, $T_2(S) = I_1$. No caso particular $S = E_n$, temos $t_0 = n + 1$ e assim $T_2(E_n) = \langle [x_1, x_2], [x_1, y_1], y_1^2, y_1 y_2 \ldots y_{n+1} \rangle^{T_2}$. □

Corolário 2.9 *Se S é uma álgebra supercomutativa, então $T(S) = T(E)$ ou $T(S) = T(E_n)$ para algum $n \in \mathbb{N}$.*

Demonstração. É imediato do resultado anterior e da Proposição 1.57. □

Proposição 2.10 *Seja $S = S_0 \oplus S_1$ uma álgebra supercomutativa tal que $y_1 y_2 \ldots y_n \notin T_2(S)$ para algum $n \in \mathbb{N}$. Então, existe um mergulho graduado de E_n em S. Ademais, se $y_1 y_2 \ldots y_n \notin T_2(S)$ para todo $n \in \mathbb{N}$ (equivalentemente, $T_2(S) = T_2(E)$), então S tem dimensão infinita.*

Demonstração. Sejam $b_1, b_2, \ldots, b_n \in S_1$ tais que $b_1 b_2 \ldots b_n \neq 0$ e seja $J_n = \{1, 2, \ldots, n\}$. Para cada $J \subseteq J_n$, definamos

$$v_J = \begin{cases} 1 & \text{, se } J = \emptyset, \\ b_{i_1} b_{i_2} \ldots b_{i_k} & \text{, se } J = \{i_1, i_2, \ldots, i_k\}. \end{cases}$$

Para mostrar que estes elementos são LI, suponhamos que $\sum_J \alpha_J v_J = 0$, onde J corre sobre todos os subconjuntos de J_n. Multiplicando esta equação por v_{J_n}, temos $\alpha_\emptyset v_{J_n} = 0$ e daí $\alpha_\emptyset = 0$. Tomando agora $I \subseteq J_n$ tal que $v_J = 0$ para todo $J \subseteq J_n$ com $|J| < |I|$ e multiplicando a equação por $v_{J_n \setminus I}$, concluímos que $\alpha_I = 0$. Assim, por indução, temos $\alpha_J = 0$ para todo $J \subseteq J_n$. Considerando agora a transformação linear $f : E_n \longrightarrow S$ tal que $f(1) = 1$ e $f(e_{i_1} e_{i_2} \ldots e_{i_k}) = b_{i_1} b_{i_2} \ldots b_{i_k}$, é fácil ver que f é um monomorfismo de álgebras e que $f((E_n)_i) \subseteq S_i$ para $i \in \mathbb{Z}_2$.

A última afirmação é imediata. □

2.3 As álgebras $M_{1,1}(S)$

Dada uma álgebra $\mathbb{Z}_2$-graduada $A = A_0 \oplus A_1$, definimos

$$M_{1,1}(A) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \middle| \ a, d \in A_0 \ , \ b, c \in A_1 \right\}.$$

É imediato que $M_{1,1}(A)$ é uma subálgebra de $M_2(A)$. Tomando agora os subespaços

$$M_{1,1}(A)_0 = \left\{ \left(\begin{array}{cc} a & 0 \\ 0 & d \end{array} \right) \middle| \ a, d \in A_0 \right\} \quad \text{e} \quad M_{1,1}(A)_1 = \left\{ \left(\begin{array}{cc} 0 & b \\ c & 0 \end{array} \right) \middle| \ b, c \in A_1 \right\}$$

de $M_{1,1}(A)$, temos $M_{1,1}(A) = M_{1,1}(A)_0 \oplus M_{1,1}(A)_1$ e $M_{1,1}(A)_i M_{1,1}(A)_j \subseteq M_{1,1}(A)_{i+j}$, para quaisquer i, $j \in \mathbb{Z}_2$. Assim, esta decomposição define uma $\mathbb{Z}_2$-graduação em $M_{1,1}(A)$, a qual estaremos considerando até o final desta seção.

Consideremos agora a álgebra $M_{1,1}(K\langle X \cup Y\rangle)$ e os elementos

$$X_i = \left(\begin{array}{cc} x_{2i-1} & 0 \\ 0 & x_{2i} \end{array} \right) \quad \text{e} \quad Y_i = \left(\begin{array}{cc} 0 & t_i \\ u_i & 0 \end{array} \right)$$

onde $i \in \mathbb{N}$, $t_i = y_{2i-1}$ e $u_i = y_{2i}$. Seja $\mathcal{M}$ a subálgebra de $M_{1,1}(K\langle X \cup Y\rangle)$ gerada por essas matrizes. Observe que $\mathcal{M}$ herda a $\mathbb{Z}_2$-graduação de $M_{1,1}(K\langle X \cup Y\rangle)$.

Consideremos agora $f(x_1, \ldots, x_n, y_1, \ldots, y_m) \in K\langle X \cup Y\rangle$. Temos que

$$f(X_1, \ldots, X_n, Y_1, \ldots, Y_m) = \left(\begin{array}{cc} f_1 & f_2 \\ f_3 & f_4 \end{array} \right)$$

onde f_1, f_2, f_3, $f_4 \in K\langle X \cup Y\rangle$. Desta forma, dada uma álgebra $\mathbb{Z}_2$-graduada qualquer $A = A_0 \oplus A_1$, temos que $f \in T_2(M_{1,1}(A))$ se, e somente se, f_1, f_2, f_3, $f_4 \in T_2(A)$. Assim, o seguinte resultado está demonstrado.

Proposição 2.11 *Sejam A e B duas álgebras $\mathbb{Z}_2$-graduadas. Se $T_2(A) \subseteq T_2(B)$, então $T_2(M_{1,1}(A)) \subseteq T_2(M_{1,1}(B))$. Ademais, se $T_2(A) = T_2(B)$, então $T_2(M_{1,1}(A)) = T_2(M_{1,1}(B))$.*

Nesta seção estamos particularmente interessados em $M_{1,1}(S)$, onde S é uma álgebra supercomutativa. Como consequência da Proposição 2.11 temos $T_2(M_{1,1}(E)) \subseteq T_2(M_{1,1}(S))$, pois $T_2(E) \subseteq T_2(S)$. Além disso, aplicando a Proposição 2.8, podemos concluir que $T_2(M_{1,1}(S)) = T_2(M_{1,1}(E))$ ou $T_2(M_{1,1}(S)) = T_2(M_{1,1}(E_n))$ para algum $n \in \mathbb{N}$. Daí, $T(M_{1,1}(S)) = T(M_{1,1}(E))$ ou $T(M_{1,1}(S)) = T(M_{1,1}(E_n))$ (pela Proposição 1.57) e portanto temos a classificação do ponto de vista da PI-teoria das álgebras $M_{1,1}(S)$.

Agora, para conhecer a forma concreta das identidades $\mathbb{Z}_2$-graduadas de $M_{1,1}(S)$ precisamos das descrições de $T_2(M_{1,1}(E))$ e $T_2(M_{1,1}(E_n))$. A descrição de $T_2(M_{1,1}(E))$, feita primeiramente em característica zero e depois generalizada para corpos infinitos de característica diferente de 2, é dada pelo seguinte teorema.

Teorema 2.12 ([12, 31]) *O T_2-ideal das identidades $\mathbb{Z}_2$-graduadas de $M_{1,1}(E)$ é gerado pelos polinômios $[x_1, x_2]$ e $y_1y_2y_3 + y_3y_2y_1$.*

Vejamos agora a descrição de $T_2(M_{1,1}(E_n))$.

Teorema 2.13 *Se $n \in \mathbb{N}$, então $T_2(M_{1,1}(E_n))$ é gerado como T_2-ideal pelos polinômios*

$$[x_1, x_2] \quad , \quad y_1y_2y_3 + y_3y_2y_1 \quad , \quad y_1y_2\cdots y_ny_{n+1}.$$

Demonstração. Seja I_n o T_2-ideal de $K\langle X \cup Y\rangle$ gerado por estes polinômios. Observe que os dois primeiros são identidades $\mathbb{Z}_2$-graduadas de $M_{1,1}(E)$ e portanto de $M_{1,1}(E_n)$. Um cálculo simples mostra que o terceiro também é identidade $\mathbb{Z}_2$-graduada de $M_{1,1}(E_n)$. Logo, $I_n \subseteq T_2(M_{1,1}(E_n))$. Suponhamos agora $f = f(x_1, \ldots, x_m, y_1, \ldots, y_q) \in T_2(M_{1,1}(E_n))$ multi-homogêneo e suponhamos também que o grau total nas variáveis y_i's de cada monômio de f é par, digamos $2s$. Se $2s > n$, então $f \in I_n$, uma vez que $y_1y_2\ldots y_{n+1} \in I_n$. Logo, podemos supor $2s \le n$. Observemos que, módulo I_n, f é uma combinação linear de termos da forma

$$x_1^{l_1}\ldots x_m^{l_m} y_{i_1} x_1^{k_1}\ldots x_m^{k_m} y_{j_1} y_{i_2} y_{j_2}\ldots y_{i_s} y_{j_s}$$

com $i_1 < i_2 < \ldots < i_s$ e $j_1 < j_2 < \ldots < j_s$, ou seja,

$$f \equiv \sum_{\alpha,B} a_{\alpha,B} x_1^{l_1}\ldots x_m^{l_m} y_{i_1} x_1^{k_1}\ldots x_m^{k_m} y_{j_1} y_{i_2} y_{j_2}\ldots y_{i_s} y_{j_s} \pmod{I_n}$$

onde $a_{\alpha,B} \in K$, α corre sobre todas as m-uplas $(l_1, l_2, \ldots, l_m)$, com $0 \le l_i \le \deg_{x_i} f$, e B corre sobre todos os subconjuntos $\{i_1, i_2, \ldots, i_s\}$ de s elementos de $\{1, 2, \ldots, q\}$. Chamando o segundo membro desta congruência de $g(x_1, \ldots, x_m, y_1, \ldots, y_q)$, temos

$$g(X_1, \ldots, X_m, Y_1, \ldots, Y_q) = \begin{pmatrix} f_1 & 0 \\ 0 & f_2 \end{pmatrix}$$

onde f_1, $f_2 \in K\langle X \cup Y\rangle_0$,

$$f_1(x_1, \ldots, x_{2m}, t_1, \ldots, t_q, u_1, \ldots, u_q) = \sum_{\alpha,B} a_{\alpha,B} x_1^{l_1}\ldots x_{2m-1}^{l_m} t_{i_1} x_2^{k_1}\ldots x_{2m}^{k_m} u_{j_1}\ldots t_{i_s} u_{j_s}$$

e

$$f_2(x_1, \ldots, x_{2m}, t_1, \ldots, t_q, u_1, \ldots, u_q) = \sum_{\alpha,B} a_{\alpha,B} x_2^{l_1}\ldots x_{2m}^{l_m} u_{i_1} x_1^{k_1}\ldots x_{2m-1}^{k_m} t_{j_1}\ldots u_{i_s} t_{j_s}.$$

Observando agora que $g \in T_2(M_{1,1}(E_n))$, concluímos que f_1 e f_2 são identidades $\mathbb{Z}_2$-graduadas de E_n. Tomando então λ_1, λ_2, $\ldots$, λ_m elementos arbitrários de K e fazendo em f_1 as substituições $x_i = 1$, para i par, e $x_{2i-1} = \lambda_i$, para $i = 1, 2, \ldots, m$, temos que o polinômio

$$\sum_{\alpha,B} a_{\alpha,B} \lambda_1^{l_1}\ldots\lambda_m^{l_m} t_{i_1} u_{j_1}\ldots t_{i_s} u_{j_s}$$

também é uma identidade $\mathbb{Z}_2$-graduada de E_n. Observe agora que neste polinômio dois monômios têm mesmo multigrau se, e somente se, correspondem ao mesmo B. Assim, fixado $B_0 = \{i_1, i_2, \ldots, i_s\}$, arbitrário, temos

$$\left(\sum_{\alpha} a_{\alpha,B_0} \lambda_1^{l_1} \ldots \lambda_m^{l_m}\right) t_{i_1} u_{j_1} \ldots t_{i_s} u_{j_s} \in T_2(E_n).$$

Tomando então $t_{i_1} = e_1$, $u_{j_1} = e_2$, $\ldots$, $t_{i_s} = e_{2s-1}$ e $u_{j_s} = e_{2s}$, podemos concluir que $\sum_\alpha a_{\alpha,B_0} \lambda_1^{l_1} \ldots \lambda_m^{l_m} = 0$. Como os λ_i's foram tomados arbitrários e K é infinito, devemos ter $a_{\alpha,B_0} = 0$ para todo α. Daí, $f \in I_n$, pois B_0 também foi tomado arbitrário. No caso do grau total de f nas variáveis y_i's ser ímpar, o procedimento é totalmente análogo. $\square$

Vamos agora estudar os T_2-espaços $C_2(M_{1,1}(S))$, onde S é supercomutativa. Como já foi visto que $T_2(M_{1,1}(S))$ é igual a $T_2(M_{1,1}(E))$ ou a $T_2(M_{1,1}(E_n))$, temos que $C_2(M_{1,1}(S))$ é igual a $C_2(M_{1,1}(E))$ ou a $C_2(M_{1,1}(E_n))$. Assim, basta estudar esses dois últimos. Como primeiro passo neste sentido, vamos ver a descrição do centro de $M_{1,1}(S)$.

Proposição 2.14 *Se S é uma álgebra supercomutativa, então*

$$Z(M_{1,1}(S)) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle|\ a, d \in S_0 \quad , \quad (a-d)S_1 = 0 \right\}.$$

Demonstração. Seja $X = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in M_{1,1}(S)$, com $(a-d)S_1 = 0$. Como $S_0 \subseteq Z(S)$ temos que X comuta com todo elemento de $M_{1,1}(S)_0$. Tomando agora $b, c \in S_1$, temos

$$X \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} = \begin{pmatrix} 0 & ab \\ dc & 0 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} X = \begin{pmatrix} 0 & db \\ ac & 0 \end{pmatrix}.$$

Como $(a-d)b = (a-d)c = 0$, temos a igualdade dessas matrizes e assim $X \in Z(M_{1,1}(S))$, uma vez que $M_{1,1}(S) = M_{1,1}(S)_0 \oplus M_{1,1}(S)_1$.

Tomemos agora $Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(M_{1,1}(S))$. Pela Proposição 1.52, temos $1 \in S_0$ e assim $E_{11} \in M_{1,1}(S)$. Como $E_{11}Y = YE_{11}$, devemos ter $b = c = 0$. Tomando agora $b_1 \in S_1$, arbitrário, e $Z = \begin{pmatrix} 0 & b_1 \\ 0 & 0 \end{pmatrix}$, segue da igualdade $ZY = YZ$ que $(a-d)b_1 = 0$. Logo, $(a-d)S_1 = 0$. $\square$

Corolário 2.15 $Z(M_{1,1}(E)) = \{aI_{2\times 2} \mid a \in E_0\}$, $Z(M_{1,1}(E_n)) = \{aI_{2\times 2} \mid a \in (E_n)_0\}$, *se n é ímpar, e* $Z(M_{1,1}(E_n)) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle|\ a - d \in \langle e_1 e_2 \ldots e_n \rangle \right\}$, *se n é par.*

Demonstração. Se n é ímpar e $x \in (E_n)_0$, então x é uma combinação linear de produtos da forma $e_{i_1}e_{i_2}\dots e_{i_k}$, onde $i_1 < i_2 < \dots < i_k$ e k é par. Logo, $k < n$ e daí podemos escolher e_m que não esteja em algum termo de x. Temos então $xe_m \neq 0$ e portanto $x(E_n)_1 \neq 0$. Segue daí que $Z(M_{1,1}(E_n)) = \{aI_{2\times 2} \mid a \in (E_n)_0\}$. Usando exatamente a mesma idéia mostramos que $Z(M_{1,1}(E)) = \{aI_{2\times 2} \mid a \in E_0\}$.

Suponhamos agora n par e $x \in (E_n)_0$ tal que $x(E_n)_1 = 0$. Usando os argumentos acima, concluímos que $x \in \langle e_1e_2\dots e_n\rangle$ e assim temos a última afirmação. $\square$

Lema 2.16 *Se S é uma álgebra supercomutativa, então $[y_1, y_2] \in C_2(M_{1,1}(S))$ e $(y_1 \circ y_2)$ sempre resulta em matriz de traço zero em $M_{1,1}(S)$.*

Demonstração. Tomando b_1, b_2, c_1, $c_2 \in S_1$, temos

$$\left[\begin{pmatrix} 0 & b_1 \\ b_2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & c_1 \\ c_2 & 0 \end{pmatrix}\right] = \begin{pmatrix} b_1c_2 + b_2c_1 & 0 \\ 0 & b_2c_1 + b_1c_2 \end{pmatrix} \in Z(M_{1,1}(S))$$

e

$$\begin{pmatrix} 0 & b_1 \\ b_2 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & c_1 \\ c_2 & 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} b_1c_2 + c_1b_2 & 0 \\ 0 & b_2c_1 + c_2b_1 \end{pmatrix}$$

que é claramente uma matriz de traço zero. Temos então as duas afirmações. $\square$

Seja W o T_2-espaço de $K\langle X \cup Y\rangle$ gerado pelo polinômio $[y_1, y_2]$. Sendo $S = S_0 \oplus S_1$ uma álgebra supercomutativa, tomemos $W_S = T_2(M_{1,1}(S)) + W$. Pelo Lema 2.16 temos que $W_S \subseteq C_2(M_{1,1}(S))$. Vamos agora mostrar que se $Z(M_{1,1}(S)) = \{aI_{2\times 2} \mid a \in S_0\}$, então vale a igualdade. Como consequência deste resultado teremos as descrições de $C_2(M_{1,1}(E))$ e de $C_2(M_{1,1}(E_n))$ para n ímpar.

