Universidade Estadual de Campinas
Instituto de Matemática Estatística e Computação Científica
Departamento de Matemática

Identidades polinomiais na álgebra das matrizes de ordem 2

Jones Colombo†

Doutorado em Matemática - Campinas - SP

Orientador: Prof. Dr. Plamen Emilov Koshkulov

†Este trabalho teve apoio financeiro do CNPq.

Identidades polinomiais na álgebra das matrizes de ordem 2

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Jones Colombo** e aprovada pela comissão julgadora.

Campinas, 27 de fevereiro de 2004.

Prof. Dr. **Plamen Emilov Koshlukov**.
Orientador

Banca examinadora:

Prof. Dr. Plamen Emilov Koshlukov

Prof. Dr. Flávio Ulhoa Coelho

Prof. Dr. Ivan Chestakov

Prof. Dr. Paulo Roberto Brumatti

Prof. Dr. Antônio José Engler

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

À minha mulher.

Agradecimentos

Ao Conselho Nacional de Desenvolvimento científico e Tecnológico, pela bolsa de doutorado que me foi concedida entre Março de 2000 e fevereiro do 2004.

À Universidade Estadual de Campinas, Unicamp e ao Instituto de Matemática, Estatística e Computação Científica, IMECC por ter permitido realizar meus estudos de Doutorado.

Ao Plamen, pela orientação, confiança e amizade.

À Gimena pelo carinho e apoio.

À minha mãe e ao meu pai pelo apoio que recebi.

Aos meus irmãos pelo carinho.

Aos amigos latino-americanos com os quais aprendi tantas coisas a respeito da cultura, e visões de mundo latino e me fizeram (re)ver/ter tantas idéias sobre a América do Sul, especialmente ao Yuri, Jorge, Beto, José Maria, Edson Arrazola, Sofia, Marina, Erhan(turco), Amauri, Jesse.

À Cidinha, Ednaldo e Tania, funcionários da secretaria de Pós-Graduação e a Ruth, Silvani e ao Reginaldo, funcionários da biblioteca do IMECC, pela ajuda na compreensão das burocracias da universidade e pela sua amizade.

Às bibliotecas maravilhosas que esta universidade possui.

Resumo

No capítulo 1 estabelecemos os resultados e notações que serão utilizados no restante do texto.

Para nós K é um corpo infinito de característica diferente de 2.

No capítulo 2 discutimos as identidades polinomiais satisfeitas pela álgebra das matrizes de ordem 2 sobre o corpo K. No final do capítulo encontramos uma base mínima para as identidades dessa álgebra nos casos em que a característica do corpo K é 3 e 5.

No capítulo 3 estudamos os polinômios centrais na álgebra das matrizes de ordem 2 sobre o corpo K. Seguindo idéias de Okhitin e utilizando os resultados do capítulo 2, descrevemos uma base do T-espaço dos polinômios centrais.

No capítulo 4 estudamos as identidades com involução para a álgebra das matrizes de ordem 2 sobre o corpo K. Descrevemos as bases das identidades com involução para esta álgebra. Consideramos os dois tipos de involução , a transposta e a simplética.

Abstract

In chapter 1 we establish the results and notations that will be used in the rest of the text.

For us K is an infinite field of characteristic different from 2.

In chapter 2 we discuss the polynomials identities satisfied by the matrix algebra of order 2 over the field K. At the end of the chapter we find a minimal basis for the identities of this algebra in the cases where a characteristic of field K is 3 and 5.

In chapter 3 we study the centrals polynomials in the matrix algebra of order 2 over field K. Following Okthitin's ideas and applying the results of chapter 2, we describe a basis of the T-space of central polynomials.

In chapter 4 we consider the identities with involution for matrix algebra of order 2 over field K. We describe the basis of the identities with involution for this algebra. We consider both of the types of involution, the transpose and the sympletic.

Sumário

Introdução

O estudo das identidades polinomiais é uma sub-área da teoria de anéis, a qual tem como um de seus principais objetivos obter uma classificação dos anéis.

Acreditamos que a comparação entre os seguintes problemas seja uma boa forma de motivar o estudo de identidades polinomiais. Começamos com $V \subset \mathbb{C}^n$ sendo um conjunto de pontos do espaço n-dimensional.

Problema 1.1. i) Encontre todos os polinômios $f(x_1, x_2, \ldots, x_n) \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ tais que $f(v_1, v_2, \ldots, v_n) = 0$ para quaisquer $v_1,\ v_2,\ \ldots,\ v_n \in V$.

ii) Considere o conjunto I de todos os polinômios que se anulam quando avaliando em V. O conjunto I (que de fato é um ideal) pode ser gerado por um número finito de polinômios?

iii) Estude as propriedades da álgebra $\mathbb{C}[x_1, x_2, \ldots, x_n]/I$.

Problema 1.2. Descreva as propriedades gerais do conjunto V no caso em que o conjunto $V \subset \mathbb{C}^n$ é definido como o conjunto de soluções de algum sistema de equações algébricas.

Esses são problemas motivadores da Geometria Algébrica e da Álgebra Comutativa.

Agora em vez de considerarmos $V \subset \mathbb{C}^n$ consideremos R uma álgebra especifica dentro de uma categoria de álgebras, por exemplo a categoria de álgebras associativas com unidade. Vamos tentar traduzir o problema anterior para essa nova situação.

Problema 2.1. i) Encontre todas as equações algébricas que se anulam sobre R, isto é, $f(r_1, r_2, \ldots, r_n) = 0$ para quaisquer $r_1,\ r_2,\ \ldots,\ r_n \in R$. Respondendo a questão do que significa uma equação algébrica chegamos no conceito de álgebra associativa livre, aos elementos dessa álgebra que se anulam sobre R, chamamos de identidades polinomiais.

ii) Considere o conjunto das identidades polinomiais da álgebra R, a esse conjunto chamamos de T-ideal (ideal que é invariante pelos endomorfismos da álgebra livre). É fácil de perceber que esse conjunto tem infinitos elementos. Então pergunta-se: este conjunto pode ser gerado por um conjunto finito de identidades? Esse problema é conhecido como problema de Specht, que formulado na linguagem de identidades polinomiais fica: Todo T-ideal de uma álgebra

associativa R é finitamente gerado como T-ideal?
iii) Estude as propriedades da álgebra livre fazendo o quociente pelo T-ideal gerado pelas identidades polinomiais satisfeitas pela álgebra R.
Problema 2.2. Descreva as propriedades da álgebra R, no caso em que somente sabe-se que ela satisfaz uma identidade polinomial.

Observe que responder a esses problemas daria uma classificação das álgebras, não para todas as álgebras, mas pelo menos para aquelas que satisfizessem alguma identidade polinomial (PI-álgebras).

Pode parecer que exigir que as álgebras satisfaçam alguma identidade polinomial seja uma restrição abusiva, entretanto já está estabelecido que as PI-álgebras formam uma classe bastante extensa dentro de todas as álgebras.

Por outro lado, essa classificação é bastante "grosseira". Podemos jutificar esta afirmação observando que as álgebras comutativas, anulam o seguinte polinômio $f(x_1, x_2) = x_1x_2 - x_2x_1$. Isso significa que do ponto de vista da teoria PI as álgebras comutativa são iguais, mas pelo que se conhece das álgebras comutativas essa classe é bastante rica e possue várias particulariedades para podermos iguala-las. Por outro lado, essa limitação é vista algumas vezes como uma virtude, pois a variedade de álgebras é um objeto muito grande e para uma primeira tentativa de classificação é razoável que a dividamos em grandes classes.

Por todas essas observações se percebe que a teoria PI fornece algo como um "esquema classificador"e algumas dicas de quais problemas deverão ser resolvidos. Como por exemplo, encontrar uma base para as identidades de algumas álgebras. Dessa forma a teoria PI se encaixa adequadamente no objetivo da teoria de anéis.

Vamos fazer algumas observações a respeito do sub-item ii) do problema 2.1. O problema de Specht foi muito famoso entre os pesquisadores da teoria PI, certamente uma fama bem justificada se levarmos em conta as suas conseqüências. Esse problema foi respondido, de maneira afirmativa, por Kemer em [33, 1987], para o caso de álgebras sobre corpos de característica zero. Já no caso de álgebras sobre corpos de característica positiva, existem exemplos de variedades de álgebras que não possuem uma base finita de identidades.

Um outro item que se poderia acrescentar ao problema 2 seria o seguinte:
Problema 2.3. Descreva as identidades polinomias de alguma álgebra "importante". Sem dúvida, a álgebra das matrizes $M_n(K)$ (de ordem $n \times n$ sobre o corpo K) seria um forte candidato a ser uma álgebra "importante"em vista de sua grande aplicação em quase todos os ramos da matemática. Além disso, existe um outro forte motivo para se estudar esta álgebra

do ponto de vista da teoria PI, pois de acordo com a teoria desenvolvida por Kemer esta álgebra seria um dos átomos fundamentais com que se constroi uma teoria de classificação do ponto de vista estrutural. Além da álgebra das matrizes existem outras 4 famílias de álgebras.

Apesar da importância da álgebra das matrizes, ainda sabe-se pouco sobre as identidades polinomiais satisfeitas por $M_n(K)$, mesmo quando K é um corpo de característica 0. Descreveremos brevemente os principais resultados conhecidos nessa direção.

Em 1973 Razmyslov [51], encontrou uma base para as identidades da álgebra $M_2(K)$, com entradas em um corpo K de característica 0. Esta base possuia 9 identidades; ressaltamos que a importância desse resultado foi a obtenção de uma base finita e não a quantidade de identidades na base. Mais tarde, em 1980, Drensky em [11] obteve uma base mínima formada de 2 identidades polinomiais. Quando K é um corpo finito, conhecemos a base das identidades polinomiais quando $n = 2$ ([45]), $n = 3$ ([22]) e $n = 4$ ([25]). No caso em que K é um corpo infinito de característica $p \neq 2$ Koshlukov em [37] encontrou uma base para as identidades de $M_2(K)$, sendo que para $p > 5$ a base era mínima; em seguida, no trabalho [8] conseguimos encontrar uma base mínima para corpos com característica 3 e 5. No caso de caracterísitca 2 continua um problema em aberto. Além disso, não se conhece quase nada a respeito das identidades polinomiais satisfeitas pela álgebra $M_3(K)$, mesmo quando o corpo é de característica 0, e menos ainda para $M_n(K)$, quando $n \geq 4$.

Com respeito a álgebra das matrizes um outro problema atraiu a atenção dos pesquisadores. Esse problema foi proposto primeiramente em 1956 por Kaplansky, ele perguntou se existe polinômio central multihomogêneo para a álgebra $M_n(K)$, com $n \geq 2$. Este problema foi respondido, para o caso geral e de maneira independente, por Formanek em [20] e por Razmyslov em [51]. Para o caso $n = 2$ temos alguns resultados a mais, como por exemplo, a descrição do S_n-módulo dos polinômios centrais multilineares, a série de Hilbert e o S_n-cocaracter, todos obtidos por Formanek em [21]. Além disso, Okhitin em [46] mostrou que o T-espaço dos polinômios centrais é finitamente gerado como T-espaço, e encontrou um conjunto mínimo de geradores quando K é um corpo de característica 0. Neste trabalho estendemos este resultado para corpos infinitos e de característica $p > 2$, veja o capítulo 3.

Como já dissemos a respeito do problema de Specht, Kemer o respondeu de maneira afirmativa. Assim, sabemos que toda álgebra associativa sobre um corpo de característica 0, admite uma base finita de identidades polinomiais. No entanto, a teoria de Kemer não diz nada a respeito da maneira de encontrar essa base. Além disso, um sentimento comum entre os pesquisadores da área é encontrar base de identidades para algumas álgebras "importantes", entretanto esse problema tem apresentado diversas dificuldades. Uma forma de contornar essas dificuldades consiste em se tentar alterar ou generalizar o conceito de identidade polinomial, com a esperança de, por um lado, as identidades generalizadas serem mais fáceis de se trabalhar e, por outro lado, tais generalizações permitirem obter mais informações a respeito das identidades polinomiais ordinárias. Em alguns casos ocorreu que as generalizações tornaram-se interessantes por si mesmas.

A primeira generalização a ser usada na teoria PI foi as identidades fracas. Discutiremos mais sobre as identidades fracas no capítulo 2 deste trabalho. Um outro tipo de generalização do conceito de identidade foi dado por Kaplansky; é a noção de polinômio central. Outra generalização é as identidades com traço, elas foram estudadas detalhadamente nos trabalhos de Procesi [49] e de Razmyslov, ver por exemplo [53], e em seguida por vários pesquisadores.

Outra generalização que desempenha um papel importante na teoria PI é as identidades graduadas. Neste trabalho não trataremos tais identidades, recordamos somente que elas foram uma das principais ferramentas na teoria de Kemer veja [35], veja também [2] para maiores detalhes.

Outra generalização é as identidades polinomiais com involução. Nos trabalhos sobre involuções feitos por Herstein e Jacobson explorou-se a conexão que existe entre as álgebras associativas com as álgebras de Lie e de Jordan. Pois a partir do produto da álgebra associativa, podemos definir o comutador $[a, b] = ab - ba$ tornando esta álgebra uma álgebra de Lie e definindo o produto de Jordan $a \circ b = ab + ba$ transformamos esta álgebra em uma de álgebra de Jordan. Percebe-se que as involuções da álgebra associativa deixam estas álgebra invariantes num certo sentido. Utilizar as involuções no estudo de identidades polinomiais é um passo bem natural, além disso, essa generalização foi muito útil na descrição de propriedades estruturais de anéis com identidades polinomiais, veja por exemplo [55]. Estudamos as identidades polinomiais com involução na álgebra $M_2(K)$, utilizando métodos do trabalho de [42] e a teoria de invariantes do grupo ortogonal.

Nesta tese estudamos as identidades polinomiais satisfeitas pela álgebra $M_2(K)$ das matrizes 2×2 sobre um corpo infinito K de característica $p \neq 2$. Faremos agora um resumo do conteúdo deste trabalho.

No capítulo 1 estabelecemos os resultados e notações que serão utilizados no restante do texto. Este capítulo é de caracter introdutório; o leitor que já possui familiaridade com os principais conceitos da teoria de anéis e de identidades polinomiais poderia omitir boa parte dele. O capítulo está baseado em várias monografias e artigos de pesquisa. Algumas das demonstrações do capítulo foram omitidas, especialmente nos casos onde precisaremos somente o enunciado do respectivo resultado. Em tais casos os resultados vêm com citação bibliográfica, onde o leitor poderia encontrar a demonstração completa.

No capítulo 2 discutimos as identidades polinomiais satisfeitas pela álgebra das matrizes 2×2 sobre um corpo infinito. O capítulo começa com uma exposição do artigo [37], que trata da base das identidades de $M_2(K)$ sobre corpos infinitos e de característica $p \neq 2$. No final do capítulo encontramos uma base mínima para as identidades de $M_2(K)$ nos casos $p = 3$ e 5.

No capítulo 3 estudamos os polinômios centrais na álgebra das matrizes 2×2 sobre corpos infinitos e de característica $p \neq 2$. Seguindo as idéias de Okhitin e utilizando os resultados do capítulo 2, descrevemos uma base do T-espaço dos polinômios centrais para a álgebra $M_2(K)$.

No capítulo 4 estudamos as identidades com involucão para a álgebra das matrizes 2×2 sobre corpos infinitos e de característica $p \neq 2$. Os principais resultados do capítulo descrevem bases das identidades com involução para esta álgebra. Consideramos os dois tipos de involução, a transposta e a simplética. No primeiro caso, utilizaremos métodos provenientes do artigo [42], combinados com os dos [9, 36] e [37]. O segundo caso resolve-se usando-se a descrição das identidades fracas de $M_2(K)$.

Capítulo 1

Conceitos Básicos

1.1 Anéis, Módulos e Álgebras

Assumiremos que o leitor tem familiaridade com as principais definições e resultados a respeito de estruturas algébricas básicas: grupos, anéis e módulos. Faremos apenas um breve resumo. Um anel é um conjuto não vazio A com operações de adição e multiplicação, tal que com respeito à adição, A é um grupo abeliano e a adição se relaciona com a multiplicação através da lei distributiva

$$x(y+z) = xy + xz, \qquad (x+y)z = xz + yz,$$

onde x, y e z são elementos arbitrários de A. Reservaremos o nome de módulo a um conceito mais limitado pois consideraremos somente módulos unitários à esquerda sobre anéis associativos com unidade. Em outras palavras, um módulo (à esquerda) sobre um anel associativo A com unidade é um grupo abeliano M tal que para todo $r \in A$ e todo $m \in M$ existe um elemento $rm \in M$ satisfazendo as seguintes regras

$$(r_1 + r_2)m = r_1m + r_2m,\ (r_1r_2)m = r_1(r_2m),\ r(m_1 + m_2) = rm_1 + rm_2,\ 1m = m,$$

onde r_1, $r_2 \in A$ e m_1, $m_2 \in M$. Muitas vezes diremos que M é A-módulo, assumindo que ele é um A-módulo à esquerda. Um anel R o qual é ao mesmo tempo um módulo sobre um anel comutativo A é chamado uma **A-álgebra** se para todo $r \in A$ e x, $y \in R$ tivermos

$$r(xy) = (rx)y = x(ry).$$

Diremos que a A-álgebra R é associativa, com unidade ou comutativa se R como anel é associativo, com unidade ou comutativo, respectivamente. Observamos ainda que quando o anel A for um corpo, R se torna um espaço vetorial sobre o corpo A, nestes casos denotaremos A por K.

1.2 Ideais e exemplos

Um subconjunto S de uma álgebra R é dito uma sub-álgebra se S for uma álgebra com respeito às operações de R, i.é., s_1, $s_2 \in S$ implica que $s_1 - s_2 \in S$, $s_1 s_2 \in S$, além disso, temos que $1 \in S$. Se R é uma álgebra comutativa temos o conceito usual de ideal de R. No caso geral precisamos fazer uma diferença entre ideais à esquerda, à direita e bilaterais. Assim, um sub-conjunto I de R é um ideal à esquerda se $RI \subset I$ (i.é., $ri \in I$ para todo $r \in R$ e $i \in I$) e satisfaz a seguinte propriedade: para cada i e $j \in I$ temos que $i - j \in I$. Diremos que I é ideal à direita quando $IR \subset I$. Reservaremos a palavra ideal para quando I for um ideal bilateral, isto é, I for ao mesmo tempo um ideal à direita e à esquerda.

Vamos denotar por $End(R)$ ao conjunto dos endomorfismos de R, e por $Aut(R) \subset End(R)$ aos elementos de $End(R)$ que são invertíveis. Observamos que o conjunto $Aut(R)$ com a operação de composição é um grupo; chamamo-no de grupo de automorfismos da álgebra R.

Seja R uma K-álgebra, onde K é um corpo com $\operatorname{char} K \neq 2$. Se R satisfaz as relações

$$\begin{aligned} a.a &= 0 \qquad \text{para todo } a \in R \\ (a.b).c + (b.c).a + (c.a).b &= 0, \quad \text{identidade de Jacobi,} \end{aligned}$$

diremos que R é uma **álgebra de Lie**. Se R satisfaz

$$\begin{aligned} ab &= ba \\ (a^2 b)a &= a^2(ba), \end{aligned}$$

para todos a, $b \in R$, diremos que R é uma **álgebra de Jordan**.

Abaixo seguem alguns exemplos de álgebras.

Exemplo 1.1. *1. Seja R uma álgebra associativa, então usando o produto de R podemos definir o seguinte produto $[r_1, r_2] = r_1 r_2 - r_2 r_1$, r_1, $r_2 \in R$ o que torna está álgebra uma álgebra de Lie. Vamos chamar está álgebra de $R^{(-)}$. Assim $R^{(-)}$ é a mesma que R como espaço vetorial com um novo produto, o produto de Lie $[r_1, r_2]$. De maneira semelhante podemos definir o seguinte produto $s_1 \circ s_2 = 1/2(s_1 s_2 + s_2 s_1)$, s_1, $s_2 \in R$, o* *que torna esta álgebra uma álgebra de Jordan, a qual chamamos de* $R^{(+)}$. *Assim* $R^{(+)}$ *é a mesma que* R *como espaço vetorial com um novo produto, o produto de Jordan* $s_1 \circ s_2$.

2. $M_n(K)$, *o conjunto de todas as matrizes* $n \times n$ *com entradas no corpo* K, *com a adição e a multiplicação usual entre matrizes. Podemos descrever essa álgebra como o conjunto dos operadores lineares* $End(V)$ *de* V *em* V, *num espaço vetorial* V *de dimensão* n *sobre* K. *Seja* $a \in M_n(K)$, *denotaremos por* $tr(a)$ *o traço e por* $\det(a)$ *o determinante da matriz* a.

3. $U_n(K)$, *o sub-conjunto de* $M_n(K)$ *consistindo de todas as matrizes triangulares superiores, é uma sub-álgebra de* $M_n(K)$.

4. $sl_n(K)$, *o conjunto das matrizes* $n \times n$ *com traço zero e com a multiplicação dada por* $[r_1, r_2]$ *é uma álgebra de Lie.*

5. $S_n(K)$, *o conjunto das matrizes simétricas* $n \times n$ *com entradas no corpo* K *e com multiplicação dada por* $s_1 \circ s_2$ *é uma álgebra de Jordan.*

Seja R uma álgebra associativa com unidade. Diremos que $a \in R$ é invertível (ou possui inverso) se existe $b \in R$, tal que $ab = ba = 1$. Definimos $U(R)$ ao conjunto de todos os elementos invertíveis de R. É fácil de verificar que $U(R)$ com a multiplicação de R é um grupo. Além disso, se todo elemento não-nulo de R é invertível, dizemos que R é um **álgebra de divisão**.

Exemplo 1.2. *Seja* $\mathbb{H}(\mathbb{R}) = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, *a álgebra associativa com a multiplicação induzida por* $i^2 = -1$, $j^2 = -1$, $j^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ *e* $ki = -ik = j$. *Logo* $\dim_{\mathbb{R}} \mathbb{H}(\mathbb{R}) = 4$ *e o centro de* $\mathbb{H}(\mathbb{R})$ *é* $\mathbb{R}1$. *Se* $\alpha = a + bi + cj + dk$ *onde* a, b, c, $d \in \mathbb{R}$, *definimos* $\bar{\alpha} = a - bi - cj - dk$. *É fácil verificar que*

$$\alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}.$$

Daí, se $\alpha \neq 0$, *então* $\alpha \in U(\mathbb{H}(\mathbb{R}))$ *e a expressão para* α^{-1} *é*

$$\alpha^{-1} = (a^2 + b^2 + c^2 + d^2)^{-1}\bar{\alpha}.$$

Em particular, $\mathbb{H}(\mathbb{R})$ *é um anel com divisão sobre* $\mathbb{R}$. *Isso decorre do fato que em* $\mathbb{R}$ *vale a seguinte propriedade: se* $(a, b, c, d) \neq (0, 0, 0, 0)$ *então* $a^2 + b^2 + c^2 + d^2 \neq 0$.

Por outro lado, se considerarmos $\mathbb{H}$ *sobre o corpo* $\mathbb{C}$ *dos complexos ao invés dos reais, então* $\mathbb{H}(\mathbb{C})$ *não é um anel de divisão. Verifica-se facilmente que, neste caso* $\mathbb{H}(\mathbb{C}) \cong M_2(\mathbb{C})$*. Logo* $\mathbb{H}(\mathbb{C})$ *conterá divisores de zero.*

Podemos ainda considerar $\mathbb{H}(\mathbb{Z})$ *como uma álgebra sobre o anel dos inteiros* $\mathbb{Z}$*. Então teremos*

$$\{a + bi + cj + dk \colon a, b, c, d \in \mathbb{Z}\}.$$

É imediato verificar que $\mathbb{H}(\mathbb{Z})$ *não é um anel de divisão, embora não tenha divisores de zero. De fato,* $U(\mathbb{H}(\mathbb{Z})) = \{\pm 1, \pm i, \pm j, \pm k\}$ *é o grupo dos quatérnios de ordem 8.*

1.2.1 Álgebra tensorial

Vamos lembrar a definição de álgebra tensorial. Começamos com a definição de produto tensorial de dois espaços vetoriais U e V sobre o corpo K. Chamamos de **produto tensorial** de U por V a todo par (Z, g), onde Z é um espaço vetorial e g é uma aplicação K-bilinear, que satisfaz a seguinte propriedade:

Dado qualquer espaço vetorial W sobre K e qualquer aplicação K-bilinear $g \colon U \times V \to W$, existe uma única aplicação linear $f' \colon Z \to W$ tal que $f = f' \circ g$. Além disso, se (Z, g) e (Z', g') são dois pares com a mesma propriedade, então existe um único isomorfismo $j \colon Z \to Z'$ tal que $j \circ g = g'$.

Denotaremos por $U \otimes V$ o espaço vetorial Z, e o chamamos de produto tensorial de U por V.

Da mesma forma que definimos o produto tensorial entre dois espaços vetoriais podemos definir o produto entre diversos espaços vetoriais.

Seja V um espaço vetorial. Para cada inteiro $r \geq 0$, temos o espaço $V^r = V \otimes \cdots \otimes V$ (r fatores). Como sabemos, $V^0 = K$ e $V^1 = V$. Consideramos, em seguida, o espaço vetorial

$$T(V) = V^0 \oplus V^1 \oplus V^2 \oplus \cdots \oplus V^r \oplus \ldots$$

soma direta dos espaços V^r, $r = 0, 1, \ldots$. Dois elementos genéricos de $T(V)$ são da forma

$$z = z_0 + z_1 + \cdots + z_k; \qquad w = w_0 + w_1 + \cdots + w_m,$$

onde $z_i, w_i \in V^i$.

Definimos o produto em $T(V)$ colocando

$$zw = z_0 w_0 + (z_0 w_1 + z_1 w_0) + (z_0 w_2 + z_1 w_1 + z_2 w_0) + \cdots + z_k w_m$$

onde cada produto $z_i w_j \in V^{i+j}$ é dado pela multiplicação dos tensores $z_i \in V^i$ e $w_j \in V^j$. Além disso, o espaço vetorial $T(V)$ com essa multiplicação é uma álgebra e a chamamos de **álgebra tensorial**.

Exemplo 1.3. *Seja V um espaço vetorial sobre um corpo K com $\dim V = n$. Consideramos a álgebra tensorial $T(V)$ de V. Se $\{e_1, e_2, \ldots, e_n\}$ é uma base de V, então $T(V)$ é essencialmente a álgebra $K\langle e_1, e_2, \cdots, e_n\rangle$ e podemos considerar vários quocientes nesta álgebra.*

Em primeiro lugar podemos considerar a álgebra simétrica $S(V)$ obtida por fazer o quociente de $T(V)$ pelo ideal gerado por todas

$$u \otimes v = v \otimes u, \quad u, v \in V.$$

Essa álgebra é isomorfa à álgebra polinomial (comutativa) $K[e_1, e_2, \cdots, e_n]$.

