Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

DISSERTAÇÃO DE MESTRADO

Álgebras com Identidades Polinomiais e suas dimensões de Gelfand-Kirillov

por

Gustavo Grings Machado†

Mestrado em Matemática - Campinas - SP

Orientador: Prof. Dr. Plamen Emilov Koshlukov

†Este trabalho contou com apoio financeiro do CNPq.

Álgebras com Identidades Polinomiais e suas dimensões de Gelfand-Kirillov

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Gustavo Grings Machado** e aprovada pela comissão julgadora.

Campinas, 21 de Fevereiro de 2011.

P Koshlukov

Prof. Dr. Plamen Emilov Koshlukov

Banca examinadora:

Prof. Dr. Plamen Emilov Koshlukov
Prof. Dr(a). Iryna Kashuba
Prof. Dr. Victor Petrogradski

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

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Fabiana Bezerra Müller – CRB8 / 6162

Machado, Gustavo Grings
M18a Álgebras com identidades polinomiais e suas dimensões de Gelfand-Kirillov/Gustavo Grings Machado-- Campinas, [S.P. : s.n.], 2011.

Orientador : Plamen Emilov Koshlukov
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

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

Título em inglês: Álgebras with polynomial identities and their Gelfand-Kirillov dimensions

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

Área de concentração: Álgebra

Titulação: Mestre em Matemática

Banca examinadora: Prof. Dr. Plamen Emilov Koshlukov (IMECC – UNICAMP)
Profa. Dra. Iryna Kashuba (IME – USP)
Prof. Dr. Victor Petrogradski (University of Uliyanovsk, Russia)

Data da defesa: 21/02/2011

Programa de Pós-Graduação: Mestrado em Matemática

Dissertação de Mestrado defendida em 21 de fevereiro de 2011 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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

Prof. (a). Dr (a). IRYNA KASHUBA

Prof. (a). Dr (a). VICTOR PETROGRADSKIY

Ao anjo em minha vida,
minha amada Juliana.

AGRADECIMENTOS

Agradeço, antes de tudo a Deus, pela vida.

À minha família pela força, pela ajuda e por acreditarem no meu potencial.

Sou muito grato ao meu ex-professor João Batista Peneireiro. E claro, ao amigo Juliano Damião que nos apresentou. Sem eles eu teria demorado muito para conseguir me encontrar no curso de Matemática.

Agradeço a todos os que foram meus professores, especialmente aos professores do departamento de Matemática da UFSM.

Aos professores e funcionários do IMECC-UNICAMP, principalmente aos que compõem a secretaria de Pós-Graduação e Biblioteca, pela forma atenciosa e respeitosa, que sempre fui tratado.

Agradeço aos amigos que fiz até aqui.

Ao meu orientador Plamen Koshlukov, pela orientação objetiva, pelas sugestões e por toda ajuda e atenção dispensada.

À CNPq, que possibilitou a realização deste trabalho e à banca examinadora, que avaliou este trabalho e cujas sugestões ajudaram a melhorá-lo consideravelmente.

Agradeço e muito a querida Juliana pelo companheirismo, amor, amizade, dedicação e incentivo.

Sem mais, sou muito grato a todos que de alguma forma ou outra participaram de minha vida até agora e possibilitaram esse momento.

ABSTRACT

In this work we study algebras with polynomial identities, focusing on the study of finitely generated unitary associative algebras. Our goal is to give an alternative proof of non PI-equivalence of algebras using an invariant known as Gelfand-Kirillov dimension. This invariant has gained importance lately since in many cases it is relatively easy to calculate and, surprisingly, it is able to differentiate the growth of two algebras. We begin with definitions and basic results of algebras, graded algebras, (graded) polynomial identities, reduction of polynomial identities, etc. Afterwards we present some results concerning finitely generated algebras with polynomial identities, which give a better comprehension of the notions of height and Gelfand-Kirillov dimension. Later on we study the Kemer's Tensor Product Theorem (TPT), from which we conclude (multilinear) PI-equivalence involving important algebras in PI-theory, the so called T-prime algebras. In particular, we deduce the PI-equivalence of $M_{1,1}(E)$ and $E \otimes E$ over fields of characteristic zero, where E is the infinite dimensional Grassman algebra. Finally, we prove the non PI-equivalence of $M_{1,1}(E)$ and $E \otimes E$ over infinite fields of prime characteristic greater than two by means of Gelfand-Kirillov dimension.

RESUMO

Neste trabalho estudamos álgebras com identidades polinomiais, focando-se no estudo de álgebras associativas unitárias finitamente geradas. Nosso objetivo é fazer uma demonstração alternativa da não PI-equivalência de álgebras utilizando um invariante conhecido como dimensão de Gelfand-Kirillov. Este invariante tem ganhado importância ultimamente, uma vez que ele é relativamente fácil de calcular e, de certa forma, é capaz de diferenciar o modo com que duas álgebras crescem. Começamos com as definições e resultados básicos de álgebras, álgebras graduadas, identidades polinomiais (graduadas), reduções de identidades polinomiais, etc. Em seguida apresentamos alguns resultados de álgebras com identidades polinomiais finitamente geradas, que permitem uma melhor compreensão dos conceitos de altura e de dimensão de Gelfand-Kirillov. Depois estudamos o Teorema do Produto Tensorial de Kemer (TPT), donde se conclui a PI-equivalência (multilinear) envolvendo álgebras importantes na teoria de PI-álgebras, as álgebras T-primas. Em particular, conclui-se a PI-equivalência sobre corpos de característica zero de $M_{1,1}(E)$ e $E\otimes E$, em que E é a álgebra de Grassmann de um espaço vetorial de base enumerável. Enfim, finalizamos mostrando a não PI-equivalência sobre corpos infinitos de característica positiva maior que dois de $M_{1,1}(E)$ e $E \otimes E$, utilizando-se da dimensão de Gelfand-Kirillov.

CONTEÚDO

INTRODUÇÃO

Esta dissertação trata de alguns tópicos de Álgebra: Teoria de Anéis, e mais especificamente, Teoria de Álgebras com Identidades Polinomiais (PI-álgebras) e as suas propriedades combinatórias.

As álgebras comutativas e as de dimensão finita são objetos de estudo de grande importância devido ao seu amplo aspecto de aplicações. Estas álgebras são exemplos de estruturas que compartilham o fato de satisfazerem relações polinomiais entre seus elementos. Mais precisamente, para cada uma das álgebras acima, existe um polinômio $f(x_1, \ldots, x_n)$ com variáveis não comutando que se anula quando avaliado nos elementos das mesmas. Esta propriedade será satisfeita também por qualquer álgebra matricial cujas entradas pertençam a tal álgebra. A álgebra que cumpre tal condição é denominada uma álgebra com identidade polinomial, ou simplesmente uma PI-álgebra. Seu estudo, a princípio, consiste em relacionar o efeito das identidades polinomiais na estrutura das álgebras que as satisfazem. Gostaríamos de deixar claro que os temas de estudo em PI-teoria são bastante amplos e diversos, e não se resumem somente a estudos da estrutura das PI-álgebras.