Lema 2.17 *Os polinômios $(y_1 \circ y_2)(y_3 \circ y_4)$ e $[y_1, y_2][y_3, y_4]$ pertencem a W_S. Ademais, W_S é multiplicativamente fechado.*

Demonstração. Observemos primeiramente que $y_1y_2y_3y_4 + y_1y_4y_3y_2 \in W_S$, pois $y_2y_3y_4 + y_4y_3y_2 \in T_2(M_{1,1}(S))$. Como $y_1y_4y_3$ tem $\mathbb{Z}_2$-grau 1, temos que $[y_1y_4y_3, y_2] \in W_S$ e daí segue que $y_1y_2y_3y_4 + y_2y_1y_4y_3 \in W_S$. De modo inteiramente análogo temos $y_1y_2y_4y_3 + y_2y_1y_3y_4 \in W_S$ e assim, como

$$[y_1, y_2][y_3, y_4] = y_1y_2y_3y_4 - y_1y_2y_4y_3 - y_2y_1y_3y_4 + y_2y_1y_4y_3$$

e

$$(y_1 \circ y_2)(y_3 \circ y_4) = \frac{1}{4}(y_1y_2y_3y_4 + y_1y_2y_4y_3 + y_2y_1y_3y_4 + y_2y_1y_4y_3)$$

temos a primeira afirmação.

Para mostrar que W_S é multiplicativamente fechado, observemos que todos os seus elementos são da forma

$$\alpha_1[f_1, g_1] + \ldots + \alpha_n[f_n, g_n] + h$$

onde $h \in T_2(M_{1,1}(S))$ e f_i e g_i são polinômios quaisquer em $K\langle X \cup Y \rangle_1$. Como $[y_1, y_2][y_3, y_4] \in W_S$, concluímos que o produto de dois elementos quaisquer de W_S ainda está em W_S, o que é exatamente a segunda afirmação. □

Teorema 2.18 *Se $Z(M_{1,1}(S)) = \{aI_{2\times 2} \mid a \in S_0\}$, então $C_2(M_{1,1}(S)) = W_S$.*

Demonstração. Basta mostrar que $C_2(M_{1,1}(S)) \subseteq W_S$, pois já sabemos que a inclusão contrária é válida. Seja $f \in C_2(M_{1,1}(S))$ multi-homogêneo (K é infinito). Suponhamos primeiramente que f depende somente de variáveis de grau 0, digamos $f = f(x_1, \ldots, x_n)$. Usando então o fato de que $[x_i, x_j] \in T_2(M_{1,1}(S))$, concluímos que $f = \alpha x_1^{l_1} \ldots x_n^{l_n} + g$, onde $g \in T_2(M_{1,1}(S))$. Como $1 \in S_0$, temos $E_{11} \in M_{1,1}(S)_0$ e daí podemos substituir cada x_i por E_{11} em f. Temos então $f(E_{11}, \ldots, E_{11}) = \alpha E_{11}$, donde segue que $\alpha = 0$ e portanto $f \in T_2(M_{1,1}(S))$. Assim, podemos supor que f depende também de variáveis de grau 1.

Sendo f multi-homogêneo, temos que também é $\mathbb{Z}_2$-homogêneo. Se $\alpha(f) = 1$, todo valor que f assume em $M_{1,1}(S)$ é uma matriz de diagonal nula. Daí, sendo central, f deve ser uma identidade.

Suponhamos agora que $\alpha(f) = 0$, o que significa que em cada termo de f o número de variáveis de grau 1 (contando com repetições) é par. Concluímos então que f é uma combinação linear de termos da forma $u_1 u_2 \ldots u_n$, u_i é um monômio de $\mathbb{Z}_2$-grau 1 e n é par. Observando agora que $u_i u_{i+1} = (u_i \circ u_{i+1}) + \frac{1}{2}[u_i, u_{i+1}]$, podemos concluir que, módulo $T_2(M_{1,1}(S))$, f é uma combinação linear de termos da forma

$$h_1 \ldots h_m v_1 \ldots v_l \qquad m, l \geq 0$$

onde cada h_i é da forma $[u_i, u_{i+1}]$ e cada v_i é da forma $(u_i \circ u_{i+1})$ (observe que a ordenação pode ser feita porque os h_i's e os v_i's têm $\mathbb{Z}_2$-grau 0 e portanto comutam módulo $T_2(M_{1,1}(S))$). Assim, $f \equiv f_1 + f_2 \pmod{T_2(M_{1,1}(S))}$, onde f_1 é uma combinação linear de termos com l par e f_2 é uma combinação linear de termos com l ímpar. Pelo lema anterior, temos $f_1 \in W_S$ e daí segue que f_2 é central. Mas, cada termo $h_1 \ldots h_m v_1 \ldots v_l$ com l ímpar resulta em matriz de traço zero, pois $h_1 \ldots h_m v_1 \ldots v_{l-1}$ é central e v_l resulta em matriz de traço zero. Logo, f_2 resulta em matriz de traço zero, pois $Z(M_{1,1}(S)) = \{aI_{2\times 2} \mid a \in S_0\}$. Observando agora que um elemento central com traço zero em $M_{1,1}(S)$ deve ser nulo, concluímos que $f_2 \in T_2(M_{1,1}(S))$ e daí $f \in W_S$, o que encerra a demonstração. □

Corolário 2.19 *a) $C_2(M_{1,1}(E))$ é gerado como T_2-espaço pelos polinômios*

$$z_1[x_1, x_2]z_2 \quad , \quad z_1(y_1 y_2 y_3 + y_3 y_2 y_1)z_2 \quad , \quad [y_1, y_2].$$

b) $C_2(M_{1,1}(E_n))$*, para* n *ímpar, é gerado como* T_2*-espaço pelos polinômios*

$$z_1[x_1,x_2]z_2 \quad , \quad z_1(y_1y_2y_3+y_3y_2y_1)z_2 \quad , \quad z_1(y_1\cdots y_ny_{n+1})z_2 \quad , \quad [y_1,y_2].$$

Demonstração. Segue do Corolário 2.15 e do Teorema 2.18 que $C_2(M_{1,1}(E)) = T_2(M_{1,1}(E)) + W$ e $C_2(M_{1,1}(E_n)) = T_2(M_{1,1}(E_n)) + W$ para n ímpar. Observando agora os Teoremas 2.12 e 2.13, temos o resultado. □

Vamos agora descrever $C_2(M_{1,1}(E_n))$ para n par. Comecemos considerando o T_2-espaço U_n dos polinômios $f(x_1,\ldots,x_m,y_1,\ldots,y_q) \in K\langle X\cup Y\rangle$ tais que $f(a_1,\ldots,a_m,b_1,\ldots,b_q)\in \langle e_1e_2\ldots e_n\rangle$ para quaisquer $a_i\in (E_n)_0$ e $b_j \in (E_n)_1$.

Lema 2.20 *Se* $f\in U_n$ *e cada termo de* f *tem grau total nas variáveis* y_i*'s menor que* n*, então* $f\in T_2(E_n)$*.*

Demonstração. Como K é infinito, podemos supor f multi-homogêneo. Assim, sendo $f = f(x_1,\ldots,x_m,y_1,\ldots,y_q)$, temos que $f\equiv \alpha x_1^{l_1}\ldots x_m^{l_m}y_1^{k_1}\ldots y_q^{k_q} \pmod{T_2(E_n)}$, onde $\alpha\in K$, $l_i = \deg_{x_i} f$ e $k_j=\deg_{y_j} f$. Se algum k_i for maior que 1, então $f\in T_2(E_n)$. Supondo então $k_1=\ldots=k_q=1$, temos $q<n$. Logo, $f(1,\ldots,1,e_1,\ldots,e_q)=\alpha e_1\ldots e_q\in\langle e_1e_2\ldots e_n\rangle$ e daí devemos ter $\alpha=0$, o que conclui a demonstração. □

Teorema 2.21 *Se* n *é par, então* $C_2(M_{1,1}(E_n))$ *é gerado como* T_2*-espaço pelos polinômios*

$$z_1[x_1,x_2]z_2 \quad , \quad z_1(y_1y_2y_3+y_3y_2y_1)z_2 \quad , \quad z_1(y_1\cdots y_ny_{n+1})z_2 \quad , \quad [y_1,y_2] \quad , \quad y_1y_2\cdots y_n.$$

Demonstração. Seja R o T_2-espaço de $K\langle X\cup Y\rangle$ gerado por esses polinômios. Pelo Teorema 2.13 temos que $T_2(M_{1,1}(E_n))\subset R$ e que $[y_1y_2\ldots y_n,x_1]$ e $[y_1y_2\ldots y_n,y_{n+1}]$ são identidades $\mathbb{Z}_2$-graduadas de $M_{1,1}(E_n)$. Logo, $R\subseteq C_2(M_{1,1}(E_n))$.

Para mostrar a inclusão contrária, tomemos $f\in C_2(M_{1,1}(E_n))$ multi-homogêneo. Se f depende apenas de variáveis de grau 0 ou se $\alpha(f)=1$, então mostramos que $f\in T_2(M_{1,1}(E_n))$ exatamente como na demonstração do Teorema 2.18. Supondo então que f não está em nenhuma dessas duas situações, temos que cada termo de f é um produto da forma uv, onde u e v são monômios de grau 1. Como $uv=(u\circ v)+\frac{1}{2}[u,v]$, temos $f=f_1+f_2$, onde f_1 é uma combinação linear de termos $(u\circ v)$ e f_2 é uma combinação linear de termos $[u,v]$. Observe que f_1 e f_2 são multi-homogêneos com mesmo multigrau que f e que $f_2\in R$. Logo, $f_1\in C_2(M_{1,1}(E_n))$. Seja $f_1=f_1(x_1,\ldots,x_m,y_1,\ldots,y_q)$. Pelo Lema 2.16, f_1 resulta em matriz de traço zero em $M_{1,1}(E_n)$ e daí, usando a última afirmação do Corolário 2.15, podemos concluir que

$$f_1(X_1,\ldots,X_m,Y_1,\ldots,Y_q)=\begin{pmatrix} g_1 & 0\\ 0 & g_2\end{pmatrix}$$

onde g_1, $g_2 \in U_n$. Observe agora que os polinômios g_1, g_2 e f têm o mesmo grau total nas variáveis y_i's. Assim, se este grau total for maior ou igual a n, então claramente $f_1 \in R$. Se for menor que n, então, pelo lema anterior, g_1, $g_2 \in T_2(E_n)$ e consequentemente $f_1 \in T_2(M_{1,1}(E_n))$. Logo, $f_1 \in R$, o que conclui a demonstração. $\square$

Observação 2.22 No enunciado do teorema anterior, o polinômio $y_1y_2 \ldots y_n$ não pode ser omitido. De fato, considerando Q_n o T_2-espaço dos polinômios $f(x_1, \ldots, x_m, y_1, \ldots, y_q) \in K\langle X \cup Y\rangle$ tais que $f(B_1, \ldots, B_m, C_1, \ldots, C_q) \in \{aI_{2\times 2} \mid a \in (E_n)_0\}$ para quaisquer $B_i \in M_{1,1}(E_n)_0$ e $C_j \in M_{1,1}(E_n)_1$, temos $T_2(M_{1,1}(E_n)) \subseteq Q_n$ e também $[y_1, y_2] \in Q_n$ (observe a demonstração do Lema 2.16). Logo, $T_2(M_{1,1}(E_n)) + W \subseteq Q_n$, lembrando que W é o T_2-espaço gerado por $[y_1, y_2]$. Observando agora a igualdade

$$\begin{pmatrix} 0 & e_1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ e_2 & 0 \end{pmatrix}\cdots\begin{pmatrix} 0 & e_{n-1} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ e_n & 0 \end{pmatrix} = \begin{pmatrix} e_1e_2\ldots e_{n-1}e_n & 0 \\ 0 & 0 \end{pmatrix}$$

concluímos que $y_1y_2 \ldots y_n \notin Q_n$ e portanto $y_1y_2 \ldots y_n \notin T_2(M_{1,1}(E_n)) + W$.

2.4 Polinômios centrais $\mathbb{Z}_2$-graduados para $E \otimes E$

A álgebra $E \otimes E$ possui uma $\mathbb{Z}_2$-graduação natural, conforme comentamos no início deste capítulo. Para definí-la, consideremos os subespaços

$$(E \otimes E)_0 = (E_0 \otimes E_0) \oplus (E_1 \otimes E_1) \quad \text{e} \quad (E \otimes E)_1 = (E_0 \otimes E_1) \oplus (E_1 \otimes E_0)$$

de $E \otimes E$. Como $E \otimes E = (E \otimes E)_0 \oplus (E \otimes E)_1$ e $(E \otimes E)_i(E \otimes E)_j \subseteq (E \otimes E)_{i+j}$, para quaisquer i, $j \in \mathbb{Z}_2$, temos de fato uma $\mathbb{Z}_2$-graduação definida em $E \otimes E$. Azevedo e Koshlukov mostraram em [31] que, para $\operatorname{char} K = 0$, as álgebras $E \otimes E$ e $M_{1,1}(E)$ possuem as mesmas identidades $\mathbb{Z}_2$-graduadas. Consequentemente, elas têm os mesmos polinômios centrais $\mathbb{Z}_2$-graduados, os quais foram descritos no Corolário 2.19. Vamos então supor que o corpo K tem característica $p > 2$. Neste caso, observa-se que x_1^p é um polinômio central $\mathbb{Z}_2$-graduado para $E \otimes E$, mas não é para $M_{1,1}(E)$. Logo, $C_2(E \otimes E) \neq C_2(M_{1,1}(E))$.

No sentido de descrever o T_2-espaço $C_2(E \otimes E)$, comecemos considerando a álgebra

$$A = \left\{ \begin{pmatrix} a+\lambda & b \\ c & d+\lambda \end{pmatrix} \middle| \; a, d \in E_0' \;,\; b, c \in E_1 \;,\; \lambda \in K \right\}$$

onde E_0' é a componente par da álgebra exterior sem unidade E'. Observemos que A é uma subálgebra de $M_{1,1}(E)$ e que possui uma $\mathbb{Z}_2$-graduação natural induzida pela $\mathbb{Z}_2$-graduação de $M_{1,1}(E)$.

Em [5] foi demonstrado que as álgebras $E \otimes E$ e A possuem o mesmo T_2-ideal de identidades $\mathbb{Z}_2$-graduadas, o qual é gerado pelos polinômios

$$[x_1, x_2] \quad , \quad (y_1y_2y_3 + y_3y_2y_1) \quad \text{e} \quad [x_1^p, y_1].$$

Segue então que $E \otimes E$ e A possuem os mesmos polinômios centrais $\mathbb{Z}_2$-graduados e assim nosso trabalho será descrever o T_2-espaço $C_2(A)$.

Sabe-se que x^p é uma identidade para a álgebra E'. Daí, para quaisquer $a, b \in E_0'$ e $\lambda \in K$, temos

$$\begin{pmatrix} a+\lambda & 0 \\ 0 & b+\lambda \end{pmatrix}^p = \begin{pmatrix} a^p+\lambda^p & 0 \\ 0 & b^p+\lambda^p \end{pmatrix} = \lambda^p I_2 \in Z(A).$$

Logo, x_1^p é um polinômio central $\mathbb{Z}_2$-graduado para A. De modo igual ao que foi feito na seção anterior, se mostra que $[y_1, y_2]$ também é um polinômio central $\mathbb{Z}_2$-graduado para A.

Consideremos agora o T_2-espaço U de $K\langle X \cup Y\rangle$ gerado pelos polinômios

$$z_1[x_1, x_2]z_2 \quad , \quad z_1(y_1y_2y_3 + y_3y_2y_1)z_2 \quad , \quad z_1[x_1^p, y_1]z_2 \quad , \quad [y_1, y_2] \quad , \quad x_1^p.$$

É fácil ver que $T_2(A) \subset U \subseteq C_2(A)$. Mostraremos agora que esta última inclusão é, na verdade, uma igualdade.

Lema 2.23 *Os polinômios $(y_1 \circ y_2)(y_3 \circ y_4)$, $[y_1, y_2][y_3, y_4]$, $x_1^p x_2^p$ e $[y_1, y_2]x_1^p$ pertencem a U. Ademais, U é multiplicativamente fechado.*

Demonstração. Para os dois primeiros polinômios a demonstração é a mesma da primeira parte do Lema 2.17. Como $[x_1, x_2] \in T_2(A)$, temos $x_1^p x_2^p \equiv (x_1x_2)^p \pmod{T_2(A)}$ e assim $x_1^p x_2^p \in U$, uma vez que $(x_1x_2)^p \in U$. Quanto ao último polinômio, observemos que $[y_1, y_2]x_1^p = [y_1x_1^p, y_2] - y_1[x_1^p, y_2]$ e assim temos $[y_1, y_2]x_1^p \in U$, uma vez que $[y_1x_1^p, y_2] \in U$ e $[x_1^p, y_2]$ é identidade.