Podemos obter uma outra álgebra de maneira semelhante, conhecida como álgebra de Grassmann (ou exterior) $E_n(V)$, obtida por fazer o quociente de $T(V)$ pelo ideal gerado pelos elementos $v \otimes v$, para todo $v \in V$ (anti-comutatividade). Quando a dimensão de V é infinita, mas contável, assumimos que V tem base $\{e_1, e_2, \ldots\}$ e denotamos a álgebra por E. Esta álgebra tem se mostrado bastante interessante e voltaremos a tratá-la mais adiante.

Exemplo 1.4. *Seja V um espaço vetorial sobre um corpo K, com base $\{e_1, e_2, \ldots, e_n\}$ equipado com uma forma bilinear simétrica $(\ ,\ ) \colon V \times V \to K$. A álgebra de Clifford de V é obtida por fazer o quociente de $T(V)$ pelo ideal gerado por todos $\{v \otimes u - u \otimes v - (u, v)\}$, para todo u, $v \in V$.*

1.3 Álgebras livres e envolventes

Começaremos essa seção tratando de conceitos que se apresentam de forma mais elegante na linguagem de Álgebras Universais, para maiores detalhes veja [7].

Seja Δ uma categoria de álgebras e seja F uma álgebra nessa categoria Δ, F é gerada pelo conjunto X. Falaremos que a álgebra F é **livre** na categoria Δ, livremente gerada pelo conjunto X, se para cada álgebra S na categoria Δ e cada aplicação $X \to S$ podemos estender a aplicação para um homomorfismo $F \to S$. A cardinalidade do conjunto X é chamada de posto de F.

Na categoria das K-álgebras associativas com unidade vamos denotar por $K\langle X\rangle$ a álgebra livre, livremente gerada pelo conjunto $X = \{x_1, x_2, \dots\}$. Na categoria das álgebras de Lie, denotemos por $L(X)$ a álgebra livre, livremente gerada pelo conjunto X acima. Em outras palavras, $K\langle X\rangle$ é simplesmente a álgebra dos polinômios associativos com unidade, onde as variáveis não comutam entre si, mas comutam com os elementos de K. Podemos considerar ainda $K\langle X\rangle$ como um K-espaço vetorial sendo a base todas as palavras no alfabeto X (inclusive a palavra vazia, que representamos por 1). A multiplicação em $K\langle X\rangle$ é induzida pela concatenação de monômios, com esta multiplicação fica fácil de se mostra que a álgebra $K\langle X\rangle$ é isomorfa a álgebra tensorial.

Com esses conceitos estabelecidos vamos relembrar alguns resultados que aparecem na teoria de Álgebras de Lie.

Definição 1.5. *Se R é uma álgebra associativa e se a álgebra de Lie G é isomorfa (como álgebra de Lie) a alguma sub-álgebra de $R^{(-)}$, então dizemos que R é uma **álgebra envolvente** de G. A álgebra associativa $U = U(G)$ é a **álgebra envolvente universal** da álgebra de Lie G, se U é uma álgebra envolvente de G e satisfaz a seguinte propriedade universal. Para cada álgebra associativa R e cada homomorfismo de álgebras de Lie $\phi\colon G \to R^{(-)}$ existe um único homomorfismo de álgebras associativas $\psi : U \to R$ que estende ϕ, isto é, ψ é igual à restrição de ϕ sobre G.*

É bem conhecido que a álgebra $U(G)$ existe e é determinada unicamente, a menos de isomorfismo.

Teorema 1.6. ***(Poincaré—Birkhoff—Witt)*** *Toda álgebra de Lie G possui uma única, a menos de isomorfismo, álgebra envolvente universal $U(G)$. Se G tem uma base $\{e_i \mid i \in I\}$, e o conjunto dos índices I é ordenado, então $U(G)$ tem uma base dada por:*

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

Assumimos que $p = 0$ corresponde à unidade 1 de $U(G)$.

Demonstração. Para uma demonstração que não necessita de muitos pré-requesitos veja [14, pág. 11].

Teorema 1.7. ***(Witt)*** *A sub-álgebra de Lie $L(X)$ de $K\langle X\rangle^{(-)}$ gerada por X é isomorfa à álgebra de Lie livre com X como conjunto de geradores livres; $U(L(X)) = K\langle X\rangle$.*

Demonstração. Seja R uma álgebra associativa e seja $\varphi\colon L(X) \to R^{(-)}$ um homomorfismo. A aplicação $\varphi_0\colon X \to R$ definida por $\varphi_0(x) = \varphi(x)$, $x \in X$, induz um homorfismo $\psi\colon K\langle X\rangle \to R$. Como $\varphi(x) = \psi(x)$, obtemos que a restrição de ψ em $L(X)$ é igual a φ. Então $U(L(X)) = K\langle X\rangle$. Se G é uma álgebra de Lie e R é a sua álgebra envolvente, então cada aplicação $X \to G \subset R$ induz um homomorfismo $K\langle X\rangle \to R$; e a sua restrição sobre $L(X)$ é um homomorfismo de $L(X)$ a $R^{(-)}$, o qual envia os geradores de $L(X)$ em G. Portanto a imagem de $L(X)$ está em G e isso nos fornece que $L(X)$ é livre na categoria de álgebras de Lie. ■

1.4 Identidades polinomiais

Sejam $f = f(x_1, x_2, \ldots, x_n) \in K\langle X\rangle$ um polinômio não-nulo e R uma álgebra associativa. Diremos que f é uma identidade polinomial de R se

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

Se uma álgebra associativa R satisfazer uma identidade polinomial, diremos que R é uma PI-álgebra.

O polinômio $f \in K\langle X\rangle$ é uma identidade polinomial de R se, e somente se, f está no núcleo de todos os homomorfismos $K\langle X\rangle \to R$.

É claro que a intersecção de todos estes núcleos é um ideal de $K\langle X\rangle$. Se tomarmos um elemento nesse ideal e substituirmos as suas entradas (variáveis) por elementos de $K\langle X\rangle$, continuaremos obtendo elementos desse ideal, ou seja, esse ideal é invariante em relação aos endomorfismos de $K\langle X\rangle$.

Definição 1.8. *Um ideal I de $K\langle X\rangle$ que é invariante com respeito aos endomorfismos de $K\langle X\rangle$ é chamado de T-ideal.*

A próxima definição tem uma clara semelhança com a conexão entre a álgebra comutativa (digamos sobre $\mathbb{C}$) e a geometria algébrica. Pois podemos associar a cada ideal radical em $K[x_1, x_2, \ldots, x_n]$ uma variedade algébrica irredutível.

Da mesma forma, para cada T-ideal da álgebra $K\langle X\rangle$ podemos associar uma subcategoria na categoria das álgebras associativas. Veja a próxima definição.

Definição 1.9. *Seja $S = \{f_i(x_1, \ldots, x_{n_i}) \in K\langle X\rangle \mid i \in I\}$ um conjunto de polinômios na álgebra livre $K\langle X\rangle$. A categoria Δ de todas as álgebras associativas satisfazendo todas as* *identidades $f_i = 0$, $i \in I$, é chamada de variedade (de álgebras associativas) determinada pelo sistema de polinômios $\{f_i(x_1, \ldots, x_{n_i}) \mid i \in I\}$. Denotemos este conjunto por $var S = \Delta$. A variedade Γ é chamada de sub-variedade de Δ se $\Gamma \subset \Delta$.*

Reciprocamente, para cada conjunto de álgebras associativas com unidade podemos associar um T-ideal, que consiste de todos os polinômios que são identidades em cada uma das álgebras dadas.

Diremos que um T-ideal $I \subset K\langle X\rangle$ tem base $J = \{f_i \mid i \in F\}$ se I é gerado como T-ideal pelo conjunto J. Isto quer dizer que I é a intersecção de todos os T-ideais que contêm o conjunto J. Neste caso denotaremos $I = \{f_i \mid i \in F\}^T$. Diremos que o T-ideal é finitamente gerado se existir um conjunto finito $\{f_i \mid i \in F\}$ tal que $I = \{f_i \mid i \in F\}^T$.

Seja R uma álgebra, diremos que ela tem uma base finita de identidades se o seu T-ideal $T(R)$ é finitamente gerado.

Um dos principais problemas da teoria de identidades polinomiais é o estudo dos T-ideais de uma álgebra dada. Podemos dividir esse problema em dois.

Problema 1. Dada uma álgebra concreta, encontrar uma base para suas identidades polinomiais.

Problema 2. Toda álgebra associativa R tem base de identidades finita?

O segundo problema é conhecido como problema de Specht.

No começo dos anos 60 o problema de Specht foi muito famoso entre os pesquisadores que trabalhavam com PI-álgebras. Um T-ideal I satisfaz a propriedade de Specht se ele tem base finita, e todo T-ideal J, $I \subseteq J$, também possui uma base finita. Uma álgebra satisfaz essa mesma propriedade se o seu T-ideal a satisfaz.

Naturalmente, o problema de Specht é um caso particular dos bem conhecidos problemas para a propriedade de base finita de um sistema algébrico. Por exemplo, para variedades de grupos, o problema análogo foi formulado por B. H. Neumann em sua tese de doutorado em 1935.

Sobre corpos de característica 0, o problema de Specht foi resolvido de maneira afirmativa por Kemer em [33] em 1987, como resultado da teoria de estrutura de T-ideais desenvolvida por ele em [34], para os casos de álgebras unitárias e não-unitárias (veja também a monografia [35] para uma exposição completa). No caso de álgebras associativas sobre corpos de característica positiva, o problema permaneceu em aberto até 1999 quando Belov em [3] (veja também [4] caso tenha dificuldades com Russo), Grishin [26] e Shchigolev em [56] construiram os primeiros exemplos de variedades de álgebras associativas nas quais não se pode definir um sistema gerador de identidades polinomias finito (para corpos de qualquer característica positiva veja os artigos de Belov e Shchigolev, e o de Grishin para corpos de característica 2).

Ressaltamos que no caso de álgebras de Lie, os primeiros exemplos de álgebras cujas identidades não admitem base finita, foram construidos por Vaughan-Lee (em característica 2), e em seguida por Drensky (em qualquer característica positiva), ver por exemplo [14, pág. 29]. Em característica 0, um resultado de Iltyakov mostra que as identidades de uma álgebra de Lie de dimensão finita, são finitamente baseadas; ainda não se sabe a resposta no caso geral.

1.4.1 Exemplos de identidades polinomiais

O polinômio standard tem um papel especial na teoria de álgebras com identidades polinomiais. A sua definição é a seguinte

$$s_n = s_n(x_1, x_2, \ldots, x_n) = \sum_{\sigma \in S_n} (-1)^\sigma x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)},$$

onde S_n é o grupo simétrico que permuta os símbolos $\{1, 2, \ldots, n\}$ e $(-1)^\sigma$ é o sinal da permutação σ. Um dos principais resultados na teoria de identidades polinomiais envolve esse polinômio. É o conhecido teorema de Amitsur e Levitzki que afirma o seguinte. Se A é um anel comutativo, então s_{2n} é uma identidade polinomial para $M_n(A)$. Recordamos que esse teorema foi um dos primeiros resultados genêricos na PI teoria.

Essencialemente, existem cinco demonstrações diferentes desse teorema; veja por exemplo [14] para mais detalhes e referências bibliográficas.

Outra polinômio importante é o polinômio de Capelli

$$d_n(x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_{n+1}) = \sum_{\sigma \in S_n} (-1)^\sigma y_1 x_{\sigma(1)} y_2 x_{\sigma(2)} \cdots y_n x_{\sigma(n)} y_{n+1}.$$

Este polinômio foi usada em inúmeros casos, como por exemplo, na construção dos polinômios centrais de $M_n(K)$ dada por Razmyslov em [52].

Observação 1.10. *Como tanto o polinômio standard como o de Capelli são anti-simétricos nas variáveis $x_1, \ldots, x_n$, podemos concluir que estes dois polinômios são identidades para álgebras que possuem dimensão menor que n. Para verificarmos isto basta ver que s_n assim* *como d_n se anula para elementos (fixos) de uma base de uma álgebra com dimensão menor que n.*

Considerando-se a álgebra de Grassmann E sobre um espaço vetorial de dimensão infinita sobre K, Krakowski e Regev em [39] mostraram que o polinômio $[x_1, x_2, x_3]$ gera o T-ideal desta álgebra, quando K é um corpo de característica zero.

Já na álgebra das matrizes triangulares superiores $n \times n$, $U_n(K)$, Maltsev em [44] mostrou que a identidade

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

é a base das identidades polinomiais, quando $\operatorname{char} K = 0$.

A álgebra das matrizes 2×2, $M_2(K)$, satisfaz as identidades standard s_4 e a identidade de Hall, que é uma expressão do fato de que o quadrado de uma matriz 2×2 com traço 0, é um múltiplo da matriz identidade. No capítulo 2 discutiremos mais sobre as identidades dessa álgebra, e entre outras coisas mostraremos que para corpos infinitos de característica positiva $p > 3$ essas duas identidades formam uma base de $T(M_2(K))$.

1.4.2 Identidades polinomiais fracas

Suponhamos agora que $S \subset R$ seja um sub-espaço vetorial da álgebra R. Admitamos ainda que S gera a álgebra R. Diremos então que $f(x_1, x_2, \ldots, x_n) \in K\langle X\rangle$ é uma identidade fraca para o par (R, S) se $f(s_1, s_2, \ldots, s_n) = 0$ para quaisquer s_1, s_2, $\ldots$, $s_n \in S$. O conjunto das identidades fracas do par (R, S) forma um ideal de $K\langle X\rangle$. Notem que enquanto os T-ideais são invariantes com respeito aos endomorfismos da álgebra $K\langle X\rangle$, o ideal das identidades fracas, em geral, não o é.

Seja $\Omega \subset K\langle X\rangle$ um conjunto não vazio de polinômios, tal que $\omega(s_1, s_2, \ldots, s_n) \in S$ para todo s_1, s_2, $\ldots$, $s_n \in S$, e $\omega \in \Omega$. A identidade fraca $g(x_1, x_2, \ldots, x_n) \in K\langle X\rangle$ é uma Ω-conseqüência de $f(x_1, x_2, \ldots, x_n) \in K\langle X\rangle$ se g está no ideal de $K\langle X\rangle$ gerado pelo conjunto

$$\{f(\omega_1, \omega_2, \ldots, \omega_n) \mid \omega_1, \ldots, \omega_n \in \Omega\}.$$

Dependendo das propriedades do conjunto S poderemos escolher vários conjuntos Ω. Por exemplo, se $R = S$ e $\Omega = K\langle X\rangle$ então obtemos que as identidades fracas do par (R, S) coincidem com o T-ideal de R.

Admitindo-se que $[S, S] \subset S$, isto é, $[a, b] \in S$ para todos a, $b \in S$, podemos escolher $\Omega = L(X) \subset K\langle X\rangle$. Então as identidades fracas do par (R, S) são conhecidas por identidades fracas de Lie de (R, S) (veja [53, cap. 16] para maiores detalhes).

Como vamos tratar somente das identidades fracas de Lie do par $(M_2(K), sl_2(K))$, vamos nos reservar o nome *identidades fracas* para significar *identidades fracas de Lie* (veja [36, 17] para maiores detalhes).

1.5 Identidades polinomiais multi-lineares

Em qualquer trabalho matemático sempre se tenta reduzir a quantidade de objetos necessários a considerar. No caso de identidades polinomiais a primeira tentativa é reduzir a classe de polinômios a ser considerada. Por outro lado, tais classes não podem ser muito pequenas pois poderíamos perder informações sobre a álgebra estudada. A medida é dada por observar que a classe restante precisa ser grande o suficiente para poder gerar o T-ideal da álgebra estudada. Vamos explicar melhor o que isso significa: diremos que um polinômio $g \in K\langle X\rangle$ é conseqüência de uma família de identidades $\{f_i \mid i \in I\}$ se $g \in \langle f_i \mid i \in I\rangle^T$, o T-ideal gerado pelos f_i, $i \in I$.

Dois conjuntos de identidades polinomiais são *equivalentes* se eles geram o mesmo T-ideal.

Um polinômio $f(x_1, \ldots, x_n)$ é homogêneo em alguma das variáveis x_i, se em cada monômio de f, o grau de x_i é o mesmo. O polinômio f é dito multi-homogêneo de grau $(r_1, r_2, \ldots, r_n)$ se em cada monômio o grau em relação à variável x_i é igual a r_i, $i = 1, 2, \ldots, n$.

Definição 1.11. *Um polinômio $f(x_1, x_2, \ldots, x_n) \in K\langle X\rangle$ é multi-linear de grau n se f é multi-homogêneo de grau $(1, 1, \ldots, 1)$ em $K\langle x_1, x_2, \ldots, x_n\rangle \subset K\langle X\rangle$.*

Proposição 1.12. *Seja $f(x_1, x_2, \ldots, x_m)$ um polinômio de grau n em x_1, então o escrevemos*

$$f(x_1, x_2, \ldots, x_m) = \sum_{i=0}^{n} f_i,$$

onde f_i é a componente homogênea de f com grau i em x_1.
(i). Se o corpo é infinito (ou se o corpo possuir mais de n elementos), então f é uma identidade polinomial se, e somente se, os f_i, $i = 0, 1, \ldots, n$ o são.
(ii). Se o corpo é de característica 0, então f é é equivalente a um conjunto de identidades multi-lineares.

Demonstração. (i) Como K é um corpo infinito (ou pelo menos tem mais que n elementos), então podemos escolher $n+1$ elementos distintos, b_0, b_1, ..., $b_n \in K$. Temos o seguinte:

$$f(b_j x_1, x_2, \ldots, x_m) = \sum_{i=1}^{n} b_j^i f_i(x_1, x_2, \ldots, x_m).$$

Consideremos o sistema linear onde as incógnitas são os f_i. Temos então que o sistema tem solução se, e somente se, o seguinte determinante é diferente de 0

$$\delta = \begin{vmatrix} 1 & b_0 & \cdots & b_0^n \\ 1 & b_1 & \cdots & b_1^n \\ \vdots & \vdots & & \vdots \\ 1 & b_n & \cdots & b_n^n \end{vmatrix} = \prod_{i \neq j} (b_i - b_j).$$

A segunda igualdade segue das propriedades do determinante de Vandermonde, e temos $\delta \neq 0$. Portanto, cada $f_i \in \langle f \rangle^T$, $i = 0, 1, \ldots$

(ii) Por (i) podemos admitir que f é multi-homogêneo. Seja d o grau de f na variável x_1. Podemos escrever $f(y_1 + y_2, x_2, \ldots, x_m)$ da seguinte forma:

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

onde f_i é um polinômio homogêneo na variável y_1 de grau i. Como $f_i \in \langle f \rangle^T$, $i = 0, 1, \ldots,$ d, e o grau nas variáveis y_1, y_2 é menor que d quando $i = 1, \ldots, d-1$, podemos usar indução para concluir a demonstração.

Precisamos verificar que esse conjunto de identidades multi-lineares é equivalente a f. Para isto, basta ver que

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

e este coeficiente é diferente de 0, pois $\operatorname{char} K = 0$.

Desse modo, quando trabalhamos com álgebras sobre corpos infinitos, basta considerar somente as identidades multi-homogêneas; quando o corpo for de característica 0, podemos restringir a nossa atenção às identidades multi-lineares.

1.6 Identidades próprias

Nesta seção discutiremos uma outra classe de polinômios que podem ser considerados como geradores de um dado T-ideal. Juntando-se a informação desta e da seção anterior, poderemos restringir bastante o conjunto de polinômios a serem considerados.

Introduziremos o conceito de polinômio próprio. Este conceito apareceu pela primeira vez no artigo [43] de A. I. Malcev (veja também [58]) e se mostrou uma ferramenta muito útil na descrição dos geradores dos T-ideais, pois reduz o conjunto de polinômios que precisamos considerar.

Começamos com a seguinte definição.

Definição 1.13. *O comutador (de Lie) de comprimento n, $n > 1$, é definido indutivamente por*

$$[x_1, x_2] = x_1x_2 - x_2x_1,$$
$$[x_1, \ldots, x_{n-1}, x_n] = [[x_1, \ldots, x_{n-1}], x_n], \ n > 2.$$

Quando o comutador é tomado como acima dizemos que o comutador é normado à esquerda.

No restante deste trabalho todos os comutadores considerados serão normados à esquerda. Sempre que dissermos comutador de comprimento n estaremos pensando em um comutador de comprimento n normado á esquerda. Se não for o caso, mencionaremos no texto explicitamente.

Definição 1.14. *Um polinômio $f \in K\langle X\rangle$ é chamado de polinômio próprio, se ele pode ser escrito como uma combinação linear de produtos de comutadores, isto é,*

$$f(x_1, x_2, \ldots, x_n) = \sum \alpha_{i,\ldots,j}[x_{i_1}, \ldots, x_{i_p}] \cdots [x_{j_1}, \ldots, x_{j_q}], \ \alpha_{i,\ldots,j} \in K.$$

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

Logo podemos considerar $B(X)$ como a sub-álgebra associativa e unitária de $K\langle X\rangle$, gerada por $\sum_{n\geq 2} L^{(n)}$ onde $L^{(n)}$ é a componente homogênea de grau n da álgebra de Lie livre $L(X) \subset K\langle X\rangle$.

Seja $B(X)^{(n)}$ a componente homogênea de grau n de $B(X)$. É fácil de perceber que $B(X)^{(0)} = K$, $B(X)^{(1)} = 0$, e $B(X)^{(2)}$ e $B(X)^{(3)}$ são geradas respectivamente por

$$\{[x_i, x_j] \mid i > j\}, \qquad \{[x_i, x_j, x_k] \mid i > j, j \leq k\}.$$

Dada a seguinte base da álgebra livre de Lie $L(X)$

$$x_1, x_2, \ldots, [x_{i_1}, x_{i_2}], [x_{j_1}, x_{j_2}], \ldots, [x_{k_1}, x_{k_2}, x_{k_3}], \ldots$$

podemos ordenar essa base colocando em primeiro lugar as variáveis (entre elas usamos a ordem lexicográfica) e depois os comutadores, colocando os comutadores de menor comprimento na frente e entre os comutadores de mesmo comprimento usamos novamente a ordem lexicográfica.

Proposição 1.15. *(i). Adotando a base e a ordem descrita acima para a álgebra livre de Lie $L(X)$ temos que o espaço vetorial $K\langle X\rangle$ tem uma base*

$$x_1^{a_1} \cdots x_m^{a_m} [x_{i_1}, x_{i_2}]^b \cdots [x_{l_1}, \ldots, x_{l_p}]^c$$

onde $a_1, \ldots, a_m, b, \ldots, c \geq 0$ e $[x_{i_1}, x_{i_2}] < \cdots < [x_{l_1}, \ldots, x_{l_p}]$ na ordem da base de $L(X)$. Os elementos de $K\langle X\rangle$ da forma acima com $a_1 = \cdots = a_m = 0$ formam uma base do espaço vetorial dos polinômios próprios $B(X)$.
(ii). Seja R uma PI-álgebra com unidade sobre um corpo infinito. Então todas as identidades polinomiais de R seguem das identidades próprias de R. Se $\operatorname{char} K = 0$, então as identidades polinomiais de R seguem das identidades próprios e multi-lineares.

Demonstração. (i) A primeira afirmação sobre a base de $K\langle X\rangle$ segue do teorema de Witt 1.7, e o teorema de Poincaré—Birkhoff—Witt 1.6 nos dá a base do $K\langle X\rangle = U(G)$ em termos da álgebra de Lie $L(X) = G$. A afirmação a respeito de $B(X)$ também segue do teorema de Poincaré—Birkhoff—Witt. Vamos dar uma idéia do porque isto funciona. Se temos x_2x_1, poderemos substituir este produto por $x_2x_1 = x_1x_2 - [x_1, x_2]$. A primeira parcela do lado direito está na ordem correta, a segunda é um comutador. O raciocínio para o caso geral é bastante parecido. Suponhamos que dois comutadores consecutivos não estão na ordem correta e definida acima no enunciado. Por exemplo, consideremos

$$\ldots [x_{b_1}, \ldots, x_{b_l}][x_{a_1}, \ldots, x_{a_k}] \ldots, \qquad [x_{b_1}, \ldots, x_{b_l}] > [x_{a_1}, \ldots, x_{a_k}]$$

os dois comutadores que não respeitam a ordem (permitimos $l = 1$ e/ou $k = 1$). Então substituímos o produto

$$[x_{b_1}, \ldots, x_{b_l}][x_{a_1}, \ldots, x_{a_k}]$$

pela soma

$$[x_{a_1}, \ldots, x_{a_k}][x_{b_1}, \ldots, x_{b_l}] + [[x_{b_1}, \ldots, x_{b_l}], [x_{a_1}, \ldots, x_{a_k}]].$$

Como a segunda parcela desta soma pertence a $L(X)$ temos que esta parcela é uma combinação linear de comutadores da base de $L(X)$. Portanto aplicando argumentos indutivos vemos que os elementos de $B(X)$ são combinações lineares de

$$[x_{i_1}, x_{i_2}]^b \cdots [x_{l_1}, \ldots, x_{l_p}]^c,$$

como requerido.

(ii) Se $f(x_1, x_2, \ldots, x_m)$ é uma identidade polinomial de R, podemos assumir que f é multi-homogêneo. Escrevemos f na seguinte forma

$$f(x_1, x_2, \ldots, x_m) = \sum \alpha_a x_1^{a_1} \cdots x_m^{a_m} \omega_a(x_1, x_2, \ldots, x_m)$$

onde $\omega_a(x_1, x_2, \ldots, x_m)$ é uma combinação linear de

$$[x_{i_1}, x_{i_2}]^b \cdots [x_{l_1}, \ldots, x_{l_p}]^c.$$

Claramente, se substituirmos por 1 uma das variáveis em um comutador $[x_{i_1}, \ldots, x_{i_p}]$, o comutador se anula. Como $f(1 + x_1, x_2, \ldots, x_m)$ é também uma identidade polinomial de R, obtemos que

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

A componente homogênea de grau mínimo a respeito de x_1 é obtida dos termos da soma com a_1 sendo o máximo entre aqueles com $\alpha_a \neq 0$. Como o T-ideal $T(R)$ é homogêneo (ou seja, $T(R)$ é gerado pelos seus elementos multi-homogêneos), obtemos que

$$\sum_{a_1 \text{máx}} \alpha_a x_2^{a_2} \cdots x_m^{a_m} \omega_a(x_1, x_2, \ldots, x_m) \in T(R).$$

Multiplicando à esquerda essa identidade polinomial por $x_1^{a_1}$ e subtraindo o produto de $f(x_1, x_2, \ldots, x_m)$, obtemos uma identidade que é equivalente a $f(x_1, x_2, \ldots, x_m)$ mas envolve valores menores de a_1. Por indução estabelecemos que

$$\sum_{a_1 \text{fixo}} \alpha_a x_2^{a_2} \cdots x_m^{a_m} \omega_a(x_1, x_2, \ldots, x_m) \in T(R),$$
$$\omega_a(x_1, x_2, \ldots, x_m) \in T(R)$$

e isto completa a demonstração. ■

1.7 Álgebras Relativamente Livres. Matrizes genéricas

Tomemos uma variedade de álgebras, descreveremos uma álgebra genérica na variedade. Ela terá um papel semelhante ao da álgebra livre $K\langle X\rangle$ na variedade de todas as álgebras associativas.