Historicamente, o desenvolvimento da Teoria de Identidades Polinomiais começou na década de 30, com os trabalhos de Dëhn e Wagner. Nesses trabalhos aparecem, embora de forma subentendida, algumas identidades polinomiais para as matrizes de ordem 2. Vale lembrar que alguns conceitos da PI-teoria encontram-se ainda em trabalhos de Sylvester, por volta de 1852. Evidentemente tais conceitos aparecem nesses trabalhos de forma bastante implícita, e têm caráter secundário. A pesquisa das PI-álgebras começou a se intensificar por volta dos anos 1950, com trabalhos de Jacobson e Kaplansky. Em 1950 foi demonstrado o célebre Teorema de Amitsur e Levitzki, um resultado clássico mostrando que a álgebra das matrizes de ordem n com entradas num corpo satisfazem o polinômio standard de grau $2n$, (isto é, o somatório alternado de todos os produtos de $2n$ matrizes de ordem n é sempre igual a matriz nula). Na mesma época, algebristas reconhecidos deram contribuições importantes para a PI-teoria. Podemos relacionar aqui os nomes de Jacobson, Kaplansky, Herstein, Malcev, Cohn, Shirshov, entre outros. Vários algebristas têm trabalhado na área; segue uma lista de nomes (sem qualquer pretensão de ser completa): Posner, Nagata, Procesi, Higman, Regev, Razmyslov, Braun, Formanek, Swan, Specht, Latyshev, Bahturin, Zelmanov, Rowen, Kemer, Drensky, Giambruno, Zaicev, Berele, Vaughan-Lee, e muito mais. O leitor interessado poderia consultar alguma das bases de dados online, tais como MathSciNet, da American Mathematical Society, ou Zentralblatt für Mathematik, da Springer e procurar pelo código de classificação 16R (ou 16A, antes de 1990).

Assim, até a década de 1980 vários pesquisadores tinham obtido diversos resultados de grande importância na área. Foram desenvolvidos métodos poderosos provenientes da Combinatória Algébrica e baseados na Teoria das Representações do Grupo Simétrico e do Grupo Geral Linear (ou na Teoria de Invariantes). Tais métodos mostraram-se extremamente úteis para a descrição das variedades de álgebras (isto é, as classes de álgebras sobre um dado corpo que satisfazem algum conjunto conhecido de identidades polinomiais). Por volta de 1985–1987, Kemer desenvolveu métodos e teorias que permitiram classificar os T-ideais em característica zero, e serviram de base para vários outros estudos. Para recordar uma parte dos principais resultados obtidos por Kemer, precisaremos alguns conceitos.

As álgebras verbalmente primas desempenham um papel proeminente na PI-teoria. Uma álgebra é verbalmente prima se seu T-ideal é primo na classe de todos os T-ideais na álgebra associativa livre. A maioria dos resultados conhecidos sobre álgebras verbalmente primas estão no caso em que estas álgebras tem como base corpos de característica zero. A teoria estrutural de T-ideais desenvolvida por Kemer classificou as álgebras verbalmente primas sobre tais corpos. Mais ainda, Kemer mostrou que os T-ideais verbalmente semiprimos são interseções finitas de T-ideais verbalmente primos, e finalmente que se I é um T-ideal, então $J^n \subseteq I \subseteq J$ para alguma escolha de n e de um T-ideal J verbalmente semiprimo.

Denotando por K o corpo base, de acordo com a teoria de Kemer as álgebras verbalmente primas são exatamente as seguintes:

- Primeiro as triviais $\{0\}$ e $K\langle X\rangle$ a álgebra associativa livre de posto infinito;
- Por conseguinte, $M_n(K)$, a álgebra das matrizes $n \times n$ com entradas em K;
- A segunda classe de álgebras verbalmente primas é dada pela álgebra das matrizes $n \times n$ com entradas em E, denotada por $M_n(E)$;
- A última classe de álgebras verbalmente primas é denotada por $M_{a,b}(E)$,

onde E é a álgebra de Grassmann (ou exterior) do espaço vetorial V com base $\{e_1, e_2, \dots\}$. Como espaço vetorial, E tem base consistindo dos elementos 1 e $e_{i_1} \dots e_{i_k}$, onde $i_1 < \cdots < i_k$, $k = 1, 2, \dots$ e a multiplicação em E é induzida por $e_i e_j = -e_j e_i$, para todos i e j. A álgebra E tem $\mathbb{Z}_2$-graduação natural definida como segue. Denotemos por E_0 o centro de E, então E_0 é gerado como espaço vetorial por todos os monômios na base de E com comprimento par, denotamos por E_1 o espaço gerado pelos monômios de comprimento ímpar. Então, os elementos de E_1 anticomutam. E $M_{a,b}$ é a subálgebra de $M_{a+b}(E)$ que consiste de todas as matrizes sob a forma $Ae_{11} + Be_{12} + Ce_{21} + De_{22}$, onde e_{ij} são matrizes unidade 2×2, $A \in M_a(E_0)$, $B \in M_{a\times b}(E_1)$, $C \in M_{b\times a}(E_1)$ e $D \in M_b(E_0)$. Aqui recordamos que a descrição acima das álgebras verbalmente primas acima vale quando K é de característica zero. A descrição das álgebras T-primas em característica positiva está em aberto; sabe-se que além destas álgebras, a lista das álgebras T-primas envolve muitas outras.

Duas álgebras A e B são ditas PI-equivalentes, escrevemos $A \sim B$, se elas satisfazem as mesmas identidades polinomiais. Como uma consequência de sua teoria estrutural, Kemer mostrou que a classe das álgebras T-primas é fechada sob produtos tensoriais. Mais precisamente, ele descreveu a PI-equivalência nos produtos tensoriais de álgebras verbalmente primas. Esta descrição é conhecida como:

Teorema do Produto Tensorial(T.P.T.). Assuma $\operatorname{char} K = 0$. Então,

(1) $M_{a,b}(E) \otimes E \sim M_{a+b}(E)$;

(2) $M_{a,b}(E) \otimes M_{c,d}(E) \sim M_{ac+bd,ad+bc}(E)$;

(3) $E \otimes E \sim M_{1,1}(E)$.

Aqui, e no que segue, todos os produtos tensoriais são considerados sobre o corpo K.

Como consequência de sua teoria estrutural, Kemer (1987) resolveu em afirmativo o famoso e antigo problema (1950) proposto por Specht: Todo T-ideal (em característica zero) é finitamente gerado como um T-ideal? Recomendamos a leitura de [11] para mais detalhes sobre a teoria estrutural de PI-álgebras e as contribuições de Kemer nesta teoria.

Se o corpo base tem característica $p > 0$, o problema de Specht tem resposta negativa; exemplos foram construídos por Grishin, Shchigolev, Belov por volta de 1999.

Uma das principais ferramentas utilizadas na teoria de Kemer foram as identidades graduadas. A álgebra de Grassmann E admite uma graduação natural com o grupo cíclico de ordem 2, $\mathbb{Z}_2$; essa graduação induz $\mathbb{Z}_2$-graduações em $M_n(E)$ e em $M_{a,b}(E)$. Logo após a teoria de Kemer, o estudo de graduações (com grupos arbitrários) e das respectivas identidades graduadas intensificou-se devido às variadas aplicações.

O Teorema do Produto Tensorial admite provas que independem da teoria estrutural. A primeira tal prova foi proposta por Regev [19], e mais tarde Di Vincenzo; Di Vincenzo e Nardozza, provaram partes deste teorema, veja ([15],[16],[22]). Estas demonstrações foram construídas sob a hipótese que o corpo base é de característica zero. Outras provas elementares de casos do T.P.T. foram dadas em ([2],[3],[4]). Voltamos nossa atenção para o fato que em ([2],[3],[4]), o comportamento dos correspondentes T-ideais em característica positiva foi estudado. Nestes, os autores provaram que o T.P.T. continua válido sobre corpos infinitos de característica positiva $p > 2$, somente considerando-se as identidades polinomiais multilineares. Mais ainda, em [3], eles provaram que a terceira afirmação do T.P.T. falha e, em [2], também provaram que a primeira afirmação falha (quando $a = b = 1$).