Para ver que U é multiplicativamente fechado basta observar que todos os seus elementos são da forma

$$[u_1, v_1] + \ldots + [u_n, v_n] + \lambda_1 f_1^p + \ldots + \lambda_m f_m^p + g$$

onde g é identidade, $\lambda_1, \ldots, \lambda_m \in K$, $u_i, v_i \in K\langle X \cup Y\rangle_1$ e $f_i \in K\langle X \cup Y\rangle_0$, e usar a primeira afirmação. □

Teorema 2.24 $C_2(A) = U$.

Demonstração. Seja $f \in C_2(A)$ multi-homogêneo. Supondo que f depende de alguma(s) variável(is) de grau 1, a demonstração de que $f \in U$ é exatamente a mesma do Teorema 2.18 para esta situação.

Vamos agora supor que f depende apenas de variáveis de grau 0, ou seja, $f = f(x_1, \ldots, x_n)$. Como $[x_1, x_2] \in T_2(A)$ temos $f = \lambda x_1^{l_1} \ldots x_n^{l_n} + g$, onde $\lambda \in K$ e $g \in T_2(A)$. Fazendo então em f as substituições

$$x_1 = \begin{pmatrix} e_1e_2 + 1 & 0 \\ 0 & 1 \end{pmatrix} \;,\; x_2 = \begin{pmatrix} e_3e_4 + 1 & 0 \\ 0 & 1 \end{pmatrix} \;,\; \ldots \;,\; x_n = \begin{pmatrix} e_{2n-1}e_{2n} + 1 & 0 \\ 0 & 1 \end{pmatrix}$$

devemos ter

$$\lambda \begin{pmatrix} (e_1e_2 + 1)^{l_1} & 0 \\ 0 & 1 \end{pmatrix} \ldots \begin{pmatrix} (e_{2n-1}e_{2n} + 1)^{l_n} & 0 \\ 0 & 1 \end{pmatrix} \in Z(A).$$

Observando agora a igualdade $(e_{2i-1}e_{2i} + 1)^{l_i} = l_ie_{2i-1}e_{2i} + 1$ e lembrando a forma dos elementos de $Z(A)$, podemos concluir que $\lambda(l_1e_1e_2 + 1) \ldots (l_ne_{2n-1}e_{2n} + 1) = \lambda$. Mas,

$$(l_1e_1e_2 + 1) \ldots (l_ne_{2n-1}e_{2n} + 1) = 1 + l_1e_1e_2 + \ldots l_ne_{2n-1}e_{2n} + h$$

onde h é uma combinação linear de termos $e_{i_1}e_{i_2} \ldots e_{i_m}$, com $m > 2$. Segue então que $\lambda l_1 = \lambda l_2 = \ldots = \lambda l_n = 0$, o que nos dá $\lambda = 0$ ou $l_1 1_K = \ldots = l_n 1_K = 0$. Na primeira situação temos $f \in T_2(A)$. Na segunda devemos ter $l_1, l_2, \ldots, l_n$ todos múltiplos de p (lembrando que $\operatorname{char} K = p$) e assim $f = \lambda(x_1^{c_1})^p \ldots (x_n^{c_n})^p + g$, que é um polinômio de U. $\square$

Capítulo 3

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

No capítulo anterior, descrevemos os polinômios centrais $\mathbb{Z}_2$-graduados para as álgebras $M_2(K)$, $E \otimes E$ e $M_{1,1}(S)$, onde S é uma álgebra supercomutativa qualquer. Para cada uma delas foram apresentados geradores do respectivo T-espaço $\mathbb{Z}_2$-graduado de polinômios centrais. Neste capítulo vamos apresentar as descrições feitas em [7] dos polinômios centrais $\mathbb{Z}_n$-graduados e dos $\mathbb{Z}$-graduados para a álgebra $M_n(K)$. Nestas descrições estaremos considerando as graduações naturais de $M_n(K)$ pelos grupos $\mathbb{Z}_n$ e $\mathbb{Z}$, as quais estão definidas no Capítulo 1.

As identidades $\mathbb{Z}_n$-graduadas e as $\mathbb{Z}$-graduadas de $M_n(K)$ foram descritas primeiramente por Vasilovsky [48, 47] em característica zero. Mais tarde, Azevedo [3, 4] generalizou esta descrição para corpos infinitos quaisquer. Estes resultados serão apresentados oportunamente neste capítulo, devido à sua importância nas composições dos conjuntos geradores de polinômios centrais que apresentaremos.

O resultado que descreve os polinômios centrais $\mathbb{Z}_n$-graduados para $M_n(K)$ é uma generalização do caso $n = 2$, feito no capítulo anterior. No entanto, enquanto para $n = 2$ trabalhamos basicamente fazendo "reduções" de polinômios através de identidades e polinômios centrais $\mathbb{Z}_2$-graduados conhecidos, no caso geral utilizaremos idéias sobre matrizes genéricas $\mathbb{Z}_n$-graduadas que podem ser encontradas em [3]. A descrição dos polinômios centrais $\mathbb{Z}$-graduados segue idéias análogas também relacionadas com matrizes genéricas graduadas, as quais estão no artigo [4].

Os conceitos e resultados básicos necessários sobre álgebras graduadas podem ser encontrados na Seção 1.7, assim como as notações utilizadas.

Em todo este capítulo K será sempre um corpo infinito.

3.1 Polinômios centrais $\mathbb{Z}_n$-graduados

Em toda esta seção $K\langle X\rangle$ denotará a álgebra associativa livre $\mathbb{Z}_n$-graduada, onde $X = \bigcup_{\gamma\in\mathbb{Z}_n} X_\gamma$. Vamos considerar as notações introduzidas na Seção 1.7 e denotar $T_{\mathbb{Z}_n}$ e $C_{\mathbb{Z}_n}$ simplesmente por T_n e C_n, respectivamente.

Nesta e na próxima seções vamos considerar, para cada inteiro positivo m, o m-ciclo $\theta_m = (1\ \ 2\ \dots\ m)$ do grupo simétrico S_m e o subgrupo cíclico $H_m = \langle\theta_m\rangle$ de S_m.

Fixemos agora um inteiro positivo n. Consideremos a álgebra $M_n(K)$ e a sua $\mathbb{Z}_n$-graduação natural, que está definida no Capítulo 1, Exemplo 1.51. A descrição das identidades $\mathbb{Z}_n$-graduadas de $M_n(K)$, feita primeiramente para char $K = 0$ e depois generalizada para K infinito, é dada pelo seguinte teorema.

Teorema 3.1 ([48, 3]) *Todas as identidades polinomiais da álgebra $\mathbb{Z}_n$-graduada $M_n(K)$ seguem de*

$$\begin{aligned} x_1x_2 - x_2x_1 = 0 \quad &, \quad \alpha(x_1) = \alpha(x_2) = \overline{0}; \\ x_1x_2x_3 - x_3x_2x_1 = 0 \quad &, \quad \alpha(x_1) = \alpha(x_3) = -\alpha(x_2). \end{aligned} \tag{3.1}$$

Claramente, os polinômios em (3.1), por serem identidades, são polinômios centrais $\mathbb{Z}_n$-graduados para $M_n(K)$. Mas, existem polinômios centrais $\mathbb{Z}_n$-graduados para $M_n(K)$ que não são identidades. Vamos agora apresentar um tipo importante de polinômio nestas condições. Para isso, precisaremos do conceito de *seqüência completa* em $\mathbb{Z}_n$ dado a seguir.

Definição 3.2 *Sejam $\gamma_1, \gamma_2, \dots, \gamma_n \in \mathbb{Z}_n$. Dizemos que a n-upla $(\gamma_1, \gamma_2, \dots, \gamma_n)$ é uma seqüência completa se $\{\gamma_1, \gamma_1+\gamma_2, \dots, \gamma_1+\gamma_2+\dots+\gamma_n\} = \mathbb{Z}_n$ e $\gamma_1+\gamma_2+\dots+\gamma_n = \overline{0}$.*

Exemplo 3.3 $(\overline{1}, \overline{2}, \overline{3}, \overline{2})$ é uma seqüência completa em $\mathbb{Z}_4$. Dado $\gamma \in \mathbb{Z}_n$, temos que $(\gamma, \gamma, \dots, \gamma)$ é uma seqüência completa se, e somente se, γ é um gerador do grupo $\mathbb{Z}_n$.

Lema 3.4 *Se $(\gamma_1, \gamma_2, \dots, \gamma_n)$ é uma seqüência completa, então $(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \dots, \gamma_{\sigma(n)})$, para $\sigma \in H_n$, e $(\gamma_n, \gamma_{n-1}, \dots, \gamma_2, \gamma_1)$ são seqüências completas.*

Demonstração. Temos $\{\gamma_1, \gamma_1+\gamma_2, \dots, \gamma_1+\gamma_2+\dots+\gamma_n\} = \mathbb{Z}_n$ e $\gamma_1+\gamma_2+\dots+\gamma_n = \overline{0}$. Assim $\gamma_1+\dots+\gamma_j = -(\gamma_{j+1}+\dots+\gamma_n)$ para todo $j = 1, \dots, n-1$, e portanto $\{\gamma_2+\dots+\gamma_n, \dots, \gamma_{n-1}+\gamma_n, \gamma_n, \overline{0}\} = \mathbb{Z}_n$. Segue daí que $(\gamma_n, \gamma_{n-1}, \dots, \gamma_2, \gamma_1)$ é uma seqüência completa.

De $\{\gamma_1, \gamma_1+\gamma_2, \dots, \gamma_1+\gamma_2+\dots+\gamma_n\} = \mathbb{Z}_n$ temos $\{\overline{0}, \gamma_2, \dots, \gamma_2+\dots+\gamma_n\} = \mathbb{Z}_n$, ou seja, $\{\gamma_2, \dots, \gamma_2+\dots+\gamma_n, \gamma_2+\dots+\gamma_n+\gamma_1\} = \mathbb{Z}_n$. Logo, $(\gamma_2, \dots, \gamma_n, \gamma_1) = (\gamma_{\theta_n(1)}, \gamma_{\theta_n(2)}, \dots, \gamma_{\theta_n(n)})$ é uma seqüência completa e assim, como $H_n = \langle\theta_n\rangle$, podemos mostrar por indução que $(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \dots, \gamma_{\sigma(n)})$ é uma seqüência completa para todo $\sigma \in H_n$. $\square$

Lema 3.5 *Seja $m = x_1 x_2 \dots x_k$ um monômio multilinear de $K\langle X \rangle$ com $\alpha(m) = \overline{0}$. Se uma substituição standard S (conforme [48])*

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

é tal que $m|_S \neq 0$, então $m_\sigma|_S \neq 0$ para todo $\sigma \in H_k$, onde $m_\sigma = x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(k)}$.

Demonstração. Sendo $m|_S \neq 0$, temos $j_1 = i_2$, $j_2 = i_3$, $\dots$, $j_{k-1} = i_k$. Como $m|_S = E_{i_1 j_k}$ e $\alpha(m) = \overline{0}$, devemos ter $i_1 = j_k$. Observemos que $m_{\theta_k} = x_2 \dots x_k x_1$ e que $m_{\theta_k}|_S = E_{i_2 j_k} E_{i_1 j_1} = E_{i_2 i_2} \neq 0$. O resultado segue então indutivamente. $\square$

Proposição 3.6 *O polinômio multilinear*

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

onde $(\alpha(x_1), \alpha(x_2), \dots, \alpha(x_n))$ é uma seqüência 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 $f|_S \in Z(M_n(K))$ para toda substituição standard S. Pelo lema anterior, se $x_1 x_2 \dots x_n|_S = 0$, então $x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(n)}|_S = 0$ para todo $\sigma \in H_n$, e daí $f|_S = 0$. Suponhamos então S uma substituição standard

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

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

$$f|_S = E_{i_1 i_1} + E_{i_2 i_2} + \dots + E_{i_n i_n}.$$

Observando agora que

$$\alpha(x_1) = \overline{i_2 - i_1} \ , \ \alpha(x_2) = \overline{i_3 - i_2} \ , \ \dots \ , \ \alpha(x_{n-1}) = \overline{i_n - i_{n-1}} \quad \text{e} \quad \alpha(x_n) = \overline{i_1 - i_n}$$

temos

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

Como $(\alpha(x_1), \alpha(x_2), \dots, \alpha(x_n))$ é uma seqüência completa, devemos ter $\overline{i_2 - i_1}$, $\overline{i_3 - i_1}$, $\dots$, $\overline{i_n - i_1}$ não nulos e dois a dois distintos, donde segue que i_1, i_2, $\dots$, i_n devem ser dois a dois incôngruos módulo n. Mas, $\{i_1, i_2, \dots, i_n\} \subseteq \{1, 2, \dots, n\}$. Logo, temos a igualdade destes dois conjuntos e portanto $f|_S = I_{n \times n} \in Z(M_n(K))$. $\square$

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 $I_n \subset C_n(M_n(K))$. Tomemos agora V como sendo o T_n-espaço gerado pelos polinômios

$$\begin{aligned} z_1[x_1,x_2]z_2 \quad &, \quad \alpha(x_1)=\alpha(x_2)=\overline{0}; \\ z_1(x_1x_2x_3-x_3x_2x_1)z_2 \quad &, \quad \alpha(x_1)=\alpha(x_3)=-\alpha(x_2); \\ \sum_{\sigma\in H_n} x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(n)} \quad &, \quad (\alpha(x_1),\alpha(x_2),\ldots,\alpha(x_n)) \text{ seqüência completa} \end{aligned} \tag{3.2}$$

onde z_1 e z_2 são variáveis em X.

Do fato de todos os polinômios em (3.2) serem centrais segue que $V \subseteq C_n(M_n(K))$. Observando agora que o T_n-espaço gerado pelos dois primeiros polinômios em (3.2) é exatamente I_n (lembre que os polinômios em (3.1) geram I_n como T_n-ideal), concluímos que $I_n \subset V$. Nosso objetivo nesta seção é mostrar que $C_n(M_n(K)) = V$ quando $\operatorname{char} K$ não divide n. Vamos começar apresentando as idéias sobre matrizes genéricas $\mathbb{Z}_n$-graduadas desenvolvidas em [3].

Seja $Y = \{y_i^{(\alpha)} \mid i \in \mathbb{N},\ \alpha \in \mathbb{Z}_n\}$ um conjunto de variáveis e consideremos a álgebra polinomial (comutativa) $\Omega = K[Y]$. Para cada $\alpha \in \mathbb{Z}_n$, consideremos o subespaço

$$M_n(\Omega)_\alpha = \{(f_{ij})_{n\times n} \mid f_{ij} \in \Omega,\ f_{ij} = 0 \text{ se } \overline{j-i} \neq \alpha\}$$

da K-álgebra $M_n(\Omega)$. Temos

$$M_n(\Omega) = \bigoplus_{\alpha\in\mathbb{Z}_n} M_n(\Omega)_\alpha$$

e esta decomposição define uma $\mathbb{Z}_n$-graduação em $M_n(\Omega)$.