Definição 1.16. *Uma álgebra $F = F(Y)$ da variedade Δ, gerada por um conjunto Y, é chamada de álgebra relativamente livre da variedade Δ, se F, com o conjunto gerador Y, é livre na categoria Δ. A cardinalidade do conjunto Y é o posto de F.*

Em outras palavras, F é livre na variedade Δ se, e somente se, para toda álgebra $S \in \Delta$, toda aplicação $Y \to S$ estende-se unicamente a um homomorfismo de álgebras $F \to S$.

Dada uma álgebra R sobre um corpo K, podemos considerar a álgebra relativamente livre $F(R)$ na variedade $var(R)$. Então $F(R)$ é exatamente a álgebra quociente da álgebra livre pelo T-ideal $T(R)$. De alguma maneira todas as informações de R estão "codificadas" em $F(R)$. Ressaltamos que se Δ é uma variedade e se F é livre em Δ, de posto infinito (e enumerável), então $\Delta = var(F)$. Às vezes pode acontecer que Δ seja gerada por alguma álgebra relativamente livre de posto finito, mas isso nem sempre ocorre.

Infelizmente, em vários casos importantes, não é claro como se pode trabalhar em $F(R)$ e muito menos fazer cálculos concretos. Há uma construção "genérica" da álgebra relativamente livre de posto infinito na variedade gerada por uma álgebra; um caso particular e bastante importante será considerado abaixo. No caso das identidades polinomias da álgebra das matrizes $M_n(K)$, $n \geq 2$, a álgebra relativamente livre $F(var(M_n(K)))$ admite uma realização que além de elegante permite que se executem cálculos. Esta realização foi introduzida por Procesi em [48].

Fixemos $n \neq 2$ e denotemos por $\Omega = \Omega_n$ a K-álgebra em infinitas variáveis comutativas

$$K[\xi] = K[\xi_{ij}^{(r)} \mid i, j = 1, 2; r = 1, 2, \ldots]$$

Definição 1.17. *Sejam* $\{e_{i,j} \mid 1 \leq i, j \leq n\}$, *onde* $e_{i,j}$ *são as matrizes que têm 1 na posição* (i, j) *e* 0 *nas outras, as matrizes que formam a base canônica do espaço vetorial* $M_n(K)$. *As matrizes* $n \times n$

$$y_r = \sum_{i,j=1}^{n} \xi_{ij}^{(r)} e_{i,j}, r = 1, 2, \ldots$$

são chamadas de matrizes genéricas $n \times n$. *A álgebra* Gen_n *gerada pelos* y_r *é chamada de álgebra das matrizes genéricas* $n \times n$.

Por exemplo, se $n = 2$, consideramos a álgebra Gen_2 gerada por apenas dois elementos. Mudando a notação para $x_{pq} = \xi_{pq}^{(1)}$ e $y_{pq} = \xi_{pq}^{(2)}$ obtemos que Gen_2 é gerada por

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

Terminamos esta seção com uma proposição que será utilizada mais adiante, sem mencioná-la explicitamente.

Sejam P e Q dois T-ideais em $K\langle X\rangle$ e seja $F = \{f_i \mid i \in I\}$ um conjunto de polinômios em $K\langle X\rangle$. Utilizaremos as mesmas letras f_i para as imagens dos f_i sob as projeções canônicas $K\langle X\rangle \to K\langle X\rangle/P$ e $K\langle X\rangle \to K\langle X\rangle/Q$.

Proposição. *Seja* $P \subseteq Q$ *e suponha que o conjunto* F *seja uma base do espaço vetorial* $K\langle X\rangle/P$. *Se* F *for linearmente independente em* $K\langle X\rangle/Q$, *então* $P = Q$.

Demonstração. A demonstração é óbvia. ∎

1.8 Invariantes e Tabelas Duplas, um Resumo

Nesta seção faremos uma exposição da parte do artigo [9], que trata da descrição da álgebra dos invariantes pelo grupo ortogonal e da álgebra dos invariantes pelo grupo especial ortogonal, em termos de tabelas duplas. Está descrição foi baseada no trabalho [10].

Sejam K um corpo qualquer e $\{x_{ij} \mid i \geq 1, 1 \leq j \leq n\}$ um conjunto de variáveis comutativas, consideremos o espaço vetorial gerado pelos vetores $x_i = (x_{i1}, x_{i2}, \ldots, x_{in})$. Definamos uma forma simétrica, bilinear (e não degenerada) dada por $x_i \circ x_k = x_{i1}x_{k1} + x_{i2}x_{k2} + \cdots + x_{in}x_{kn}$. Vamos descrever a álgebra dos invariantes do grupo ortogonal O_n e do grupo especial ortogonal SO_n obtida em [9]. Observamos que a descrição dada em [9] não depende da característica do corpo K. A álgebra dos invariantes pelo grupo O_n coincide com a álgebra dos polinômios (comutativos) $K[(x_i \circ x_j)]$, e podemos indexar (veja [9]) uma base do espaço desses polinômios com as tabelas duplas standard T, onde T é da seguinte forma:

$$T = \left(\begin{array}{cccc|cccc} p_{11} & p_{12} & \dots & p_{1m_1} & q_{11} & q_{12} & \dots & q_{1m_1} \\ p_{21} & p_{22} & \dots & p_{2m_2} & q_{21} & q_{22} & \dots & q_{2m_2} \\ \dots & \dots & \ddots & \dots & \dots & \dots & \ddots & \dots \\ p_{k1} & p_{k2} & \dots & p_{km_k} & q_{k1} & q_{k2} & \dots & q_{km_k} \end{array} \right).$$

Aqui $n \geq m_1 \geq m_2 \geq \dots \geq m_k \geq 1$ e p_{ij}, q_{ij} são inteiros positivos. A tabela T é chamada de standard se

$$p_{i1} < \dots < p_{im_i}, \quad q_{i1} < \dots < q_{im_i}, \quad p_{ij} \leq q_{ij} \leq p_{i+1,j}$$

para todos i e j. Se formamos a tabela simples T', inserindo a segunda metade de cada linha imediatamente abaixo da sua primeira metade, a tabela obtida será

$$T' = \begin{pmatrix} p_{11} & p_{12} & \dots & p_{1m_1} \\ q_{11} & q_{12} & \dots & q_{1m_1} \\ p_{21} & p_{22} & \dots & p_{2m_2} \\ q_{21} & q_{22} & \dots & q_{2m_2} \\ \dots & \dots & \ddots & \dots \\ p_{k1} & p_{k2} & \dots & p_{km_k} \\ q_{k1} & q_{k2} & \dots & q_{km_k} \end{pmatrix}$$

de acordo com as desigualdades acima, quando olharmos (da esquerda para a direita) as linhas serão estritamente crescentes, e as colunas (de cima para baixo) serão crescentes com possíveis repetições. Como tais tabelas são chamadas de “standard” na teoria das representações do grupo geral linear, adotamos o mesmo adjetivo para o nosso caso de tabelas duplas.

Associamos à tabela T um elemento $\widetilde{\varphi}(T)$ de $K[(x_i \circ x_j)]$ da seguinte forma.

Se $T = (p_1\, p_2\, \dots\, p_m \mid q_1\, q_2\, \dots\, q_m)$ é uma tabela de uma única linha, então

$$\widetilde{\varphi}(T) = \sum (-1)^{\sigma} (x_{p_1} \circ x_{q_{\sigma(1)}})(x_{p_2} \circ x_{q_{\sigma(2)}}) \dots (x_{p_m} \circ x_{q_{\sigma(m)}}),$$

onde σ percorre todas as permutações do grupo simétrico S_m e $(-1)^{\sigma}$ representa o sinal da permutação σ. No caso em que T é uma tabela com várias linhas, podemos denotar por $T^{(1)}$, $T^{(2)}$, ..., $T^{(k)}$ as linhas da tabela dupla T, então

$$\widetilde{\varphi}(T) = \widetilde{\varphi}(T^{(1)})\, \widetilde{\varphi}(T^{(2)}) \dots \widetilde{\varphi}(T^{(k)}).$$

Note que, no caso de T ser uma tabela de uma única linha, temos $\widetilde{\varphi}(T) = \det\big((x_{p_i} \circ x_{q_j})\big)$, onde $1 \leq i, j \leq m$. Além disso, se $p_i = p_j$ ou $q_i = q_j$ para algum $i \neq j$ então $\widetilde{\varphi}(T) = 0$.

Exemplo 1.18. *Seja $T = (1\ 2 \mid 3\ 4)$ uma tabela dupla com uma única linha, então associamos a seguinte matriz*

$$a' = \begin{pmatrix} x_{13} & x_{14} \\ x_{23} & x_{24} \end{pmatrix}$$

e $\widetilde{\varphi}(T) = det(a') = x_{13} \circ x_{24} - x_{14} \circ x_{23}$, aqui calculamos o determinante substíndo o produto por $\circ$.

Tomemos uma tabela dupla cujas primeiras k entradas, onde $1 \leq k \leq n$, da primeira linha são vazias e as preenchemos consecutivamente com os valores $-(k-1), \ldots, -1, 0$, respectivamente. Observe que n é no máximo o tamanho da primeira meia linha. Chamaremos a uma tabela dupla preenchida dessa forma de k-tabela.

Ao longo dessa dissertação, associaremos polinômios a tais tabelas. Como isso dependerá da situação concreta, deixamos tais associações para frente. Tais associações serão feitas com o objetivo de "cindir" uma parte do polinômio correspondente à tabela se considerarmos ela preenchida usualmente.

Vamos definir uma ordem no conjunto das k-tabelas duplas. Seja T uma tabela dupla, definimos $m(T)$ por ser o vetor $m(T) = (m_1, m_2, \ldots, m_k)$, onde m_i representa o comprimento da respectiva (meia-)linha de T, e por $p(T)$,

$$p(T) = (p_{11}, p_{12}, \ldots, p_{1m_1}, q_{11}, \ldots, q_{12}, \ldots, q_{1m_1}, p_{21}, \ldots, q_{km_k}).$$

Chamamos $m(T)$ o **contorno** e $p(T)$ a **forma** de T. Seja

$$d(T) = (d_{-k}, \ldots, d_{-1}, d_1, d_2, \ldots)$$

onde d_i é o número de entradas de T que são igual a i, $i = \pm 1, \pm 2, \ldots$, e o chamamos de **conteúdo** da tabela dupla T.

Sejam T e Q duas k-tabelas duplas com o mesmo conteúdo, isto é, $d(T) = d(Q)$. Diremos que $T > Q$ se, e somente se, $m(T) > m(Q)$ na ordem lexicográfica usual ou se ocorrer $m(T) = m(Q)$ então $p(T) < p(Q)$ também com a ordem lexicográfica usual.

De Concini e Procesi demonstraram os seguintes teoremas.

Teorema 1.19. ([9], Teorema 1.5) *Os polinômios $\widetilde{\varphi}(T)$ onde T percorre todas as tabelas duplas standard e tais que $m_1 \leq n$, formam uma base do espaço vetorial $K[(z_i \circ z_j)]$.*

Seja

$$T = \left(\begin{array}{cccccc|cccccc} p_1 & \ldots & p_s & r_1 & \ldots & r_k & r_{k+1} & \ldots & r_{n+1} & q_1 & \ldots & q_{k-1} \end{array} \right)$$

uma tabela de apenas uma linha tal que $n = s + k$. Denotemos

$$\widetilde{T} = \sum (-1)^\sigma \widetilde{\varphi} \left(\begin{array}{cccccc|cccccc} p_1 & \ldots & p_s & r_{\sigma(1)} & \ldots & r_{\sigma(k)} & r_{\sigma(k+1)} & \ldots & r_{\sigma(n+1)} & q_1 & \ldots & q_{k-1} \end{array} \right),$$

onde a somatória do lado direito percorre as permutações $\sigma \in S_{n+1}$ tais que

$$\sigma(1) < \ldots < \sigma(k), \qquad \sigma(k+1) < \ldots < \sigma(n+1).$$

Denotemos S_{n+1}^k ao conjunto destas permutações.

Lema 1.20. ([9], Lema 15.2) $\widetilde{T} = 0$ *em* $K[(x_i \circ x_j)]$.

Aproveitamos e citamos um resutado que nos será útil mais a frente.

Lema 1.21. ([62], Lema 1.9) *Seja*

$$T = \left(\begin{array}{cccccc|cccccc} s_1 & \ldots & s_k & s_{k+1} & \ldots & s_n & q_1 & \ldots & q_{k-1} & r_{k+1} & \ldots & r_{n+1} \\ r_1 & \ldots & r_k & q_{k+1} & \ldots & q_m & t_1 & \ldots & t_{k-1} & t_k & \ldots & t_m \end{array} \right)$$

uma tabela dupla. Então a igualdade

$$\sum (-1)^\sigma \widetilde{\varphi} \left(\begin{array}{cccccc|cccccc} s_1 & \ldots & s_k & s_{k+1} & \ldots & s_n & r_{\sigma(1)} & \ldots & r_{\sigma(k)} & q_{k+1} & \ldots & q_m \\ q_1 & \ldots & q_{k-1} & r_{\sigma(k+1)} & \ldots & r_{\sigma(n+1)} & t_1 & \ldots & t_{k-1} & t_k & \ldots & t_m \end{array} \right) = \sum \alpha_l \widetilde{\varphi}(T_l)$$

vale em $K[(x_i \circ x_j)]$. *A soma do lado esquerdo percore todas as* $\sigma \in S_{n+1}^k$, $1 \leq k \leq m \leq n$, *e a da direita percorre um conjunto finito de tabelas duplas standard* T_l, *cujas primeiras linhas são da forma*

$$\left(\begin{array}{c|ccc} \ldots & r_1 & \ldots & r_{n+1} \end{array} \right).$$

Agora vamos descrever os invariantes do grupo SO_n. Consideremos o determinate $\det(x_{i_1}, \ldots, x_{i_n})$ da matriz $n \times n$, cujas linhas são formadas pelas coordenadas dos vetores $x_{i_1}, \ldots, x_{i_n}$. Denotemos este determinante por $< x_{i_1}, \ldots, x_{i_n} >$. Então pelo Teorema 5.6 de [9], os invariantes do grupo SO_n coincidem com a álgebra gerada por $K[(x_i \circ x_j)]$ e por todos os polinômios $< x_{i_1}, \ldots, x_{i_n} >$.

Uma base linear da álgebra dos invariantes do grupo especial ortogonal SO_n é dada por todas as tabelas duplas standard como descrito acima, acrescentando-se os produtos do tipo $< x_{i_1}, \ldots, x_{i_n} > \widetilde{\varphi}(T)$ (e preservando-se a propriedade standard).

Podemos fazer a seguinte interpretação. Formamos a tabela ordinária T' da tabela dupla standard T, conforme feito anteriormente, e em seguida colocamos a linha $(i_1, i_2, \ldots, i_n)$ em cima da tabela. A tabela T'' obtida desta maneira, tem de ser standard.

Usando a terminologia de [37], dizemos que o polinômio

$$\varphi(T) =< x_{i_1}, \ldots, x_{i_n} > \widetilde{\varphi}(T) = det(x_{i_1}, \ldots, x_{i_n})\widetilde{\varphi}(T^{(1)})\,\widetilde{\varphi}(T^{(2)}) \ldots \widetilde{\varphi}(T^{(k)})$$

é representado por uma n-tabela T. Portanto associamos ao polinômio acima uma tabela que tem as primeiras n entradas, da primeira linha, vazias. Por convenção designamos a essas entradas os valores $-(n-1)$, $\ldots$, -1, 0. Se todas as entradas da tabela dupla são inteiros positivos colocamos $\varphi(T) = \widetilde{\varphi}(T)$.

Capítulo 2

Identidades polinomiais em $M_2(K)$

É conhecido, que as identidades polinomiais da álgebra das matrizes 2×2, são geradas pelo polinômio de Hall h_5 e pela identidade standard s_4, quando $\operatorname{char} K = 0$.

Vamos contar um pouco a respeito da história desse resultado. Razmyslov em [51] encontrou uma base para as identidades de $M_2(K)$, assim como $sl_2(K)$, quando $\operatorname{char} K = 0$ (veja também o livro dele [53]). Ele também demonstrou que toda álgebra na variedade das álgebras de Lie gerada por $sl_2(K)$ tem uma base finita de suas identidades. Ele utilizou o fato que em álgebras sobre corpos de $\operatorname{char} K = 0$, pode-se restringir às identidades multilineares.

Em [60], Tki demonstrou que bastavam 4 identidades para gerar o T-ideal de $M_2(K)$. Em seguida Drensky, utilizando métodos da teoria das representações do grupo simétrico, em [11] encontrou uma base mínima com apenas duas identidades. Em [19] Filippov demonstrou que as identidades da álgebra de Lie sl_2 seguiam de apenas uma. Além disso, eles descreveram vários aspectos numéricos do T-ideal de $M_2(K)$. Percebe-se que o T-ideal de $M_2(K)$ no caso em que $\operatorname{char} K = 0$ foi descrito em detalhes por esses autores.

Sobre corpos finitos, Malcev e Kuzmin em [45] demonstraram que as identidades de $M_2(K)$ seguem de duas identidades. Para $n = 3$ e 4 veja [22, 25], respectivamente.

No caso de corpos infinitos, mas de característica positiva, destacamos os seguintes resultados: Vasilovsky em [62] provou que quando $\operatorname{char} K \neq 2$ as identidades polinomais da álgebra de Lie seguem de apenas uma (a mesma que em corpos de característica 0). Por outro lado, Vaughan-Lee em [61] provou que quando $\operatorname{char} K = 2$ as identidades de $M_2(K)$ considerada como álgebra de Lie, não admitem base finita.

Resultados parciais no caso de característica 2 podem ser encontrados em [38, 13].

Quando o corpo é infinito e de $\operatorname{char} K = p \neq 2$, Koshlukov em [37] mostrou que quando

$p > 5$ o T-ideal de $M_2(K)$ é gerado por duas identidades (as mesmas que no caso de característica 0). No caso de característica $p = 3$ e 5 ele exibiu uma base formada por 4 identidades. Finalmente em [8] mostramos que no caso $p = 5$ bastam as duas identidades anteriores e quando $p = 3$ são necessárias 3 identidades, as duas anteriores mais o r_6. Recordamos que a necessidade de mais identidades em característica 3 foi obtida em [24].

Neste capítulo vamos repetir a construção feita em [37] e no final acrescentar o resultado obtido por nós em [8].

2.1 Identidades em $M_2(K)$

Nesta seção vamos introduzir algumas identidades na álgebra das matrizes 2×2 e descrever o T-ideal gerado por elas em termos de uma transformação definida mais abaixo.

Lema 2.1. *Os seguintes polinômios são identidades em $M_2(K)$:*

1. *A identidade standard s_4;*
2. *A identidade de Hall $h_5 = [[x_1, x_2] \circ [x_3, x_4], x_5]$;*
3. *A identidade de Lie $v_5 = [y, z, [t, x], x] + [y, x, [z, x], t]$.*

Observação 2.2. 1. *A identidade standard é o polinômio de menor grau satisfeito por $M_2(K)$. Além disso, podemos reescrevê-lo da seguinte forma:*

$$s_4 = 1/2([x_1, x_2] \circ [x_3, x_4] - [x_1, x_3] \circ [x_2, x_4] + [x_1, x_4] \circ [x_2, x_3]).$$

2. *A identidade v_5 é uma base das identidades da álgebra $sl_2(K)$. Isto foi provado em [19] no caso de $char\, K = 0$ e por Vasilovsky em [62] para um corpo infinito arbitrário, com $char(K) \neq 2$.*

O espaço vetorial $L(X)$ tem base consistindo dos elementos x_i e dos elementos u_i, onde u_i são comutadores de grau ≥ 2. Como em [62], vamos definir o operador $L'(a, b)$ com a, $b \in L(X)$, sobre a sub-álgebra de Lie gerada pelos u_i, da seguinte maneira. Se $[w_1, w_2]$ é um comutador em $L(X)$ então

$$\begin{aligned}[w_1, w_2]L'(a, b) &= (1/16)([w_1, a, b, w_2] + [w_1, b, a, w_2] + [w_1, a, w_2, b] + [w_1, b, w_2, a] \\ &\quad -[w_2, a, b, , w_1] - [w_2, b, a, w_1] - [w_2, a, w_1, b] - [w_2, b, w_1, a]).\end{aligned}$$

Usando a identidade de Jacobi, obtemos

$$[w_1, w_2]L'(a, b) = (1/8)([w_1, a, b, w_2] + [w_1, b, a, w_2] - [w_2, a, w_1, b] - [w_2, b, w_1, a]). \quad (2.1)$$

A igualdade $[c, a, b] = 4((a \circ b) \circ c - a \circ (b \circ c))$ é válida em qualquer álgebra associativa. Logo obtemos a seguinte identidade fraca

$$[x_1, x_2]\ L'(a, b) = [x_1, x_2] \circ (a \circ b).$$

Portanto é válida a seguinte identidade em $M_2(K)$.

$$[x_1, x_2] \circ (a \circ b) \quad = \quad (1/8)([x_1, a, b, x_2] + [x_1, b, a, x_2] - [x_2, a, x_1, b] - [x_2, b, x_1, a]),$$

onde $a = [x_3, x_4]$ e $b = [x_5, x_6]$ são comutadores de comprimento 2. Chamaremos a essa identidade de r_6. Note que as 3 seguintes identidades são válidas na álgebra de Lie $sl_2(K)$.

$$\begin{aligned}
[x_1, x_2, x_3]L'(a, b) &= [[x_1, x_2]L'(a, b), x_3] \\
[x_1, a]\, L'(x_2, b) - [x_2, a]L'(x_1, b) &= (1/4)[x_1, x_2, b, a] \\
[x_1, x_2]\, L'(a, b)\, L'(c, d) &= [x_1, x_2]\, L'(c, d)\, L'(a, b)
\end{aligned}$$

Veja [62], identidades (3), (4) e (5) para sua dedução.

Lema 2.3. *[53, lema 41.2, pág. 205] Se $f \in B(X)$ é um polinômio próprio, então módulo as identidades h_5 e r_6, o polinômio f pode ser representado na forma $f = l + g$ onde $l \in L(X)$ e g é uma combinação linear de produtos da seguinte forma: $g_i \circ [x_i, x_n]$. Aqui $g_i \in L(X)$, e x_n é uma variável fixa (mas arbitrária) da qual f depende.*

Suponhamos que $f \in B(X)$ é um polinômio próprio, então $f = l + g$ como no lema acima. Observamos que f é uma identidade de $M_2(K)$ se, e somente se, l e g o são, pois os valores que o polinômio l assume quando suas variáveis substituem-se por matrizes 2×2, resulta em uma matriz com traço 0. Por outro lado, os valores de g em $M_2(K)$ são múltiplos da matriz I. Mas somando-se uma matriz com traço 0 com um múltiplo de I, obteremos a matriz nula se, e somente se, ambas as matrizes são nulas. (Este raciocínio deixa de ser verdadeiro em característica 2.)

Observamos ainda que todas identidades de $M_2(K)$ da forma $l \in L(X)$ seguem de v_5 conforme o teorema de Vasilovsky. Portanto se T_1 é o T-ideal gerado pelas identidades s_4,

h_5, v_5 e r_6, então $T_1 \subset T(M_2(K))$, e podemos escolher uma base de identidades de $M_2(K)$, módulo T_1, entre as identidades com a forma de g.

Vamos definir a transformação $L(a,b)$ para polinômios da forma de g. Se $g = g_1 \circ g_2$, onde g_1 e g_2 são comutadores de grau ≥ 2, então colocamos $gL(a,b) = g_1 \circ (g_2 L'(a,b))$. Logo para a boa definição de $L(a,b)$ precisamos que valham as seguintes identidades em $M_2(K)$.

$$\begin{aligned} &([x_1,a,b,x_2] + [x_1,b,a,x_2] - [x_2,a,x_1,b] - [x_2,b,x_1,a]) \circ [y_1,y_2] \\ &= ([y_1,a,b,y_2] + [y_1,b,a,y_2] - [y_2,a,y_1,b] - [y_2,b,y_1,a]) \circ [x_1,x_2] \end{aligned} \tag{2.2}$$

e

$$\begin{aligned} &([x_1,a,b,x_2,x_3] + [x_1,b,a,x_2,x_3] - [x_2,a,x_1,b,x_3] - [x_2,b,x_1,a,x_3]) \circ [y_1,y_2] \\ &= ([y_1,a,b,y_2] + [y_1,b,a,y_2] - [y_2,a,y_1,b] - [y_2,b,y_1,a]) \circ [x_1,x_2,x_3] \end{aligned} \tag{2.3}$$

É fácil de verificar que essas duas identidades são válidas em $M_2(K)$, basta usar a identidade fraca $[x_1,x_2]\, L'(a,b) = [x_1,x_2] \circ (a \circ b)$ e lembrar que $a \circ b$ é central em $M_2(K)$.

Vamos estabelecer mais alguns resultados e depois provaremos que o operador L é bem definido.

A linearização de v_5 é o polinômio

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

que é uma identidade para $sl_2(K)$ assim como para $M_2(K)$. Como $\operatorname{char} K \neq 2$ temos que o polinômio linearizado é equivalente a v_5, também vamos chamar o polinômio linearizado de v_5.

Escrevendo a linearização de v_5 como $v_5 = \sum \alpha_i [a_i, b_i]$, onde $\alpha_i \in K$ e a_i, b_i são comutadores, e o comprimento de $a_i \geq 2$. Então o polinômio $v_5' = \sum \alpha_i (a_i \circ [b_i, x_6])$ é uma identidade para $M_2(K)$ uma vez que é uma identidade fraca. De fato, se tivessemos escrito como a identidade fraca da forma $\sum \alpha_i [a_i, b_i] \circ x_6$, então o que segue é claramente uma identidade fraca.