Em [4] os autores construíram um modelo apropriado para a álgebra relativamente livre na variedade das álgebras determinadas por $E \otimes E$ quando $\operatorname{char} K = p > 2$. Este modelo é a álgebra genérica de $\mathcal{A} = K \oplus M_{1,1}(E')$ onde E' denota a álgebra de Grassmann sem unidade. Eles provaram que as álgebras $\mathcal{A}$ e $E \otimes E$ satisfazem as mesmas identidades polinomiais ordinárias. Usando propriedades da álgebra $\mathcal{A}$, em [3], os autores provaram que $T(M_{1,1}(E)) \subsetneq T(E \otimes E)$ em característica positiva.

A dimensão de Gelfand-Kirillov foi introduzida originalmente por Gelfand e Kirillov (1966) para estudar o crescimento de álgebras de Lie de dimensão finita, posteriormente tornou-se um importante invariante para álgebras afins, pois a mesma independe da escolha de seu conjunto de geradores (ao contrário das séries de Hilbert). Uma referência padrão sobre GK-dimensão é o livro de Krause e Lenagan (veja [12]), que também contém os principais resultados sobre GK-dimensão para PI-álgebras.

Berele em [5] construiu modelos para as álgebras relativamente livres (também chamadas de universais) de posto m, $F_m(M_n(E))$ e $F_m(M_{a,b}(E))$, nas variedades determinadas por $M_n(E)$ e $M_{a,b}(E)$, respectivamente. No que segue, vamos assumir que o posto das respectivas álgebras relativamente livres é ≥ 2. Em [17], Procesi calculou a GK-dimensão da álgebra gerada por m matrizes genéricas de ordem n, ou seja, mostrou que $\operatorname{GKdim} F_m(M_n(K)) = (m-1)n^2 + 1$. Em [5], Berele mostrou que $\operatorname{GKdim} F_m(M_n(E)) = (m-1)n^2 + 1$ e também que $\operatorname{GKdim} F_m(M_{a,b}(E)) = (m-1)(a^2+b^2) + 2$.

Neste trabalho apresentaremos alguns resultados sobre identidades graduadas em álgebras associativas, bem como sobre a dimensão de Gelfand–Kirillov de tais álgebras. Consideramos uma demonstração do Teorema de Shirshov sobre a altura, um dos feitos mais significativos da teoria combinatória de anéis, e relacionamos brevemente a altura com a dimensão de Gelfand–Kirillov. No final faremos uma demonstração de não PI-equivalência usando a dimensão de Gelfand–Kirillov

O texto está organizado em três capítulos, os quais, vale ressaltar, procuramos tornar independentes, conforme possível. Os capítulos foram estruturados da seguinte forma:

- O Capítulo 1 é dedicado as definições preliminares e apresentação de alguns dos nossos objetos de estudo, bem como alguns aspectos históricos e resultados clássicos que motivaram o desenvolvimento da teoria das Identidades Polinomiais, ou simplesmente PI-teoria. Este capítulo auxilia o leitor como referência aos resultados básicos. Na medida do possível, tentamos colocar as demonstrações de resultados clássicos com a linguagem de álgebras graduadas. Ressaltamos que para um leitor com bom conhecimento da PI-teoria, este capítulo pode ser evitado sem comprometimento dos demais. Optamos por não discutir a dimensão de Gelfand-Kirillov neste capítulo e deixar isso para o segundo capítulo. Em nossa opinião o Capítulo 1 tornou-se mais leve e o Capítulo 2 mais fechado e pouco dependente dos outros.

- O Capítulo 2 é dedicado ao teorema de Shirshov, e a dimensão de Gelfand-Kirillov, apresentando resultados importantes para álgebras finitamente geradas. Iniciamos com o teorema de Shirshov que nos diz que toda PI-álgebra finitamente gerada possui altura finita. Em seguida apresentamos conceitos básicos e estudamos o comportamento da GK-dimensão com respeito a altura. Depois, apresentamos um breve estudo sobre a GK-dimensão das álgebras relativamente livres.

- O Capítulo 3 é dedicado ao Teorema do Produto Tensorial de Kemer, com objetivo de tornar claro que este é um resultado a respeito de identidades multilineares, que não pode ser transportado para álgebras com corpo base de característica $p > 2$. Inicialmente, apresentamos um resultado mais recente (a versão multilinear do Teorema do Produto Tensorial) que independe da característica do corpo base, donde conclui-se facilmente a PI-equivalência de $M_{1,1}(E)$ e $E \otimes E$, quando o corpo base é de característica zero. Num segundo momento deste capítulo, apresentamos uma demonstração usando a dimensão de Gelfand-Kirillov de que $M_{1,1}(E)$ e $E \otimes E$ não são PI-equivalentes, quando o corpo base é infinito de característica $p > 2$.

CAPÍTULO 1

PI-ÁLGEBRAS: CONCEITOS BÁSICOS

Neste capítulo apresentaremos os conceitos básicos e alguns resultados que são utilizados ao longo do texto. Começaremos com a definição de álgebra. Para evitar repetir "...sobre o corpo K" frequentemente, a menos que se diga algo em contrário, sempre consideraremos os espaços vetoriais, e as álgebras como sendo sobre o corpo K. Além disso, utilizaremos muitas vezes, quando n for um número natural, I_n para denotar o subconjunto natural $\{1, 2, \ldots, n\}$.

1.1 Álgebras, PI-Álgebras e Variedades

Nesta seção introduzimos os conceitos de Álgebra, Álgebra com Identidade Polinomial, que é uma importante classe de álgebras, Variedades e Álgebras Relativamente Livres.

1.1.1 Álgebras: Conceitos Gerais

Uma álgebra nada mais é que um espaço vetorial sobre um corpo K, com uma multiplicação de vetores compatível com a soma e multiplicação por escalar.

Definição 1.1.1. *Diremos que $(A, *)$ é uma álgebra sobre K (ou diremos simplesmente que A é álgebra, quando estiver claro qual é a operação $*$), se A é um K-espaço vetorial munido* *de uma operação binária, $*: A \times A \to A$, denominada de multiplicação, que é uma aplicação bilinear, ou seja, para qualquer $\alpha \in K$ e quaisquer a, b, $c \in A$, valerem:*

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

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

(3) $\alpha(a*b) = (\alpha a)*b = a*(\alpha b)$.

Por simplicidade, omitiremos o sinal de $*$, distinguindo a multiplicação por escalar da multiplicação ao usar letras gregas no primeiro caso.

Diremos que:

(i) *A é **comutativa**, se a multiplicação for simétrica, isto é $ab = ba$ para quaisquer $a, b \in A$;*

(ii) *A é **associativa**, se $(ab)c = a(bc)$ para quaisquer a, b, $c \in A$, ou seja, $(A, +, *)$ é um anel. Neste caso os parenteses podem ser omitidos;*

(iii) *A é **unitária**, se existir $1_A \in A$, $1_A \neq 0_A$, tal que $1_A a = a 1_A = a$ para qualquer $a \in A$ (vamos escrever $\underline{1}$ em vez de $\underline{1_A}$).*

(iv) *A é uma **Álgebra de Lie** se para quaisquer a, b, $c \in A$ valem:*

$$a*a = 0\,(anticomutatividade)\,,$$

$$(a*b)*c + (b*c)*a + (c*a)*b = 0\,(identidadedeJacobi)\,.$$

(v) *A é uma **álgebra de Jordan** se para quaisquer a, $b \in A$ valem:*

$$a*b = b*a,$$

$$(a^2*b)*a = a^2*(b*a),\ onde\ a^2 = a*a.$$

A seguir providenciamos alguns exemplos de álgebras.

Exemplo 1.1.2. O espaço vetorial $M_n(K)$ das matrizes $n \times n$ com entradas em K, com a multiplicação sendo a multiplicação usual de matrizes, é uma álgebra associativa unitária.