Observe que se $\alpha \in \mathbb{Z}_n$ e $k \in \{1,2,\ldots,n\}$ é tal que $\alpha = -\overline{k}$, então $M_n(\Omega)_\alpha$ é o conjunto das matrizes da forma

$$\begin{pmatrix} 0 & \cdots & 0 & f_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & f_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & f_k \\ f_{k+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & f_n & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Lema 3.7 *Sejam* $\alpha_l \in \mathbb{Z}_n$ *e*

$$B_l = \begin{pmatrix} 0 & \cdots & 0 & f_l^{(\overline{0})} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & f_l^{(\overline{1})} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & f_l^{(-\alpha_l-\overline{1})} \\ f_l^{(-\alpha_l)} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & f_l^{(\overline{n-1})} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

pertencente a $M_n(\Omega)_{\alpha_l}$*, para* $l = 1, 2, \ldots, m$*. Então cada entrada não nula de* $B_1B_2\ldots B_m$ *é da forma* $f_1^{(\beta_1)}f_2^{(\beta_2)}\ldots f_m^{(\beta_m)}$*, onde* $\beta_q - \beta_p = \alpha_p + \alpha_{p+1}\ldots + \alpha_{q-1}$*, para* $1 \leq p < q \leq m$*.*

Demonstração. É imediato que se g é uma entrada não nula de $B_1B_2\ldots B_m$, então g é da forma $f_1^{(\beta_1)}f_2^{(\beta_2)}\ldots f_m^{(\beta_m)}$. Sendo i_l e j_l os números da linha e da coluna, respectivamente, do elemento $f_l^{(\beta_l)}$ na matriz B_l, $l = 1, 2, \ldots, m$, temos $\overline{j_l - i_l} = \alpha_l$ e $\overline{i_l - 1} = \beta_l$. Como g é uma entrada do produto $B_1B_2\ldots B_m$, devemos ter $j_1 = i_2$, $j_2 = i_3$, $\ldots$, $j_{m-1} = i_m$, e portanto $\alpha_p + \alpha_{p+1} + \ldots + \alpha_{q-1} = \overline{i_q - i_p}$. Tendo em vista que $\beta_q = \overline{i_q - 1}$ e $\beta_p = \overline{i_p - 1}$, o resultado está demonstrado. □

Lema 3.8 *Sejam* $\alpha, \beta \in \mathbb{Z}_n$*, com* $\alpha = -\beta$*,* $A \in M_n(\Omega)_\alpha$ *e* $B \in M_n(\Omega)_\beta$*. Se* $AB = diag(f_{\overline{0}}, f_{\overline{1}}, \ldots, f_{\overline{n-1}})$*, então* $BA = diag(f_\beta, f_{\beta+\overline{1}}, \ldots, f_{\beta+\overline{n-1}})$*.*

Demonstração. Para cada $i = 1, \ldots, n$, denote por $g_{\overline{i-1}}$ a entrada não nula da i-ésima linha de A e por $h_{\overline{i-1}}$ a entrada não nula da i-ésima linha de B. Pelo lema anterior, temos $AB = diag(g_{\overline{0}}h_\alpha, g_{\overline{1}}h_{\alpha+\overline{1}}, \ldots, g_{\overline{n-1}}h_{\alpha+\overline{n-1}})$ e daí $f_\gamma = g_\gamma h_{\gamma+\alpha}$ para todo $\gamma \in \mathbb{Z}_n$. Segue também do lema anterior que $BA = diag(h_{\overline{0}}g_\beta, h_{\overline{1}}g_{\beta+\overline{1}}, \ldots, h_{\overline{n-1}}g_{\beta+\overline{n-1}})$. Mas, para $\gamma \in \mathbb{Z}_n$, vale $f_{\gamma+\beta} = g_{\gamma+\beta}h_{\gamma+\beta+\alpha} = g_{\gamma+\beta}h_\gamma$ e assim temos o resultado. □

Seja $f(x_1, x_2, \ldots, x_m) \in K\langle X\rangle$. Tomando

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

temos $A_i \in M_n(\Omega)_{\alpha(x_i)}$ e $f(A_1, A_2, \ldots, A_m) = (F_{ij})_{n\times n}$, onde $F_{ij} \in \Omega$. De K ser infinito segue que F_{ij} se anula para quaisquer valores de $y_i^{(\alpha)}$ em K se, e somente se, F_{ij} é o polinômio nulo. Logo, $f \in I_n$ se, e somente se, $f(A_1, A_2, \ldots, A_m) = 0$.

Lembrando que o centro de $M_n(K)$ é o conjunto das matrizes escalares e novamente observando que K é um corpo infinito, podemos concluir que $f \in C_n(M_n(K))$ se, e somente se, $f(A_1, A_2, \ldots, A_m) = diag(F, F, \ldots, F)$ para algum $F \in \Omega$.

Definição 3.9 *Sejam* $\omega = y_{i_1}^{(\alpha_1)} y_{i_2}^{(\alpha_2)} \ldots y_{i_q}^{(\alpha_q)}$ *um monômio em* Ω *e* $\delta \in \mathbb{Z}_n$. *Definimos*

$$\omega_\delta = y_{i_1}^{(\alpha_1+\delta)} y_{i_2}^{(\alpha_2+\delta)} \ldots y_{i_q}^{(\alpha_q+\delta)}.$$

Se ω é um monômio de Ω e δ, $\theta \in \mathbb{Z}_n$, observa-se imediatamente que $\omega_{\overline{0}} = \omega$ e que $(\omega_\delta)_\theta = \omega_{\delta+\theta}$. Também não é difícil verificar que se ω_1 e ω_2 são monômios de Ω e $\delta \in \mathbb{Z}_n$, então $(\omega_1)_\delta = (\omega_2)_\delta$ se, e somente se, $\omega_1 = \omega_2$.

Lema 3.10 ([3], Lema 4) *Se* $m = m(x_1, x_2, \ldots, x_k) = x_{i_1} x_{i_2} \ldots x_{i_q}$ *é um monômio em* $K\langle X\rangle$ *e* $\alpha = \alpha(m)$, *então existem* $\alpha_1, \alpha_2, \ldots, \alpha_q \in \mathbb{Z}_n$ *tais que*

$$m(A_1, A_2, \ldots, A_k) = \begin{pmatrix} 0 & \cdots & 0 & \omega_{\overline{0}} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_{\overline{1}} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_{-\alpha-\overline{1}} \\ \omega_{-\alpha} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_{\overline{n-1}} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

com $\omega = y_{i_1}^{(\alpha_1)} y_{i_2}^{(\alpha_2)} \ldots y_{i_q}^{(\alpha_q)}$.

Demonstração. Fixemos $l \in \{1, 2, \ldots, n\}$, arbitrário. Pelo Lema 3.7, temos que a entrada não nula da l-ésima linha de $m(A_1, A_2, \ldots, A_k)$ é igual a $y_{i_1}^{(\beta_1)} y_{i_2}^{(\beta_2)} \ldots y_{i_q}^{(\beta_q)}$, com $\beta_j - \beta_1 = \alpha(A_{i_1}) + \ldots + \alpha(A_{i_{j-1}})$, para $2 \leq j \leq q$. Tomemos então $\alpha_j = \alpha(A_{i_1}) + \ldots + \alpha(A_{i_{j-1}})$, para $2 \leq j \leq q$, e $\alpha_1 = \overline{0}$. Observando agora que $\beta_1 = \overline{l-1}$, temos $\beta_j = \alpha_j + \overline{l-1}$ e daí segue o resultado. □

Corolário 3.11 *Se* γ *é um gerador do grupo* $\mathbb{Z}_n$ *e* $x_1 \in X$ *é tal que* $\alpha(x_1) = \gamma$, *então* $f(x_1) = x_1^n \in C_n(M_n(K))$.

Demonstração. Pelo Lema 3.7 temos que a entrada não nula da primeira linha de A_1^n é $\omega = y_1^{(\overline{0})} y_1^{(\gamma)} y_1^{(2\gamma)} \ldots y_1^{((n-1)\gamma)}$. Usando agora o fato de que $\{\overline{0}, 2\gamma, \ldots, (n-1)\gamma\} = \mathbb{Z}_n$ e o lema anterior, podemos concluir que $f(A_1) = A_1^n = diag(\omega, \omega, \ldots, \omega)$ e assim $f \in C_n(M_n(K))$. □

Observação 3.12 Observamos que o corolário anterior é válido independentemente da característica de K. Quando $\operatorname{char} K$ não divide n, temos que f é conseqüência do polinômio $\sum_{\sigma \in H_n} x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n)}$, onde $\alpha(x_1) = \alpha(x_2) = \ldots = \alpha(x_n) = \gamma$.

Lema 3.13 ([3], Lema 5) *Sejam $m_1(x_1, x_2, \ldots, x_m)$ e $m_2(x_1, x_2, \ldots, x_m)$ monômios de $K\langle X\rangle$. Se as matrizes $m_1(A_1, A_2, \ldots, A_m)$ e $m_2(A_1, A_2, \ldots, A_m)$ têm numa mesma posição a mesma entrada não nula, então $m_1 \equiv m_2 \pmod{I_n}$.*

Demonstração. É imediato do Lema 3.10 e do fato de $(\omega_1)_\delta = (\omega_2)_\delta$ implicar em $\omega_1 = \omega_2$, para $\delta \in \mathbb{Z}_n$ e ω_1 e ω_2 monômios de Ω. □

Lema 3.14 *Seja $m = m(x_1, x_2, \ldots, x_k)$ um monômio de $K\langle X\rangle$ com $\alpha(m) = \overline{0}$. Então existem um inteiro d divisor de n e um monômio $\omega \in \Omega$ tais que*

$$m(A_1, A_2, \ldots, A_k) = diag(\omega_{\overline{0}}, \ldots, \omega_{\overline{d-1}}, \omega_{\overline{0}}, \ldots, \omega_{\overline{d-1}}, \ldots, \omega_{\overline{0}}, \ldots, \omega_{\overline{d-1}}).$$

Demonstração. Pelo Lema 3.10 existe um monômio $\omega \in \Omega$ tal que $m(A_1, A_2, \ldots, A_k) = diag(\omega_{\overline{0}}, \omega_{\overline{1}}, \ldots, \omega_{\overline{n-1}})$. Consideremos agora $G = \{\delta \in \mathbb{Z}_n \mid \omega_\delta = \omega\}$. Como G é não vazio, aditivamente fechado e finito, concluímos que G é um subgrupo de $\mathbb{Z}_n$. Tomando então $d = \frac{n}{|G|}$, temos $G = \langle \overline{d} \rangle = \{\overline{0}, \overline{d}, \overline{2d}, \ldots, \overline{(|G|-1)d}\}$.

Para $\theta \in \mathbb{Z}_n$ consideremos $G_\theta = \{\delta \in \mathbb{Z}_n \mid (\omega_\theta)_\delta = \omega_\theta\}$. Como $(\omega_\theta)_\delta = \omega_{\theta+\delta} = (\omega_\delta)_\theta$, temos claramente $G \subseteq G_\theta$. Por outro lado, se $\delta \in G_\theta$ então $\omega_\theta = (\omega_\theta)_\delta = (\omega_\delta)_\theta$, o que nos dá $\omega_\delta = \omega$. Logo, $G_\theta \subseteq G$.

Mostramos então que $G_\theta = G$ para todo $\theta \in \mathbb{Z}_n$, e daí podemos concluir que $\omega_\delta = \omega_{\delta + \overline{kd}}$, para quaisquer $\delta = \overline{0}, \overline{1}, \ldots, \overline{d-1}$ e $k = 0, 1, \ldots, |G|-1$, e também que $\omega_{\overline{0}}, \omega_{\overline{1}}, \ldots, \omega_{\overline{d-1}}$ são todos distintos. Assim, temos o resultado. □

Lema 3.15 *Seja $m = m(x_1, x_2, \ldots, x_k) = x_{i_1} x_{i_2} \ldots x_{i_q}$ um monômio de $K\langle X\rangle$ tal que $\alpha(m) = \overline{0}$ e uma das entradas de $m(A_1, A_2, \ldots, A_k)$ tem a forma $y_{i_1}^{(\alpha_1)} y_{i_2}^{(\alpha_2)} \ldots y_{i_q}^{(\alpha_q)}$ com $\{\alpha_1, \alpha_2, \ldots, \alpha_q\} = \mathbb{Z}_n$. Então existem monômios $m_1, m_2, \ldots, m_n \in K\langle X\rangle$ tais que $m = m_1 m_2 \ldots m_n$ e $(\alpha(m_1), \alpha(m_2), \ldots, \alpha(m_n))$ é uma seqüência completa.*

Demonstração. Como $\{\alpha_1, \alpha_2, \ldots, \alpha_q\} = \mathbb{Z}_n$ podemos escolher $1 = j_1 < j_2 < \ldots < j_n \leq q$ de modo que $\{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_n}\} = \mathbb{Z}_n$. Para não carregar a notação, vamos renomear as variáveis denotando x_{i_l} por z_l, para $l = 1, 2, \ldots, q$. Daí, $m = z_1 z_2 \ldots z_q$. Tomemos agora

$$m_1 = z_1 \ldots z_{j_2 - 1} \ , \ m_2 = z_{j_2} \ldots z_{j_3 - 1} \ , \ \ldots \ , \ m_{n-1} = z_{j_{n-1}} \ldots z_{j_n - 1} \ , \ m_n = z_{j_n} \ldots z_q.$$

Pelo Lema 3.7 temos

$$\alpha(m_1) = \alpha_{j_2} - \alpha_{j_1} \ , \ \alpha(m_2) = \alpha_{j_3} - \alpha_{j_2} \ , \ \ldots \ , \ \alpha(m_{n-1}) = \alpha_{j_n} - \alpha_{j_{n-1}}$$

e assim

$$\alpha(m_1) = \alpha_{j_2} - \alpha_{j_1}\ ,\ \alpha(m_1) + \alpha(m_2) = \alpha_{j_3} - \alpha_{j_1}\ ,\ \ldots\ ,\ \alpha(m_1) + \ldots + \alpha(m_{n-1}) = \alpha_{j_n} - \alpha_{j_1}.$$

Como $\{\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_n}\} = \mathbb{Z}_n$, temos que $\{\overline{0}, \alpha_{j_2} - \alpha_{j_1}, \ldots, \alpha_{j_n} - \alpha_{j_1}\} = \mathbb{Z}_n$ e, além disso, $\alpha(m_1) + \alpha(m_2) + \ldots + \alpha(m_n) = \alpha(m) = \overline{0}$. Logo, $(\alpha(m_1), \alpha(m_2), \ldots, \alpha(m_n))$ é uma seqüência completa. □

Vamos agora ao principal resultado desta seção, o qual afirma, em outras palavras, que todo polinômio central $\mathbb{Z}_n$-graduado para $M_n(K)$ é conseqüência dos polinômios em (3.2), quando $\operatorname{char} K$ não divide n.

Teorema 3.16 *Se* $\operatorname{char} K$ *não divide* n, *então* $C_n(M_n(K)) = V$.

Demonstração. Seja $f = f(x_1, x_2, \ldots, x_m) \in C_n(M_n(K))$. Como K é infinito, podemos supor que f é multi-homogêneo. Assim, todos os monômios de f têm exatamente as mesmas variáveis com os mesmos graus, donde todos esses monômios têm o mesmo $\mathbb{Z}_n$-grau. Segue então que f é homogêneo com respeito à $\mathbb{Z}_n$-graduação de $K\langle X\rangle$. Se $\alpha(f) \neq \overline{0}$, então todo valor que f toma em $M_n(K)$ é uma matriz de diagonal nula. Logo, f é uma identidade $\mathbb{Z}_n$-graduada de $M_n(K)$ e portanto $f \in V$. Suponhamos então $\alpha(f) = \overline{0}$.

Seja $f = \lambda_1 m_1 + \lambda_2 m_2 + \ldots \lambda_l m_l$, onde $\lambda_i \in K$ e $m_i = m(x_1, x_2, \ldots, x_m)$ é um monômio. Como $I_n \subset V$, podemos supor que $m_i \not\equiv m_j \ (mod\ I_n)$, ou seja, $m_i(A_1, A_2, \ldots, A_m) \neq m_j(A_1, A_2, \ldots, A_m)$ para $i \neq j$.

Consideremos agora monômios $\omega_1,\ \omega_2,\ \ldots,\ \omega_l \in \Omega$ tais que $m_i(A_1, A_2, \ldots, A_m) = diag((\omega_i)_{\overline{0}}, (\omega_i)_{\overline{1}}, \ldots, (\omega_i)_{\overline{n-1}})$ para $i = 1,\ 2,\ \ldots,\ l$. Temos então

$$f(A_1, A_2, \ldots, A_m) = diag(F_{\overline{0}}, F_{\overline{1}}, \ldots, F_{\overline{n-1}})$$

onde $F_\delta = \lambda_1(\omega_1)_\delta + \lambda_2(\omega_2)_\delta + \ldots + \lambda_l(\omega_l)_\delta$ para $\delta \in \mathbb{Z}_n$. Como $f \in C_n(M_n(K))$, devemos ter $F_{\overline{0}} = F_{\overline{1}} = \ldots = F_{\overline{n-1}}$. Ademais, como $m_i(A_1, A_2, \ldots, A_m) \neq m_j(A_1, A_2, \ldots, A_m)$, para $i \neq j$, devemos ter $\omega_i \neq \omega_j$ (observe o Lema 3.13). Assim, para cada $\delta \in \mathbb{Z}_n$, deve existir $i \in \{1, 2, \ldots, l\}$ tal que $(\omega_i)_\delta = \omega_1$. Consequentemente, para cada $\delta \in \mathbb{Z}_n$, ω_1 contém pelo menos uma variável da forma $y_i^{(\delta)}$. Segue então, pelo Lema 3.15, que existem alguns monômios $p_1,\ p_2,\ \ldots,\ p_n$ em $K\langle X\rangle$, onde $p_i = p_i(x_1, x_2, \ldots, x_m)$, tais que

$$m_1 = p_1 p_2 \ldots p_n \quad \text{e} \quad (\alpha(p_1), \alpha(p_2), \ldots, \alpha(p_n)) \text{ é uma seqüência completa.}$$

Observe que se tomarmos $\delta_j = \alpha(p_{n+1-j} \ldots p_n)$ para $j = 1,\ 2,\ \ldots,\ n$, teremos, pelo Lema 3.4, que $\{\delta_1, \delta_2, \ldots, \delta_n\} = \mathbb{Z}_n$. Consideremos agora $P_j = p_j(A_1, A_2, \ldots, A_m)$, para $j = 1,\ \ldots,$

n, e o polinômio

$$g(x_1, x_2, \ldots, x_m) = \sum_{\sigma \in H_n} p_{\sigma(1)} p_{\sigma(2)} \cdots p_{\sigma(n)} = \sum_{j=1}^{n} p_{n+1-j} \cdots p_n p_1 \cdots p_{n-j}$$

que claramente pertence a V. Observando que

$$P_1 P_2 \ldots P_n = m_1(A_1, A_2, \ldots, A_m) = diag((\omega_1)_{\overline{0}}, (\omega_1)_{\overline{1}}, \ldots, (\omega_1)_{\overline{n-1}})$$

temos, pelo Lema 3.8,

$$P_{n+1-j} \ldots P_n P_1 \ldots P_{n-j} = diag((\omega_1)_{\delta_j}, (\omega_1)_{\delta_j + \overline{1}}, \ldots, (\omega_1)_{\delta_j + \overline{n-1}})$$

e assim, como $\{\delta_1, \delta_2, \ldots, \delta_n\} = \mathbb{Z}_n$,

$$g(A_1, A_2, \ldots, A_m) = \sum_{\delta \in \mathbb{Z}_n} diag((\omega_1)_\delta, (\omega_1)_{\delta+\overline{1}}, \ldots, (\omega_1)_{\delta+\overline{n-1}}).$$