Vamos estender o T-ideal T_1. Denotemos por T_2 o T-ideal gerado por T_1, e as identidades (2.2) e (2.3) e v_5'. Como todas essas identidades são válidas em $M_2(K)$ segue que $T_2 \subset T(M_2(K))$.

Lema 2.4. *Cada polinômio próprio $f \in B(X)$ de grau par ≥ 4 pode ser escrito, módulo as identidades de T_2, da seguinte forma*

$$f = \sum_i \alpha_i [x_{i_1}, x_{i_2}] \circ [x_{i_3}, x_{i_4}] \prod_j L(a_{ij}, b_{ij})$$

para a_{ij}, $b_{ij} \in X$ e $\alpha_i \in K$ adequados. Além disso, podemos supor que $i_1 < i_2$, $i_3 < i_4$ e $i_1 \leq i_3$. Quando o grau de f for igual a 4 podemos supor ainda que $i_2 \leq i_4$.

Lema 2.5. *Cada polinômio próprio $f \in B(X)$ de grau ímpar ≥ 5 pode ser escrito, módulo as identidades de T_2, da seguinte forma*

$$f = \sum_i \alpha_i \sum_\sigma (-1)^\sigma [x_{i_{\sigma(1)}}, x_{i_{\sigma(2)}}] \circ [x_{i_{\sigma(3)}}, x_{i_4}] \prod_j L(a_{ij}, b_{ij})$$

para a_{ij}, $b_{ij} \in X$ e $\alpha_i \in K$ adequados (σ assume os elementos de seu respectivo grupo simétrico). Além disso, quando o grau de f é 5 podemos supor $i_1 \leq i_2 \leq i_3$, $i_4 \leq i_5$ e $i_1 \leq i_4$.

Demonstração. Vamos dar apenas uma idéia da demonstração. Use as identidades (3) e (4) de [62] e observe que

$$\begin{aligned} 4[x_1, x_2] \circ [x_3, x_4, x_5] &= \sum_\sigma (-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}] \circ [x_{\sigma(3)}, x_4, x_5] \\ &- \sum_\sigma (-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}] \circ [x_{\sigma(4)}, x_3, x_5]. \end{aligned}$$

Agora a identidade

$$\sum_\sigma (-1)^\sigma [x_{\sigma(1)}, x_{\sigma(2)}] \circ [x_{\sigma(3)}, [x_{i_4}, x_5]] = 0$$

é válida em $M_2(K)$ e segue de h_5 (veja [37, pág. 421]). ■

Além disso, a identidade

$$\sum_{\sigma \in S_4} (-1)^\sigma [x_{i_{\sigma(1)}}, x_{i_{\sigma(2)}}] \circ [x_{i_{\sigma(3)}}, x_{i_{\sigma(4)}}, x_5]$$

pertence ao T-ideal gerado por s_4 (veja [37, pág. 422]).

2.2 Tabelas Duplas

Nesta seção vamos mostrar que o operador $L(a, b)$ está bem-definido. Iniciamos definindo $L(a, b)$ para os polinômios próprios com grau 4 e 5, dados acima, agora por indução sobre o grau dos polinômios definimos $L(a, b)$ sobre os elementos básicos, ou seja, para os polinômios correspondentes a tabelas duplas standard e estendemos o operador usando a linearidade do mesmo.

Seja $B(M_2(K))$ a imagem de $B(X)$ através da projeção canônica

$$K\langle X\rangle \longrightarrow K\langle X\rangle/T(M_2(K)).$$

Então $B(M_2(K)) = B_2 \oplus L_2$, onde B_2 é o sub-espaço de $B(M_2(K))$ consistindo de todos os polinômios próprios centrais e L_2 é o sub-espaço dos polinômios de Lie. Pelo principal resultado de [62] sabemos que precisamos considerar somente o sub-espaço B_2. Vamos mostrar que L está bem definido sobre B_2.

Lema 2.6. *As transformações $L(a, b)$ são bem definidas sobre o espaço vetorial B_2.*

Demonstração. Vamos começar observando que se $f \in B_2$ é uma identidade em $M_2(K)$ então o polinômio $fL(a, b) \in B_2$ também é (isto é claro pela definição de L). A linearidade de $L(a, b)$ é clara e portanto o lema está demonstrado. ■

O lema acima mostra que os operadores $\{L(a, b)\}$ geram uma sub-álgebra comutativa da álgebra das transformações lineares de B_2.

Vamos associar a cada tabela dupla T o seguinte polinômio F_T em B_2. Depois mostraremos que podemos nos restringir a uma classe menor de tabelas duplas, que chamaremos de *Adm*. Começamos com a seguinte definição:

Definição 2.7. *Seja*

$$T = \left(\begin{array}{cccc|cccc} p_{11} & p_{12} & \dots & p_{1m_1} & q_{11} & q_{12} & \dots & q_{1m_1} \\ p_{21} & p_{22} & \dots & p_{2m_2} & q_{21} & q_{22} & \dots & q_{2m_2} \\ \dots & \dots & \ddots & \dots & \dots & \dots & \ddots & \dots \\ p_{k1} & p_{k2} & \dots & p_{km_k} & q_{k1} & q_{k2} & \dots & q_{km_k} \end{array}\right)$$

uma tabela dupla. Então definimos F_T por ser

a. $F_T = [x_{p_{11}}, x_{p_{12}}] \circ [x_{q_{11}}, x_{q_{12}}]\, l_2 \cdots l_k$, *se $m_1 = 2$. Aqui as l_j são transformações definidas por*

$$l_j = \Sigma(-1)^\sigma L(x_{p_{j1}}, x_{q_{j\sigma(1)}}) \cdots L(x_{p_{jm}}, x_{q_{j\sigma(m)}}), \quad \sigma \in S_m,\ m = m_j.$$

b. $F_T = 1/2 \sum_\sigma (-1^\sigma)[x_{p_{11}}, x_{p_{12}}] \circ [x_{1\sigma(1)}, x_{p_{1\sigma(2)}}] L(x_{13}, x_{q_{1\sigma(3)}}\ l_2 \cdots l_k$, *se T é uma 0-tabela e $m_1 = 3$.*

c. $F_T = 1/2\sum_\sigma(-1)^\sigma(\sum_\tau(-1)^\tau\left[x_{q_{1\sigma(1)}}, x_{q_{1\sigma(2)}}\right] \circ [x_{q_{1\sigma(3)}}, x_{p_{21}}, x_{q_{2\tau(1)}}]l'_2)\ l_3\cdots l_k,$, *se* T *é uma 3-tabela e* $m_1 = 3$. *Neste caso* $\sigma \in S_3$, $\tau \in S_{m_2}$. *Além disso,* $l'_2 = L(x_{p_{22}}, x_{p_{2\tau(2)}})\cdots L(x_{p_{m_2}}, x_{q_{2\tau(m_2)}})$. *Este último caso somente é necessário quando* $m_2 \geq 1$.

Denotemos por *Adm* (de admissível) ao conjunto das tabelas duplas standard T tal que $m_1 = 2$ ou 3, T é uma 0-tabela ou uma 3-tabela, no caso de T ser uma 3-tabela então $m_1 \neq 0$.

Lema 2.8. *Os polinômios* F_T, $T \in \mathrm{Adm}$, *são linearmente independentes módulo o T-ideal* $T(M_2(K))$.

Demonstração. veja [37, pág. 425]. ■

2.3 $T(M_2(K))$ é finitamente gerado

Vamos mostrar que, módulo um certo T-ideal contido em $T(M_2(K))$, cada polinômio próprio é expresso como combinação linear de polinômios F_T, $T \in Adm$. Portanto, nosso T-ideal deverá ser finitamente gerado, e depois vamos minimizar a base deste T-ideal sendo esse o principal resultado deste capítulo.

Comecemos com o seguinte lema.

Lema 2.9. *A seguinte expressão é uma identidade em* $M_2(K)$*:*

$$\sum_{\sigma\in S_3}[x_1, x_2] \circ [y_{\sigma(1)}, y_{\sigma(2)}]L(x_3, y_{\sigma(3)}) = \sum_{\sigma\in S_3}[x_1, x_2]L(x_3, y_{\sigma(3)}) \circ [y_{\sigma(1)}, y_{\sigma(2)}]$$

Demonstração. Como todas as variáveis participam em comutadores, é suficiente verificar que é uma identidade fraca. Usando a identidade (10) de [36], obtemos que o polinômio do lado esquerdo é igual a

$$4\sum_{\sigma\in S_3}(-1)^\sigma(x_1 \circ y_{\sigma(1)})(x_2 \circ y_{\sigma(2)})(x_3 \circ y_{\sigma(1)}),$$

como identidade fraca. Analogamente, o lado direito é igual a

$$4\sum_{\sigma\in S_3}(-1)^\sigma(x_{\sigma(1)} \circ y_1)(x_{\sigma(2)} \circ y_2)(x_{\sigma(1)} \circ y_3).$$

Isto conclui o lema, pois ambos os lados são iguais a um determinante de ordem 3. ■

Seja T_3 o T-ideal gerado pelo ideal T_2 e a identidade do lema anterior. É imediato que temos $T_3 \subset T(M_2(K))$.

Lema 2.10. *Denotemos por*

$$\begin{aligned}\varphi(x_1,x_2,x_3,y_1,y_2,y_3) &= \varphi(1,2,3,4,5,6)\\ &= \sum_{\sigma\in S_3}[x_1,x_2]\circ[y_{\sigma(1)},y_{\sigma(2)}]L(x_3,y_{\sigma(3)})\end{aligned}$$

o polinômio que aparece no lema anterior. Então na álgebra $A_3 = K\langle X\rangle/T_3$ temos as seguintes identidades

$$\sum_{\sigma\in S_4^1}(-1)^\sigma\varphi(\sigma(1),\sigma(2),\sigma(3),\sigma(4),5,6)=0,$$
$$\sum_{\sigma\in S_4^1}(-1)^\sigma\varphi(1,\sigma(2),\sigma(3),\sigma(4),\sigma(5),6)=0,$$
$$\sum_{\sigma\in S_4^1}(-1)^\sigma\varphi(1,2,\sigma(3),\sigma(4),\sigma(5),\sigma(6))=0,$$

onde σ assume valores em S_4^i conforme o índice.

Demonstração. O polinômio $\varphi(1,2,3,4,5,6)$ é anti-simétrico em x_1, x_2, x_3. A primeira identidade é obtida deste polinômio fazendo a anti-simetrização de x_1, x_2, x_3, y_1. Agora usamos o seguinte resultado: Se $f\in B(X)$ é multilinear e é anti-simétrico em 4 ou mais variáveis, então $f\in T_2\subset T_3$. Esse resultado é fácil de provar em $sl_2(K)$, pois $\dim sl_2(K)=3$.

A segunda e terceira identidade seguem por usar uma idéia semelhante. ■

Lema 2.11. *A identidade*

$$\begin{aligned}&4\sum_{\sigma\in S_3}(-1)^\sigma[x_1,x_2]\circ[y_1,y_2]L(z_1,t_{\sigma(1)})L(z_2,t_{\sigma(2)})L(z_3,t_{\sigma(3)})\\ &=\sum_{k<l}(\sum_{\sigma\in S_3}(-1)^\sigma[x_1,x_2]\circ[t_{\sigma(k)},t_{\sigma(l)}])L(t_{\sigma(j)},z_j)L(z_l,y_2)\end{aligned}$$

é válida em $M_2(K)$ onde $\{j,k,l\}=\{1,2,3\}$.

Demonstração. A demonstração é a mesma como a da identidade (14) de [62]. ■

Seja $g=g_1\circ g_2$ um polinômio próprio onde g_1 e g_2 são comutadores de grau ≥ 2. Denotaremos por $gL(p_1\cdots p_n|\,q_1\cdots q_n)$ o polinômio

$$\sum_{\sigma\in S_n} g_1\circ g_2 L(x_{p_1},x_{q_{\sigma(2)}})\cdots L(x_{p_n},x_{q_{\sigma(n)}}).$$

Se T é uma tabela dupla com linhas $T^{(1)},\ldots,T^{(k)}$ denotemos por $L(T)$ a transformação $L(T)=L(T^{(1)})\ldots L(T^{(k)})$. Esta transformação deverá agir somente sobre g_2.

Proposição 2.12. *Seja V o espaço vetorial gerado em A_3 por todos os produtos $g = g_1 \circ g_2$, onde g_1 e g_2 são comutadores nas variáveis X. Então $L(a,b)$ são transformações bem definidas em V.*

Demonstração. Quando o grau de g é igual a 4 ou 5, segue do fato que os F_T, $T \in Adm$ são linearmente independentes.

Quando o grau de $g_1 = 2$ e o grau de $g_2 = 4$ usamos os lemas 2.9 e 2.10.

Quando o grau de $g_2 = 5$, use a identidade (4) de [62] em g_2 e o resultado segue de maneira semelhante ao caso anterior. ∎

Lema 2.13. *Seja T uma tabela dupla e suponha que $F_T \neq 0$ em A_3. Então $m_1 = 2$ ou 3.*

Demonstração. Se alguma das (meias)linhas tem comprimento maior que 3, então F_T é anti-simétrico em pelo menos 4 variáveis, além disso, F_T é um polinômio próprio então necessariamente F_T se anula em A_3. ∎

Já haviámos provado que em A_3 cada polinômio próprio é uma combinação linear de polinômios do tipo F_T. Agora necessitamos demonstrar que cada F_T é combinação linear de $F_{Q's}$ onde os Q's são tabelas duplas standard.

As duas seguintes identidades são válidas em M_2:

Sejam g_1 e g_2 comutadores de grau ≥ 2, e seja

$$T = \left(\begin{array}{cccccc|cccccc} p_1 & \dots & p_s & r_1 & \dots & r_k & r_{k+1} & \dots & r_{n+1} & q_1 & \dots & q_{k-1} \end{array} \right)$$

uma tabela de uma linha tal que $n = s + k \leq 3$. Então vale a seguinte identidade:

$$\sum_{\sigma \in S_{n+1}^k} (-1)^\sigma g_1 \circ g_2 L(p_1 \dots p_s \; r_{\sigma(1)} \dots r_{\sigma(k)} | r_{\sigma(k+1)} \dots r_{\sigma(n+1)} \; q_1 \dots q_{k-1}) = 0. \tag{2.4}$$

Agora se T é uma tabela dupla como no lema 1.21, então vale a seguinte identidade

$$\sum (-1)^\sigma g_1 \circ g_2 L \left(\begin{array}{ccccccc|cccccc} s_1 & \dots & s_k & s_{k+1} & \dots & s_n & & r_{\sigma(1)} & \dots & r_{\sigma(k)} & q_{k+1} & \dots & q_m \\ q_1 & \dots & q_{k-1} & r_{\sigma(k+1)} & \dots & r_{\sigma(n+1)} & & t_1 & \dots & t_{k-1} & t_k & \dots & t_m \end{array} \right) = \sum \alpha_l g_1 \circ g_2 L(T_l) \tag{2.5}$$

A demonstração dessa identidade segue dos lemas 1.20 e 1.21.

Denotemos por T_4 o T-ideal gerado por T_3 e pelas identidades (2.4) e (2.5) e o lema 2.11. Como essas identidades valem para $M_2(K)$ segue que $T_4 \subset T(M_2(K))$.

Proposição 2.14. *Seja T uma 0-tabela com $m_1 = 2$ ou 3, e suponha que T não é standard. Então em A_4, o polinômio F_T é igual a uma combinação linear de $F_{Q's}$, onde os $Q's$ são 0-tabelas duplas. As tabelas duplas $Q's$ têm o mesmo conteúdo de T, as suas primeiras linhas têm comprimento 2 ou 3 e $Q's > T$.*

Demonstração. Suponhamos que T não é standard, ou seja, pelo menos uma das desigualdades entre os elementos da tabela T não é cumprido. Suponhamos ainda que a primeira linha de T tenha comprimento 3. Se alguma das desigualdades da primeira linha deixa de ser cumprida aplique os lemas 2.9 e/ou 2.10. Caso a quebra de alguma desigualdade ocorre abaixo da primeira linha aplique a identidade (2.4) e/ou a identidade (2.5). Então o único caso que resta ser verificado é quando a quebra de alguma desigualdade ocorre entre a primeira e a segunda linha, nesse caso aplique o lema 2.10. Assim o caso de linhas com comprimento 3 está concluído.

Suponhamos agora que a primeira linha tem comprimento 2. Se aparecer uma linha de comprimento 3, aplicamos o lema 2.11 e reduzimos este caso ao caso anterior. Então podemos supor que todas as linhas são de comprimento ≤ 2. Então aplicamos o lema 2.2 e as regras da operação $L(a, b)$. ■

Proposição 2.15. *Seja T uma 3-tabela que não é standard. Então em A_4, o polinômio F_T é igual a uma combinação linear de $F_{Q's}$, onde os $Q's$ são 3-tabelas duplas. As tabelas duplas $Q's$ têm o mesmo conteúdo de T e $Q's > T$.*

Demonstração. Segue de maneira semelhante a anterior. ■

Teorema 2.16. *Seja $g \in A_4$ um polinômio próprio e não-nulo. Então g pode ser representado em A_4 como combinação linear: $g = \sum \alpha_w F_{T_w}$, onde $T_w \in \mathrm{Adm}$ são tabelas duplas standard, $\alpha_w \in K$, e no mínimo um $\alpha_w \neq 0$.*

Demonstração. Segue imediatamente das duas últimas proposições. ■

Assim demonstramos que $T_4 = T(M_2(K))$, e portanto, o T-ideal de $M_2(K)$ possui uma base finita (embora longe de ser mínima).

2.4 Minimização da base

Vamos provar nessa seção que algumas das identidades que definem o T-ideal T_4 são consequências de outras identidades do próprio T_4. Com isso obtemos uma base mínima das identidades de $M_2(K)$. Vamos começar dando uma lista das identidades que participam em T_4.

$$s_4 = 1/2([x_1,x_2]\circ[x_3,x_4] - [x_1,x_3]\circ[x_2,x_4] + [x_1,x_4]\circ[x_2,x_3]); \tag{2.6}$$

$$h_5 = [[x_1,x_2]\circ[x_3,x_4],x_5]; \tag{2.7}$$

$$h_5 = [x_1,x_2,x_3]\circ[x_4,x_5] + [x_1,x_2]\circ[x_4,x_5,x_3]; \tag{2.8}$$

$$v_5 = [y,z,[t,x],x] + [y,x,[z,x],t]; \tag{2.9}$$

$$\begin{aligned} v_5' = {} & [x_1,x_2,[x_3,x_4]]\circ[x_5,x_6] + [x_1,x_2,[x_3,x_5]]\circ[x_4,x_6] \\ & +[x_1,x_4,[x_2,x_5]]\circ[x_3,x_6] + [x_1,x_5,[x_2,x_4]]\circ[x_3,x_6]; \end{aligned} \tag{2.10}$$

$$\begin{aligned} r_6 = {} & [x_1,x_2]\circ([x_3,x_4]\circ[x_5,x_6]) + (1/8)(-[x_1,[x_3,x_4],[x_5,x_6],x_2] - [x_1,[x_5,x_6],[x_3,x_4],x_2] \\ & +[x_2,[x_3,x_4],x_1,[x_5,x_6]] + [x_2,[x_5,x_6],x_1,[x_3,x_4]]); \end{aligned} \tag{2.11}$$

$$[x_1,x_2]\circ[y_1,y_2]L(a,b) - [x_1,x_2]\circ L(a,b)[y_1,y_2]; \tag{2.12}$$

$$[x_1,x_2,x_3]\circ[y_1,y_2]L(a,b) - [x_1,x_2,x_3]\circ L(a,b)[y_1,y_2]; \tag{2.13}$$

$$\begin{aligned} & 4\sum_{\sigma\in S_3}(-1)^\sigma[x_1,x_2]\circ[y_1,y_2]L(z_1,t_{\sigma(1)})L(z_2,t_{\sigma(2)})L(z_3,t_{\sigma(3)}) \\ & = \sum_{k<l}(\sum_{\sigma\in S_3}(-1)^\sigma[x_1,x_2]\circ[t_{\sigma(k)},t_{\sigma(l)}])L(t_{\sigma(j)},z_j)L(z_l,y_2) \text{ onde } \{j,k,l\}=\{1,2,3\} \end{aligned} \tag{2.14}$$

$$\sum_{\sigma\in S_3}[x_1,x_2]\circ[y_{\sigma(1)},y_{\sigma(2)}]L(x_3,y_{\sigma(3)}) - \sum_{\sigma\in S_3}[x_1,x_2]L(x_3,y_{\sigma(3)})\circ[y_{\sigma(1)},y_{\sigma(2)}] \tag{2.15}$$

$$\sum_{\sigma\in S_{n+1}^k}(-1)^\sigma g_1\circ g_2 L\left(\begin{array}{ccccccc|ccccccc} p_1 & \ldots & p_s & r_{\sigma(1)} & \ldots & r_{\sigma(k)} & & r_{\sigma(k+1)} & \ldots & r_{\sigma(n+1)} & q_1 & \ldots & q_{k-1} \end{array}\right); \tag{2.16}$$

$$\sum_{\sigma\in S_{n+1}^k}(-1)^\sigma g_1\circ g_2 L(\sigma(T)) = \sum \alpha_i g_1\circ g_2 L(T_l). \tag{2.17}$$

Acima g_1 e g_2 são comutadores com grau ≥ 2, e $\sigma(T)$ e T_l estão definidos como no lema 1.21.

Já sabemos que as identidades (2.12)–(2.17) são consequências das identidades (2.6)–(2.11), além disso, as identidades (2.7) e (2.8) são duas apresentações diferentes do polinômio de Hall.

Lema 2.17. *A identidade*

$$\begin{aligned} v_5 &= [y,z,[t,x],x] + [y,x,[z,x],t] \\ &= s_4(z,y,x,tx) + xs_4(z,y,x,t) - s_4(xz,y,x,t) - s_4(x,xy,x,t) \end{aligned}$$

vale para cada x, y, z e t na álgebra livre $K\langle X\rangle$.

Demonstração. A demonstração é feita através da expansão de ambos os lados da igualdade e observando-se que ambos os lados se cancelam. ■

Já haviámos observado que as identidades da álgebra de Lie $sl_2(K)$ seguiam de v_5, portanto, por esse lema temos o seguinte resultado. Cada polinômio de Lie que é uma identidade em $M_2(K)$, é consequência de s_4.

Logo a identidade v_5 é redundante em nossa base. Portanto, as identidades s_4, h_5, v_5' e r_6 formam uma base para as identidades de $M_2(K)$.

Lema 2.18. *Denote por $u = [x_3, x_4]$. Então os polinômios r_6 e*

$$r_6' = [x_1, x_2] \circ u^2 - (1/4)([x_1, u, u, x_2] - [x_2, u, x_1, u])$$

são equivalentes módulo as identidades s_4 e h_5. Em outras palavras os T-ideais gerados por $\{s_4, h_5, r_6\}$ e por $\{s_4, h_5, r_6'\}$ coincidem.

Demonstração. A linearização do polinômio $[x_3, x_4]^2$ é igual à componente multilinear do polinômio $[x_3 + x_5, x_4 + x_6]^2$. Isto é, ela é igual a

$$2[x_3, x_4] \circ [x_5, x_6] + 2[x_3, x_6] \circ [x_5, x_4].$$

e isso é equivalente a $[x_3, x_4]^2$ uma vez que a característica $p \neq 2$.

Permutando as variáveis temos

$$2[x_3, x_5] \circ [x_4, x_6] + 2[x_3, x_6] \circ [x_5, x_4], 2[x_3, x_6] \circ [x_4, x_5] + 2[x_3, x_5] \circ [x_4, x_6].$$

Agora somando todas as 3 linearizações acima obtemos

$$2([x_3, x_4] \circ [x_5, x_6] + [x_3, x_5] \circ [x_4, x_6] - [x_3, x_6] \circ [x_4, x_5]).$$

Por outro lado escrevemos o polinômio standard $s_4(x_3, x_4, x_5, x_6)$ como

$$2([x_3, x_4] \circ [x_5, x_6] - [x_3, x_5] \circ [x_4, x_6] + [x_3, x_6] \circ [x_4, x_5]).$$

Levando em conta que o último polinômio é uma identidade em $M_2(K)$, obtemos que o primeiro termo da soma de r_6 é equivalente a $[x_1, x_2] \circ [x_3, x_4]^2$.

Então aplicamos as 3 linearizações acima para os polinômios r_6'. O polinômio obtido será uma identidade para $M_2(K)$. Todas as outras parcelas da soma de r_6 e de r_6' são comutadores. Então usando a equivalência acima para os primeiros 3 termos obtemos um polinômio de Lie que é uma identidade em $M_2(K)$. Então pelo lema anterior ele segue de s_4. Portanto os polinômios são equivalentes módulo a identidade s_4.

O polinômio r_6' implica r_6 facilmente. ■

Lema 2.19. *Na álgebra associativa livre $K\langle X\rangle$, o polinômio $24r_6'$ é igual à seguinte expressão*

$$\begin{gathered}
[x_1, s_4([x_3,x_4],x_2,x_3,x_4]] + [s_4([x_3,x_4],x_1,x_3,x_4),x_2] \\
+x_3 s_4([x_3,x_4],x_1,x_2,x_4) + x_4 s_4([x_4,x_3],x_1,x_2,x_3) \\
-2s_4(x_2\circ[x_3,x_4],x_1,x_3,x_4) + 2s_4(x_1\circ[x_3,x_4],x_2,x_3,x_4) \\
+s_4([x_3,x_4]x_4,x_1,x_2,x_3) + s_4([x_4,x_3]x_3,x_1,x_2,x_4) \\
-s_4(x_3x_1,[x_3,x_4],x_2,x_4) + s_4(x_3x_2,[x_3,x_4],x_1,x_4) \\
+s_4(x_4x_1,[x_3,x_4],x_2,x_3) - s_4(x_4x_2,[x_3,x_4],x_1,x_3) \\
+2s_4(x_1,x_2,x_3,x_4)[x_3,x_4] \\
+4h_5(x_3x_1,x_4,x_3,x_4,x_2) - 4h_5(x_3x_2,x_4,x_3,x_4,x_1) \\
-4h_5(x_4x_1,x_3,x_3,x_4,x_2) + 4h_5(x_4x_2,x_3,x_3,x_4,x_1) \\
+4h_5([x_3,x_4],x_1,x_3,x_4,x_2) + 4h_5([x_4,x_3],x_2,x_3,x_4,x_1) \\
-8x_1h_5(x_3,x_4,x_3,x_4,x_2) + 8x_2h_5(x_3,x_4,x_3,x_4,x_1) \\
-4x_3h_5(x_1,x_2,x_3,x_4,x_4) + 4x_4h_5(x_1,x_2,x_3,x_4,x_3).
\end{gathered}$$

Demonstração. A igualdade acima foi obtida com o programa Mathematica®. Em primeiro lugar escrevemos todas as possíveis consequências dos polinômios s_4 e h_5, e então montamos um sistema linear e o resolvemos. ∎

Vamos mostrar que o polinômio v_5' segue de s_4 e de h_5. Mas isto vai ser mais complicado, pois com v_5' não temos uma simetrização tão óbvia como em r_6.