Exemplo 1.1.3. O espaço vetorial $\mathbb{R}^3$ sobre o corpo dos reais com o produto vetorial $\times$ usual é uma álgebra de Lie.

Exemplo 1.1.4. O espaço vetorial $\mathbb{R}^3$ sobre o corpo dos reais com base $\{e_1, e_2, e_3\}$ e multiplicação $*$ comutativa induzida por: $e_1 * e_2 = e_1$, $e_1 * e_3 = e_3$, $e_2 * e_3 = e_2$, $e_i * e_i = e_i$, é uma álgebra não associativa. Também é uma álgebra de Jordan.

Exemplo 1.1.5. O anel $K[x_1, \ldots, x_n]$ dos polinômios em n variáveis comutativas com as operações usuais é uma álgebra utilizando as mesmas operações do anel, pois ele também é um K-espaço vetorial. Ela é associativa, comutativa e unitária.

Exemplo 1.1.6. Se $K \subseteq L$ é uma extensão de corpos, então L é um K-espaço vetorial que é álgebra sobre K associativa, comutativa, unitária, quando consideramos as operações de corpo em L.

Exemplo 1.1.7. O subespaço $U_n(K)$ de $M_n(K)$ das matrizes triangulares superiores com a multiplicação "herdada" de $M_n(K)$, também é uma álgebra associativa unitária.

Exemplo 1.1.8. Se A é uma álgebra associativa com multiplicação $*$, então o espaço vetorial A se torna uma álgebra de Lie com a multiplicação dada pelo comutador $[a_1, a_2] = a_1 * a_2 - a_2 * a_1$. Essa álgebra $(A, [,])$ é denotada por $A^{(-)}$.

Exemplo 1.1.9. Considerando a álgebra $A = M_n(K)$, denotaremos por $gl_n(K)$ a álgebra $A^{(-)}$, ou seja, o espaço vetorial das matrizes $n \times n$ com entradas em K equipado com multiplicação $*$ dada por $a * b = ab - ba$.

Exemplo 1.1.10. Como no caso de álgebras de Lie, se A é uma álgebra associativa sobre um corpo K, $\operatorname{char} K \neq 2$, substituindo-se o produto de A pelo produto simétrico $a * b = (ab + ba)/2$ obteremos uma álgebra de Jordan, denotada por $A^{(+)}$.

Definição 1.1.11. *Sejam $(A, *_A)$ e $(B, *_B)$ duas álgebras sobre um mesmo corpo. Seja $f : A \to B$ uma transformação linear.*

Diremos que f é um homomorfismo de álgebras se $f(x *_A y) = f(x) *_B f(y)$. Definimos por $\ker(f) = f^{-1}(0_B)$ e por $Im(f) = f(A)$ ao núcleo e à imagem de f, respectivamente. Agora podemos definir ideal (bilateral) e subálgebra.

Continuando na mesma notação, $C \subseteq B$ é uma subálgebra de B se C é imagem de um homomorfismo de álgebras com contradomínio B. Outra forma equivalente é se C é um subespaço vetorial de B, tal que equipado com a restrição de $*_B$ a $C \times C$, C é uma álgebra.

Diremos que I é ideal (bilateral) de A se I for núcleo de algum homomorfismo de álgebras com domínio A. Outra forma equivalente bem conhecida é quando I é um subespaço de A tal que $AI \subseteq I$ (isto é, I é ideal à esquerda) e $IA \subseteq I$ (isto é, I é ideal à direita).

Observação 1.1.12. Quando estivermos lidando com álgebras unitárias, exigimos que para C ser subálgebra, ela deve ser unitária, e ter a mesma unidade de B. Desse modo, ideais não triviais de álgebras (unitárias) não são subálgebras. Na verdade, quando se considera como objetos álgebras unitárias com $1 \neq 0$, torna-se interessante estudar apenas os morfismos tais que $f(1_A) = 1_B$. Costuma-se chamar aos ideais nesta categoria de próprios.

Exemplo 1.1.13. O subespaço $U_n(K)$ é uma subálgebra de $M_n(K)$. O subespaço I de $U_n(K)$ que consiste das matrizes em que todos os elementos da diagonal são 0 é um ideal bilateral (e próprio) de $U_n(K)$ (mas não de $M_n(K)$).

Exemplo 1.1.14. O subespaço $sl_n(K)$ das matrizes $n \times n$ e traço nulo é uma subálgebra de $gl_n(K)$. Notemos que ambas as álgebras são álgebras de Lie.

Exemplo 1.1.15. Seja A uma álgebra e I um ideal bilateral de A. Temos que $A/I = \{+_a(I); a \in A\}$ o espaço quociente de A por I, em que $+_a : x \in A \to a + x \in A$, possui uma estrutura natural de álgebra considerando a multiplicação $* : (+_a(I), +_b(I)) \in A/I \times A/I \to +_{ab}(I) \in A/I$ que fica bem definida, tendo em vista a bilateralidade de I e o fato de A/I ser uma partição de A.

Notação 1.1.16. *Usualmente denota-se os conjuntos (ou elementos conforme o ponto de vista) $+_a(I)$ do exemplo anterior por $a + I$ (em alguns casos costuma-se usar $\overline{a}$). A partir de agora faremos uso da notação usual.*

Exemplo 1.1.17. Seja $\{A_\gamma\}_{\gamma\in\Gamma}$ uma família de álgebras sobre um mesmo corpo. Os espaços produto (direto), $\prod_{\gamma\in\Gamma} A_\gamma$ e soma direta, $\bigoplus_{\gamma\in\Gamma} A_\gamma$ tornam-se naturalmente álgebras considerando a multiplicação coordenada a coordenada usuais. Observamos que a soma direta $\bigoplus_{\gamma\in\Gamma} A_\gamma$ de uma infinidade de álgebras unitárias não é unitária.

Exemplo 1.1.18. Sejam $(A, *_A)$ e $(B, *_B)$ duas álgebras sobre um mesmo corpo K. Sabemos que o produto tensorial $A \otimes B$ tem a estrutura de espaço vetorial. Podemos definir uma multiplicação $*$ natural em $A \otimes B$ que opera da seguinte forma nos geradores

$$(a_0 \otimes b_0) * (a_1 \otimes b_1) = (a_0 *_A a_1) \otimes (b_0 *_B b_1).$$

Assim temos que $(A \otimes B, *)$ é uma álgebra. Deste modo, o produto tensorial de duas álgebras é uma álgebra e satisfaz uma propriedade semelhante à propriedade universal do produto tensorial de espaços vetoriais. A saber, para toda aplicação bilinear $\varphi : A \times B \to C$, onde C é uma álgebra, tal que $\varphi(a *_A a', b *_B b') = \varphi(a, b) *_C \varphi(a', b')$ existe um único homomorfismo de álgebras $\overline{\varphi} : A \otimes B \to C$, tal que $\overline{\varphi}(a \otimes b) = \varphi(a, b)$.

Exemplo 1.1.19. É bem conhecido que como K é corpo, toda álgebra de Lie é isomorfa a uma subálgebra de alguma álgebra de Lie do tipo $A^{(-)}$, onde A é associativa. Esta afirmação é conhecida como Teorema de Poincaré–Birkhoff–Witt. Considerando-se álgebras de Jordan, isso deixa de ser verdadeiro. As álgebras de Jordan que são subálgebras de $A^{(+)}$ são chamadas de **especiais**, e as demais **excepcionais**.