De acordo com o Lema 3.14, seja d o divisor de n tal que $(\omega_1)_\delta = (\omega_1)_{\delta+\overline{kd}}$ para quaisquer $\delta = \overline{0}, \overline{1}, \ldots, \overline{d-1}$ e $k = 0, 1, \ldots, \frac{n}{d} - 1$. Novamente observando que $F_{\overline{0}} = F_{\overline{1}} = \ldots = F_{\overline{n-1}}$, podemos concluir, reordenando os m_i's se necessário, que

$$(\omega_1)_{\overline{1}} = \omega_2 \ , \ (\omega_1)_{\overline{2}} = \omega_3 \ , \ \ldots \ , \ (\omega_1)_{\overline{d-1}} = \omega_d.$$

Logo, temos $\lambda_1 = \lambda_2 = \ldots = \lambda_d$ e

$$m_{i+1}(A_1, A_2, \ldots, A_m) = diag((\omega_1)_{\overline{i}}, (\omega_1)_{\overline{i}+\overline{1}}, \ldots, (\omega_1)_{\overline{i}+\overline{n-1}})$$

para $i = 0, 1, \ldots, d-1$. Segue então de $(\omega_1)_\delta = (\omega_1)_{\delta+\overline{kd}}$ que

$$\sum_{\delta \in \mathbb{Z}_n} diag((\omega_1)_\delta, (\omega_1)_{\delta+\overline{1}}, \ldots, (\omega_1)_{\delta+\overline{n-1}}) = \frac{n}{d} \sum_{i=1}^{d} m_i(A_1, A_2, \ldots, A_m)$$

e portanto

$$g(A_1, A_2, \ldots, A_m) = \frac{n}{d} \sum_{i=1}^{d} m_i(A_1, A_2, \ldots, A_m).$$

Como char K não divide n, temos

$$\sum_{i=1}^{d} m_i(A_1, A_2, \ldots, A_m) = \frac{d}{n} g(A_1, A_2, \ldots, A_m)$$

e assim $m_1 + m_2 + \ldots + m_d \equiv \frac{d}{n} g \pmod{I_n}$. Como conseqüência desta afirmação e das igualdades $\lambda_1 = \lambda_2 = \ldots = \lambda_d$ demonstradas acima, temos $f \equiv \lambda_{d+1} m_{d+1} + \ldots + \lambda_l m_l \pmod{V}$ e assim o resultado segue por indução em l. □

Observação 3.17 Vamos observar agora o caso particular $n = 2$. Mostramos no capítulo anterior que os polinômios centrais $\mathbb{Z}_2$-graduados para $M_2(K)$ (com $\operatorname{char} K \neq 2$) seguem de

$$z_1[x_1, x_2]z_2 \quad , \quad z_1(y_1y_2y_3 - y_3y_2y_1)z_2 \quad \text{e} \quad y_1^2$$

onde as variáveis x_i's têm grau $\overline{0}$ e as y_i's têm grau $\overline{1}$.

Agora, os polinômios em (3.2), no caso $n = 2$, são

$$z_1[x_1, x_2]z_2 \quad , \quad z_1(x_1x_2x_3 - x_3x_2x_1)z_2 \quad , \quad z_1(y_1y_2y_3 - y_3y_2y_1)z_2 \quad \text{e} \quad y_1y_2 + y_2y_1$$

uma vez que a única seqüência completa em $\mathbb{Z}_2$ é $(\overline{1}, \overline{1})$. Observe que $z_1(x_1x_2x_3 - x_3x_2x_1)z_2$ é conseqüência de $z_1[x_1, x_2]z_2$ e que, para $\operatorname{char} K$ diferente de 2, y_1^2 e $y_1y_2 + y_2y_1$ são conseqüências um do outro.

Para concluir esta seção vamos fazer um estudo da quantidade de polinômios centrais $\mathbb{Z}_n$-graduados definidos pela Proposição 3.6. Fixado n inteiro positivo, consideremos os conjuntos

$$SC = \{s = (\gamma_1, \gamma_2, \ldots, \gamma_n) \in \mathbb{Z}_n^n \mid s \text{ é seqüência completa}\}$$

e

$$\mathcal{B} = \{(a_1, a_2, \ldots, a_n) \in \mathbb{Z}_n^n \mid \{a_1, a_2, \ldots, a_n\} = \mathbb{Z}_n \ , \ a_n = \overline{0}\}.$$

É imediato que $|\mathcal{B}| = (n-1)!$. Considerando agora a aplicação $p : SC \longrightarrow \mathcal{B}$, definida por $p(\gamma_1, \gamma_2, \ldots, \gamma_n) = (\gamma_1, \gamma_1 + \gamma_2, \ldots, \gamma_1 + \gamma_2 + \ldots + \gamma_n)$, temos que p é uma bijeção e daí concluímos que $|SC| = (n-1)!$. Apesar de existirem $(n-1)!$ seqüências completas em $\mathbb{Z}_n$, o número de polinômios centrais $\mathbb{Z}_n$-graduados determinados por elas é menor, e o objetivo deste estudo é determinar este número.

Para $\sigma \in H_n$ e $s = (\gamma_1, \gamma_2, \ldots, \gamma_n) \in SC$, definimos $\sigma \cdot s = (\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \ldots, \gamma_{\sigma(n)})$. Pelo Lema 3.4, $\sigma \cdot s \in SC$ e, além disso, $Id \cdot s = s$ (onde Id é a identidade de H_n) e $\sigma_1 \cdot (\sigma_2 \cdot s) = (\sigma_1\sigma_2) \cdot s$ para quaisquer σ_1, $\sigma_2 \in H_n$. Logo, temos uma ação de H_n em SC. Tomemos agora x_1, x_2, $\ldots$, $x_n \in X$ variáveis distintas tais que $\alpha(x_i) = \gamma_i$, para $1 \leq i \leq n$. Sendo $\pi \in H_n$, é fácil ver que os polinômios

$$\sum_{\sigma \in H_n} x_{\sigma(1)}x_{\sigma(2)} \cdots x_{\sigma(n)} \quad \text{e} \quad \sum_{\sigma \in H_n} x_{\pi(\sigma(1))}x_{\pi(\sigma(2))} \cdots x_{\pi(\sigma(n))}$$

determinados pelas seqüências completas s e $\pi \cdot s$, respectivamente, são iguais. Assim, duas seqüências completas numa mesma órbita da ação de H_n em SC determinam o mesmo polinômio. Ademais, seqüências completas em órbitas distintas determinam polinômios distintos. Assim, devemos determinar o número r de órbitas distintas da ação de H_n em SC.

De acordo com a fórmula de Burnside que dá o número de órbitas (veja [18], página 222) temos

$$r = \frac{1}{n} \sum_{\sigma \in H_n} |SC_\sigma|$$

onde $SC_\sigma = \{s \in SC \mid \sigma \cdot s = s\}$. Para determinar $|SC_\sigma|$, observemos primeiramente que se $\sigma_1, \sigma_2 \in H_n$, então σ_1 e σ_2 têm a mesma ordem se, e somente se, $\langle \sigma_1 \rangle = \langle \sigma_2 \rangle$. Logo, se σ_1 e σ_2 têm a mesma ordem, então $SC_{\sigma_1} = SC_{\sigma_2}$. Assim, fixando-se um divisor d de n, tomemos $q = \frac{n}{d}$ e $\delta = \theta_n^q$. Temos que o número de elementos de ordem d do grupo H_n é exatamente $\phi(d)$, onde ϕ é a função de Euler, e que δ é um destes elementos. Desta forma,

$$r = \frac{1}{n} \sum_{d|n} \phi(d)|SC_\delta|$$

e agora vamos determinar $|SC_\delta|$. Para $s = (\gamma_1, \gamma_2, \ldots, \gamma_n) \in SC$, temos que $s \in SC_\delta$ se, e somente se, $\gamma_i = \gamma_{i+q}$ para todo $i = 1, 2, \ldots, n-q$, ou seja, $s \in SC_\delta$ se, e somente se, $s = (\gamma_1, \ldots, \gamma_q, \gamma_1, \ldots, \gamma_q, \ldots, \gamma_1, \ldots, \gamma_q)$. Observe agora que s tem esta forma se, e somente se, $p(s) = (a_1, \ldots, a_{q-1}, a_q, a_q + a_1, \ldots, a_q + a_{q-1}, 2a_q, \ldots, (d-1)a_q + a_1, \ldots, da_q)$, onde $a_j = \gamma_1 + \ldots + \gamma_j$, para $j = 1, 2, \ldots, q$. Como $p(s) \in \mathcal{B}$, temos que $p(s)$ tem esta forma se, e somente se, a_q é um gerador do subgrupo N de ordem d de $\mathbb{Z}_n$ e as classes laterais $a_1 + N$, $\ldots$, $a_{q-1} + N$, N são todas distintas. Nestas condições, o número de possibilidades para a_q é $\phi(d)$ e o número de possibilidades para a seqüência $(a_1, a_2, \ldots, a_{q-1})$ é $d^{q-1}(q-1)!$, pois para cada permutação das classes laterais $a_1 + N, \ldots, a_{q-1} + N$, existem d^{q-1} possibilidades de escolha das entradas da seqüência, lembrando que cada classe lateral tem exatamente d elementos. Concluímos então que $|SC_\delta| = \phi(d)d^{q-1}(q-1)!$ e portanto

$$r = \frac{1}{n} \sum_{d|n} \phi(d)^2 d^{\frac{n}{d}-1} \left(\frac{n}{d} - 1\right)!.$$

3.2 Polinômios centrais $\mathbb{Z}$-graduados

Nesta seção, vamos considerar $K\langle X \rangle$ como sendo a álgebra associativa livre $\mathbb{Z}$-graduada, com $X = \bigcup_{m \in \mathbb{Z}} X_m$, onde X_m é o conjunto das variáveis de $\mathbb{Z}$-grau m.

Fixemos um inteiro positivo n. Consideremos a álgebra $M_n(K)$ e a sua $\mathbb{Z}$-graduação natural, que está definida no Capítulo 1, Exemplo 1.51. A descrição das identidades $\mathbb{Z}$-graduadas de $M_n(K)$, feita primeiramente para char $K = 0$ e depois generalizada para K infinito, é dada pelo seguinte teorema.

Teorema 3.18 ([47, 4]) *Todas as identidades polinomiais da álgebra $\mathbb{Z}$-graduada $M_n(K)$ seguem de*

$$\begin{array}{rcl} x = 0 & , & |\alpha(x)| \geq n; \\ [x_1, x_2] = 0 & , & \alpha(x_1) = \alpha(x_2) = 0; \\ x_1x_2x_3 - x_3x_2x_1 = 0 & , & \alpha(x_1) = \alpha(x_3) = -\alpha(x_2). \end{array} \tag{3.3}$$

Seja I o $\mathrm{T}_{\mathbb{Z}}$-ideal das identidades $\mathbb{Z}$-graduadas de $M_n(K)$ e consideremos o $\mathrm{T}_{\mathbb{Z}}$-espaço W gerado pelos polinômios

$$\begin{array}{rcl} z_1xz_2 & , & |\alpha(x)| \geq n; \\ z_1[x_1, x_2]z_2 & , & \alpha(x_1) = \alpha(x_2) = 0; \\ z_1(x_1x_2x_3 - x_3x_2x_1)z_2 & , & \alpha(x_1) = \alpha(x_3) = -\alpha(x_2); \\ \sum_{\sigma \in H_n} x_{\sigma(1)}x_{\sigma(2)} \dots x_{\sigma(n)} & , & (\overline{\alpha(x_1)}, \overline{\alpha(x_2)}, \dots, \overline{\alpha(x_n)}) \text{ seqüência completa} \end{array} \tag{3.4}$$

onde $|\alpha(x_i)| < n$ e z_1 e z_2 são variáveis em X. Observemos que os três primeiros polinômios em (3.4) são identidades $\mathbb{Z}$-graduadas de $M_n(K)$ e geram I como $\mathrm{T}_{\mathbb{Z}}$-espaço. O quarto é um polinômio central $\mathbb{Z}$-graduado, que não é identidade, para $M_n(K)$, sendo a demonstração deste fato praticamente igual à da Proposição 3.6.

Assim, tomando $C_{\mathbb{Z}}(M_n(K))$ como sendo o $\mathrm{T}_{\mathbb{Z}}$-espaço dos polinômios centrais $\mathbb{Z}$-graduados para $M_n(K)$, temos $I \subset W \subseteq C_{\mathbb{Z}}(M_n(K))$. Nosso objetivo nesta seção é mostrar que $C_{\mathbb{Z}}(M_n(K)) = W$.

Como na seção anterior, vamos considerar a álgebra polinomial (comutativa) $\Omega = K[Y]$, sendo que agora Y será o conjunto $\{y_i^{(k)} \mid i \in \mathbb{N},\ 1 \leq k \leq n\}$. Para cada $k \in \mathbb{Z}$, definimos

$$M_n(\Omega)_k = \{(f_{ij})_{n\times n} \mid f_{ij} \in \Omega,\ f_{ij} = 0 \text{ se } j - i \neq k\}$$

se $|k| < n$, e $M_n(\Omega)_k = \{0\}$, se $|k| \geq n$. Claramente, $M_n(\Omega)_k$ é um subespaço de $M_n(\Omega)$ e

$$M_n(\Omega) = \bigoplus_{k \in \mathbb{Z}_n} M_n(\Omega)_k.$$

Ademais, esta decomposição define uma $\mathbb{Z}$-graduação em $M_n(\Omega)$.

Seja $f(x_1, x_2, \dots, x_m) \in K\langle X \rangle$. Tomando

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

se $0 \leq \alpha(x_i) < n$, ou

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

se $-n < \alpha(x_i) < 0$, temos $A_i \in M_n(\Omega)_{\alpha(x_i)}$ e $f(A_1, A_2, \ldots, A_m) = (F_{ij})_{n\times n}$, onde $F_{ij} \in \Omega$. Observemos que $f \in I$ se, e somente se, $f(A_1, A_2, \ldots, A_m) = 0$, e que $f \in C_{\mathbb{Z}}(M_n(K))$ se, e somente se, $f(A_1, A_2, \ldots, A_m) = diag(F, F, \ldots, F)$ para algum $F \in \Omega$.

Lema 3.19 ([4], Lema 3) *Seja $m(x_1, x_2, \ldots, x_k) = x_{i_1}x_{i_2}\ldots x_{i_q}$ um monômio de $\mathbb{Z}$-grau α em $K\langle X\rangle$. Se $m(A_1, A_2, \ldots, A_k) \neq 0$, então existem s, $t \in \mathbb{N}$, com $1 \leq s \leq t \leq n$, tais que*

$$m(A_1, A_2, \ldots, A_k) = \sum_{l=s}^{t} \omega_l E_{l,l+\alpha}$$

onde $\omega_l = y_{i_1}^{(h_{1,l})} y_{i_2}^{(h_{2,l})} \ldots y_{i_q}^{(h_{q,l})}$ e $h_{j,l+1} = h_{j,l} + 1$ para $s \leq l \leq t-1$ e $1 \leq j \leq q$.