Consideremos os seguintes polinômios

$$\begin{aligned}
t_1 \quad = \quad & +4x_3h_5(x_1,x_2,x_5,x_6,x_4) + 4x_4h_5(x_1,x_2,x_5,x_6,x_3) \\
& +8x_4h_5(x_1,x_2,x_3,x_5,x_6) + 2x_5h_5(x_1,x_2,x_3,x_4,x_6) \\
& +6x_6h_5(x_1,x_2,x_3,x_5,x_4) + 4x_6h_5(x_1,x_2,x_3,x_4,x_5) \\
+\sum_{\sigma\in S_2} (-1)^\sigma \quad & (-x_3h_5(x_{\sigma(1)},x_4,x_{\sigma(2)},x_5,x_6) - 2x_4h_5(x_{\sigma(1)},x_5,x_3,x_6,x_{\sigma(2)}) \\
& -2x_5h_5(x_{\sigma(1)},x_4,x_3,x_6,x_{\sigma(2)}) + h_5(x_{\sigma(1)},x_3,x_4,x_5,x_{\sigma(2)})x_6),
\end{aligned}$$

$$\begin{aligned}
t_2 \quad = \quad & +3h_5(x_1,x_4,x_2,x_5,[x_3,x_6]) - 3h_5(x_1,x_5,x_2,x_4,[x_3,x_6]) \\
& +5h_5(x_1,x_5,x_2,x_4,x_6x_3) - 5h_5(x_1,x_4,x_2,x_5,x_6x_3) \\
& -6h_5(x_1,x_2,x_5,x_6,x_3x_4) - 6h_5(x_1,x_2,x_4,x_6,x_3x_5) \\
& -h_5(x_1,x_2,x_5,x_6,x_4x_3) - 5h_5(x_1,x_2,x_3,x_5,x_4x_6) \\
& +3h_5(x_1,x_2,x_4,x_6,x_5x_3) + h_5(x_1,x_2,x_3,x_4,x_5x_6) \\
+\sum_{\sigma\in S_2} (-1)^\sigma \quad & 4(h_5(x_{\sigma(2)},x_4,x_3,x_6,x_5x_{\sigma(1)}) + h_5(x_{\sigma(2)},x_5,x_3,x_6,x_4x_{\sigma(1)})),
\end{aligned}$$

$$\begin{aligned}
t_3 \quad = \quad & -7h_5(x_4x_3,x_5,x_1,x_2,x_6) - 5h_5(x_5x_3,x_4,x_1,x_2,x_6) \\
& -6h_5(x_6x_3,x_4,x_1,x_2,x_5) + 4h_5([x_1,x_2],x_3,x_5,x_6,x_4) \\
& +6h_5([x_1,x_2],x_4,x_3,x_5,x_6) + 4h_5([x_1,x_2],x_5,x_3,x_4,x_6) \\
+\sum_{\sigma\in S_2} (-1)^\sigma \quad & (-2h_5(x_3x_4,x_{\sigma(1)},x_{\sigma(2)},x_5,x_6)+4h_5(x_4x_{\sigma(1)},x_{\sigma(2)},x_5,x_6,x_3) \\
& +4h_5(x_4x_{\sigma(1)},x_{\sigma(2)},x_3,x_5,x_6) + 4h_5(x_5x_{\sigma(1)},x_{\sigma(2)},x_3,x_4,x_6) \\
& +4h_5(x_5x_{\sigma(1)},x_{\sigma(2)},x_4,x_6,x_3) - 3h_5(x_6x_3,x_{\sigma(1)},x_4,x_5,x_{\sigma(2)}) \\
& +h_5(x_6x_4,x_{\sigma(1)},x_{\sigma(2)},x_5,x_3) + h_5(x_6x_5,x_{\sigma(1)},x_{\sigma(2)},x_4,x_3)),
\end{aligned}$$

$$\begin{aligned}
t_4 \quad = \quad & -[x_3,x_4]s_4(x_1,x_2,x_5,x_6) + 2[s_4(x_3,x_4,x_5,x_6),[x_1,x_2]] \\
& +x_4x_3s_4(x_1,x_2,x_5,x_6) + 3[x_6x_3,s_4(x_1,x_2,x_4,x_5)] \\
& -2[[x_3,x_6],s_4(x_1,x_2,x_4,x_5)] - [x_6,x_4]s_4(x_1,x_2,x_3,x_5) \\
& +2(s_4(x_1,x_2,x_3,x_5))\circ(x_4x_6) - [x_6,x_5]s_4(x_1,x_2,x_3,x_4) \\
& -[s_4(x_1,x_2,x_3,x_4),x_5]x_6 + 2x_5(s_4(x_1,x_2,x_3,x_4)\circ x_6) \\
& -[x_3,x_5]s_4(x_1,x_2,x_4,x_6) + 2x_5(s_4(x_1,x_2,x_4,x_6)\circ x_3) \\
& +x_4s_4(x_1,x_2,x_5,x_6)x_3 \\
-2\sum_{\sigma\in S_2} (-1)^\sigma \quad & (x_5x_{\sigma(1)}s_4(x_{\sigma(2)},x_3,x_4,x_6) + x_4x_{\sigma(1)}s_4(x_{\sigma(2)},x_3,x_5,x_6)),
\end{aligned}$$

$$\begin{aligned}
t_5 \quad = \quad & +2x_3s_4(x_6x_4,x_1,x_2,x_5)+2x_3s_4(x_6x_5,x_1,x_2,x_4)\\
& -2x_4s_4(x_3x_5,x_1,x_2,x_6)+2x_4s_4(x_6x_5,x_1,x_2,x_3)\\
& -2x_5s_4(x_3x_4,x_1,x_2,x_6)+2x_5s_4(x_6x_4,x_1,x_2,x_3)\\
& +2x_6s_4([x_1,x_2],x_3,x_4,x_5)-x_4s_4([x_1,x_2],x_3,x_5,x_6)\\
& -3s_4([x_1,x_2],x_3,x_4,x_5)x_6-3x_6s_4(x_3x_4,x_1,x_2,x_5)\\
& -x_6s_4(x_3x_5,x_1,x_2,x_4)+s_4(x_4x_3,x_1,x_2,x_5)x_6\\
& -s_4(x_5x_3,x_1,x_2,x_4)x_6\\
+\sum_{\sigma\in S_2}(-1)^\sigma \quad & (+2x_{\sigma(1)}s_4(x_4x_{\sigma(2)},x_3,x_5,x_6)+2x_{\sigma(1)}s_4(x_5x_{\sigma(2)},x_3,x_4,x_6)\\
& +2x_4s_4(x_{\sigma(1)}x_5,x_{\sigma(2)},x_3,x_6)+2x_5s_4(x_{\sigma(1)}x_4,x_{\sigma(2)},x_3,x_6)),
\end{aligned}$$

$$\begin{aligned}
t_6 \quad = \quad & +2s_4([[x_1,x_2],x_3],x_4,x_5,x_6)-4s_4(x_5[x_1,x_2],x_3,x_4,x_6)\\
& +2s_4([x_1,x_2]x_5,x_3,x_4,x_6)-2s_4([x_1,x_2]x_4,x_3,x_5,x_6)\\
& +3s_4(x_4x_1,[x_3,x_6],x_2,x_5)+3s_4([x_1,x_4],x_6x_3,x_2,x_5)\\
& +s_4([x_1,x_2],x_3x_4,x_5,x_6)-s_4([x_1,x_2],x_5x_3,x_4,x_6)\\
& -2s_4([x_1,x_2],x_6x_5,x_3,x_4)+3s_4([x_1,x_2],x_4x_3,x_5,x_6)\\
& +5s_4([x_1,x_2],x_3x_5,x_4,x_6)-2s_4([x_1,x_2],x_4x_6,x_3,x_5)\\
& -3s_4(x_4x_2,[x_3,x_6],x_1,x_5)+3s_4(x_6x_3,[x_2,x_4],x_1,x_5)\\
& +2s_4(x_3x_4,x_6x_5,x_1,x_2)-2s_4(x_6x_4,x_3x_5,x_1,x_2)\\
& +2s_4([x_1,x_2],[x_5,x_6],x_3,x_4)-x_5s_4([x_1,x_2],x_3,x_4,x_6)\\
+\sum_{\sigma\in S_2}(-1)^\sigma \quad & (+3s_4(x_6x_3,x_{\sigma(1)}x_5,x_{\sigma(2)},x_4)-3s_4(x_3x_6,x_5x_{\sigma(1)},x_{\sigma(2)},x_4)\\
& -s_4(x_4x_{\sigma(1)},x_{\sigma(2)}x_5,x_3,x_6)-s_4(x_5x_{\sigma(1)},x_{\sigma(2)}x_4,x_3,x_6)\\
& -s_4(x_5[x_{\sigma(1)},x_4],x_{\sigma(2)},x_3,x_6)-5s_4(x_{\sigma(1)}x_4x_{\sigma(2)},x_3,x_5,x_6)\\
& -5s_4(x_{\sigma(1)}x_5x_{\sigma(2)},x_3,x_4,x_6)-s_4(x_4[x_{\sigma(1)},x_5],x_{\sigma(2)},x_3,x_6)).
\end{aligned}$$

Lema 2.20. *Na álgebra associativa livre $K\langle X\rangle$ temos a seguinte igualdade*

$$2v_5' = 2t_1+2t_2+2t_3+t_4+t_5+t_6.$$

Demonstração. Segue como no lema anterior.

Lema 2.21. *Seja char $K=3$, então a identidade r_6 não pertence ao T-ideal de $K\langle X\rangle$ gerado por s_4 e h_5.*

Demonstração. Consiste em mostrar que a álgebra de Grassmann E de dimensão infinita sobre um corpo K de caracterítica 3 satisfaz as identidades s_4 e h_5, mas não satisfaz a identidade r_6, ver [24]. ■

Observação 2.22. *Observe o coeficiente $24 = 3 \times 2^3$ na espressão acima de r'_6. Quando $\operatorname{char} K = 3$ este coeficiente é igual a 0, e isto não contradiz o lema acima.*

Combinando estes dois últimos lemas obtemos uma base mínima para as identidades da álgebra das matrizes $M_2(K)$, sobre um corpo infinito K, com $\operatorname{char} K = p \neq 2$. Notemos que para $p > 5$ isto já havia sido feito em [37].

Teorema 2.23. *Seja K um corpo infinito de característica $p \neq 2$. Uma base mínima para as identidades de $M_2(K)$ é dada pelos seguintes polinômios:*

a) s_4 e h_5 quando $p = 0$ ou $p > 3$;

b) s_4, h_5 e r_6 quando $p = 3$.

Este teorema nos dá uma resposta afirmativa à Questão 1. proposta em [37, pág. 433].

Capítulo 3

Polinômios Centrais

Em 1956 Kaplansky em [31] (veja também a versão revisada [32] de 1970), elaborou uma lista de problemas que motivou a uma grande quantidade de pesquisadores nas décadas seguintes. Um dos problemas propostos foi o seguinte:

Problema (Kaplansky): Existe polinômio central multihomogêneo para a álgebra $M_n(K)$, com $n \geq 2$?

A resposta a esse problema foi dado em 1972–1973, independente e simultaneamente, por Formanek em [20] e por Razmyslov em [51], respectivamente. Este resultado foi muito frutífero para a teoria de identidades polinômiais, pois muitos resultados importantes foram estabelecidos, ou pelo menos, muitas de suas demonstrações foram simplificadas. Para exemplos veja: Jacobson [30] e Rowen [55].

A descrição do espaço vetorial em $K\langle X\rangle$ dos polinômios centrais é conhecida somente no caso de $n = 2$. Como este espaço é fechado com respeito a endomorfismos de $K\langle X\rangle$, ele é chamado de T-espaço. Formanek em [21] descreveu o S_n-módulo dos polinômios centrais multilineares de $M_2(K)$. Ele também calculou a série de Hilbert, e o S_n-cocaracter. Okhitin, em [46], mostrou que o T-espaço dos polinômios centrais é finitamente gerado, como T-espaço, e encontrou um conjunto mínimo de geradores quando K é um corpo de característica 0.

Nosso objetivo neste capítulo é obter uma generalização do resultado obtido por Okhitin, no seguinte sentido: descrever uma base mínima para o T-espaço dos polinômios centrais de $M_2(K)$, quando o corpo K é infinito e de característica positiva, mas diferente de dois.

3.1 Introdução

É bem conhecido que, em uma álgebra associativa com unidade R, o conjunto $Z(R) = \{r \in R|\ ra = ar, \text{ para todo } a \in R\}$ é um sub-álgebra de R e a chamamos de centro de R. Diremos que $f(x_1, \ldots, x_n) \in K\langle X\rangle$ é um **polinômio central** de R se, e somente se, para todo $r_1, \ldots, r_n \in R$ tivermos $f(r_1, \ldots, r_n) \in Z(R)$ e f não é um polinômio constante. Denotaremos por $C(R) \subseteq K\langle X\rangle$ ao conjunto de todos os polinômios centrais de R.

As identidades polinomiais de R são claramente polinômios centrais, chamamos a esses polinômios de **polinômios centrais triviais**.

Exemplo 3.1. *Seja $R = M_2(K)$, onde K é um corpo. Então $f(x_1, x_2) = [x_1, x_2]^2$ é um polinômio central não trivial de R.*

O polinômio standard s_{2n} e um polinômio central trivial para $M_n(K)$ pois ele é uma identidade em $M_n(K)$.

Um espaço vetorial de $K\langle X\rangle$ é chamado de T-espaço, se ele for invariante pelos endomorfismos da álgebra $K\langle X\rangle$. Suponhamos que $\Omega \subset K\langle X\rangle$ é um conjunto arbitrário de polinômios. Denotamos por $V(\Omega)$ ao menor T-espaço obtido de Ω através do seguinte processo:

1. $\Omega \subseteq V(\Omega)$;
2. Se fizermos combinações lineares dos elementos de $V(\Omega)$ eles devem continuar em $V(\Omega)$;
3. Substituindo as variáveis dos elementos $V(\Omega)$ por polinômios arbitrários de $K\langle X\rangle$ o resultado contínua em $V(\Omega)$.

Claramante $V(\Omega) = \bigcap S$, onde os conjuntos S são todos os T-espaços tais que $\Omega \subseteq S$, ou seja, $V(\Omega)$ é o menor T-espaço que contém Ω.

3.2 Corpos infinitos de característica positiva

Proposição 3.2. *Seja R uma álgebra associativa, com unidade, sobre um corpo infinito K, e seja $f \in K\langle X\rangle$ um polinômio central de R. Então todas as componentes (multi)-homogêneas de f são também polinômios centrais.*

Demonstração. Suponhamos que $f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{m} f_i \in K\langle x\rangle$, onde f_i são as componentes homogêneas de f com grau i em x_1. Sejam a_1, a_2, $\ldots$, a_n elementos, dois-a-dois distintos, de K.

Multiplicando x_1 por a_j obtemos o seguinte:

$$f(a_j x_1, x_2, \ldots, x_n) = \sum_{i=1}^{m} a_j^i \, f_i(x_1, x_2, \ldots, x_n), \; j = 0, 1, \ldots, n.$$

Quando substituímos x_1, x_2, $\ldots$, x_n por elementos de R obtemos elementos de $Z(R)$. Considerando estas equações como um sistema linear nas variáveis f_i, $i = 0$, 1, $\ldots$, n, resolveremos o sistema. O determinante é

$$\delta = \begin{vmatrix} 1 & a_0 & \ldots & a_0^n \\ 1 & a_1 & \ldots & a_1^n \\ \vdots & \vdots & & \vdots \\ 1 & a_n & \ldots & a_n^n \end{vmatrix} = \prod_{i \neq j} (a_i - a_j) \neq 0.$$

A segunda igualdade vale pois o determinante é de Vandermonde, e $\delta \neq 0$ por construção, e portanto, podemos resolver o sistema. Obtemos assim que os f_i são também elementos de $Z(R)$. ■

A proposição nos diz que o T-espaço $T(M_2(K))$ é gerado pelas suas componentes multi-homogêneas. Portanto, vamos trabalhar somente com polinômios multi-homogêneos.

Vamos lembrar que usando o lema 2.17 pelo principal resultado de [62], temos que cada polinômio de Lie que é uma identidade em $M_2(K)$ é uma consequência de s_4.

Observemos que o polinômio

$$h(x_1, x_2, x_3, x_4) = [x_1, x_2] \circ [x_3, x_4] \tag{3.1}$$

é um polinômio central, mas não é uma identidade em $M_2(K)$. Recordamos que o polinômio standard s_4 é um polinômio central (trivial) em $M_2(K)$.

Vamos fazer uma observação sobre o polinômio de Hall, até esse momento viemos chamando de h_5. Vamos denotar por H, o polinômio obtido de h_5 pela seguinte permutação $\sigma = (354)$, ou seja, $\sigma h_5 = H = [h, x_5]$. Como são essencialmente os mesmos polinômios continuaremos chamando-o de polinômio de Hall.

Seja x_0 uma variável de $K\langle X\rangle$, denotemos por V ao T-espaço de $K\langle X\rangle$ gerado pelos polinômios h e $x_0 s_4(x_1, x_2, x_3, x_4)$.

Lema 3.3. *a) Se W é o T-espaço gerado por h então $W \subsetneqq V$, quando $\operatorname{char} K = p > 3$.*

b) $V \subseteq C(M_2(K))$.

Demonstração. Para demonstrar a afirmação (a), é suficiente observar que a álgebra de Grassmann E, $\dim E = \infty$, satisfaz a identidade $[h, x_5]$. Ressaltamos que a álgebra de Grassmann E não satisfaz nenhuma identidade standard em característica 0, e satisfaz s_{p+1} quando a característica do corpo for p. Logo a identidade $[x_0 s_4(x_1, x_2, x_3, x_4), x_5]$ não é satisfeita. A afirmação (b) é óbvia uma vez que ambos h e $x_0 s_4$ são polinômios centrais em $M_2(K)$. ∎

Lema 3.4 (cf. [46]). *Existe um polinômio de Lie $l \in L(X)$, tal que o polinômio $c = x_0 h + l$ é central em $M_2(K)$. Além disso, $c \in V$.*

Demonstração. Comecemos com a seguinte identidade na algebra livre $K\langle X\rangle$,

$$x_0[x_1, x_2] \circ [x_3, x_4]) + x_1([x_0, x_2] \circ [x_3, x_4]) = c_1 + l_1, \tag{3.2}$$

onde

$$\begin{aligned} c_1 &= [x_0 x_1, x_2] \circ [x_3, x_4] - [x_0, x_2, x_1] \circ [x_3, x_4] \\ &\quad -(1/2)([x_3, x_4, x_0] \circ [x_1, x_2] + [x_3, x_4, x_1] \circ [x_0, x_2]), \\ l_1 &= (1/4)([x_1, x_2, [x_3, x_4, x_0]] + [x_0, x_2, [x_3, x_4, x_1]]). \end{aligned}$$

Logo c_1 é um polinômio central em $M_2(K)$, pois é uma consequência de h, e $l_1 \in L(X)$. Aplicando a seguinte permutação (130)(24) na identidade (3.2) e invertendo o sinal obtemos

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

onde obviamente $c_2 \in V$ e $l_2 \in L(X)$. Aplicando agora a permutação (103) na identidade (3.2) obtemos

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

onde temos $c_3 \in V$ e $l_3 \in L(X)$. Somando essas 3 identidades obtemos

$$x_0[x_1, x_2] \circ [x_3, x_4]) - x_0([x_2, x_3] \circ [x_1, x_4]) = c_4 + l_4,$$

onde $c_4 = c_1 + c_2 + c_3 \in V$ e $l_4 = l_1 + l_2 + l_3 \in L(X)$. E por fim, aplicamos a permutação (34) e depois somamos com $2x_0 s_4(x_1, x_2, x_3, x_4)$, onde

$$s_4 = 1/2([x_1, x_2] \circ [x_3, x_4] - [x_1, x_3] \circ [x_2, x_4] + [x_1, x_4] \circ [x_2, x_3]).$$

Agora invertemos o sinal do resultado e depois aplicamos a permutação (23) para obtermos o resultado desejado. ■

Lema 3.5. *Non caso que* $\operatorname{char} K = p > 3$. *Então* $T(M_2(K)) \subseteq V$.

Demonstração. É suficiente mostrar que s_4, h_5, $x_0 s_4$, $x_0 h_5 \in V$. Obviamente $s_4 \in V$, e pelo lema anterior, $x_0 s_4 \in V$. Podemos escrever h_5 como

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

Como $h_5 \in V$, pelo Lema 3.4 temos que $x_0 h_5 + l \in V$ para algum $l \in L(X)$. Mas então l é um polinômio central de $M_2(K)$. Como ele é um polinômio de Lie, ele produzirá sempre matrizes com traço 0. Logo ele é uma identidade de $M_2(K)$ e essa segue de s_4. Portanto, $x_0 h_5 \in V$ e isto conclui o lema. ■

Agora dividimos em dois casos.

3.2.1 Caso 1: char $K > 3$

Seja f multi-homogêneo. Podemos escrevê-lo da seguinte forma:

$$f(x_1, x_2, \ldots, x_n) = \sum_i \alpha_i x_1^{a_{i_1}} x_2^{a_{i_2}} \cdots x_n^{a_{i_n}} g_i, \quad \alpha_i \in K.$$

Aqui os $g_i \in B(X)$ são polinômios próprios e $a_i = (a_{i_1}, a_{i_2}, \ldots, a_{i_n})$ é uma n-upla de inteiros não-negativos. Seja $b_i = a_{i_1} + a_{i_2} + \cdots + a_{i_n}$, usando a unicidade da representação de f acima, definimos o posto $r(f)$ de f como sendo o maior de todos os b_i tais que o correspondente α_i é não nulo. Obviamente $f \in B(X)$ se, e somente se, $r(f) = 0$.

Lema 3.6. *Seja* $f \in C(M_2(K))$ *e seja* $r(f) = 0$. *Então* $f = c + g$ *onde* $c = \sum_i v_i \circ w_i$ *para* v_i, $w_i \in L(X)$ *de grau* ≥ 2 *e* $g \in T(M_2(K)) \cap L(X)$.

Demonstração. Começamos observando que f é um polinômio próprio, e como tal, pode ser representado como uma soma de monômios que são produtos de comutadores. Sem perda de generalidade, podemos admitir que $f = u_1 u_2 \cdots u_n$ é um produto de comutadores. Então como $u_1 u_2 = (1/2)[u_1, u_2] + u_1 \circ u_2$ temos que f é soma de dois polinômios. O primeiro é um produto de $n-1$ comutadores; o segundo é $(u_1 \circ u_2) u_3 \cdots u_n$. Aplicando a identidade r_6 que vale em $M_2(K)$ escrevemos $(u_1 \circ u_2) u_3$ como uma combinação linear de comutadores. E daí obtemos um produto de $n-2$ comutadores. O resultado segue por indução sobre n.

Para provarmos que $g \in T(M_2(K))$, notemos que $f \in C(M_2(K))$ e $v \circ w \in C(M_2(K))$ para quaisquer comutadores v, w de graus ≥ 2. Temos que o polinômio de Lie g é central em $M_2(K)$. Qualquer avaliação de g em $M_2(K)$ sempre produz matrizes de traço zero. Segue disso que g é uma identidade em $M_2(K)$. ∎

Sejam $m_1 = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} n_1$ e $m_2 = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n} n_2$ dois polinômios tendo o mesmo multi-grau, onde n_1 e n_2 são produtos de comutadores com comprimento ≥ 2. Diremos que $a = (a_1, a_2, \ldots, a_n) > b = (b_1, b_2, \ldots, b_n)$ se $a_i > b_i$ para algum i enquanto $a_t = b_t$ para $1 \leq t \leq i-1$. Observamos que a ordem $>$ é a ordem lexicográfica usual.

Observação 3.7. *O posto $r(f)$ de $f = f(x_1, x_2, \ldots, x_n)$ é igual ao maior número de variáveis que aparecem nos monômios que podemos substituir por 1 sem que isto anule o polinômio. Para vermos isto escrevemos $f_1 = f(x_1+1, x_2+1, \ldots, x_n+1)$ como soma de componentes multi-homogêneas*

$$f_1 = \sum \alpha_{i,j} x_1^{ai_1} x_2^{a_{i_2}} \cdots x_n^{a_{in}} u_{j_1} u_{j_2} \cdots u_{j_m}.$$

Então cada substituição de 1 em um comutador o anula. Portanto, $r(f)$ é determinado pelo menor grau da componente não nula f_m de f_1. Isto é, $r(f)$ é igual ao $\deg f - \deg f_m$.

Teorema 3.8. *Se $\operatorname{char} K > 3$ então $C(M_2(K)) = V$. Em outras palavras, o T-espaço dos polinômios centrais de $M_2(K)$ é gerado por h e $x_0 s_4$. Além disso, os polinômios h e o $x_0 s_4$ são independentes como polinômios centrais.*

Demonstração. Seja $f \in C(M_2(K))$ um polinômio multi-homogêneo, demonstraremos por indução sobre $r(f)$ que $f \in V$. Quando $r(f) = 0$, isso segue do lema anterior.

Suponhamos que f é multi-homogêneo e $r(f) > 0$. Então

$$f(x_1, x_2, \ldots, x_n) = \alpha x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n} g + \sum \alpha_a x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} g_a,$$

onde g e os g_a estão em $B(X)$ e a n-upla $(r_1, r_2, \ldots, r_n)$ é a maior que aparece em f com respeito a ordem definida acima.

Vamos mostrar em primeiro lugar que $g \in C(M_2(K))$. Para isto, consideremos o polinômio central $f(x_1+1, x_2, \ldots, x_n)$. Já sabemos que as suas componentes homogêneas são centrais. Tome a componente homogênea de menor grau em x_1, isto é,

$$f'(x_1, x_2, \ldots, x_n) = \alpha x_2^{r_2} \cdots x_n^{r_n} g + \sum_a \beta_a x_2^{a_2} \cdots x_n^{a_n} g_a.$$

A somatória é sobre todo a, tal que $a_1 = r_1$. Observamos que se substituírmos 1 por x_1 em algum outro comutador, este último se anula. Repetimos o mesmo procedimento para $f'(x_1, x_2 + 1, x_3, \ldots, x_n)$ e fazemos o mesmo até chegarmos em x_n. Finalmente temos que $g \in C(M_2(K))$.