Exemplo 1.1.20. Álgebra de Grassmann. Seja V um espaço vetorial de dimensão infinita, com base ordenada enumerável $\{e_i\}_{i \in \mathbb{N}}$. Definimos a álgebra de Grassmann ou álgebra exterior de V, denotada por E, como sendo a álgebra associativa com base, como espaço vetorial, consistente dos produtos $D = \{1\} \cup \{e_{i_1}e_{i_2}\ldots e_{i_k}; i_1 < i_2 < \ldots < i_k,\ k \geqslant 1\}$ e satisfazendo as relações $e_i^2 = 0$ e $e_ie_j = -e_je_i$ para quaisquer $i,\ j \in \mathbb{N}$. Sejam E_0 e E_1 os subespaços vetoriais de E gerados pelos conjuntos $D_0 = \{1\} \cup \{e_{i_1}e_{i_2}\ldots e_{i_m}; m \text{ par}\}$, e $D_1 = \{\ e_{i_1}e_{i_2}\ldots e_{i_k}; k \text{ ímpar}\}$, respectivamente. É fácil ver que

$$(e_{i_1}\ldots e_{i_m})(e_{j_1}\ldots e_{j_k}) = (-1)^{mk}(e_{j_1}\ldots e_{j_k})(e_{i_1}\ldots e_{i_m}),$$

para quaisquer $m,\ k \in \mathbb{N}$, e assim podemos concluir que $g_0x = xg_0$ para quaisquer $g_0 \in E_0$ e $x \in E$, e $g_1g_2 = -g_2g_1$ para quaisquer $g_1,\ g_2 \in E_1$.

Além disso, se V_n é o subespaço vetorial de V gerado por $\{e_i\}_{i \in I_n}$ denotaremos por $E(V_n)$ sua álgebra de Grassmann correspondente.

Exemplo 1.1.21. Centro de uma álgebra. Sendo A uma álgebra, o conjunto

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

é uma subálgebra de A, chamada de centro de A. No exemplo anterior, $Z(E) = E_0$, se $\operatorname{char} K \neq 2$. Se $\operatorname{char} K = 2$, então a álgebra E é comutativa e neste caso $Z(E) = E$.

Exemplo 1.1.22. Um exemplo importante de produto tensorial de álgebras é a álgebra $E \otimes E$, onde E é a álgebra de Grassmann (construída sobre um espaço vetorial de dimensão infinita e enumerável).

Exemplo 1.1.23. Seja A uma álgebra. Podemos definir uma álgebra de matrizes $n \times n$ com entradas em A, $M_n(A) = \{a : I_n \times I_n \to A\}$ sobre o mesmo corpo, definindo a soma e o produto por escalar coordenada a coordenada, e definindo a multiplicação $*$ da seguinte forma

$$(a * b)(i, j) = \sum_{k=1}^{n} a(i, k)b(k, j).$$

Exemplo 1.1.24. Álgebras de matrizes com entradas na álgebra de Grassmann. Um exemplo importante é $M_n(E)$, a álgebra das matrizes $n \times n$ com entradas na álgebra de Grassmann E, munido com a multiplicação definida no exemplo anterior. Sejam a, $b \in \mathbb{N}$ com $a + b = n$, mostra-se facilmente que o subespaço de $M_{a+b}(E)$ das matrizes da forma

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}, \text{ onde } A \in M_a(E_0), B \in M_{a\times b}(E_1), C \in M_{b\times a}(E_1), D \in M_b(E_0),$$

é uma subálgebra de $M_{a+b}(E)$. Denotaremos tal subálgebra por $M_{a,b}(E)$.

Definição 1.1.25. *Um homomorfismo de álgebras $\varphi : A \to B$ é dito:*

- ***monomorfismo**, se* $\ker(\varphi) = \{0\}$*;*
- ***epimorfismo**, se $Im(\varphi) = B$;*
- ***isomorfismo**, se é monomorfismo e epimorfismo. Neste caso denotamos $A \cong B$;*
- ***endomorfismo**, se $B = A$;*
- ***automorfismo**, se é isomorfismo e endomorfismo.*

Exemplo 1.1.26. Seja A uma álgebra. Considere $A^{op} = A$, como espaço vetorial. Definimos em A^{op} a multiplicação $*$ como $a * b = b *_A a$, para todo $a, b \in A^{op}$. Dessa forma, A^{op} é uma álgebra, chamada de *álgebra oposta de A*. É imediato que $A^{op} \cong A$.

Exemplo 1.1.27. Da propriedade universal de produto tensorial conclui-se facilmente que $M_n(A) \cong M_n(K) \otimes A$. Em particular, notamos que $M_n(E) \cong M_n(K) \otimes E$ e também que se L é uma extensão do corpo K então $M_n(L) \cong M_n(K) \otimes L$, onde consideramos L como sendo uma K-álgebra.

Vale um resultado análogo ao Teorema dos Isomorfismos para anéis, grupos e espaços vetoriais, o qual também chamaremos de Teorema dos Isomorfismos. A sua demonstração é análoga em todos estes casos.

Teorema 1.1.28. ***Teorema dos Isomorfismos*** *Seja* $\varphi : R_1 \longrightarrow R_2$ *um homomorfismo de álgebras. Então* $\ker(\varphi)$ *é um ideal bilateral de* R_1 *e a álgebra quociente* $R_1/\ker(\varphi)$ *é isomorfa à* $Im(\varphi)$*.*

1.1.2 Álgebras Livres, Identidades Polinomiais e PI-Álgebras

Nesta seção definiremos as Álgebras Livres, que são importantes, pois são o "ambiente" onde são introduzidos o conceito de identidades polinomiais, através do qual definimos a classe das álgebras com identidades polinomiais. Começaremos com a definição de Álgebras Livres.

Definição 1.1.29. *Seja* $\mathcal{B}$ *uma classe de álgebras e* $F \in \mathcal{B}$ *uma álgebra gerada por um conjunto* X*. A álgebra* F *é dita livre na classe* $\mathcal{B}$*, livremente gerada pelo conjunto* X*, se satisfaz a seguinte propriedade universal: Para toda álgebra* $R \in \mathcal{B}$*, qualquer aplicação* $X \to R$ *pode ser estendida a um homomorfismo* $F \to R$*. A cardinalidade* $|X|$ *do conjunto* X *será chamada de* ***posto de*** F*.*

A seguir construímos uma álgebra livre na classe das K-álgebras associativas e unitárias. Seja X um conjunto. Seja $\overline{X} = X \cup \{\phi\}$, onde $\phi \notin X$. Consideremos o conjunto

$$Pal = \{p : \mathbb{N} \to \overline{X}; p^{-1}(X) = \emptyset \text{ ou } p^{-1}(X) = I_n, \text{ para algum } n \in \mathbb{N}\},$$

também conhecido como conjunto das palavras de X e $p_0 \in Pal$ palavra constante ϕ é a palavra vazia. Agora considere $K\langle X\rangle = \{\varphi : Pal \to K; \varphi \text{ tem suporte finito}\}$ (lembramos que o suporte de φ é o conjunto $\varphi^{-1}(\{0\}^c)$) é um espaço vetorial com base as funções característica de apenas um elemento de Pal. Em especial, a função característica da palavra vazia será denotada por 1. Outra forma de descrever isto: uma palavra é uma sequência $x_{i_1}x_{i_2}\dots x_{i_n}$, onde $n \in \mathbb{N}$ e $x_{i_j} \in X$. A palavra vazia será denotada por 1. Denotaremos por $K\langle X\rangle$ o espaço vetorial que tem como base o conjunto de todas as palavras sobre X. Assim, os elementos de $K\langle X\rangle$ são somas (formais) de termos que são produtos (formais) de um escalar por uma palavra em X.