Observação 3.20 a) No lema acima, observamos que $\omega_{l_1} \neq \omega_{l_2}$, para $s \leq l_1 < l_2 \leq t$. Assim, em $m(A_1, A_2, \ldots, A_k)$ não existem duas entradas não nulas iguais.
b) Usando as idéias da demonstração do Lema 3.7, é possível mostrar que para $1 \leq j < k \leq q$ temos

$$h_{k,l} - h_{j,l} = \alpha(x_{i_j}x_{i_{j+1}}\ldots x_{i_{k-1}}) = \alpha(x_{i_j}) + \alpha(x_{i_{j+1}}) + \ldots + \alpha(x_{i_{k-1}}).$$

Lema 3.21 ([4], Lema 5) *Sejam $m_1(x_1, x_2, \ldots, x_m)$ e $m_2(x_1, x_2, \ldots, x_m)$ dois monômios de $K\langle X\rangle$. Se as matrizes $m_1(A_1, A_2, \ldots, A_m)$ e $m_2(A_1, A_2, \ldots, A_m)$ têm numa mesma posição a mesma entrada não nula, então $m_1 \equiv m_2 \pmod{I}$.*

Lema 3.22 *Seja $m = m(x_1, x_2, \ldots, x_k) = x_{i_1}x_{i_2}\ldots x_{i_q}$ um monômio de $K\langle X\rangle$ com $\alpha(m) = 0$. Se uma das entradas de $m(A_1, A_2, \ldots, A_k)$ é da forma $\omega = y_{i_1}^{(h_1)} y_{i_2}^{(h_2)} \ldots y_{i_q}^{(h_q)}$, com $\{h_1, h_2, \ldots, h_q\} = \{1, 2, \ldots, n\}$, então existem monômios m_1, m_2, $\ldots$, $m_n \in K\langle X\rangle$ tais que $m = m_1m_2\ldots m_n$ e $(\overline{\alpha(m_1)}, \overline{\alpha(m_2)}, \ldots, \overline{\alpha(m_n)})$ é uma seqüência completa em $\mathbb{Z}_n$.*

Demonstração. Observe 3.20.b e a demonstração do Lema 3.15. $\square$

Lema 3.23 *Se $B_1, B_2, \ldots, B_n$ são matrizes homogêneas com respeito à $\mathbb{Z}$-graduação de $M_n(\Omega)$ tais que $(\overline{\alpha(B_1)}, \overline{\alpha(B_2)}, \ldots, \overline{\alpha(B_n)})$ é uma seqüência completa em $\mathbb{Z}_n$, então*

$$\sum_{\sigma \in H_n} B_{\sigma(1)} B_{\sigma(2)} \ldots B_{\sigma(n)} = \sum_{\sigma \in H_n} diag(\omega_{\sigma(1)}, \omega_{\sigma(2)}, \ldots, \omega_{\sigma(n)})$$

onde $\omega_1, \omega_2, \ldots, \omega_n \in \Omega$ são tais que $B_1 B_2 \ldots B_n = diag(\omega_1, \omega_2, \ldots, \omega_n)$.

Demonstração. Considere primeiramente A e C duas matrizes $\mathbb{Z}$-homogêneas de $M_n(\Omega)$ tais que $\alpha(A) = -\alpha(C)$. Através de um cálculo simples podemos ver que se $AC = diag(f_1, f_2, \ldots, f_n)$, então $CA = diag(f_{\theta^k(1)}, f_{\theta^k(2)}, \ldots, f_{\theta^k(n)})$, onde $k = \alpha(C)$ e θ é a permutação $(1\ 2\ \ldots\ n)$ de S_n. Assim,

$$B_{n+1-j} \ldots B_n B_1 \ldots B_{n-j} = diag(\omega_{\theta^{k_j}(1)}, \ldots, \omega_{\theta^{k_j}(n)})$$

onde $k_j = \alpha(B_{n+1-j} \ldots B_n)$. Pelo Lema 3.4 temos $\{\overline{k_1}, \ldots, \overline{k_n}\} = \mathbb{Z}_n$ e daí segue que $\{\theta^{k_1}, \ldots, \theta^{k_n}\} = H_n$, o que conclui a demonstração. $\square$

Vamos demonstrar agora o principal resultado desta seção.

Teorema 3.24 $C_{\mathbb{Z}}(M_n(K)) = W$.

Demonstração. Seja $f = f(x_1, x_2, \ldots, x_m) \in C_{\mathbb{Z}}(M_n(K)) - I$. Podemos supor f multi-homogêneo e com $\mathbb{Z}$-grau igual a 0 (observe os argumentos iniciais da demonstração do Teorema 3.16).

Seja $f = \lambda_1 m_1 + \lambda_2 m_2 + \ldots \lambda_l m_l$, com $\lambda_i \in K$ e $m_i = m(x_1, x_2, \ldots, x_m)$ monômio. Como $I \subset W$, podemos supor que $m_i \not\equiv m_j \pmod I$, ou seja, $m_i(A_1, A_2, \ldots, A_m) \neq m_j(A_1, A_2, \ldots, A_m)$ para $i \neq j$.

Consideremos monômios ω_{ij}, $1 \leq i \leq l$ e $1 \leq j \leq n$, de Ω tais que

$$m_i(A_1, A_2, \ldots, A_m) = diag(\omega_{i1}, \omega_{i2}, \ldots, \omega_{in}).$$

Temos então

$$f(A_1, A_2, \ldots, A_m) = diag(F_1, F_2, \ldots, F_n)$$

onde $F_j = \lambda_1 \omega_{1j} + \lambda_2 \omega_{2j} + \ldots + \lambda_l \omega_{lj}$. Segue do Lema 3.21 que se $\omega_{i_1 j}$ e $\omega_{i_2 j}$, com $i_1 \neq i_2$, são não nulos, então $\omega_{i_1 j} \neq \omega_{i_2 j}$. Como $f \in C_n(M_n(K)) - I$, devemos ter $F_1 = F_2 = \ldots = F_n \neq 0$ e assim podemos supor, sem perda de generalidade, que $\omega_{11} \neq 0$. Daí, observando 3.20.a e reordenando os m_i's (se necessário), podemos concluir que $l \geq n$ e $\omega_{11} = \omega_{22} = \ldots = \omega_{nn}$. Segue daí que $\lambda_1 = \lambda_2 = \ldots = \lambda_n$ e que para cada $j \in \{1, 2, \ldots, n\}$ aparece em ω_{11} pelo menos uma variável da forma $y_i^{(j)}$. Logo, pelo Lema 3.22, devem existir monômios p_1, p_2, $\ldots$, p_n em $K\langle X\rangle$ ($p_i = p_i(x_1, x_2, \ldots, x_m)$) tais que

$$m_1 = p_1 p_2 \ldots p_n \quad \text{e} \quad (\overline{\alpha(p_1)}, \overline{\alpha(p_2)}, \ldots, \overline{\alpha(p_n)}) \text{ é uma seqüência completa em } \mathbb{Z}_n.$$

Considerando agora o polinômio

$$g(x_1, x_2, \ldots, x_m) = \sum_{\sigma \in H_n} p_{\sigma(1)} p_{\sigma(2)} \cdots p_{\sigma(n)}$$

que claramente pertence a W, devemos ter

$$g(A_1, A_2, \ldots, A_m) = \sum_{\sigma \in H_n} diag(\omega_{1\sigma(1)}, \omega_{1\sigma(2)}, \ldots, \omega_{1\sigma(n)})$$

pelo Lema 3.23. Segue então do Lema 3.21 e das igualdades $\omega_{11} = \omega_{22} = \ldots = \omega_{nn}$ que $g(x_1, x_2, \ldots, x_m) \equiv m_1 + m_2 + \ldots + m_n \pmod{I}$. Logo, $m_1 + m_2 + \ldots + m_n \in W$. Como conseqüência disto e das igualdades $\lambda_1 = \lambda_2 = \ldots = \lambda_n$, temos $f \equiv \lambda_{n+1} m_{n+1} + \ldots + \lambda_l m_l \pmod{W}$ e assim o resultado segue por indução em l. $\square$

Capítulo 4

Polinômios Centrais para Álgebras com Involução

Devido à importância das álgebras com involução, as descrições de suas identidades e de seus polinômios centrais são questões de grande interesse. No caso particular de $M_2(K)$, a descrição das identidades com involução já é conhecida, tendo sido feita primeiramente para $\operatorname{char} K = 0$ e para K finito por Levchenko [35, 36] e depois para K infinito de característica diferente de 2 por Colombo e Koshlukov [10].

Neste capítulo vamos apresentar as descrições feitas em [8] dos polinômios centrais com involução para a álgebra $M_2(K)$, considerando as involuções transposta e simplética. Antes, porém, será necessário um breve estudo sobre involuções, o qual será feito nas duas primeiras seções. Nesse estudo apresentaremos conceitos e resultados básicos e veremos que, em se tratando de identidades e polinômios centrais com involução do primeiro tipo para $M_2(K)$, só é preciso realmente considerar as involuções transposta e simplética.

Em todo este capítulo K será sempre um corpo infinito de característica diferente de 2.

4.1 Álgebras com involução

Nesta seção estudaremos o conceito de involução. Vamos ver exemplos, propriedades e as idéias básicas sobre identidades e polinômios centrais para álgebras com involução.

Definição 4.1 *Seja A uma álgebra. Dizemos que uma aplicação $* : A \longrightarrow A$ é uma involução se*

$$(a^*)^* = a \quad , \quad (a+b)^* = a^* + b^* \quad e \quad (ab)^* = b^*a^*$$

para quaisquer $a, b \in A$.

Sendo $*$ uma involução em A e $a \in A$, observamos que $a1^* = 1^*a = a$ e assim $1^* = 1$. Observamos também que $*$ é uma transformação linear se, e somente se, $*|_K = Id_K$.

Quando uma involução é também uma transformação linear dizemos que ela é do *primeiro tipo*. Caso contrário, dizemos que é do *segundo tipo*. Neste trabalho trataremos apenas de involuções do primeiro tipo.

Exemplo 4.2 A aplicação $t : M_n(K) \longrightarrow M_n(K)$, definida por $A^t =$ transposta de A, é uma involução do primeiro tipo em $M_n(K)$.

Exemplo 4.3 A aplicação $s : M_{2n}(K) \longrightarrow M_{2n}(K)$, definida por

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^s = \begin{pmatrix} D^t & -B^t \\ -C^t & A^t \end{pmatrix}$$

onde A, B, C, $D \in M_n(K)$, é uma involução do primeiro tipo em $M_{2n}(K)$, chamada de involução simplética.

Exemplo 4.4 Considerando $M_2(\mathbb{C})$ como $\mathbb{C}$-álgebra, temos que $* : M_2(\mathbb{C}) \longrightarrow M_2(\mathbb{C})$, definida por

$$\begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix}^* = \begin{pmatrix} \overline{z_1} & \overline{z_3} \\ \overline{z_2} & \overline{z_4} \end{pmatrix}$$

é uma involução do segundo tipo.

Observação 4.5 Se $*$ é uma involução em A, então $G_* = \{x \in U(A) \mid x^*x = 1\}$ é um subgrupo de $U(A)$. No caso $A = M_n(K)$, temos $U(A) = GL_n(K)$, o grupo linear, e $G_t = O_n(K)$, o grupo ortogonal (por esta razão a involução transposta é também chamada de ortogonal). Sendo n par, temos $G_s = Sp_n(K)$, o grupo simplético.

Seja $(A, *)$ uma álgebra com involução. Dizemos que um elemento a em $(A, *)$ é *simétrico* se $a^* = a$ e que é *anti-simétrico* se $a^* = -a$. É fácil ver que $A^+ = \{a \in A \mid a^* = a\}$ e $A^- = \{a \in A \mid a^* = -a\}$ são subespaços de A e que $A^+ \cap A^- = \{0\}$. Ademais, dado $a \in A$, temos

$$a = \frac{a + a^*}{2} + \frac{a - a^*}{2}$$

e assim, como o primeiro termo no segundo membro é simétrico e o segundo anti-simétrico, temos $A = A^+ \oplus A^-$.

Definimos um *homomorfismo de álgebras com involução* $\varphi : (A_1, *) \longrightarrow (A_2, \eta)$ como sendo um homomorfismo $\varphi : A_1 \longrightarrow A_2$ que satisfaz $\varphi(a^*) = \varphi(a)^\eta$ para todo $a \in A_1$. Quando existe um isomorfismo nestas condições, dizemos que as álgebras com involução $(A_1, *)$ e (A_2, η) são isomorfas e denotamos $(A_1, *) \simeq (A_2, \eta)$.

Vamos agora falar de identidades e polinômios centrais com involução. Para isso, precisamos definir a álgebra associativa livre com involução. Sejam $X = \{x_1, x_2, x_3, \ldots\}$ e $Y = \{y_1, y_2, y_3, \ldots\}$ conjuntos disjuntos de variáveis e tomemos a álgebra associativa livre $K\langle X \cup Y\rangle$. Consideremos a aplicação linear $* : K\langle X \cup Y\rangle \longrightarrow K\langle X \cup Y\rangle$ que satisfaz $1^* = 1$, $x_i^* = x_i$ e $y_i^* = -y_i$ para todo $i \in \mathbb{N}$, e

$$(z_1 z_2 \ldots z_k)^* = z_k^* \ldots z_2^* z_1^*$$

para quaisquer $z_1, z_2, \ldots, z_k \in X \cup Y$. Sendo então $m_1 = z_1 \ldots z_l$ e $m_2 = z_{l+1} \ldots z_n$ monômios em $K\langle X \cup Y\rangle$ temos

$$(m_1 m_2)^* = z_n^* \ldots z_{l+1}^* z_l^* \ldots z_1^* = m_2^* m_1^*.$$

Ademais, é fácil ver que $m_1^{**} = m_1$. Logo, $*$ é uma involução e $K\langle X \cup Y\rangle$ é chamada de *álgebra associativa livre com involução*, sendo X o conjunto das *variáveis simétricas* e Y o das *variáveis anti-simétricas*. Dizemos que um endomorfismo φ de $K\langle X \cup Y\rangle$ é um $*$-*endomorfismo* se $\varphi(x_i)$ é simétrico e $\varphi(y_i)$ é anti-simétrico para todo $i \in \mathbb{N}$ (isto é equivalente a dizer que φ comuta com $*$).

Estamos prontos agora para definir identidades e polinômios centrais para uma álgebra com involução.

Definição 4.6 *Sejam $f(x_1, \ldots, x_n, y_1, \ldots, y_m) \in K\langle X \cup Y\rangle$ e $(A, *)$ uma álgebra com involução. Dizemos que f é uma identidade de $(A, *)$ se $f(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0$ para quaisquer $a_i \in A^+$ e $b_j \in A^-$. Dizemos que f é um polinômio central para $(A, *)$ se $f(a_1, \ldots, a_n, b_1, \ldots, b_m) \in Z(A)$ para quaisquer $a_i \in A^+$ e $b_j \in A^-$.*

Exemplo 4.7 Consideremos a álgebra $M_2(K)$ com a involução transposta. Se A_1 e A_2 são elementos anti-simétricos e B é um elemento simétrico de $(M_2(K), t)$, então $[A_1, A_2] = 0$ e $[A_2, A_1 \circ B] = 0$ (é fácil ver que $(A_1 \circ B)^t = -A_1 \circ B$ e que duas matrizes anti-simétricas 2×2 comutam). Logo,

$$0 = [A_2, A_1 \circ B] = [A_2, A_1] \circ B + A_1 \circ [A_2, B] = A_1 \circ [A_2, B]$$

e assim $f(x_1, y_1, y_2) = y_1 \circ [y_2, x_1]$ é identidade de $(M_2(K), t)$. Conforme veremos na Seção 4.3, $g(y_1, y_2) = y_1 y_2$ é um polinômio central para $(M_2(K), t)$.

Dizemos que um ideal (resp. subespaço) J de $K\langle X \cup Y\rangle$ é um $*$-*ideal* (resp. $*$-*espaço*) se $\varphi(J) \subseteq J$ para todo $*$-endomorfismo φ de $K\langle X \cup Y\rangle$ (isto equivale a dizer que $f(g_1, \ldots, g_n, h_1, \ldots, h_m) \in J$ para quaisquer $f(x_1, \ldots, x_n, y_1, \ldots, y_m) \in J$ e $g_1, \ldots, g_n$ elementos simétricos e $h_1, \ldots, h_m$ elementos anti-simétricos de $K\langle X \cup Y\rangle$). Temos que o conjunto $T(A,*)$ das identidades da álgebra com involução $(A,*)$ é um $*$-ideal e que o conjunto $C(A,*)$ dos polinômios centrais para $(A,*)$ é um $*$-espaço.

As idéias de $*$-ideal e $*$-espaço gerados por um conjunto e de redução para polinômios multi-homogêneos (lembrando que K é infinito) são análogas àquelas relacionadas com identidades e polinômios centrais ordinários e graduados.

Encerraremos esta seção falando de *polinômios $*$-próprios* e *posto de um polinômio.* Vamos definir um comutador de grau 1 como sendo simplesmente uma variável de $X \cup Y$.

Definição 4.8 *Dizemos que um polinômio $f \in K\langle X \cup Y\rangle$ é $*$-próprio se f é uma combinação linear de produtos de variáveis anti-simétricas seguidas por comutadores de grau maior ou igual a 2.*

Observando o que foi desenvolvido na Seção 1.4, consideremos uma base ordenada de $L(X \cup Y)$ formada por

$$x_1,\ x_2,\ x_3,\ \ldots, y_1,\ y_2,\ y_3,\ \ldots, u_1,\ u_2,\ u_3,\ \ldots$$

onde $u_i = [z_{i_1}, z_{i_2}, \ldots, z_{i_k}]$, com $z_{i_j} \in X \cup Y$ e $k \geq 2$. Temos então que existe uma base de $K\langle X \cup Y\rangle$ formada pelos elementos

$$x_{i_1}^{n_1} x_{i_2}^{n_2} \ldots x_{i_p}^{n_p} y_{j_1}^{m_1} y_{j_2}^{m_2} \ldots y_{j_q}^{m_q} u_{l_1} u_{l_2} \ldots u_{l_k} \quad , \quad p,\ q,\ k,\ n_i,\ m_j \geq 0.$$

Definição 4.9 *Seja f um polinômio multi-homogêneo em $K\langle X \cup Y\rangle$. Escrevendo*

$$f = \sum_a \alpha_a x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} g_a$$

onde g_a é um polinômio $*$-próprio, definimos o posto de f, denotado por $r(f)$, como sendo a maior n-upla $a = (a_1, a_2, \ldots, a_n)$ na ordem lexicográfica.