No entanto, o polinômio g é próprio. Portanto, de acordo com o lema anterior, $g = \sum_i u_i \circ v_i + l$ para alguns comutadores u_i e v_i, todos de grau ≥ 2, e l é um polinômio de Lie que é uma identidade em $M_2(K)$ pois $l \in T(M_2(K)) \subseteq V$. Obviamente $\sum u_i \circ v_i \in V$.

Agora temos que $\alpha x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n} l \in T(M_2(K))$. Além disso, $x(u \circ v)$ pode ser representado como no lema 3.4 para $x = x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n}$. Se considerarmos x como uma nova variável então $r(x(u \circ v)) < r(f)$ e de acordo ao lema 3.4, $x(u \circ v) = c + l$ para $c \in V$, onde l é uma identidade de Lie em $M_2(K)$. Portanto $r(l) < r(f)$. Notamos que se voltarmos, em l, então a nova variável x assume o valor inicial, isto é, $x = x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n}$ e colocando todas as variáveis iguais a 1 obtemos 0. E daí $r(l) < r(f)$. Com isso conseguimos reduzir o posto de f e a demonstração segue por indução. ■

A última afirmação do teorema foi estabelecida anteriormente. Mostramos que na álgebra de Grassmann E, os comutadores são centrais. Portanto h é um polinômio central. No entanto, $x_0 s_4$ não é quando $\operatorname{char} K \neq 3$ e $\dim E = \infty$.

3.2.2 Caso 2: $\operatorname{char} K = 3$

No caso em que o corpo tem $\operatorname{char} K = 3$ aplicaremos argumentos similares, e por isto omitimos algumas demonstrações.

Lema 3.9. *Seja U o T-espaço gerado pelos polinômios h, $x_0 s_4$, $x_0 r_6$. Então $T(M_2(K)) \subseteq U$.*

Demonstração. Precisamos provar somente que $r_6 \in U$. Como $r_6 = [x_1, x_2] \circ ([x_3, x_4] \circ [x_5, x_6]) + q$ onde q é um polinômio de Lie, de acordo com o lema 3.4 podemos escrever $r_6 = c + l + q$ com $c \in V$ e $l \in T(M_2(K))$. Entretanto r_6 é uma identidade em $M_2(K)$. Logo $l + q \in L(X)$ é um polinômio central em $M_2(K)$ e portanto uma identidade de $M_2(K)$. Como $l + q$ é consequência de s_4, seque que $r_6 \in U$. ■

Agora procedemos da mesma forma que no caso de $\operatorname{char} K = p > 3$. Estabelecemos o seguinte teorema.

Teorema 3.10. *Se $\operatorname{char} K = 3$ o T-espaço $C(M_2(K))$ é gerado por h, $x_0 s_4$ e $x_0 r_6$. Isto é, $C(M_2(K)) = U$. Estes três polinômios são independentes como polinômios centrais.*

Demonstração. A única afirmação que falta ser demonstrada é a que trata da independência. Para as outras características utilizamos a álgebra de Grassmann E, contruída sobre um espaço vetorial de dimensão infinita. Pois, já havíamos observado que h e x_0s_4 são polinômios centrais de E, mas x_0r_6 não o é. Para provarmos que os polinômios centrais h e x_0s_4 são independentes fazemos uso do seguinte lema.

Lema 3.11. *O T-espaço na álgebra associativa livre $K(X)$ gerado por h não contém o T-espaço gerado pelo polinômio x_0s_4.*

Demonstração. Suponhamos por absurdo que $x_0s_4(x_1, x_2, x_3, x_4)$ pertence ao T-espaço gerado pelo polinômio $h = [x_1, x_2] \circ [x_3, x_4]$. O sub-espaço de grau 5 do T-espaço gerado pelo polinômio h é gerado por todos os polinômios do tipo $[y_1, y_2] \circ [y_3, y_4]$, onde três das letras y_i assumem diferentes x_j, $0 \leq j \leq 4$, e a variável y_i que ainda não assumiu nenhum x_i é o produto do x_j ainda não usado com um dos três x_j usados. Então podemos escrever x_0s_4 como combinação linear desses polinômios, e colocamos os coeficientes como se segue.

Primeiro colocamos, a menos de sinal, somente três possibilidades de grau 4 no T-espaço em $K(x_1, x_2, x_3, x_4)$ gerado por h, isto é,

$$[x_1, x_2] \circ [x_3, x_4], \quad [x_1, x_3] \circ [x_2, x_4], \quad [x_1, x_4] \circ [x_2, x_3].$$

Agora substituindo na seguinte ordem: x_1 por x_1x_0, e por x_0x_1 nesses polinômios, e colocando os coeficientes a_1, b_1, c_1, d_1 e e_1, respectivamente, obtemos os polinômios. Então substituindo x_2 por x_2x_0 e por x_0x_2 e para estes polinômios colocamos os coeficientes a_2, b_2, c_2, d_2 e e_2, respectivamente. Por exemplo,

$$\begin{aligned}
&a_1[x_1x_0, x_2] \circ [x_3, x_4], \quad b_1[x_0x_1, x_2] \circ [x_3, x_4], \quad c_1[x_1x_0, x_3] \circ [x_2, x_4],\\
&d_1[x_0x_1, x_3] \circ [x_2, x_4], \quad e_1[x_1x_0, x_4] \circ [x_2, x_3], \quad f_1[x_0x_1, x_4] \circ [x_2, x_3];\\
&a_2[x_1, x_2x_0] \circ [x_3, x_4], \quad b_2[x_1, x_0x_2] \circ [x_3, x_4], \quad c_2[x_1, x_3] \circ [x_2x_0, x_4],\\
&d_2[x_1, x_3] \circ [x_0x_2, x_4], \quad e_2[x_1, x_4] \circ [x_2x_0, x_3], \quad f_2[x_1, x_4] \circ [x_0x_2, x_3].
\end{aligned}$$

Continuamos, da mesma forma, escrevendo as outras consequências do polinômio central h:

$$\begin{aligned}
&a_3[x_1, x_2] \circ [x_3x_0, x_4], \quad b_3[x_1, x_2] \circ [x_0x_3, x_4], \quad c_3[x_1, x_3x_0] \circ [x_2, x_4],\\
&d_3[x_1, x_0x_3] \circ [x_2, x_4], \quad e_3[x_1, x_4] \circ [x_2, x_3x_0], \quad f_3[x_1, x_4] \circ [x_2, x_0x_3];\\
&a_4[x_1, x_2] \circ [x_3, x_4x_0], \quad b_4[x_1, x_2] \circ [x_3, x_0x_4], \quad c_4[x_1, x_3] \circ [x_2, x_4x_0],\\
&d_4[x_1, x_3] \circ [x_2, x_0x_4], \quad e_4[x_1, x_4x_0] \circ [x_2, x_3], \quad f_4[x_1, x_0x_4] \circ [x_2, x_3].
\end{aligned}$$

Agora consideramos os polinômios

$$[x_0, x_2] \circ [x_3, x_4], \quad [x_0, x_3] \circ [x_2, x_4], \quad [x_0, x_4] \circ [x_2, x_3]$$

e substituindo x_i por $x_i x_1$ e por $x_1 x_i$, $i = 2, 3, 4$, e colocamos os coeficientes como se segue:

$$\begin{aligned}
&a_5[x_0, x_2x_1] \circ [x_3, x_4], \quad b_5[x_0, x_1x_2] \circ [x_3, x_4], \quad c_5[x_0, x_3] \circ [x_2x_1, x_4],\\
&d_5[x_0, x_3] \circ [x_1x_2, x_4], \quad e_5[x_0, x_4] \circ [x_2x_1, x_3], \quad f_5[x_0, x_4] \circ [x_1x_2, x_3];\\
&a_6[x_0, x_2] \circ [x_3x_1, x_4], \quad b_6[x_0, x_2] \circ [x_1x_3, x_4], \quad c_6[x_0, x_3x_1] \circ [x_2, x_4],\\
&d_6[x_0, x_1x_3] \circ [x_2, x_4], \quad e_6[x_0, x_4] \circ [x_2, x_3x_1], \quad f_6[x_0, x_4] \circ [x_2, x_1x_3];\\
&a_7[x_0, x_2] \circ [x_3, x_4x_1], \quad b_7[x_0, x_2] \circ [x_3, x_1x_4], \quad c_7[x_0, x_3] \circ [x_2, x_4x_1],\\
&d_7[x_0, x_3] \circ [x_2, x_1x_4], \quad e_7[x_0, x_4x_1] \circ [x_2, x_3], \quad f_7[x_0, x_1x_4] \circ [x_2, x_3].
\end{aligned}$$

Então temos os polinômios

$$[x_1, x_0] \circ [x_3, x_4], \quad [x_1, x_3] \circ [x_0, x_4], \quad [x_1, x_4] \circ [x_0, x_3]$$

os quais, depois da substituição de x_i por $x_i x_2$ e por $x_2 x_i$, $i = 3, 4$, nos dá

$$\begin{aligned}
&a_8[x_1, x_0] \circ [x_3x_2, x_4], \quad b_8[x_1, x_0] \circ [x_2x_3, x_4], \quad c_8[x_1, x_3x_2] \circ [x_0, x_4],\\
&d_8[x_1, x_2x_3] \circ [x_0, x_4], \quad e_8[x_1, x_4] \circ [x_0, x_3x_2], \quad f_8[x_1, x_4] \circ [x_0, x_2x_3];\\
&a_9[x_1, x_0] \circ [x_3, x_4x_2], \quad b_9[x_1, x_0] \circ [x_3, x_2x_4], \quad c_9[x_1, x_3] \circ [x_0, x_4x_2],\\
&d_9[x_1, x_3] \circ [x_0, x_2x_4], \quad e_9[x_1, x_4x_2] \circ [x_0, x_3], \quad f_9[x_1, x_2x_4] \circ [x_0, x_3].
\end{aligned}$$

Finalmente para

$$[x_1, x_2] \circ [x_0, x_4], \quad [x_1, x_0] \circ [x_2, x_4], \quad [x_1, x_4] \circ [x_2, x_0]$$

substituímos x_4 por $x_4 x_3$ e por $x_3 x_4$, e obtemos

$$\begin{aligned}
&a_{10}[x_1, x_2] \circ [x_0, x_4x_3], \quad b_{10}[x_1, x_2] \circ [x_0, x_3x_4], \quad c_{10}[x_1, x_0] \circ [x_2, x_4x_3],\\
&d_{10}[x_1, x_0] \circ [x_2, x_3x_4], \quad e_{10}[x_1, x_4x_3] \circ [x_2, x_0], \quad f_{10}[x_1, x_3x_4] \circ [x_2, x_0].
\end{aligned}$$

A soma desses 60 polinômios é igual a $(1/2)x_0 s_4(x_1, x_2, x_3, x_4)$, (o coeficiente $(1/2)$ é colocado por conveniência). Expandimos todos os termos dessa soma e escrevemos os coeficientes dos monômios correspondentes na álgebra livre. Podemos resolver (por exemplo usando o método de redução de linhas de Gauss) e obtemos um sistema linear que envolve 120 equações em 60 variáveis. A resolução de tal sistema pode ser complicada. Usaremos o seguinte fato: cada equação contém somente quatro variávies. E isso vai ser o suficiente para mostrar que o sistema é incompatível.

Primeiro observamos que $a_1 + b_2 = 0$. Isto pode ser feito da seguinte forma. O monômio $x_3x_1x_4x_0x_2$ na sua expansão tem coeficiente $d_2 + c_4 + a_6 + b_7$ e deve ser igual a 0 uma vez que esse monômios não aparece em x_0s_4. Agora escrevemos o coeficiente zero de $x_2x_0x_3x_1x_4$ que é $e_2 + f_3 - a_6 - b_7$, e eliminamos b_7 e a_6. Assim obtemos que $d_2 + e_2 + f_3 + c_4 = 0$.

Além disso, os monômios $x_1x_4x_3x_2x_0$, $x_4x_3x_1x_0x_2$, $x_4x_1x_0x_3x_2$ têm os respectivos coeficientes abaixo

$$-e_2 + b_7 - e_8 + e_{10}, \quad -a_1 - b_2 - a_6 + e_{10}, \quad e_1 + f_3 + e_7 - e_8,$$

e todos eles são iguais a 0. Subtraindo o segundo do terceiro e o terceiro do primeiro, obtemos

$$a_1 + b_2 - e_1 - e_2 - f_3 + a_6 + b_7 - e_7 = 0.$$

Subtraímos desta equação $d_2 + c_4 + a_6 + b_7 = 0$ e obtemos

$$a_1 + b_2 - e_1 - d_2 - e_2 - f_3 - c_4 - e_7 = 0.$$

Por outro lado, dos monômios $x_2x_3x_4x_1x_0$ e $x_1x_0x_2x_3x_4$ obtemos $-e_1 - e_7 + b_8 + d_{10} = 0$ e $a_1 + b_2 + b_8 + d_{10} = 0$, respectivamente; subtraindo a primeira da segunda expressão obtemos $a_1+b_2+e_1+e_7 = 0$. Agora somando as expressões acima com $a_1+b_2-e_1-d_2-e_2-f_3-c_4-e_7 = 0$, chegamos em $2(a_1 + b_2) - (d_2 + e_2 + f_3 + c_4) = 0$. Já haviámos estabelecido que o segundo termo dessa soma é igual a 0 e então $a_1 + b_2 = 0$.

Agora vamos calcular a_1+b_2 de outra forma. Olhando os seguintes monômios $x_0x_2x_3x_4x_1$, $x_3x_4x_1x_0x_2$ e $x_4x_1x_0x_2x_3$, segue

$$-f_2 + a_7 - f_8 + f_{10} = -1, \quad a_1 + b_2 + a_7 + f_{10} = 0, \quad -e_1 - f_2 - e_7 - f_8 = 0,$$

e subtraindo as últimas duas equações da primeira obtemos $-(a_1 + b_2) + e_1 + e_7 = -1$. Já haviámos estabelecido que $(a_1 + b_2) + e_1 + e_7 = 0$ então $-2(a_1 + b_2) = -1$. Como $\operatorname{char} K = p \neq 2$ isto contradiz $a_1 + b_2 = 0$ e nosso lema, e junto com ele, o teorema, está demonstrado. ■

Gostaríamos de conseguir um exemplo de alguma álgebra “natural” e relativamente mais simples que satisfizesse a identidade polinômial $[[x_1, x_2] \circ [x_3, x_4], x_5]$ mas não satisfazesse $[x_5, x_6]s_4(x_1, x_2, x_3, x_4)$. É fácil de ver que desta forma podemos substituir as contas acima por esse exemplo. Para vermos isto observe que a primeira identidade expressa o fato de que h é um polinômio central. O polinômio x_0s_4 seria central se $[x_0s_4, x_5] = 0$ e desde que s_4 é central podemos reescrever $[x_0, x_5]s_4 = 0$. Se $\operatorname{char} K = p \neq 3$ então a álgebra de Grassmann E é um tal exemplo, mas quando $p = 3$ isto falha, pois s_4 é uma identidade em E.

3.3 Mais sobre polinômios centrais

Começamos observando que os polinômios exibidos por Razmyslov tinham grau igual a $3n^2 - 2$ e os polinômios exibidos por Formanek tinham grau n^2, ou seja, em termos computacionais eram preferíveis os polinômios exibidos por Formanek. Entretanto, Halpin em [27], usando uma outra identidade fraca que a usada por Razmyslov em [52], exibiu outros polinômios centrais para $M_n(K)$, $n \geq 2$, que possuiam grau n^2.

Além disso, o método de Razmyslov para exibir polinômios centrais em $M_n(K)$ usa o conceito de identidade fraca [51, 52] e a transformação conhecida como transformada de Razmyslov [52]. E estes conceitos permitiram a obtenção de novos polinômios centrais. Para uma outra constução veja também Giambruno e Valenti [25].

No caso de $n = 3$, Drensky e Kasparian em [16] exibiram um polinômio central de grau 8. Para isso, usaram idéias desenvolvidas por Rosset para a demonstração do teorema de Amitsur e Levitzki [54]. Além disso, provaram em [15] que em $M_3(K)$ não existe polinômio central de grau 7.

Para $n = 4$, Drensky e Piacentini Cattaneo em [18] encontraram um novo polinômio central de grau 13. A construção usa uma identidade fraca de grau 9 e combina os métodos de Razmyslov e Formanek. O resultado foi generalizado por Drensky em [12] que construiu polinômios centrais de grau $(n-1)^2 + 4$, para todo $M_n(K)$, $n > 2$. Os polinômios centrais de [18, 12] usaram essencialmente a seguinte identidade fraca

$$\begin{aligned} \omega(x, y_1, \ldots, y_n) &= s_{2n-2}(x, x^2, \ldots, x^{n-3}, x^n, y_1, \ldots, y_n) \\ &+ \textstyle\sum_{i=1}^{n} x s_{2n-2}(x, x^2, \ldots, x^{n-3}, x^{n-2}, y_1, \ldots, y_i x, \ldots, y_n) \\ &+ \textstyle\sum_{1 \leq i \leq j \leq n} s_{2n-2}(x, x^2, \ldots, x^{n-3}, x^{n-2}, y_1, \ldots, y_i x, \ldots, y_j x, \ldots, y_n) \end{aligned}$$

em $M_n(K)$ a qual se anula quando substiuímos x por elementos de $sl_n(K)$ e y_1, y_2, $\ldots$, y_n por quaisquer matrizes de $M_n(K)$.

A existência de identidades fracas de grau 3 em $M_2(K)$ nos fornece um polinômio central de grau 4 . Igualmente, a construção de polinômios centrais de grau 8 e 13 para as álgebras $M_3(K)$ e $M_4(K)$ respectivamente, usam identidades fracas de graus 6 e 9 respectivamente, o que significa do ponto de vista computacional um grande avanço. Sugerimos a leitura do artigo [5] o qual, entre outros tópicos, mostra aspectos computacionais dos polinômios centrais e das identidades fracas.

Outra questão que tem interessado os pesquisadores é a de saber qual é o grau mínimo dos polinômios centrais em $M_n(K)$. Formanek em [21] propôs os seguintes problemas:

Problema Encontre o grau mínimo dos polinômios centrais de $M_n(K)$, $\operatorname{char} K = 0$. Encontre o grau mínimo dos polinômios centrais em duas variáveis.

Além disso, Formanek conjecturou que o grau mínimo dos polinômios centrais em $M_n(K)$ sobre um corpo de característica 0 é dado pela seguinte função

$$mingrau(n) = 1/2(n^2 + 3n - 2)$$

Observe que $mingrau(1) = 1$, $mingrau(2) = 4$ e $mingrau(3) = 8$, e portanto, até o momento essa conjectura parece verdadeira.

Capítulo 4

$*$-PI na álgebra $M_2(K)$

Em [42] Levchenko exibiu uma base para as identidades polinomiais com involução, da álgebra das matrizes $(M_2(K), *)$, sobre corpos com característica 0. Neste capítulo vamos estender o resultado de Levchenko, no seguinte sentido. Vamos exibir uma base para as identidades polinomiais com involução da álgebra das matrizes 2×2 sobre corpos infinitos de caracterítica $p \neq 2$.

4.1 Introdução

Tomemos R uma álgebra associativa e com unidade sobre um corpo K. Uma involução em R é um anti-isomorfismo de segunda ordem, isto é, um automorfismo (como espaço vetorial) satisfazendo $(ab)^* = b^*a^*$ e $a^{**} = a$.

As K-álgebras com involução formam uma categoria, vamos chamar as álgebras desta categoria de $*$-álgebras sobre o corpo K.

Seja $Z(R) = \{a \in R : ar = ra \text{ para todo } r \in R\}$ o centro da álgebra R. É claro que $Z(R)$ é um sub-anel de R. Denotamos $Z(R,*) = \{a \in Z(R) : a^* = a\}$.

Diremos que $*$ é do primeiro tipo se $Z(R) = Z(R,*)$ caso contrário diremos que é do segundo tipo.

Na categoria das $*$-álgebras associativas sobre um corpo K podemos definir a álgebra livre com unidade da seguinte maneira. Sejam X e Y dois conjuntos contáveis de letras (variáveis) disjuntos, formamos a álgebra associativa livre $K\langle X, Y\rangle$. Definimos um anti-automorfismo

$$* : K\langle X, Y\rangle \longrightarrow K\langle X, Y\rangle$$

tal que $x_i^* = y_i$ e $y_i^* = x_i$. Então $*$ é determinado unicamente. Escreveremos X^* ao invés de Y. Denotaremos esta álgebra por $K\langle X, X^*\rangle$.

Analogamente ao caso de identidade polinomial (PI) em uma álgebra R, vamos definir uma identidade polinomial com involução ($*$-PI) em uma álgebra $(R, *)$ com involução.

Definição 4.1. *Seja $f = f(x_1, x_2, \ldots, x_n, x_1^*, x_2^*, \ldots, x_n^*) \in K\langle X, X^*\rangle$ um $*$-polinômio. Diremos que f é uma identidade polinomial com invoção ($*$-PI) da álgebra $(R, *)$ se, e somente se, $f(a_1, a_2, \ldots, a_n, a_1^*, a_2^*, \ldots, a_n^*) = 0$ para quaisquer a_1, a_2, $\ldots$, $a_n \in R$.*

Diremos que uma $*$-PI f é uma $*$-PI especial se substituírmos as entradas x_i^* por quaisquer elementos de R e obtemos uma PI no sentido ordinário, ou seja, se fizermos $x_i^* = y_i$, obtemos que $f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n)$ é uma identidade polinomial em R. Vamos considerar somente involução do primeiro tipo, pois é possível mostrar que no caso de involuções do segundo tipo, em álgebras primas, que satisfaçam identidade polinomial, todas as $*$-PI são especiais (veja [55, pág.132]).

Observação 4.2. *Dado qualquer polinômio podemos supor que todas as suas entradas ou são simétricas ou anti-simétricas, pois caso apareça uma variável z que não é simétrica nem anti-simétrica, podemos tomar a parte simétrica $x = z + z^*$ e a parte anti-simétrica $y = z - z^*$ de z. Temos ainda $z = 1/2(x + y)$. Então podemos substituir a variável z pela expressão $1/2(x + y)$ e podemos fazer isto para todas as variáveis que ainda não foram reduzidas, portanto podemos concluir a afirmação inicial.*

Vamos reservar as letras do conjunto X para serem variáveis simétricas e as letras do conjunto Y para serem variáveis anti-simétricas, e quando quisermos falar de uma variável que ainda não foi reduzida vamos utilizar o conjunto Z.

Observação 4.3. *Considerando o T-ideal da álgebra R com involução $*$ sobre um corpo infinito K e de característica $\neq 2$, e desde que as álgebra consideradas aqui possuem unidade, é possível demonstrar que podemos nos restringir aos polinômios multi-homogêneos. Ainda mais, com uma pequena adaptação do teorema de Poincaré—Birkhoff—Witt podemos demonstrar que podemos nos restringir à família de polinômios multihomogêneos que são escritos como combinações lineares de produtos de variáveis anti-simétricas seguidas por comutadores de grau ≥ 2. As variáveis simétricas participam apenas em comutadores. Vamos chamar a esses polinômios de* ***polinômios $*$-próprios****.*

4.2 Involuções nas álgebras simples e centrais

Seja R uma álgebra associativa, com unidade, simples e central. Como já mencionado no capítulo 1, $U(R)$ é o grupo multiplicativo dos elementos invertíveis da álgebra R.

Denotemos por $Inn(R) = \{f \in Aut(R) : \ f(x) = r^{-1}xr, \text{ para algum } r \in U(R)\}$. Existe um automorfismo de grupos $\xi : U(R) \to Inn(R)$ dado por $x \to r^{-1}xr$. Vamos denotar por $\xi(r)$ o automorfismo de R que é a imagem de r por ξ. Observe que $\ker(\xi) = Z(R) \cap U(R)$. Vamos denotar por $Inv(R)$ o conjunto de todas as involuções de R.

Observe que se $*$ é um anti-isomorfismo de R e $r \in U(R)$, então $(r^{-1}xr)^* = r^*x^*(r^{-1})^* = r^*x^*(r^*)^{-1}$, isto é, $\xi(r)* = *\xi((r^*)^{-1})$.

Definição 4.4. *Diremos que $*$ e $J \in Inv(R)$ são equivalentes se, e somente se, existe $r \in U(R)$ que é $*$-simétrico, tal que $* = J\xi(r)$.*

Observação 4.5. *Sejam $*$, $J \in Inv(R)$ e $* = J\xi(r_1)$. Suponhamos que $r_2 \in R$ e $r_i^J = \mu_i r_i$ para $\mu_i = \pm 1$, $i = 1, 2$. Então $(r_2r_1) = r_1^* r_1^{-1} r_2^J r_1 = (\mu_1\mu_2)(r_2r_1)$.*

Observação 4.6. *Sejam r, $x \in R$ tais que $rx \in Z(R)$ e $xr \neq 0$, $rx \neq 0$. Então $rx = xr$. Pois, $x(rx) = rx^2$, então $[x,r]x = 0$ e daí $[x,r] = 0$.*

Essas duas observações servem para verificar a boa definição acima.

Definição 4.7. *Seja $(R, *)$ um anel com involução, diremos que $r \in R$ é apropriado se r é simétrico ou anti-simétrico.*

Lema 4.8. *Suponha que R é uma álgebra prima. Se $* = J\xi(r)$ para $*$, $J \in Inv(R)$ e $r \in U(r)$, então $r^* = r^J = \pm r$.*

Demonstração. Temos $J = J^{**} = JJ\xi(r)* = \xi(r)* = *\xi((r^*)^{-1}) = J\xi(r)\xi((r^*)^{-1})$. Isto implica que $r(r^*)^{-1} \in ker(\xi) \subseteq Z(R)$, e daí $r^* = zr$ para algum $z \in Z(R)$. Como $r = r^* = (zr)^* = z^2r$, segue que $(z^2-1)r = 0$, então $0 = z^2 - 1 = (z-1)(z+1)$. Como $Z(R)$ é um corpo, concluimos que $z = \pm 1$. Isto é, r é $*$-apropriado, e $r^* = r^J$. ■

Vamos demonstrar um resultado devido a Albert, que nos possibilitará caracterizar as involuções do primeiro tipo em uma álgebra simples e central. Para isto vamos precisar do seguinte teorema:

Teorema de Skolem e Noether. [28] *Suponha que R é simples e uma PI-álgebra com centro $Z(R)$, e A_1, A_2 são isomorfas, simples $Z(R)$-sub-álgebras de R. Então cada isomorfismo $\psi\colon A_1 \to A_2$ (de $Z(R)$-álgebras) pode ser extendido a um automorfismo interno de R.*

Como conseqüência temos que todos os automorfismos de R são automorfismos internos, isto é, $Aut(R) = Inn(R)$.