Definição 1.1.30. *Os elementos $x \in X$ são chamados de **variáveis**, os produtos (formais) de um escalar não nulo de K por uma palavra são chamados de **monômios** (no primeiro formato apresentado são as funções que atribuem a uma palavra um elemento não nulo de K e às demais palavras 0, ou seja, múltiplos não nulos das funções característica de apenas um elemento de Pal) e os elementos de $K\langle X\rangle$ são chamados de **polinômios**. Seja $f \in K\langle X\rangle$, dizemos que f **depende da variável** x se existe uma palavra p, tal que $x \in p(\mathbb{N})$ e $f(p) \neq 0$. Denotamos $f = f(x_1, \dots, x_n)$ se $f \in K\langle X\rangle$ não depende das variáveis distintas de $x_1, \dots, x_n$. Um monômio M tem **grau** k em x se a variável x ocorre em M exatamente k vezes, denotamos $\deg_x(M) = k$ (no primeiro formato o grau de M em x é a cardinalidade de $p^{-1}(x)$, onde p é a única palavra tal que $M(p) \neq 0$). Dizemos que dois monômios M e N tem o mesmo **multigrau** se $\deg_x(M) = \deg_x(N)$, para todo $x \in X$. Dizemos que um monômio M tem **grau total** k se $\sum_{x\in X} \deg_x(M) = k$, denotando isto por $\deg(M) = k$. Um polinômio que é soma de monômios de grau total k é dito **homogêneo de grau** k, denotaremos por $\deg(f) = k$. Um polinômio f é **homogêneo de grau** k **em** x, se todos os seus monômios tem grau k em x, denotamos este fato por $\deg_x f = k$. Dizemos que f é **multi-homogêneo**, se para cada variável x todos os seus monômios têm o mesmo grau em x. Um polinômio **linear em** x é um polinômio de grau 1 em x. Se f é linear em toda variável da qual ele dependa, dizemos que f é **multilinear**.*

Consideremos agora em $K\langle X\rangle$ a multiplicação definida na base por

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

(no primeiro formato apresentado definimos primeiro a multiplicação das palavras p e q,

$$pq(t) := \begin{cases} p(t) & \text{, se } t \in p^{-1}(X) \\ q(t-n) & \text{, onde } n = |p^{-1}(X)|\text{, caso contrário} \end{cases}$$

e depois a multiplicação da função característica de p pela função característica de q, que é a função característica de pq).

Munido deste produto, $K\langle X\rangle$ é uma álgebra associativa, com unidade, que é a palavra vazia, o 1. A proposição a seguir garante que $K\langle X\rangle$ é livre na classe das álgebras associativas com unidade.

Proposição 1.1.31. *A álgebra $K\langle X\rangle$ é livre na classe das álgebras associativas com unidade.*

Demonstração. Para ver isto considere A uma álgebra associativa com unidade e $h : X \longrightarrow A$ uma aplicação qualquer, para cada $x \in X$ denotaremos por a_x a imagem de x por h. Consideremos agora a aplicação linear $\varphi_h : K\langle X\rangle \longrightarrow A$ tal que $\varphi_h(1) = 1_A$ e $\varphi(p) = a_{p_1}a_{p_2}\ldots a_{p_n}$, onde $p : j \in \mathbb{N} \mapsto p_j \in \overline{X}$ é uma palavra com $p^{-1}(X) = I_n$ (lembre que $\overline{X} = X \cup \{\phi\}$ e $\phi \notin X$). Ela é bem definida, pois está definida na base de $K\langle X\rangle$. Além disso é fácil ver que φ_h é um homomorfismo de álgebras e é o único satisfazendo $\varphi_h|_X = h$. $\square$

Observação 1.1.32. Este resultado é de todo interessante, pois em suma diz que para se conhecer um homomorfismo em $K\langle X\rangle$ basta conhecer como ele age em X.

Se $f = f(x_1, \ldots, x_n) \in K\langle X\rangle$, denotaremos por $f(a_1, \ldots, a_n)$ a imagem de f por φ_h. Na verdade $f(a_1, \ldots, a_n)$ é o elemento de A que se obtém substituindo x_i por a_i em f.

Observação 1.1.33. Existem várias construções deste objeto, a seguir daremos mais uma. Seja X um conjunto (não vazio) qualquer. Considerando-se

$$V = \{f : X \to K \text{ de suporte finito}\},$$

temos que V é um K-espaço vetorial (lembre que K é corpo), com base de mesma cardinalidade de X, a saber as funções características χ_p de um único elemento $p \in X$. Ponha $T(V)^1 := V$ e defina indutivamente os espaços vetoriais $T(V)^{n+1} := T(V)^n \otimes V$ para todo $n \in \mathbb{N}$. É claro que os elementos

$$\otimes_{k\in J^{-1}(X)}\chi_{J_k} := \chi_{J_1} \otimes \cdots \otimes \chi_{J_n},$$

onde $J : k \in I_n \mapsto J_k \in X$ formam uma base para $T(V)^n$. Agora $T(V) := \bigoplus_{n\in\mathbb{N}} T(V)^n$ é um espaço vetorial. Também é fácil notar que os elementos $\otimes_{k\in J^{-1}(X)}\chi_{J_k}$, onde J é uma função de domínio I_n para algum $n \in \mathbb{N}$ e contradomínio X formam uma base de $T(V)$. Definimos finalmente a multiplicação em $T(V)$, $* : T(V) \times T(V) \to T(V)$ na base por

$$\otimes_{k\in J^{-1}(X)}\chi_{J_k} * \otimes_{k\in H^{-1}(X)}\chi_{H_k} := (\otimes_{k\in J^{-1}(X)}\chi_{J_k}) \otimes (\otimes_{k\in H^{-1}(X)}\chi_{H_k}) = \otimes_{k\in(J*H)^{-1}(X)}\chi_{J*H}(k),$$

onde

$$J * H(k) := \begin{cases} J(k) & \text{, se } t \in J^{-1}(X) \\ H(t-n) & \text{, onde } n = |J^{-1}(X)|\text{, caso contrário} \end{cases}.$$

Claramente essa multiplicação $*$, definida acima, é bilinear e assim $T(V)$ é álgebra, conhecida também como álgebra tensorial de V (sem unidade).

Demonstra-se facilmente que $T(V)$ é livre na classe das álgebras associativas (não necessariamente unitárias) e de posto $|X|$.

Observação 1.1.34. Podemos fazer uma "adjunção da unidade" em $T(V)$, $A = K \oplus T(V)$ e definimos no espaço vetorial A a multiplicação $*$ por $(\alpha \oplus f) * (\beta \oplus g) := \alpha\beta \oplus (\alpha g + \beta f + fg)$. Claramente $*$ é bilinear e assim A é uma álgebra com unidade (o $1 \oplus 0$). Mostra-se que $(A, *)$ é uma álgebra livre na classe das álgebras associativas com unidade e de posto $|X|$. Com estas informações, lembrando que as álgebras associativas constituem uma variedade, utilizando o Teorema 1.1.66, temos que A é isomorfa a $K\langle X\rangle$.

De agora em diante, a menos que se diga algo em contrário X denota um conjunto enumerável $X = \{x_1, x_2, \dots\}$.

Definição 1.1.35. *Seja A uma álgebra associativa. Um polinômio $f(x_1, \dots, x_n) \in K\langle X\rangle$ (ou a própria expressão $f(x_1, \dots, x_n) = 0$) é dito ser uma* ***identidade polinomial*** *de A se $f(a_1, \dots, a_n) = 0$ para quaisquer $a_1, \dots, a_n \in A$. Neste caso diremos que A* ***satisfaz a identidade*** *$f(x_1, \dots, x_n) = 0$. Denotaremos por $T(A)$ o conjunto de todas as identidades polinomiais de A. Dizemos A é uma* ***álgebra com identidade polinomial*** *ou* ***PI-álgebra*** *se $T(A) \neq \{0\}$. Se A_1 e A_2 são álgebras associativas, dizemos que A_1 e A_2 são* ***PI-equivalentes*** *se $T(A_1) = T(A_2)$.*

Observação 1.1.36. Claramente esta definição pode ser estendida, considerando-se apenas A álgebra, e considerando-se as identidades polinomiais em $K\{X\}$, a álgebra unitária livre dos polinômios não associativos, ou até mesmo no espaço vetorial dos polinômios em $K\{X\}$ com componente homogênea no grau total zero sendo nula (a álgebra livre). Justificamos nossa definição restrita pelo problema que estamos interessados e também porque na maioria das bibliografias tratam-se apenas as identidades polinomiais no contexto associativo. Assim, a partir de agora sempre vamos considerar as álgebras associativas e unitárias, salvo menção em contrário.