Como f possui uma única expressão na forma acima, temos que $r(f)$ está bem definido. Observemos que, de acordo com esta definição, f é $*$-próprio se, e somente se, $r(f) = (0, 0, \ldots, 0)$. É importante observar também que a ordem lexicográfica é uma boa ordem no conjunto $\mathbb{N}_0^n = \mathbb{N}_0 \times \ldots \times \mathbb{N}_0$ ($\mathbb{N}_0 = \mathbb{N} \cup \{0\}$) e assim o princípio da indução é válido, sendo portanto possível fazer indução em $r(f)$.

Vejamos agora o que há de importante por trás do conceito de polinômio $*$-próprio. Considere um polinômio multi-homogêneo

$$f(x_1, \ldots, x_n, y_1, \ldots, y_m) = \alpha x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n} g + \sum_a \alpha_a x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} g_a \tag{4.1}$$

onde α, $\alpha_a \in K - \{0\}$, g e g_a são $*$-próprios e $a = (a_1, a_2, \ldots, a_n) < (b_1, b_2, \ldots, b_n) = r(f)$ (na ordem lexicográfica). Observe que quanto maior a entrada a_1 na n-upla a, menor é o grau de x_1 em g_a.

Como em g e em g_a não aparecem variáveis simétricas fora de comutadores, a substituição de x_i por $x_i + 1$ não altera estes polinômios e assim

$$f(x_1+1, x_2, \ldots, x_n, y_1, \ldots, y_m) = \alpha(x_1+1)^{b_1} x_2^{b_2} \ldots x_n^{b_n} g + \sum_a \alpha_a (x_1+1)^{a_1} x_2^{a_2} \ldots x_n^{a_n} g_a.$$

Observe que a componente de menor grau em x_1 deste polinômio é

$$f_1 = \alpha x_2^{b_2} \ldots x_n^{b_n} g + \sum_a \alpha_a x_2^{a_2} \ldots x_n^{a_n} g_a$$

onde o somatório é sobre todos os a's tais que $a_1 = b_1$. Observe também que para $a_1 = b_1$, temos $(b_2, \ldots, b_n) > (a_2, \ldots, a_n)$.

Consideremos agora o polinômio $f_1(x_1, x_2+1, x_3, \ldots, x_n, y_1, \ldots, y_m)$ e tomemos a sua componente de menor grau em x_2, que é

$$f_2 = \alpha x_3^{b_3} \ldots x_n^{b_n} g + \sum_a \alpha_a x_3^{a_3} \ldots x_n^{a_n} g_a$$

onde o somatório é sobre todos os a's tais que $a_1 = b_1$ e $a_2 = b_2$. Temos que para $a_1 = b_1$ e $a_2 = b_2$ vale $(b_3, \ldots, b_n) > (a_3, \ldots, a_n)$.

Substituindo x_3 por $x_3 + 1$ em f_2 e continuando com esse processo, vamos chegar ao polinômio $f_n = \alpha g$. A partir dessas idéias, temos o seguinte resultado.

Proposição 4.10 *Sejam V um $*$-espaço de $K\langle X \cup Y \rangle$ e $f \in V$ (f como em (4.1)). Então $g \in V$. Ademais, se V é um $*$-ideal, então os polinômios g_a's também estão em V. Consequentemente, todo $*$-ideal é gerado por seus polinômios $*$-próprios.*

Demonstração. Como 1 é simétrico, temos que $x_1 + 1$ é simétrico e daí o polinômio $f(x_1+1, x_2, \ldots, x_n, y_1, \ldots, y_m)$ pertence a V. Como K é infinito, temos $f_1 \in V$ (veja a Seção 1.5) e assim, como $x_2 + 1$ é simétrico, temos $f_1(x_1, x_2+1, x_3, \ldots, x_n, y_1, \ldots, y_m) \in V$. Novamente usando o fato de K ser infinito, concluímos que $f_2 \in V$. Seguindo assim chegamos a $f_n \in V$ e daí $g \in V$.

Se V é um $*$-ideal, temos $\alpha x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n} g \in V$ e portanto o somatório em (4.1) também pertence a V. Usando então indução no posto, concluímos que os g_a's também estão em V, donde segue a última afirmação. □

Observemos que este processo de "eliminação" de variáveis simétricas fora de comutadores usado na proposição anterior não funciona para variáveis anti-simétricas, pois a substituição de y_i por $y_i + 1$ não define um $*$-endomorfismo de $K\langle X \cup Y \rangle$, uma vez que $y_i + 1$ não é anti-simétrico.

4.2 Involuções em álgebras centrais simples

Seja A uma álgebra central simples de dimensão finita. Nosso objetivo nesta seção é estudar a idéia de equivalência de involuções em A (na Seção 1.1 apresentamos conceitos e resultados importantes aqui). Como resultado deste estudo, teremos a classificação das involuções do primeiro tipo na álgebra $M_n(K)$.

Sejam $*, J \in Inv(A)$, o conjunto das involuções do primeiro tipo em A.

Lema 4.11 *Se $* = J\zeta_r$ para algum $r \in U(A)$, então $r^* = r^J = \pm r$.*

Demonstração. Temos $r^{J*} = r^{JJ\zeta_r} = r^{\zeta_r} = r$ e daí $r^J = r^*$. Para x qualquer em A temos $x = x^{**} = (x^{J\zeta_r})^* = (r^{-1}x^J r)^* = r^* x^{J*}(r^*)^{-1} = r^* r^{-1} x r (r^*)^{-1}$ e assim $r^* r^{-1} \in Z(A)$. Logo, existe $\lambda \in K$ tal que $r^* = \lambda r$. De $r^{**} = r$ segue que $\lambda^2 r = r$ e portanto $\lambda^2 = 1$. Como K é um corpo, devemos ter $\lambda = \pm 1$, o que conclui a demonstração. □

Teorema 4.12 (Albert) *Existe $r \in U(A)$, com $r^J = r^* = \pm r$, tal que $* = J\zeta_r$. Reciprocamente, se $r \in U(A)$ e $r^J = \pm r$, então $J\zeta_r \in Inv(A)$.*

Demonstração. Como $J*$ é um automorfismo de A, temos, pela Proposição 1.13 , que $J* = \zeta_r$ para algum $r \in U(A)$, e daí $* = J\zeta_r$. Pelo lema anterior temos $r^J = r^* = \pm r$. Reciprocamente, tomando $J_1 = J\zeta_r$, com $r \in U(A)$ e $r^J = \pm r$, temos $a^{J_1 J_1} = r^{-1}(r^{-1}a^J r)^J r = r^{-1} r^J a (r^J)^{-1} r = a$ para todo $a \in A$. As outras condições são de verificação imediata. □

Definição 4.13 *Dizemos que $*$ e J são equivalentes se existe $r \in U(A)$ $*$-simétrico tal que $* = J\zeta_r$.*

Observemos que a definição acima nos dá uma relação de equivalência em $Inv(A)$. De fato, a reflexividade é imediata. Para ver a simetria, basta observar que $* = J\zeta_r$ implica em $J = *\zeta_{r^{-1}}$ e aplicar o Lema 4.11. Quanto a transitividade, supondo $J_1, J_2, J_3 \in Inv(A)$ e $r_1, r_2 \in U(A)$, com $r_1^{J_1} = r_1$ e $r_2^{J_2} = r_2$, tais que $J_1 = J_2\zeta_{r_1}$ e $J_2 = J_3\zeta_{r_2}$, temos $J_1 = J_3\zeta_{r_2 r_1}$ e $(r_2 r_1)^{J_1} = r_1^{J_1} r_2^{J_1} = r_1 r_2^{J_2\zeta_{r_1}} = r_2 r_1$. Logo, J_1 e J_3 são equivalentes.

Teorema 4.14 *A relação dada na Definição 4.13 determina, no máximo, duas classes de equivalência em $Inv(A)$. Ademais, se $* = J\zeta_r$ para algum $r \in U(A)$ $*$-anti-simétrico, então $*$ e J não são equivalentes.*

Demonstração. Sejam $J_1, J_2, * \in Inv(A)$, com J_1 e J_2 não equivalentes e $*$ não equivalente a J_2. Existem então $r_1, r_2 \in U(A)$, com $r_1^{J_1} = r_1^{J_2} = -r_1$ e $r_2^{J_2} = r_2^* = -r_2$, tais que $J_1 = J_2\zeta_{r_1}$ e $J_2 = *\zeta_{r_2}$. Daí, $J_1 = *\zeta_{r_2 r_1}$ e $(r_2 r_1)^{J_1} = r_1^{J_1} r_2^{J_1} = -r_1(r_1^{-1} r_2^{J_2} r_1) = r_2 r_1$. Logo, $*$ é equivalente a J_1.

Supondo agora $* = J\zeta_r$ e $* = J\zeta_{r_1}$, com $r^* = -r$ e $r_1^* = r_1$, temos $\zeta_r = \zeta_{r_1}$ e daí $r_1 r^{-1} \in Z(A)$. Logo, $r_1 = \lambda r$ para algum $\lambda \in K$, o que nos dá $r_1^* = -r_1$. Mas, isto é uma contradição e assim $*$ e J não podem ser equivalentes. □

Vamos agora olhar para a álgebra $M_n(K)$. Sendo $n = 2m$ e $X = \begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$, com $X_1, X_2, X_3, X_4 \in M_m(K)$. temos

$$X^t = \begin{pmatrix} X_1^t & X_3^t \\ X_2^t & X_4^t \end{pmatrix} \quad \text{e} \quad X^s = \begin{pmatrix} X_4^t & -X_2^t \\ -X_3^t & X_1^t \end{pmatrix}$$

donde observamos que $t = s\zeta_C$ para $C = \begin{pmatrix} 0 & I_{m\times m} \\ -I_{m\times m} & 0 \end{pmatrix}$. Como $C^t = -C$, temos que t e s não são equivalentes e assim há duas classes de equivalência em $Inv(M_n(K))$.

Supondo agora n ímpar e $*$ uma involução qualquer em $M_n(K)$, temos $t = *\zeta_B$ para algum $B \in GL_n(K)$ tal que $B^t = \pm B$. Mas, se $B^t = -B$, então $detB = det(-B) = -detB$ e assim $detB = 0$, o que é um absurdo. Logo, $B^t = B$ e portanto $*$ é equivalente a t.

Teorema 4.15 *Seja $*$ uma involução do primeiro tipo em $M_n(K)$. Se $*$ é equivalente a t (resp. a s), então para alguma extensão L do corpo K, estendendo naturalmente $*$ para $M_n(L) = M_n(K) \otimes_K L$, temos $(M_n(L), *) \simeq (M_n(L), t)$ (resp. $(M_n(L), *) \simeq (M_n(L), s)$). Consequentemente, como K é um corpo infinito, temos $T(M_n(K), *) = T(M_n(K), t)$ (resp. $T(M_n(K), *) = T(M_n(K), s)$).*

Demonstração. Veja [45], página 169, Teorema 3.1.61. □

Segue imediatamente deste teorema que $C(M_2(K), *) = C(M_2(K), t)$, se $*$ é equivalente a t, ou $C(M_2(K), *) = C(M_2(K), t)$, se $*$ é equivalente a s. Assim, precisamos estudar apenas os $*$-espaços $C(M_2(K), t)$ e $C(M_2(K), s)$.

4.3 A involução transposta

A involução transposta na álgebra $M_2(K)$ é a aplicação $t : M_n(K) \longrightarrow M_n(K)$, definida por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Observemos que os elementos simétricos de $(M_2(K), t)$ são as matrizes da forma $\begin{pmatrix} a & b \\ b & d \end{pmatrix}$ e os anti-simétricos são as da forma $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$.

A descrição das identidades de $(M_2(K), t)$, feita primeiramente para char $K = 0$ e depois generalizada para K infinito de característica diferente de 2, é dada pelo seguinte teorema.

Teorema 4.16 ([35, 10]) *O $*$-ideal $T(M_2(K), t)$ é gerado pelos polinômios*

$$[y_1 y_2, x_1] \tag{4.2}$$

$$[y_1, y_2] \tag{4.3}$$

$$[x_1, x_2][x_3, x_4] - [x_1, x_3][x_2, x_4] + [x_2, x_3][x_1, x_4] \tag{4.4}$$

$$[y_1 x_1 y_2, x_2] - y_1 y_2 [x_2, x_1]. \tag{4.5}$$

Consideremos agora os seguintes polinômios

$$y_1 \circ [y_2, x_1] \tag{4.6}$$

$$[y_1, x_1][y_2, x_2] - 2 y_1 y_2 [x_2, x_1] + [y_1, x_1, x_2] y_2. \tag{4.7}$$

Conforme vimos no Exemplo 4.7, o polinômio (4.6) é uma identidade de $(M_2(K), t)$. O polinômio (4.7) também é uma identidade de $(M_2(K), t)$. Para ver isso, basta observar que ele é multilinear e verificar que se anula para quaisquer valores de x_1 e x_2 em $\{E_{11}, E_{22}, E_{12}+E_{21}\}$ (que é uma base para as matrizes simétricas) e para $y_1 = y_2 = E_{12} - E_{21}$. Uma outra demonstração pode ser encontrada em [10], seção 2.

A partir de agora, vamos denotar $T(M_2(K), t)$ por I. Seja V o $*$-espaço de $K\langle X \cup Y\rangle$ gerado pelos polinômios

$$\begin{gathered} y_1 y_2 \quad , \quad z_1[y_1 y_2, x_1] z_2 \quad , \quad z_1[y_1, y_2] z_2 \\ z_1([x_1, x_2][x_3, x_4] - [x_1, x_3][x_2, x_4] + [x_2, x_3][x_1, x_4]) z_2 \\ z_1([y_1 x_1 y_2, x_2] - y_1 y_2 [x_2, x_1]) z_2. \end{gathered} \tag{4.8}$$

Observemos que $I \subset V$. Mais precisamente, $V = I + V_1$, onde V_1 é $*$-espaço de $K\langle X \cup Y\rangle$ gerado por $y_1 y_2$. Nosso objetivo nesta seção é mostrar que $C(M_2(K), t) = V$. Como

$$\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix} = \begin{pmatrix} -ab & 0 \\ 0 & -ab \end{pmatrix} \in Z(M_2(K))$$

para quaisquer a, $b \in K$, concluímos que $y_1 y_2 \in C(M_2(K), t)$. Ademais, os outros polinômios em (4.8) são identidades e portanto centrais para $(M_2(K), t)$. Logo, $V \subseteq C_2(M_2(K), t)$.

No sentido de demonstrar a inclusão contrária, nosso primeiro passo será mostrar que todos os polinômios $*$-próprios de $C(M_2(K), t)$ estão em V.

Observação 4.17 Através de cálculos simples e rápidos, podemos verificar que os polinômios $(x_1 \circ y_1)$, $[x_1, x_2]$, $[y_1, y_2]$ e $y_1 y_2 y_1$ são anti-simétricos e que o polinômio $[x_1, y_1]$ é simétrico.

Lema 4.18 $y_1y_2\dots y_{2n-1}y_{2n} \in V$ *para todo* $n \geq 1$.

Demonstração. Vamos usar indução em n. Para $n = 1$ o resultado é imediato. Suponhamos então que é válido para $n \geq 1$. Pela observação anterior, $y_{2n+1}y_{2n}y_{2n+1}$ é anti-simétrico e assim, trocando y_{2n} por $y_{2n+1}y_{2n}y_{2n+1}$ em $y_1\dots y_{2n-1}y_{2n}$ (que pertence a V), temos que $y_1\dots y_{2n-1}y_{2n+1}y_{2n}y_{2n+1} \in V$. Segue da identidade (4.3) que

$$y_1\cdots y_{2n-1}y_{2n+1}y_{2n}y_{2n+1} \equiv y_1\cdots y_{2n-1}y_{2n}y_{2n+1}^2 \pmod{I}$$

Como $I \subset V$ e $y_{2n+1} + y_{2n+2}$ é anti-simétrico, podemos afirmar que

$$y_1\cdots y_{2n-1}y_{2n}(y_{2n+1} + y_{2n+2})^2 \in V.$$

Mas, este último polinômio é congruente módulo I a

$$y_1\cdots y_{2n}y_{2n+1}^2 + 2y_1\cdots y_{2n}y_{2n+1}y_{2n+2} + y_1\cdots y_{2n}y_{2n+2}^2$$

e como o primeiro e o terceiro termos deste polinômio estão em V, temos o resultado. □

Lema 4.19 *Todo comutador de grau maior ou igual a* 2 *em* $K\langle X \cup Y\rangle$ *é congruente módulo* I *a uma combinação linear de produtos de comutadores das formas:*

$$y_i \quad , \quad [y_i, x_{i_1}, \dots, x_{i_k}]\ (k \geq 1) \quad , \quad [x_{i_1}, \dots, x_{i_l}]\ (l \geq 2). \tag{4.9}$$

Demonstração. Vamos usar indução no grau do comutador. Se v é um comutador de grau 2, então $v = [x_i, x_j]$, $v = [x_i, y_j] = -[y_j, x_i]$ ou $v = [y_i, y_j]$. Como $[y_i, y_j] \in I$ e os demais têm uma das formas em (4.9), temos o resultado válido para comutadores de grau 2.