Teorema 4.9. *(Albert) Se R é uma álgebra central e simples, com $*$, $J \in Inv(R)$, então $* = J\xi(r)$ para algum $r \in U(R)$ que é J-apropriado. Reciprocamente, se $J \in Inv(R)$ e $r \in U(R)$ é J-apropriado, então $J\xi(r) \in Inv(R)$.*

Demonstração. Observamos que $*J$ é um automorfismo da álgebra R. Pelo resultado enunciado acima, existe $r \in U(R)$ tal que $*J = \xi(r)$; aplicando J de ambos os lados temos $* = J\xi(r)$ e pelo lema anterior temos que r é J-apropriado. A recíproca é imediata. ∎

Teorema 4.10. *(i) A relação definida em 4.4 é uma relação de equivalência.*

(ii) Se R é simples e central, então $Inv(R)$ tem no máximo duas classes de equivalência.

(iii) Se $*$, $J \in Inv(R)$ e $* = J\xi(r)$ para algum $*$-anti-simétrico $r \in U(R)$, então $*$ e J não são equivalentes.

Demonstração. (i) Esta afirmação é imediata. Quanto a afirmação (ii) suponhamos que J_1, J_2 e $J_3 \in Inv(R)$. Afirmamos que duas delas estão na mesma classe de equivalência. Sejam $J_1 = J_2\xi(r_1)$ e $J_2 = J_3\xi(r_2)$ para r_i e J_i-anti-simétricas. Então $J_1 = J_3(r_2r_1)$ e r_2r_1 é J_1-simétrica. Logo J_1 e J_3 são equivalentes.

(iii) Suponhamos $* = J\xi(r_i)$ para alguns $r_i \in U(R)$, $i = 1, 2$, com $r_1^* = -r_1$ e $r_2^* = r_2$. Então $r_1r_2^{-1} \in \ker(\xi) \subseteq Z(R)$, e $(r_1r_2^{-1})^* = -r_1r_2^{-1}$, o que é impossível. ∎

Vamos especializar os resultados para a álgebra das matrizes $M_n(K)$, com $\operatorname{char} K \neq 2$. Obtemos o seguinte resultado.

Quando n é par, (t) (transposta) e (s) (simplética) são as representantes das duas classes de involuções não equivalentes. Quando n é ímpar existe somente uma classe de involução, a que correspondente à transposta.

4.3 $*$-PI em $M_2(K)$ com involução transposta

Seja $M_2(K)$ a $*$-álgebra das matrizes 2×2 com a involução $*$, sobre o corpo K. Daqui para frente K é um corpo infinito com $\operatorname{char} K \neq 2$. Vamos nos restringir a involuções do primeiro tipo. Como acabamos de mostrar neste caso temos duas classes de involuções. A primeira classe é representada pela involução transposta (t) dada por

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

e a segunda classe é representada pela involução simplética (s), dada por

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

Observação 4.11. *Daqui para frente para simplificar a notação vamos falar em comutadores de grau igual a 1, entenderemos com isto, que estes comutadores são na realidade variáveis.*

Vamos estudar, nesta secção, as identidades polinomiais com a involução **transposta** e $(t) = *$. Os seguintes polinômios são $*$-PI em $M_2(K)$.

$$[y_1y_2, x] \tag{4.1}$$

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

$$[x_1, x_2][x_3, x_4] - [x_1, x_3][x_2, x_4] + [x_2, x_3][x_1, x_4] \tag{4.3}$$

$$[y_1x_1y_2, x_2] - y_1y_2[x_2, x_1] \tag{4.4}$$

Recordamos que as letras x denotam variáveis simétricas, e as y representam variáveis anti-simétricas.

A verificação das identidades acima pode ser feita por substítuição direta das variáveis anti-simétricas, por matrizes do tipo $(e_{12} - e_{21})$, e as simétricas, por combinações lineares de matrizes da forma $(e_{11} - e_{22})$ e $(e_{12} + e_{21})$, onde e_{ij} são as matrizes com 1 na entrada (i, j) e zeros nas outras entradas. Como as variáveis simétricas participam somente em comutadores, não é necessário incluir nas combinações lineares a matriz identidade $I = e_{11} + e_{22}$.

Seja R_2 a álgebra obtida por tomarmos o quociente da álgebra livre pelo ideal gerado pelas quatro identidades com involução listadas acima.

Procuremos algumas conseqüências destas identidades e com estas obteremos uma melhor apresentação dos elementos de R_2.

Seja $a \circ b = 1/2(ab + ba)$ (Produto de Jordan), essa operação satisfaz as seguintes relações com a involução:

$$(x \circ y)^* = -(x \circ y). \tag{4.5}$$

Por (4.2) temos $[x \circ y_1, y_2] = 0$. O produto de Jordan e o comutador satizfazem a seguinte relação na álgebra livre:

$$[a \circ b, c] = a \circ [b, c] + b \circ [a, c]$$

e portanto por (4.2) temos

$$y_1 \circ [x, y_2] = 0 \tag{4.6}$$

Expandindo temos $y_1\, x\, y_2 = y_2\, x\, y_1$. Temos também que qualquer elemento $z \in M_2(K)$ é igual a $1/2(x + y)$ e por (4.2) temos que

$$y_1 z y_2 = y_2 z y_1. \tag{4.7}$$

Além disso, valem as seguintes identidades:

$$[y_1, y_2]^* = -[y_1, y_2] \tag{4.8}$$

$$[y_1, x]^* = [y_1, x] \tag{4.9}$$

$$[x_1, x_2]^* = -[x_1, x_2]. \tag{4.10}$$

Por (4.7) temos

$$[y_1, x_1, y_2] = [y_1, x_1]\; y_2 - y_2\; [y_1, x_1] = 2\, [y_1, x_1]\; y_2 \tag{4.11}$$

e por (4.11), (4.1) e por (4.4) temos

$$[y_1, x_1, y_2, x_2] = 2[[y_1, x_1]y_2, x_2] = 2y_1y_2[x_2, x_1] + 2[y_1x_1y_2, x_2] = 4y_1y_2[x_2, x_1]. \tag{4.12}$$

Se aplicarmos a identidade de Jacobi a esta última identidade obtemos

$$[y_1, x_1, y_2, x_2] = [[y_1, x_1], [y_2, x_2]] + [y_1, x_1, x_2, y_2]$$

e aplicando (4.11) e (4.10) no primeiro comutador temos que $[y_1, x_1, x_2]$ é anti-simétrico. Agora aplicando (4.2) e (4.12) obtemos

$$[[y_1, x_1], [y_2, x_2]] = 4y_1y_2[x_2, x_1]. \tag{4.13}$$

Por outro lado

$$[[y_1, x_1], [y_2, x_2]] = [y_1, x_1, y_2, x_2] = 2\,[[y_1, x_1], y_2, x_2] = 2\,[y_1, x_1]\;[y_2, x_2] + 2\,[y_1, x_1, x_2]\;y_2$$

e daí

$$[y_1, x_1]\;[y_2, x_2] = 2\,y_1\;y_2\;[x_1, x_2] - [y_1, x_1, x_2]\;y_2. \tag{4.14}$$

Lema 4.12. *(cf. [42]) Seja $f \in R_2$ e $*$-próprio. Então f se escreve como $f = f_1 + f_2 + f_3$, onde f_1, f_2 e f_3 são combinações lineares de polinômios da seguinte forma:*

$$u_1 u_2 \cdots u_{2k}; \qquad u_1 u_2 \cdots u_{2k+1}; \qquad u_1 u_2 \cdots u_{2k+1} w;$$

respectivamente. Ainda os u_i são comutadores anti-simétricos de graus ≥ 1, e w é um comutador simétrico de grau ≥ 2. Além disso, entre os comutadores de grau ≥ 2 aparece apenas uma vez uma variável anti-simétrica.

Demonstração. Conforme a observação 4.3 podemos nos restringir a polinômios $*$-próprios, isto é, pode-se escrever f como uma combinação linear de $u_1 u_2 \cdots u_l$, onde cada u_i é um comutador de grau ≥ 1, onde todas as variáveis simétricas aparecem em comutadores de grau ≥ 2. Vamos começar mostrando que podemos supor que em cada um dos comutadores existe somente uma variável anti-simétrica. É um exercício fácil mostrar, utilizando as identidades (4.2), (4.12) e a identidade de Jacobi, que nenhum comutador de grau ≤ 4 pode ter mais que uma variável anti-simétrica. Quando u é um comutador de grau > 4, podemos escrever como $u = [w, z_1, z_2]$ onde w é um comutador de grau ≥ 2 e analizando com as identidades mencionadas acima todas as possibilidades de w, z_1, z_2 (por exemplo: se w e z_2 são anti-simétricos e z_1 é simétrico, etc.), temos que o resultado segue por indução sobre o grau dos comutadores.

Consideramos um produto em que podem aparecer comutadores simétricos de comprimento ≥ 2 e também comutadores anti-simétricos de comprimento ≥ 1. Precisamos mostrar que este produto pode ser reordenado de tal forma que os comutadores anti-simétrico de comprimento menor apareçam na frente e no fim pode aparecer apenas um comutador simétrico.

Para se conseguir fazer essa reordenação, basta utilizar as identidades (4.2) e (4.14), e também a seguinte identidade:

$$[v, x_1, x_2, \ldots, x_{2k}]\;[y_1, x_1', x_2', \ldots x_s'] = y_1\;[v, x_1, x_2, \ldots, x_{2k}, x_1', x_2', \ldots, x_s']. \tag{4.15}$$

Aqui v é comutador anti-simétrico de grau ≥ 2, as variáveis x_i, $i = 1, \ldots, 2k$ e x'_j $j = 1, \ldots, s$, são simétricas e $k, s = 0, 1, 2, \ldots$ A verificação desta identidade segue facilmente por indução sobre s. Isto conclui o lema. ■

4.3.1 Matrizes genéricas com involuções

Recordamos a definição da álgebra das matrizes genéricas, que foi dada na seção 1.17, para o caso de $n = 2$. Sejam a_r definidos por

$$a_r = \begin{pmatrix} \theta_{11}^{(r)} & \theta_{12}^{(r)} \\ \theta_{21}^{(r)} & \theta_{22}^{(r)} \end{pmatrix}, \ r = 1, 2, \ldots$$

como já vimos denotamos por Gen_2 a sub-álgebra que eles geram em $M_2(K[\theta_{ij}^{(r)}])$. Então Gen_2 é a álgebra relativamente livre na variedade de álgebras definida por $M_2(K)$. Podemos definir a involuçãotransposta $*$ em Gen_2; a álgebra $(Gen_2, *)$ é relativamente livre na variedade de álgebras com involução determinada por $(M_2(K), *)$. Denotemos por s_r e por t_r os geradores livres simétricos e o anti-simétricos, respectivamente, da álgebra $(Gen_2, *)$. Desde que $s_r = (1/2)(a_r + a_r^*)$ e $t_r = (1/2)(a_r - a_r^*)$, temos que

$$s_r = \begin{pmatrix} \chi_{11}^{(r)} & \chi_{12}^{(r)} \\ \chi_{12}^{(r)} & \chi_{22}^{(r)} \end{pmatrix}, \chi_{ij}^{(r)} = \frac{1}{2}(\theta_{ij}^{(r)} + \theta_{ji}^{(r)}); t_r = \begin{pmatrix} 0 & \xi^{(r)} \\ -\xi^{(r)} & 0 \end{pmatrix}, \xi_{ij}^{(r)} = \frac{1}{2}(\theta_{12}^{(r)} - \theta_{21}^{(r)}).$$

Então as novas variávies comutativas $\chi_{ij}^{(r)}$, $\xi^{(r)}$ são algebricamente independentes sobre K.

Lema 4.13. *Seja $f = f_1 + f_2 + f_3$, onde f_1, f_2 e f_3 são como descritos no lema 4.12. Então f é uma identidade com involução de $M_2(K)$ se, e somente se, f_1, f_2 e f_3 são identidades.*

Demonstração. Suponhamos que $f = f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$ seja uma identidade e vamos provar que f_1, f_2 e f_3 são identidades. Tomemos s_i e t_j matrizes genéricas, e avaliando $f = f(s_1, s_2, \ldots, s_n, t_1, t_2, \ldots, t_m)$ temos

$$f = \overbrace{p_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}^{f_1} + \overbrace{p_2 \begin{pmatrix} 0 & -r_1 \\ r_1 & 0 \end{pmatrix}}^{f_2} + \overbrace{p_3 \begin{pmatrix} q_1 & r_2 \\ r_2 & -q_1 \end{pmatrix} + p_4 \begin{pmatrix} r_3 & -q_2 \\ -q_2 & -r_3 \end{pmatrix}}^{f_3} \tag{4.16}$$

onde $p_1, \ldots, p_4$, $r_1, \ldots, r_3$, q_1 e q_2 são polinômios nas variáveis $\{\chi_{ij}^k, \xi_{ij}^k\}$ com $i, j = \{1, 2\}$; $k = 1, 2, \ldots$ Observe que f_1 é uma matriz multipla da identidade e f_2 é uma matriz anti-simétrica. Portanto a única forma de $f = 0$ é quando $f_1 + f_2 = -f_3$. Observamos que o traço de $-f_3 = 0$ implica que $f_1 = 0$; de maneira semelhante se mostra que $f_2 = 0$ e como a recíproca é imediata, o lema está demonstrado.

Lema 4.14. *Sejam f_1, f_2 e f_3 como no Lema 4.12 identidades com involução em $M_2(K)$. Então cada f_i é equivalente a f_i', $i = 1, 2, 3$, onde f_i' têm grau menor ou igual ao de f_i respectivo, e dependem de no máximo uma variável anti-simétrica.*

Demonstração. Consideramos somente polinômios multihomogenêos. O resultado segue por observar que no lema 4.12 podemos escolher qual das variáveis anti-simétricas tiramos fora dos comutadores. Observe que com respeito à identidade (4.7) temos que $[y_1, x_1, y_2] = [y_2, x_1, y_1] = 2\,[y_1, x_1]\, y_2 = 2\,[y_2, x_1]\, y_1$. Podemos escolher qual das variáveis anti-simétricas tiramos para fora do comutador essa identidade e a identidade de Jacobi. Então se $f_i = f_i(x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s) = 0$, sem perda de generalidade podemos admitir que y_1 está no comutador e o restante das variáveis anti-simétricas fora.

Consideremos a álgebra das matrizes genéricas com involução $K[a_r, a_r^*]$ e o conjunto multiplicativo $S = \{m \in K[a_r, a_r^*] \mid \det(m) \neq 0\}$. Construimos a álgebra $S^{-1}K[a_r, a_r^*]$. Vamos tomar novamente as matrizes genéricas s_i e t_i como descrito anteriormente. Fazendo $f_i(s_1, s_2, \ldots, s_r, t_1, t_2, \ldots, t_s)$ obtemos $PQ = 0$, onde P é obtido por colocar os termos y_i em evidência e fazê-los assumir $y_i = t_i = \begin{pmatrix} 0 & \xi^i \\ -\xi^i & 0 \end{pmatrix}$, com $i = 2, 3, \ldots, r$. Portanto, $\det(P) = (\xi^2 \cdots \xi^r)^2 \neq 0$ e em $S^{-1}K[a_r, a_r^*]$ existe P^{-1} e segue $Q = 0$. Como estamos tratando com matrizes genéricas concluimos o lema. ∎

Observação 4.15. *Observemos que se v é um comutador de grau ≥ 1, então vale a seguinte igualdade, $[v, x_2, x_1] = [v, x_1, x_2] + [v, [x_2, x_1]]$. Se v é um comutador anti-simétrico, por (4.2) temos*

$$[v, x_2, x_1] = [v, x_1, x_2]. \tag{4.17}$$

Daí, utilizando (4.12) temos que

$$\begin{aligned} [v, x_1, x_3, x_2, x_4] &= [v, x_1, x_2, x_3, x_4] + [v, x_1, [x_3, x_2], x_4] \\ &= [v, x_1, x_2, x_3, x_4] + 4\, v\, [x_3, x_2]\, [x_4, x_1]. \end{aligned} \tag{4.18}$$

Então por (4.17) e (4.18) temos

$$\begin{aligned} [v, x_3, x_4, x_1, x_2] &= [v, x_3, x_1, x_4, x_2] + 4\, v\, [x_4, x_1]\, [x_2, x_3] \\ &= [v, x_1, x_3, x_2, x_4] + 4\, v\, [x_4, x_1]\, [x_2, x_3] \\ &= [v, x_1, x_3, x_4, x_2] + 4\, v\, [x_3, x_2]\, [x_4, x_1] + 4\, v\, [x_4, x_1]\, [x_2, x_3] \end{aligned}$$

e usando (4.12) obtemos

$$[v, x_3, x_4, x_1, x_2] = [v, x_1, x_2, x_3, x_4]. \tag{4.19}$$

Isto quer dizer que podemos comutar os pares de variáveis dentro do comutador. Portanto para qualquer comutador anti-simétrico podemos ordenar as entradas de tal forma que as colocamos em ordem crescente.

Observação 4.16. *Façamos um raciocíonio semelhante para o caso de comutador simétrico. Iniciemos com a identidade* $[y_1, x_1, x_2, \ldots, x_n, y_2] = [y_2, x_1, x_2, \ldots, x_n, y_1]$ *que se verifica utilizando a identidade (4.7). Além disso, vale a seguinte identidade* $[v, x_1, x_3, x_2] = [v, x_1, x_2, x_3] + [v, x_1, [x_3, x_2]]$*, onde* v *é um comutador anti-simétrico de grau* ≥ 1*. Utilizando (4.11) obtemos*

$$[v, x_1, x_3, x_2] = [v, x_1, x_2, x_3] + 2\,[[x_3, x_2], x_1]\,v = [v, x_1, x_2, x_3] + 2\,[x_1, x_2, x_3]\,v$$

Lema 4.17. *Sejam* f_2*,* f_3 *polinômios como no lema 4.14, que dependem de apenas uma variável anti-simétrica, escritos como combinações lineares de apenas um comutador com grau* ≥ 4*. Então podemos escrever:*

$$f_2(y_1, x_1, x_2, \ldots, x_n) = \alpha[y_1, x_1, x_2, \ldots, x_n] + 4y_1\, g_1(x_1, x_2, \ldots, x_n)$$

e

$$f_3(y_1, x_1, x_2, \ldots, x_n) = \beta[y_1, x_1, x_2, \ldots, x_n] + 4y_1\, g_3(x_1, x_2, \ldots, x_n),$$

onde α *e* β *são elementos de* K *e* g_1*,* g_3 *são polinômios do tipo* f_1 *e* f_3*, respectivamente, como no lema 4.12.*

Demonstração. Para o polinômio do tipo f_2, utilizando a observação 4.15 temos

$$f_2(y_1, x_1, x_2, \ldots, x_n) = \alpha[y_1, x_1, x_2, \ldots, x_n] + 4y_1 g_1(x_1, x_2, \ldots, x_n).$$

Para o polinômio do tipo f_3, utilizando as observações 4.15 e 4.16 obtemos

$$f_3(y_1, x_1, x_2, \ldots, x_n) = \beta[y_1, x_1, x_2, \ldots, x_n] + 4y_1\, g_3(x_1, x_2, \ldots, x_n).$$

■

Teorema 4.18. *Sejam* f_1*,* f_2 *e* f_3 *como no lema 4.14 que são* $*$*-identidades em* $M_2(K)$*. Então podemos rescrevê-los em* R_2 *da seguinte maneira:*

a. *O polinômio f_1 é representado como combinação linear de produtos de dois comutadores anti-simétricos, onde um deles tem grau 2.*

b. *O polinômio f_2 com grau ≥ 4 é representado como combinação linear de comutadores anti-simétricos.*

c. *O polinômio f_3 com grau ≥ 4 é representado como combinação linear de comutadores simétricos.*

Em todos os casos podemos admitir que os polinômios não dependem de variáveis anti-simétricas.

Demonstração Sabemos que os f_i, $i = 1, 2, 3$, definidos no lema 4.12 podem ser escritos como combinação linear de produtos de comutadores, e cada produto depende de no máximo uma variável anti-simétrica, e que esta pode ser colocada na primeira entrada do primeiro comutador.

Vamos utilizar as identidades (4.11), (4.12) e (4.15), mas de maneira diferente da que viemos utilizando. Pois até o momento as utilizavámos para retirar as variáveis anti-simétricas para fora de um comutador e agora vamos utilizá-las para aglutinar dois ou três comutadores em 1.

Comecemos com um polinômio do tipo f_1. Utilizando a identidade (4.12) e em seguida a identidade de Jacobi, podemos rescrevê-lo como produto de dois comutadores anti-simétricos. Temos dois casos, sendo o primeiro onde f_1 não dependa de variável anti-simétrica. Utilizando a identidade (4.15), podemos fazer que um dos comutadores tenha grau dois. No segundo caso f_1 depende de uma variável anti-simétrica, $f_1 = f(y_1, x_1, \ldots, x_n)$. Usando a identidade (4.15) podemos rescrevê-lo da seguinte forma

$$f_1(y_1, x_1, \ldots, x_n) = y_1 f_2(x_1, \ldots, x_n).$$

Portanto esta identidade é equivalente a uma identidade do tipo f_2, a qual não depende de variáveis anti-simétricas.

Consideremos agora uma identidade do tipo f_2. Utilizando a identidade (4.12) podemos escrevê-la como combinação linear de comutadores anti-simétricos. No caso que f_2 não depende de variável anti-simétrica, o lema está demonstrado. No caso que depende de uma variável anti-simétrica, pelo lema anterior podemos escrevê-lo da seguinte forma:

$$f_2(y_1, x_1, x_2, \ldots, x_n) = \alpha[y_1, x_1, x_2, \ldots, x_n] + 4y_1 f_1(x_1, x_2, \ldots, x_n)$$

para algum polinômio do tipo f_1. Fazemos a seguinte avaliação:

$$y_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ x_1 = x_2 = \cdots = x_n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Então $[y_1, x_1, x_2, \ldots, x_n]$ será igual, a menos de múltiplo da forma $\pm 2^{n/2} \neq 0$ em K, a $e_{12} - e_{21}$ pois n é par. Mas esta última matriz é invertível. Por outro lado, f_1 é um produto de comutadores e está sendo avaliado em um mesmo elemento, então temos que $f_1(x_1, x_2, \ldots, x_n) = 0$. Portanto $\alpha = 0$ em K, e utilizando a mesma idéia do lema 4.14 para $y_1 f_1$ podemos verificar que f_1 é uma $*$-identidade. Portanto $f_2(y_1, x_1, x_2, \ldots, x_n)$ é equivalente a uma identidade do tipo $f_1(x_1, x_2, \ldots, x_n)$ que não depende de variáveis anti-simétricas.

No caso de uma identidade do tipo f_3, aplicamos a identidade (4.11) no comutador simétrico e em um dos anti-simétricos. Sem perda de generalidade podemos admitir que f_3 pode ser escrita como combinação linear de comutadores simétricos. Utilizando o lema anterior podemos seguir a idéia como no caso de polinômios do tipo f_2. Isto concluí o teorema. ■

Todos os polinômios na definição abaixo dependem somente de variáveis simétricas.

Definição 4.19. *1. Seja $F_1 = \{f \in K\langle X, Y\rangle \mid f$ é combinação linear de produtos de dois comutadores anti-simétricos, sendo um deles de grau 2$\}$.*

2. Seja $F_2 = \{f \in K\langle X, Y\rangle \mid f$ é combinação linear de comutadores anti-simétricos de grau maior ou igual a 4$\}$.

3. Seja $F_3 = \{f \in K\langle X, Y\rangle \mid f$ é combinação linear de comutadores simétricos de grau maior ou igual que 4$\}$.

4.3.2 O operador L e as identidades com involução

Em [8, Teorema 5] demonstramos qe as identidades ordinárias de $M_2(K)$ quando K é um corpo infinito, $\operatorname{char} K = p \neq 2$, seguem das seguintes identidades

$$s_4 = \sum_{\sigma \in S_4} (-1)^{\sigma} x_{\sigma(1)} x_{\sigma(2)} x_{\sigma(3)} x_{\sigma(4)}, \quad h_5 = [[x_1, x_2] \circ [x_3, x_4], x_5],$$

e, no caso que $p = 3$, precisamos de mais uma identidade,

$$\begin{aligned} r_6 = [x_1, x_2] \circ (u \circ v) \quad &- \quad (1/8)([x_1, u, v, x_2] + [x_1, v, u, x_2] \\ &- \quad [x_2, u, x_1, v] - [x_2, v, x_1, u]) \end{aligned}$$

onde $u = [x_3, x_4]$ e $v = [x_5, x_6]$.

Claramente h_5 segue das identidade (4.1 e (4.2). Para r_6 observe primeiramente que

$$[x_1, u, v, x_2] = -[u, x_1, x_2, v] = -4uv[x_2, x_1] = [x_1, v, u, x_2]$$

pela identidade (4.12). Por outro lado $[x_2, u, x_1]$ é anti-simétrico então os dois últimos comutadores de r_6 se anulam em R_2. Temos que r_6 se anula em R_2.

Isso nos motiva a definir o operador linear $L(a, b)$ para a, b variáveis simétricas, sobre a soma direta $F_1 \oplus F_2 \oplus F_3$.

Definição 4.20. *Sejam w_1, w_2 variáveis simétricas ou comutadores e a, b variáveis simétricas, defina*

$$[w_1, w_2]L(a, b) = (1/8)([w_1, a, b, w_2] + [w_1, b, a, w_2] - [w_2, a, w_1, b] - [w_2, b, w_1, a]).$$

Se w_1 e w_2 são comutadores anti-simétricos e $\deg w_2 = 2$ então definimos $(w_1 w_2)L(a, b) = w_1(w_2 L(a, b))$.

Facilimente se verifica que para x_1, x_2 variáveis simétricas, a, $b \in R_2$ temos

$$[x_1, x_2]L(a, b) = (1/4)[x_1, x_2, a, b].$$

Note que $L(a, b) = L(b, a)$.