Observação 1.1.37. Não é difícil ver que $f = f(x_1, \dots, x_n)$ é uma identidade de A se, e somente se, f pertence aos núcleos de todos os homomorfismos de $K\langle X\rangle$ em A.

Exemplo 1.1.38. A álgebra $K\langle X\rangle$ não é uma PI-álgebra na nossa definição, pois se $f \neq 0$, $f \in T(K\langle X\rangle)$ para $h : X \to K\langle X\rangle$ a inclusão, o homomorfismo induzido φ_h é a identidade de $K\langle X\rangle$ e assim $\varphi_h(f) = f \neq 0$, portanto $T(K\langle X\rangle) = \{0\}$.

Definição 1.1.39. ***Comutador (de Lie) de comprimento*** $n > 1$***.*** *O comutador (de Lie) de comprimento* $n > 1$ *é definido indutivamente por*

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

$$[x_1, x_2, \ldots, x_{n+1}] = [[x_1, x_2, \ldots, x_n], x_{n+1}].$$

Exemplo 1.1.40. Se A é uma álgebra comutativa (e associativa), então $[x_1, x_2] \in K\langle X\rangle$ é uma identidade polinomial para A. Em particular qualquer álgebra comutativa é uma PI-álgebra.

Exemplo 1.1.41. O polinômio $[x_1, x_2, x_3]$ é uma identidade polinomial da álgebra de Grassmann E. Para ver isto, basta observar que $[a, b] \in E_0 = Z(E)$ para quaisquer a, $b \in E$. Assim E é uma PI-álgebra.

Teorema 1.1.42. *(Regev, [7]) Se* A *e* B *são PI-álgebras, então* $A \otimes B$ *é PI-álgebra.*

Agora enunciaremos um teorema muito famoso na teoria de PI-álgebras, o Teorema de Amitsur–Levitzki.

Teorema 1.1.43. *(Teorema de Amitsur–Levitzki, [7]) A álgebra* $M_n(K)$ *satisfaz o polinômio standard de grau* $2n$

$$s_{2n}(x_1, \ldots, x_{2n}) = \sum_{\sigma \in S_{2n}} (-1)^{\sigma} x_{\sigma(1)} \ldots x_{\sigma(2n)},$$

onde S_{2n} *é o grupo das permutações de* I_{2n} *e* $(-1)^{\sigma}$ *é o sinal da permutação* σ*. Além disso, para todo* k *não satisfaz identidades da forma* s_m^k*, quando* $m < 2n$*.*

Assim, com este teorema, temos que as álgebras de matrizes $M_n(K)$ são PI-álgebras.

Sabemos que o conjunto das identidades polinomiais satisfeitas por uma determinada álgebra é um ideal de $K\langle X\rangle$. Além disso ele apresenta uma propriedade importante: esse conjunto é invariante por endomorfismos. Ideais com essa propriedade são denominados T-ideais.

Definição 1.1.44. *Dizemos que um ideal* I *de* $K\langle X\rangle$ *é um T-ideal se* $\varphi(I) \subseteq I$*, para todo* $\varphi \in \mathbf{End}(K\langle X\rangle)$*, ou equivalentemente, se* $f(g_1, \ldots, g_n) \in I$ *para quaisquer* $f(x_1, \ldots, x_n) \in I$ *e* $g_1, \ldots, g_n \in K\langle X\rangle$*.*

Proposição 1.1.45. *Se A é uma álgebra, então $T(A)$ é um T-ideal de $K\langle X\rangle$. Reciprocamente, se I é um T-ideal de $K\langle X\rangle$, então existe alguma álgebra B tal que $T(B) = I$.*

Demonstração. Sejam $\psi \in \mathbf{End}(K\langle X\rangle)$ e $f(x_1, \ldots, x_m) \in T(A)$. Denotando $\psi(x_i) = g_i(x_1, \ldots, x_{n_i})$ para todo $i \in I_m$ temos $\psi(f) = f(g_1, \ldots, g_m) \in K\langle X\rangle$. Seja $h : X \to A$ uma aplicação, φ_h o homomorfismo induzido em $K\langle X\rangle$, $\varphi_h(g_i) = g_i(h(x_1), \ldots, h(x_{n_i})) \in A$. Portanto $\varphi_h(\psi(f)) = \varphi_h(f(g_1, \ldots, g_n)) = f(\varphi_h(g_1), \ldots, \varphi_h(g_n)) = 0$. Assim $\psi(f) \in T(A)$ e $T(A)$ é T-ideal. Agora se I é T-ideal de $K\langle X\rangle$, então é fácil ver que $B = K\langle X\rangle/I$ é uma álgebra tal que $T(B) = I$. □

1.1.3 Álgebras e Geradores

Nesta seção olharemos para as álgebras do ponto de vista de geradores, com o objetivo de fixar notação. Para isso, começamos com espaços vetoriais.

Definição 1.1.46. *Seja $X \subseteq V$ um subconjunto não vazio de um espaço vetorial V. Diremos que X* gera *V se para todo $v \in V$, v é combinação linear finita de elementos de X.*

Diremos que X é linearmente dependente *se existe uma combinação linear finita não trivial de elementos de X que é nula. Caso contrário, X será dito* linearmente independente*. Caso X gera V e X é linearmente independente, X é dito uma* base de V*.*

Observação 1.1.47. É bem conhecido que espaços vetoriais possuem uma base, utilizando-se para isso o lema de Zorn. Além disso, dado um conjunto X não vazio, existe um espaço vetorial com base B de mesma cardinalidade de X. A saber,

$$K^{(X)} = \{f : X \to K; f \text{ tem suporte finito}\}$$

é um espaço vetorial com as operações usuais, e $B = \{\chi_x; x \in X\}$ é uma base, onde

$$\chi_x(y) = \begin{cases} 1, & \text{se } y = x \\ 0, & \text{caso contrário} \end{cases}.$$

Um fato importante é que para se conhecer uma transformação linear T de domínio V basta conhecer como ela age numa base de V. Em outras palavras, se X é uma base de V, dado $w : X \to W$, onde W é um espaço vetorial, existe uma única transformação linear T de V em W que estende w.

Assim, podemos dizer que X gera V, se μ é transformação linear sobrejetiva, onde

$$\begin{array}{rcl} \mu: K^{(X)} & \longrightarrow & V \\ \chi_x & \longmapsto & x \end{array}.$$

Definição 1.1.48. *Seja $X \subseteq V$ um subconjunto não vazio de um espaço vetorial V. Denotaremos o espaço vetorial gerado pelo conjunto X em V por $spanX$ e escrevemos*

$$spanX = \left\{ \sum_{x \in \alpha^{-1}(\{0\}^c)} \alpha(x)x; \alpha \in K^{(X) \setminus \{0\}} \right\} \cup \{0\}.$$

Observação 1.1.49. É fácil ver que

$$spanX = \bigcap \{W; W \text{ é subespaço vetorial de } V \text{ e } X \subseteq W\},$$

ou seja, $spanX$ é o menor subespaço vetorial de V que contém X.

Assim é imediato que $span(spanX) = spanX$. Também é imediato que $spanX = X$, se e só se, X é subespaço vetorial de V. Além disso $spanX = V$, se e só se X gera V.