Suponhamos agora que o resultado vale para comutadores de grau $n \geq 2$ e tomemos v um comutador de grau $n + 1$. Temos que $v = [w, x]$ ou $v = [w, y]$, onde w é um comutador de grau n. Por hipótese de indução, w é uma combinação linear de produtos $w_1w_2\dots w_l$, onde cada w_i tem uma das formas em (4.9). No caso $v = [w, x]$, observemos que

$$[w_1w_2\dots w_l, x] = \sum_{i=1}^{l} w_1\dots w_{i-1}[w_i, x]w_{i+1}\dots w_l.$$

Como $[w_i, x]$ tem necessariamente uma das formas em (4.9), este caso está concluído. Já no caso $v = [w, y]$, basta observar que

$$[w_1w_2\dots w_l, y] = w_1w_2\dots w_ly - yw_1w_2\dots w_l$$

e que ambos os termos no segundo membro têm a forma desejada. □

Lema 4.20 *Seja $f \in K\langle X \cup Y\rangle$ $*$-próprio. Então, módulo I, f se escreve como uma soma $f_1 + f_2 + f_3$, onde f_1, f_2 e f_3 são combinações lineares de polinômios das formas*

$$u_1u_2\ldots u_{2n} \quad , \quad u_1u_2\ldots u_{2n}u_{2n+1} \quad , \quad u_1\ldots u_m w$$

respectivamente, onde cada u_i é um comutador anti-simétrico de grau maior ou igual a 1 e w é um comutador simétrico de grau maior ou igual a 2.

Demonstração. Sendo f $*$-próprio, temos que f é uma combinação linear de produtos de comutadores, sendo os comutadores de grau 1 variáveis anti-simétricas. Assim, pelo lema anterior, f é congruente módulo I a uma combinação linear de produtos $w_1w_2\ldots w_l$, onde cada w_i tem uma das formas em (4.9). Vamos então analisar estes produtos. Se para algum i temos w_i simétrico e w_{i+1} anti-simétrico, então necessariamente $w_i = [v, x]$, onde v é um comutador anti-simétrico e x é uma variável simétrica (observe (4.9)). Logo, segue da identidade (4.6) que $w_iw_{i+1} \equiv -w_{i+1}w_i \pmod{I}$.

Considerando agora a situação w_i e w_{i+1} simétricos para algum i, temos $w_i = [v_1, x_{i_1}]$ e $w_{i+1} = [v_2, x_{i_2}]$, onde v_1 e v_2 são comutadores anti-simétricos. Usando a identidade (4.7), concluímos que

$$w_iw_{i+1} = [v_1, x_{i_1}][v_2, x_{i_2}] \equiv 2v_1v_2[x_{i_2}, x_{i_1}] - [v_1, x_{i_1}, x_{i_2}]v_2 \pmod{I}.$$

Tendo em vista que os elementos $[x_{i_2}, x_{i_1}]$ e $[v_1, x_{i_1}, x_{i_2}]$ são anti-simétricos, a demonstração está concluída. □

Proposição 4.21 *Se $f \in C(M_2(K), t)$ é $*$-próprio, então f é congruente a f_1 módulo I, onde f_1 é uma combinação linear de produtos de um número par de comutadores anti-simétricos. Consequentemente, $f \in V$.*

Demonstração. Sejam f_1, f_2 e f_3 como no lema anterior. Pelo Lema 4.18, $f_1 \in V$ e assim $f - f_1 \in C(M_2(K), t)$. Logo, $f_2 + f_3 \in C(M_2(K), t)$. Como toda matriz anti-simétrica em $(M_2(K), t)$ tem traço zero e $u_1 \ldots u_{2n}$ é central, temos que f_2 sempre resulta numa matriz de traço zero em $(M_2(K), t)$. Para ver que f_3 resulta em matriz de traço zero, basta observar que w (que é comutador de grau maior ou igual a 2) resulta em matriz de traço zero e que o produto de uma matriz anti-simétrica por uma simétrica também tem traço zero. Segue então que $f_2 + f_3$ resulta em matriz de traço zero, além de ser central. Logo, temos $f_2 + f_3 \in I$, o que nos dá $f \equiv f_1 \pmod{I}$. Como $f_1 \in V$ e $I \subset V$, segue que $f \in V$. □

Vamos agora estudar o caso geral. Para esse estudo vamos precisar dos polinômios h_n que definiremos a seguir. O conceito de posto (Definição 4.9) terá grande importância na demonstração do resultado principal desta seção, pois através dele obteremos uma redução para polinômios $*$-próprios e daí utilizaremos a proposição anterior.

Definição 4.22 *Sejam $z_0, z_1, z_2, \ldots$ variáveis em $X \cup Y$. Definimos $h_1(z_1, z_0) = z_1 \circ z_0$, $h_2(z_2, z_1, z_0) = z_2 \circ (z_1 \circ z_0)$ e, indutivamente,*

$$h_{n+1}(z_{n+1}, z_n, \ldots, z_1, z_0) = z_{n+1} \circ h_n(z_n, \ldots, z_1, z_0).$$

Como $(x_1 \circ y_1)$ é um polinômio anti-simétrico (Observação 4.17), podemos facilmente concluir que se u_0 é anti-simétrico e $v_1, \ldots, v_n$ são simétricos, então $h_n(v_n, \ldots, v_1, u_0)$ é anti-simétrico para todo $n \geq 1$.

Lema 4.23 *Sejam $u_1, \ldots, u_m$ comutadores anti-simétricos de graus maiores ou iguais a 1, com m par, e $x_1, x_2, \ldots, x_n$ variáveis simétricas. Então*

$$x_n x_{n-1} \ldots x_2 x_1 u_1 u_2 \ldots u_m = h_n(x_n, \ldots, x_1, u_1) u_2 \ldots u_m + s$$

onde s é uma soma de polinômios da forma $x_{i_1} x_{i_2} \ldots x_{i_k} g$, onde $0 \leq k < n$ e g é um polinômio $*$-próprio. Ademais, $x_n \ldots x_1 u_1 u_2 \ldots u_m \equiv s \pmod{V}$.

Demonstração. Vamos usar indução em n. Como $x_1 u_1 = \frac{1}{2}[x_1, u_1] + (x_1 \circ u_1)$, temos

$$x_1 u_1 \ldots u_m = \frac{1}{2}[x_1, u_1] u_2 \ldots u_m + h_1(x_1, u_1) u_2 \ldots u_m.$$

Mas, $[x_1, u_1] u_2 \ldots u_m$ é $*$-próprio (podemos ordenar os termos usando a relação $ab = ba + [a, b]$), donde temos que o resultado é válido para $n = 1$.

Supondo agora que o resultado vale para $n \geq 1$, temos

$$x_{n+1} x_n \ldots x_1 u_1 u_2 \ldots u_m = x_{n+1} h_n(x_n, \ldots, x_1, u_1) u_2 \ldots u_m + x_{n+1} s.$$

Observemos que

$$x_{n+1} h_n(x_n, \ldots, x_1, u_1) = \frac{1}{2}[x_{n+1}, h_n(x_n, \ldots, x_1, u_1)] + h_{n+1}(x_{n+1}, x_n, \ldots, x_1, u_1)$$

e que $h_n(x_n, \ldots, x_1, u_1)$ é uma combinação linear de produtos de $u_1, x_1, \ldots, x_n$. Pela igualdade (1.2) podemos ver que $[x_{n+1}, h_n(x_n, \ldots, x_1, u_1)]$ é uma combinação linear de produtos nos quais aparecem no máximo n variáveis simétricas (que estão em $\{x_1, \ldots, x_n\}$) fora de comutadores. Assim, usando a relação $ab = ba + [a, b]$ para reordenar os termos, mostramos que $[x_{n+1}, h_n(x_n, \ldots, x_1, u_1)] u_2 \ldots u_m$ é um somatório de produtos da forma $x_{i_1} x_{i_2} \ldots x_{i_k} g$, onde $0 \leq k < n + 1$ e g é um polinômio $*$-próprio. Observando agora que $x_{n+1} s$ também é um somatório de produtos da forma apresentada, temos a primeira parte do resultado.

A última afirmação se verifica facilmente, pois $h_n(x_n, \ldots, x_1, u_1) u_2 \ldots u_m \in V$, uma vez que m é par e $h_n(x_n, \ldots, x_1, u_1)$ é anti-simétrico. □

Teorema 4.24 $C(M_2(K), t) = V$.

Demonstração. Como a inclusão $V \subseteq C(M_2(K), t)$ já foi verificada, basta mostrar a inclusão contrária. Seja então $f(x_1, \ldots, x_n, y_1, \ldots, y_m) \in C(M_2(K), t)$ multi-homogêneo. Vamos usar indução no posto de f. Se $r(f) = (0, 0, \ldots, 0)$, então f é $*$-próprio e assim, pela Proposição 4.21, $f \in V$. Suponhamos então que $r(f) = (b_1, b_2, \ldots, b_n) > (0, 0, \ldots, 0)$ e que o resultado é válido para todos os polinômios em $C(M_2(K), t)$ de posto menor que $r(f)$. Temos

$$f = \alpha x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n} g + \sum_a \alpha_a x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} g_a$$

onde g e g_a são polinômios $*$-próprios e $a = (a_1, a_2, \ldots, a_n) < r(f)$. Pela Proposição 4.10 g pertence a $C(M_2(K), t)$ e assim, pela Proposição 4.21, g deve ser congruente módulo I a uma combinação linear de produtos da forma $u_1 u_2 \ldots u_l$, onde l é par e u_i é um comutador anti-simétrico de grau maior ou igual a 1. Segue então que

$$f \equiv v + \sum_a \alpha_a x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} g_a \pmod{I}$$

onde v é uma combinação linear de termos da forma $x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n} u_1 u_2 \ldots u_l$. Vamos então analisar esses termos. Usando o Lema 4.23 (e a relação $ab = ba + [a, b]$ para reordenar termos) podemos afirmar que

$$x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n} u_1 u_2 \ldots u_l \equiv s \pmod{V}$$

onde s é uma combinação linear de polinômios da forma $x_1^{c_1} x_2^{c_2} \ldots x_n^{c_n} q$, onde q é $*$-próprio, $c_i \leq b_i$ e $c_1 + \ldots + c_n < b_1 + \ldots + b_n$. Temos então $(c_1, \ldots, c_n) < (b_1, \ldots, b_n) = r(f)$ e portanto f é congruente módulo V a um polinômio $\overline{f}$ de posto menor que $r(f)$. Mas, como f é central, devemos ter $\overline{f}$ também central e daí, por hipótese de indução, $\overline{f} \in V$, o que nos dá $f \in V$. $\square$

4.4 A involução simplética

A involução simplética na álgebra $M_2(K)$ é a aplicação $s : M_n(K) \longrightarrow M_n(K)$, definida por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^s = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Observemos que os elementos simétricos de $(M_2(K), s)$ são exatamente as matrizes escalares e os anti-simétricos são as matrizes de traço zero.

Em [10] foi provado que o $*$-ideal J das identidades de $(M_2(K), s)$ é gerado pelos polinômios $[x_1, x_2]$ e $[x_1, y_1]$. Consideremos agora o $*$-espaço de $K\langle X \cup Y\rangle$ gerado pelos polinômios

$$x_1 \quad , \quad z_1[x_1, x_2]z_2 \quad , \quad z_1[x_1, y_1]z_2. \tag{4.10}$$

Denotando por W este $*$-espaço, temos $J \subset W \subseteq C(M_2(K), s)$. Para ver isso, basta observar que todo elemento simétrico de $(M_2(K), s)$ é central e assim todo polinômio simétrico de $K\langle X \cup Y\rangle$ é central para $(M_2(K), s)$. Ademais, os outros dois polinômios em (4.10) são identidades e portanto centrais para $(M_2(K), s)$.

Teorema 4.25 $C(M_2(K), s) = W$

Demonstração. Como já vimos que $W \subseteq C(M_2(K), s)$, basta mostrar a inclusão contrária. Seja então $f \in C(M_2(K), s)$. Temos

$$f = \frac{f + f^*}{2} + \frac{f - f^*}{2}$$

onde $(f + f^*)/2$ é simétrico e $(f - f^*)/2$ é anti-simétrico em $K\langle X \cup Y\rangle$. Como f e $(f + f^*)/2$ são centrais, temos que $(f - f^*)/2$ deve ser central. Mas, $(f - f^*)/2$ resulta em matriz de traço zero, pois todo elemento anti-simétrico em $(M_2(K), s)$ é uma matriz de traço zero. Assim, $(f - f^*)/2 \in J$. Logo, como $J \subset W$ e $(f + f^*)/2 \in W$, devemos ter $f \in W$. $\square$

Bibliografia

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

[2] N. Anisimov, *Z_p-codimensions of Z_p-identities of Grassmann algebra*, Special issue dedicated to Alexei Ivanovich Kostrikin. Commun. Algebra **29 (9)**, 4211–4230 (2001).

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

[4] S. S. Azevedo, *A basis for $\mathbb{Z}$-graded identities of matrices over infinite fields*, Serdica Math. Journal **29 (2)**, 149–158 (2003).

[5] S. S. Azevedo, M. Fidelis, P. Koshlukov, *Tensor product theorems in positive characteristic*, J. Algebra **276 (2)**, 836–845 (2004).

[6] A. Belov, *No associative PI algebra coincides with its commutant*, Siberian Math. J. **44 (6)**, 969–980 (2003).

[7] A. Brandão, *Graded central polynomials for the algebra $M_n(K)$*, Quarterly Journal of Mathematics, submited in 06/2006.

[8] A. Brandão, P. Koshlukov, *Central polynomials for $\mathbb{Z}_2$-graded algebras and for algebras with involution*, J. Pure Appl. Algebra, 2006, in press.

[9] J. Colombo, P. Koshlukov, *Central polynomials in the matrix algebra of order two*, Linear Algebra Appl. **377**, 53–67 (2004).

[10] J. Colombo, P. Koshlukov, *Identities with involution for the matrix algebra of order two in characteristic p*, Israel J. Math. **146**, 337–355 (2005).

[11] C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, John Wiley and Sons, New York-London, 1962.

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

[13] 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).

[14] V. Drensky, *New central polynomials for the matrix algebra*, Israel J. Math. **92**, 235–248 (1995).

[15] V. Drensky, *Free algebras and PI-algebras*, Springer-Verlag, Singapore, 1999.

[16] J. Dubnov, V. Ivanov, *Sur l'abaissement du degré des polynômes en affineurs*, C. R. (Doklady) Acad. Sci. USSR **41**, 96-98 (1943).

[17] E. Formanek, *Central polynomials for matrix rings*, J. Algebra **23**, 129–132 (1972).

[18] J. B. Fraleigh, *A first course in abstract algebra*, 5ª edição, Addison-Wesley, USA, 1994.

[19] A. Giambruno, P. Koshlukov, *On the identities of the Grassmann algebras in characteristic* $p > 0$, Israel J. Math. **122**, 305–316 (2001).

[20] A. Giambruno, A. Valenti, *Central polynomials and matrix invariants*, Israel J. Math. **96**, 281–297 (1996).

[21] A. V. Grishin, V. V. Shchigolev, *T-spaces and their applications*, J. Math. Sci. **134 (1)**, 1789–1878 (2006).

[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**, Math. Assoc. Amer., New York, 1968.

[24] N. Jacobson, *Structure theory of algebraic algebras of bounded degree*, Annals of Math. **46**, 695–707 (1945).

[25] I. Kaplansky, *Rings with a polynomial identity*, Bull. Amer. Math. Soc. **54**, 575–580, (1948).

[26] 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).

[27] A. Kemer, *Varieties and $\mathbb{Z}_2$-graded algebras*, Math. USSR, Izv. **25**, 359–374 (1985).

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

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

[30] 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).

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

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

[33] D. Krakowski, A. Regev, *The polynomial identities of the Grassmann algebra*, Transactions of the American Mathematical Society **181**, 429–438 (1973).

[34] V. N. Latyshev, *On the choice of basis in a T-ideal* (Russo), Sibirskii Matematicheskii Zhurnal **4** **(5)**, 1122–1126 (1962).

[35] D. Levchenko, *Finite basis property of identities with involution of a second-order matrix algebra* (Russo), Serdica **8** **(1)**, 42–56 (1982).

[36] D. Levchenko, *Bases of identities with involution of second-order matrix algebra over finite fields* (Russo), Serdica **10** **(1)**, 55–67 (1984).

[37] J. Levitzki, *On a problem of A. Kurosch*, Bull. Amer. Math. Soc. **52**, 1033–1035, (1946).

[38] S. Okhitin, *Central polynomials of the algebra of second order matrices*, Moscow Univ. Math. Bull. **43** **(4)**, 49–51 (1988).

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

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

[41] Yu. P. Razmyslov, *On a problem of Kaplansky*, Math. USSR, Izv. **7**, 479–496 (1973).

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

[43] Yu. P. Razmyslov, *Identities of algebras and their representations*, Translations Math. Monographs, **138**, AMS, Providence, RI, 1994.

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

[45] L. H. Rowen, *Polynomial identities in Ring theory*, Acad. Press, NY, 1980.

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

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

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