As seguintes identidades são satisfeitas na álgebra de Lie $sl_2(K)$:

$$\begin{aligned} [x_1, x_2, x_3]L(a, b) &= [[x_1, x_2]L(a, b), x_3] \qquad (4.20) \\ [x_1, a]L(x_2, b) - [x_2, a]L(x_1, b) &= (1/4)[x_1, x_2, b, a] \\ [x_1, x_2]L(a, b)L(c, d) &= [x_1, x_2]L(c, d)L(a, b), \end{aligned}$$

Veja [62, Identidades (3), (4), (5)]. Todas estas (assim como todas as identidades de $sl_2(K)$ quando $\operatorname{char} K \neq 2$) seguem de uma identidade de grau 5, veja o principal resultado de [62]. É bem conhecido que todas as identidades de Lie da álgebra das matrizes $M_2(K)$ seguem do polinômio standard s_4 de grau 4, veja por exemplo [24]. Mas por outro lado o polinômio standard s_4 pode ser escrito como

$$s_4 = 2([x_1, x_2] \circ [x_3, x_4] - [x_1, x_3] \circ [x_2, x_4] + [x_1, x_4] \circ [x_2, x_3]),$$

e se os x_i são variáveis simétricas, $[x_i, x_j]$ são anti-simétricos e comutam em R_2. Portanto o polinômio standard s_4 é igual em R_2 à identidade (4.3). Logo todas as identidades de $sl_2(K)$ acima são satisfeitas em R_2 quando as variáveis são elementos simétricos.

Desde que todas as identidades de $M_2(K)$ são satisfeitas como identidades com involução em R_2 obtemos imediatamente que se w_1 e w_2 são comutadores anti-simétricos então $w_1(w_2L(a, b)) = (w_1L(a, b))w_2$ em R_2. Do que foi discutido obtemos o seguinte lema.

Lema 4.21. *A transfromação L é um operador bem definido em $F_1 \oplus F_2 \oplus F_3$.*

Note que precisamos utilizar a identidade (4.15) na verificação da boa definição de L sobre F_1.

Lema 4.22. *Assuma que $f_i \in F_i$, $i = 1, 2, 3$ de grau ≥ 4. Então, módulo as identidades de (4.1)–(4.4), podemos escrevê-los da seguinte forma. No caso de f_1:*

$$f_1 = \sum_i \alpha_i [x_{i_1}, x_{i_2}][x_{i_3}, x_{i_4}] \prod_j L(a_{ij}, b_{ij}).$$

Aqui a_{ij}, $b_{ij} \in X$ e $\alpha_i \in K$. Além disso, podemos supor que $i_1 < i_2$, $i_3 < i_4$, e $i_1 \leq i_3$, $i_2 \leq i_4$. Para f_2:

$$f_2 = \sum_i \beta_i [x_{i_1}, x_{i_2}] \prod_j L(a_{ij}, b_{ij})$$

com a_{ij}, $b_{ij} \in X$ e $\beta_i \in K$ adequados. Além disso, $i_1 < i_2$. Finalmente, para f_3 temos

$$f_3 = \sum_i \gamma_i [x_{i_1}, x_{i_2}, x_{i_3}] \prod_j L(a_{ij}, b_{ij})$$

com a_{ij}, $b_{ij} \in X$ e $\gamma_i \in K$ adequados. Além disso, podemos supor que $i_1 < i_2 \leq i_3$.

Demonstração. Salvo uma observação o lema segue pelo que já foi exposto. A observação necessária é que as desigualdades entre os índices do polinômio do tipo F_1 obtêm-se por utilizar a identidade (4.3).

4.3.3 Idéia Geral

Vamos dar uma idéia geral do que pretendemos fazer. Nós utilizaremos algumas idéias de [42] e do capítulo sobre as identidades ordinárias em $M_2(K)$. Em primeiro lugar, podemos estender o corpo base. Para isso, assumimos que P é uma extensão do corpo K e denotamos por $R_P = R \otimes_K P$. Se $K \subset P$ então $K(X) \subset P(X)$ e nesta situação teremos $T(R_P) \cap K(X) = T(R)$. Isto é, as identidades polinomiais de R_P com coeficientes em K são as mesmas como as de R. Logo, sem perda de generalidade podemos assumir que K é algebricamente fechado. Então as matrizes

$$e_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; e_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \; e_2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \; e_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

formam uma base do espaço vetorial das matrizes dois por dois, e_1, e_2, e_3 são uma base da álgebra de Lie $sl_2(K)$. Em $sl_2(K)$ temos uma forma bilinear não degenerada definida por

$$< a, b >= a \circ b, \quad a, b \in sl_2.$$

A menos de um multiplo esta é a forma de Cartan—Killing multiplicada pela matriz e_0. Como $K \cong Ke_0$, a forma é exatamente a de Cartan—Killing. Utilizaremos este mesmo produto interno, mas nos restringindo ao espaço gerado por e_1, e_2, ou seja, o espaço das matrizes anti-simétricas.

Observamos que, dada uma matriz $m \in M_2$, teremos $m' = m - (1/2)tr(m) \in sl_2(K)$ para cada $m \in M_2$, identificando Ke_0 com K. O centro da álgebra M_2 consiste de todas as matrizes escalares. Se substituírmos elementos centrais em um comutador obteremos 0. E daí se tivermos $f(x_1, x_2, \ldots, x_n) \in B(X)$ um polinômio próprio, então $f(m_1, m_2, \ldots, m_n) = f(m'_1, m'_2, \ldots, m'_n)$ para quaisquer m_1, m_2, $\ldots$, $m_n \in M_2$. Portanto, um polinômio próprio é uma identidade em M_2 se, e somente se, anula-se em $sl_2(K)$. Em outras palavras, para concluir que um polinômio próprio é uma identidade em $M_2(K)$, basta saber que ele é uma identidade fraca.

Temos um espaço vetorial com um produto interno. Sabemos descrever em termos de tabelas duplas os invariantes do grupo ortogonal O_n. Através dos operadores L conectamos esta teoria aos polinômios do tipo F_i, $i = 1$, 2, 3. Então mostramos que módulo as identidades (4.1)–(4.4), podemos escrever todos os elementos de R_2 como combinação linear dos polinômios $\widetilde{\varphi}(T)$, onde T são tabelas duplas standard, os mesmos que geram a álgebra dos invariantes do grupo O_n (como espaço vetorial). Como conseguimos demonstrar que eles são linearmente independentes, concluindo assim o raciocínio.

4.3.4 Tabelas Admissíveis

Voltamos a lembrar que nos restringimos a variáveis simétricas. Além disso, observamos que nossas variáveis também são elementos da álgebra de Lie sl_2.

Vamos associar a uma k-tabela T um polinômio $\varphi(T)$ em R_2, da seguinte maneira.

Definição 4.23. *Seja $T = (p_1, p_2, \ldots, p_m \mid q_1, q_2, \ldots, q_m)$ é uma k-tabela com apenas uma linha*

1. *Se T é uma 0-tabela então associamos*

$$\varphi(T) = (1/4) \sum_{\sigma \in S_m} (-1)^\sigma [x_{p_1}, x_{p_2}][x_{q_{\sigma(1)}}, x_{q_{\sigma(2)}}] L(x_{p_3}, x_{q_{\sigma(3)}}) \ldots L(x_{p_m}, x_{q_{\sigma(m)}}).$$

2. *Se T é uma 1-tabela então*

$$\varphi(T) = -(1/4) \sum_{\sigma \in S_m} (-1)^\sigma [x_{q_{\sigma(1)}}, x_{q_{\sigma(1)}}, x_{p_2}] L(x_{p_3}, x_{q_{\sigma(3)}}) \ldots L(x_{p_m}, x_{q_{\sigma(m)}}).$$

3. *Se T é uma 2-tabela com $m = 2$ então $\phi(T) = -(1/4)[x_{q_1}, x_{q_2}]$. No caso que $m \geq 3$ então associamos*

$$\varphi(T) = \sum_{\sigma \in S_m} -(1/4)(-1)^\sigma [x_{q_{\sigma(1)}}, x_{q_{\sigma(2)}}] L(x_{p_3}, x_{q_{\sigma(3)}}) \ldots L(x_{p_m}, x_{q_{\sigma(m)}}).$$

No caso geral, sejam T_1, T_2, ..., T_k as sucessivas linhas de T. Então associamos $\varphi(T) = \varphi(T_1) l_2 \ldots l_k$ onde l_j denota o produto de transformações lineares, que comutam entre si,

$$l_j = \sum_{\sigma \in S_m} (-1)^\sigma L(x_{p_{j1}}, x_{q_{j\sigma(1)}}) \ldots L(x_{p_{jm}}, x_{q_{j\sigma(m)}}), \quad m = m_j,$$

onde S_m é o grupo simétrico agindo em $\{1, 2, \ldots, m\}$ e $(-1)^\sigma$ é o sinal de σ.

Note que l_j é o "determinante" de uma matriz $m \times m$ onde $L(x_{p_{ab}}, x_{q_{p\sigma(b)}})$ é a entrada (a, b).

Lema 4.24. *Suponhamos que T é uma k-tabela, $k = 0$, 1, 2. Se $m_1 \geq 3$ então $\varphi(T) = 0$ em R_2.*

Demonstração. É suficiente demonstrar o lema no caso de uma tabela T consistindo de apenas uma linha e $m_1 = 3$. Se $T = (123 \mid 456)$ é 0-tabela então

$$\begin{aligned}\varphi(T) &= (1/8)[x_1,x_2]([x_4,x_5,x_3,x_6] - [x_4,x_6,x_3,x_5] + [x_5,x_6,x_3,x_4]) \\ &= (1/8)[x_1,x_2]([x_4,x_5,x_6,x_3] - [x_4,x_6,x_5,x_3] + [x_5,x_6,x_4,x_3]),\end{aligned}$$

pois temos que $[v, x_i, x_j] = [v, x_j, x_i]$ para qualquer elemento v anti-simétrico e então a segunda expresão se anula devido a identidade de Jacobi.

Seja agora $T = (012 \mid 345)$ uma 1-tabela. Então

$$\varphi(T) = (-1/8)([x_3,x_4,x_2,x_5,x_1] - [x_3,x_5,x_2,x_4,x_1] + [x_4,x_5,x_2,x_3,x_1]) = 0$$

da mesma forma que a 0-tabela. Analogamente no caso de uma 2-tabela $T = (-101 \mid 234)$:

$$\varphi(T) = (-1/8)([x_2,x_3,x_1,x_4] - [x_2,x_4,x_1,x_3] + [x_3,x_4,x_1,x_2]) = 0.$$

Vamos aplicar a discussão, feita em 1.8, sobre os geradores da álgebra dos invariantes do grupo ortogonal, ao caso em que o espaço vetorial é o espaço gerado pelas matrizes 2×2 simétricas e de traço nulo e o produto interno é definido por $u \circ v = (1/2)(uv + vu)$. Vamos mostrar que os polinômios $\tilde{T}$ tais que T é standard e $m_1 \leq 2$ são linearmente independentes

Definição 4.25. *Denotemos por Adm o conjunto de todas as k-tabelas duplas T, $i = 0$, 1, 2, tais que T é standard e o comprimento da primeira linha de T satisfaz $m_1 \leq 2$.*

Proposição 4.26. *Os polinômios $\{\varphi(T) \mid T \in Adm\}$ geram o espaço vetorial $F_1 \oplus F_2 \oplus F_3$ de todos os poliômios $*$-próprios em R_2 que dependem somente de variáveis simétrcias.*

Demonstração. É suficiente mostrar que cada polinômio $f_k \in F_k$ é uma combinação linear de polinômios $\varphi(T_j)$ onde as $T_j \in Adm$ são k-tabelas.

Começamos com $f_1 \in F_1$. Pela proposição 4.22 podemos escrever $f_1 = \sum \alpha_i \varphi(T_i)$ onde $\alpha_i \in K$ e T_i são 0-tabelas. Sem perda de generalidade podemos assumir que todas as linhas de T_i são de comprimento ≤ 2. É suficiente mostrar que cada $\varphi(T_i)$ pode ser expresso como combinação linear de polinômios correspondentes a 0-tabelas standard. Escreva então $T = T_i$.

Cada meia linha de T pode ser colocada em ordem ascendente. Se isto não ocorre podemos reordenar as entradas, provocando com isso no máximo uma mudança de sinal. Suponhamos que T não é standard. Se é na primeira linha usamos a proposição 4.22.

Além disso, se a violação ocorre abaixo da primeira linha podemos aplicar palavra por palavra os argumentos de [36, Lemma 2.7] e expressamos $\varphi(T)$ como uma combinação de tabelas standard de ordem maior (veja 1.8). Se por outro lado tivermos que $p_{1r} > q_{1r}$ então aplicamos novamente a Proposição 4.22. Portanto o único caso a considerar é $q_{1r} > p_{2r}$, $r = 1$ ou 2. Mas isto se resolve aplicando [37, Lema 4.2, Proposição 4.2], e a observação anterior ao lema 4.21. Portanto, $\varphi(T)$ é uma combinação linear da seguinte forma $\varphi(T) = \sum_i \beta_i \varphi(T_i)$, $\beta_i \in K$, $T_i > T$. Na sequência consideramos os polinômios $\varphi(T_i)$ e as suas tabelas correspondentes T_i. Repetindo o processo acima deveremos obter outras tabelas que são maiores na ordem estabelecida entre as tabelas. Claramente este processo termina, pois existem finitos polinômios com o mesmo multigrau.

Seja agora T uma 2-tabela. Como acima podemos supor que T não é standard. Se T deixa de ser standard da seguinte maneira $q_{1r} > p_{2r}$ procedemos como no caso acima, usando as identidades da álgebra de Lie $sl_2(K)$ em [62, Proposição 2.1] com argumentos semelhantes aos que usamos no capítulo 2.

O último caso a considerar é quando T é uma 1-tabela, e como nos outros dois casos, supomos que a violação é $q_{1r} > p_{2r}$. Novamente solucionamos usando a [62, Proposição 2.1], e com isso concluimos a proposição. ■

Teorema 4.27. *As identidades (4.1),(4.2), (4.3) e (4.4) formam uma base das identidades com involução de $M_2(K)$ quando $*$ é a involução transposta.*

Demonstração. Recordemos que I é o ideal com involução gerado pelas identidades (4.1) – (4.4). Precisamos demonstrar que $I = T(M_2(K), *)$. Desde que $I \subseteq T(M_2(K), *)$ é imediato que temos o epimorfismo canônico $K(X,Y)/I \to K(X,Y)/T(M_2(K),*) = \overline{R_2}$. Portanto, a imagem é o conjunto $\{\varphi(T) \mid T \in Adm\}$ que gera o espaço vetorial de todos os polinômios $*$-próprios em $\overline{R_2}$, que dependem somente de variáveis simétricas. O teorema estará estabelecido se conseguirmos mostrar que as imagens dos polinômios $\varphi(T)$, $T \in Adm$ são linearmente independentes.

Aqui faremos uso da seguinte identidade fraca para o par $(M_2(K), sl_2(K))$. Primeiro temos que $[x_1, x_2]L(a,b) = [x_1, x_2] \circ (a \circ b)$. Como consequência de $[x_1 \circ x_2, x_3] = 0$ obtemos $[x_1, x_2] \circ x_3 = x_1 \circ [x_2, x_3]$. Então é fácil de verificar que a identidade fraca

$$[x_1, x_2] \circ [x_3, x_4] = -4((x_1 \circ x_3)(x_2 \circ x_4) - (x_1 \circ x_4)(x_2 \circ x_3)) = -4\tilde{T},$$

vale para $T = (12 \mid 34)$, veja por exemplo [36, Lema 2.1] Vamos necessitar do seguinte lema.

Lema 4.28. *Seja T uma k-tabela, $k = 0$, 1, 2. Então valem as seguintes igualdades em $\overline{R_2}$.*

1. *Quando T é uma 0-tabela, $\varphi(T) = -2\tilde{T}$.*

2. *Quando T é uma 1-tabela, $x_0 \circ \varphi(T) = -2\tilde{T}$.*

3. *Quando T é uma 2-tabela, $[x_{-1}, x_0] \circ \varphi(T) = \tilde{T}$.*

Estamos usando as mesmas notações $\varphi(T)$ para os polinômios em R_2 assim como para as suas respectivas imagens em $\overline{R_2}$.

Demonstração. A primeira afirmação foi provada acima. Observamos que a igualdade $x_0 \circ [x_3, x_2, x_1] = [x_1, x_2] \circ [x_3, x_4]$ é uma identidade fraca para $(M_2(K), sl_2(K))$, de acordo com [36, pp.616]. A última afirmação demonstra-se da mesma forma que a primeira. ■

Retornemos ao nosso teorema. Os polinômios $\tilde{T}$ para T standard e $m_1 \leq 2$ são linearmente independentes em $\overline{R_2}$. Pelo Lema 4.28 temos que os polinômios $\{\varphi(T) \mid T \in Adm\}$ são linearmente independentes em $\overline{R_2}$. Note que para uma 0-tabela T, o polinômio $\varphi(T)$ representa matrizes escalares em $M_2(K)$; se T é uma 1-tabela, $\varphi(T)$ nos fornece matrizes simétricas de traç nulo, e para 2-tabelas, $\varphi(T)$ nos fornece matrizes anti-simétricas em $M_2(K)$.

Portanto, $\{\varphi(T) \mid T \in Adm\}$ são linearmente independentes em R_2, e eles formam uma base do espaço vetorial $F_1 \oplus F_2 \oplus F_3$. Isso demonstra o teorema. ■

Nós utilizamos identidades fracas do par $(M_2(K), sl_2(K))$; todas as identidades são consequências da identidade fraca $[x_1 \circ x_2, x_3] = 0$, onde x_i são variáveis simétricas (veja [36] para maiores detalhes). Precisamos demonstrar que a identidade $[x_1 \circ x_2, x_3]$ segue das identidades (4.1)–(4.4). Isto ocorre, pois $[x_1 \circ x_2, x_3] = x_1 \circ [x_2, x_3] + x_2 \circ [x_1, x_3]$ e o polinômio à direita é nulo por utilizar a identidade (4.5), uma vez que x_i, $i = 1, 2, 3$ são variáveis simétricas.

4.4 $*$-PI em $M_2(K)$ com a involução simplética

Vamos estudar as $*$-identidades de $M_2(K)$, onde $* = (s)$, isto é, $*$ indica a involução simplética. O seguinte polinômio é uma $*$-PI em $M_2(K)$.

$$[y_1, z_1]$$

A verificação que este polinômio é uma $*$-identidade, é imediata. Seja, como na seção anterior, R_2 a álgebra obtida por tomarmos o quociente da álgebra livre pelo ideal das identidades com involução gerado por essa identidade.

Teorema 4.29. *Seja K um corpo de característica $\neq 2$. Então as identidades polinomiais da álgebra $M_2(K)$ com a involução simplética tem base que consiste da identidade $[y_1, z_1]$.*

Demonstração. Começamos observando que se $f = f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$ é uma identidade então existe $\widetilde{f}(y_1, y_2, \ldots, y_m)$, tal que $f = x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n} \widetilde{f}$, onde r_1, r_2, $\ldots$, r_n são inteiros não negativos. Portanto, utilizando as idéias do lema 4.14 podemos admitir que se f é uma $*$-identidade, então ela depende somente de variáveis anti-simétricas.

Ainda mais, se f é uma $*$-identidade, então f também é uma identidade fraca no par $(M_2(K), sl_2(K))$. Então pelo principal resultado de [36] podemos escrever

$$f(y_1, y_2, \ldots, y_m) = \sum_i \alpha_i u_i [v_i' \circ v_i'', t_i] w_i,$$

onde $\alpha_i \in R_2$, u_i, v_i são polinômios adequados, e v_i', v_i'' são comutadores em y_1, y_2, $\ldots$, y_m. Agora observemos que

$$[y_1, y_2]^* = -[y_1, y_2],$$

e utilizando isso podemos mostrar, por indução, que v_i', v_i'' também são anti-simétricos.

Temos ainda

$$y_1 \circ y_2 = y_1 y_2 + (y_1 y_2)^*.$$

Isto quer dizer que $y_1 \circ y_2$ é simétrico. Este último fato conclui a demonstração. ∎

Referências Bibliográficas

[1] M. Artin, *On Azumaya algebras and finite dimensional representations of rings*, J. Algebra **11**(1969), 532–563.

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

[3] A. Ya. Belov, *On non-Specht varieties* (em russo), Fundam. Prikl. Mat. **5**, No. 1(1999), 47–66.

[4] A. Ya. Belov, *Counterexamples to the Specht problem*, Sb. Math.**191**, No. 3(2000), 329–340.

[5] F. Bennati, J. Demmel, V. Drensky, P. Koev, *Computational approah to polynomial identities of matrices — a survey, in "Ring theory: Polynomial Identities and Combinatorial Methods, Proc. of the Conf. in Pantelleria"* ; Eds. A. Giambruno, A. Regev e M. Zaicev, Lect. Notes Pure Appl. Math., Dekker, 2003.

[6] P. Zh. Chiripov, P. N. Siderov, *On bases for identities of some varieties of associative algebras* (em russo), Pliska Stud. Math. Bulgar. **2**(1981), 103–115.

[7] P. M. Cohn, *"Universal algebras"*, Harper, New York, 1965.

[8] J. Colombo, P. Koshlukov, *Central Polynomial in the matrix of order two*, Lin. Algebra Appl. **377**(2004), 53–67.

[9] C. De Concini e C. Procesi, *A characteristic free approach to invariant theory*, Adv. Math. **21**, No. 3(1976), 330–354.

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

[11] V. Drensky, *A minimal basis for the identities of a second-order matrix algebra over a field of characteristic 0*, Algebra and Logic **20**, No. 3(1980), 188–194.

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

[13] V. Drensky, *Identities of representations of nilpotent Lie algebras*, Commun. Algebra **25**, No. 7(1997), 2115–2127.

[14] V. Drensky, *"Free algebras and PI algebras: Graduate Course in Algebra"*, Springer, Singapore, 1999.

[15] V. Drensky, A. Kasparian, *Polynomial identities of eigth degree for* 3×3 *matrices*, Ann. Univ. Sofia, Fac. Math. Mecan., Livre 1, Math. **77**(1983), 175–195.

[16] V. Drensky, A. Kasparian, *A new central polynomial for* 3×3 *matrices*, Commun. Algebra **13**(1985),745–752.

[17] V. Drensky, P. E. Koshlukov, *Polynomial identities for Jordan algebras of degree two*, J. Indian Math. Soc. **55**(1990), 1–30.

[18] V. Drensky e G. M. Piacentini Cattaneo, *A central polynomial of low degree for* 4×4 *matrices*, J. Algebra **168**(1994), 469–478.

[19] V. T. Filippov, *Varieties of Mal'tsev algebras*, Algebra Logic **20**, No. 3(1981), 200–210.

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

[21] E. Formanek, *Invariants and the ring of generic matrices*, J. Algebra **89**(1984), 178–223.

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

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

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

[25] A. Giambruno, A. Valenti, *Central polynomial and matrix invariant*, Israel J. Math. **96**(1996),281–297.

[26] A. V. Grishin, *Examples of T-spaces and T-ideals over a field of characteristic 2 without the finite basis property* (em russo, resumo em inglês), Fundam. Prikl. Mat. **5**, No. 1(1999), 101–118.

[27] P. Halpin, *Central and weak identities for matrices*, Commun. Algebra **11**(1983), 2237–2248.

[28] I. N. Herstein, *"Noncommutative Rings"*, Carus Math. Monographs **15**, Wiley and Sons, Inc., New York, 1968.

[29] A. V. Iltyakov, *Specht ideals of identities of certain simple nonassociative algebras*, Algebra Logic **24** (1985), 210–228.

[30] N. Jacobson, *"PI-Algebras: An introdution"*, Lect. Notes Math. **441**, Springer-Verlag, Berlin-New York, 1975.

[31] I. Kaplansky, *Problems in theory of rings*, Report of a Coference on Linear Algebras, June, 1956, in National Acad. Sci. National Research Council, Washington, Publ. **502**(1957), 1–3.

[32] I. Kaplansky, *Problems in the theory of rings revised*, Amer. Math. Monthly **77**(1970), 445–454.

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

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

[35] A. R. Kemer, *"Ideals of identities of associative algebras"*, Transl. Math. Monographs **87**, AMS, Providence, RI, 1991.

[36] P. Koshlukov, *Weak polynomial identities for the matrix algebra of order two*, J. Algebra **188**, No. 2(1997), 610–625.

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

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

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

[40] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignl, *"The book of involutions"*, Colloquium Publications **44**, Amer. Math. Soc., 1998.

[41] T. Y. Lam, *"A first course in noncommutative rings"*, Sringer-Verlag, New York, 1991.

[42] D. V. Levchenko, *Finite basis property of identities with involution for second-order matrix algebra*(em russo), Serdica **8**, No. 1(1982), 42–56.

[43] A. I. Malcev, *On algebras defined by identities* (em russo), Mat. Sb. **26**(1950), 19–33.

[44] Yu. N. Maltsev, *A basis for the identities of the algebra of upper triangular matrices*, Algebra and Logic **10**(1971), 242–247.

[45] Yu. N. Maltsev, E. N. Kuzmin, *A basis for the identities of the algebra of second-order over a finite field*, Algebra and Logic **17**, No. 1(1978), 18–21.

[46] S. Okhitin, *Central polynomials of the algebra of second order matrices*, Moscow Univ. Math. Bull. **43**, No. 4(1988), 49–51.

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

[48] C. Procesi, *Non-commutative affine rings*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. **8**(1967), 239–255.

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

[50] C. Procesi, *Computing with* 2×2 *matrices*, J. Algebra **87**, No. 2(1984), 342–359.

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

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

[53] Y. Razmyslov, *"Identities of Algebras and Their Representations"*, Translations of Math. Monographs, vol. **138**, AMS, Providence, 1994.

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

[55] L. H. Rowen, *"Polynomial identities in ring theory"*, Academic Press, 1980.

[56] V. V. Shchigolev, *Examples of infinitely based T-ideals* (em russo, resumo em inglês), Fundam. Prikl. Mat. **5**, No. 1(1999), 307–312.

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

[58] W. Specht, *Gesetze un Ringen. I*, Math. Z., **52**(1950), 557–589.

[59] J. Szigeti, Z. Tuza e G. Rèvèz, *Eulerian polynomial identities on matrix rings*, J. Algebra **161**(1993), 90–101.

[60] B. T Tki, *On basis of the identities of the matrix algebra of second order over a field of characteristic zero*, Serdica **7**, No. 3(1981), 187–194.

[61] M. R. Vaughan-Lee, *Abelian-by-nilpotent varieties of Lie algebra*, J. London Math. Soc. **2**, No. 11(1975), 263–266.

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

[63] A. H. Stojanova–Venkova, *Bases of identities of Grassmann algebras*, (em russo) Serdica **6**, No. 1(1980), 63–72.

[64] H. Weyl, *"The classical Groups, their invariants and representations"*, Princeton Univ. Press, Princeton, N.J., 1946.