Observação 1.1.50. Também é interessante observar que quando X é um subconjunto finito e não vazio de V, ou seja, $X = \{x_i\}_{i \in I_n}$ podemos simplificar a notação escrevendo

$$spanX = \left\{ \sum_{i=1}^{n} \alpha_i x_i; \text{ onde } \alpha_i \in K \right\}.$$

Agora podemos fazer algo semelhante com álgebras.

Definição 1.1.51. *Seja $R \subseteq A$ um subconjunto não vazio de uma álgebra A. Diremos que R* gera A (como álgebra) *se para todo $a \in A$, a é combinação linear finita de produtos finitos de elementos de R. Muitas vezes diremos monômios em R, em lugar de produtos finitos de elementos de R, além disso também chamaremos de polinômios em R às combinações lineares de monômios em R.*

Diremos que R é algebricamente dependente *se existe um polinômio em R não trivial que é nulo. Caso contrário, R será dito* algebricamente independente. *Caso R gera A e R é algebricamente independente, R é dito uma* base algébrica de A.

Observação 1.1.52. De agora em diante, diremos apenas R gera A quando quisermos dizer R gera A como álgebra. Observamos que se R gera linearmente A, então R gera A como álgebra. Podemos dizer que R gera a álgebra associativa unitária A, se μ é homomorfismo(que leva unidade em unidade) sobrejetivo, onde

$$\begin{array}{rccc} \mu : & K\langle R\rangle & \longrightarrow & A \\ & \chi_p & \longmapsto & p(1)\dots p(n) \end{array},$$

onde p é uma palavra de comprimento n. Notemos que como espaços vetoriais $K\langle X\rangle = K^{(Pal)}$.

Definição 1.1.53. *Seja $R \subseteq A$ um subconjunto não vazio de uma álgebra associativa e unitária A. Denotaremos a álgebra gerado pelo conjunto R em A por $K(R)$ e escrevemos*

$$K(R) = \left\{ \sum_{p\in\alpha^{-1}(\{0\}^c)} \alpha(p)\mu(\chi_p); \alpha \in K\langle R\rangle\backslash\{\boldsymbol{0}\} \right\} \cup \{0\}.$$

Observação 1.1.54. É fácil ver que

$$K(R) = \bigcap\{B; B \text{ é subálgebra de } A \text{ e } R \subseteq B\},$$

ou seja, $K(R)$ é a menor subálgebra de A que contém R.

Assim é imediato que $K(K(R)) = K(R)$. Também é imediato que $K(R) = R$, se e só se, R é subálgebra de A. Além disso $K(R) = A$, se e só se R gera A.

Observação 1.1.55. Também é interessante observar que quando R é um subconjunto finito e não vazio de A, ou seja, $R = \{r_i\}_{i\in I_n}$ podemos simplificar a notação escrevendo

$$K(R) = \left\{ \sum_{i=1}^{k} \alpha_i r_{f_i(1)} r_{f_i(2)} \dots r_{f_i(j_i)}; \text{ onde para todo } i \in I_k, \alpha_i \in K \text{ e } f_i : I_{j_i} \to R \right\}.$$

Definição 1.1.56. *Diremos que uma álgebra A é* finitamente gerada *se existir um subconjunto finito R que gera A.*

Em particular, toda álgebra de dimensão finita é finitamente gerada, em vista da Observação 1.1.52.

Ainda podemos relacionar um pouco mais essas duas formas de "gerar".

Definição 1.1.57. *Seja $R \subseteq A$ um subconjunto não vazio de uma álgebra A. Definimos o n-ésimo span de R em A*

$$R^n = span\{monômios\ de\ comprimento\ n,\ com\ letras\ em\ R\}.$$

Em particular, $R^1 = spanR$.

Essa definição será retomada em Definição 2.2.1, quando iremos definir a dimensão de Gelfand-Kirillov.

Observação 1.1.58. Agora podemos observar que se A é uma álgebra unitária $K(R) = K \cdot 1_A + \sum_{n\in\mathbb{N}} R^n$. Além disso, quando A é uma álgebra unitária, e $1 \in R$, temos que $\sum_{n=1}^{k} R^n = R^k$.

1.1.4 Variedades e Álgebras Relativamente Livres

Nesta seção, apresentaremos os conceitos de variedades (de álgebras associativas) e de álgebras relativamente livres.

Definição 1.1.59. *Seja $\{f_i \in K\langle X\rangle; i \in I\}$ um conjunto de polinômios da álgebra associativa livre $K\langle X\rangle$. A classe $\mathcal{B}$ de todas as álgebras associativas que satisfazem as identidades $f_i = 0$, $i \in I$, é chamada de* ***variedade (de álgebras associativas) determinada pelo sistema de identidades polinomiais*** *$\{f_i \in K\langle X\rangle; i \in I\}$. A variedade $\mathcal{M}$ é chamada de* ***subvariedade*** *de $\mathcal{B}$ se $\mathcal{M} \subseteq \mathcal{B}$. O conjunto $T(\mathcal{B})$ de todas as identidades polinomiais satisfeitas por todas as álgebras da variedade $\mathcal{B}$ é denominado* ***o T-ideal de*** *$\mathcal{B}$. Dizemos que o T-ideal $T(\mathcal{B})$ é* ***gerado, como T-ideal,*** *pelo conjunto $\{f_i \in K\langle X\rangle; i \in I\}$. Usaremos a notação $T(\mathcal{B}) = \langle f_i \in K\langle X\rangle; i \in I\rangle^T$ e dizemos que o conjunto $\{f_i \in K\langle X\rangle; i \in I\}$ é uma* ***base para as identidades polinomiais de*** *$\mathcal{B}$. Os elementos de $T(\mathcal{B})$ são chamados* ***consequências*** *das identidades polinomiais da base.*

De maneira análoga define-se variedade de álgebras de Lie, de Jordan, etc.

Já vimos, na Proposição 1.1.45, que o conjunto $T(A)$ das identidades polinomiais satisfeitas por uma álgebra A é um T-ideal. Não é difícil ver que a interseção de T-ideais também é um T-ideal, e portanto o conjunto $T(\mathcal{B})$ das identidades polinomiais satisfeitas por todas as álgebras de uma variedade $\mathcal{B}$ também é um T-ideal, o que justifica termos denominado $T(\mathcal{B})$ "o T-ideal de $\mathcal{B}$".

Exemplo 1.1.60. A classe das álgebras comutativas é a variedade definida pelo conjunto $I = \{[x_1, x_2]\}$.

Exemplo 1.1.61. A classe das álgebras associativas é a variedade definida pelo conjunto $I = \emptyset$.

Um dos principais problemas na teoria das álgebras com identidades polinomiais é encontrar uma base para as identidades dessa álgebra. Esse é, em geral, um problema bastante complicado. Apenas para se ter uma ideia ainda não são conhecidas bases para as identidades polinomiais de $M_n(K)$ quando $n \geqslant 3$, nem para $M_2(K)$ (quando $|K| = \infty$ e $\operatorname{char} K$ é 2).

A seguir daremos alguns exemplos de bases para algumas das PI-álgebras.

Exemplo 1.1.62. Se K é um corpo infinito então $T(K) = \langle [x_1, x_2] \rangle^T$.

Exemplo 1.1.63. O T-ideal das identidades da álgebra de Grassmann E é gerado pela identidade $[x_1, x_2, x_3]$, quando o corpo K satisfaz $\operatorname{char} K = 0$.

Veja [7], página 50, Teorema 5.1.2 para maiores detalhes.

Exemplo 1.1.64. Se K é um corpo infinito, então

$$T(U_n(K)) = \langle [x_1, x_2][x_3, x_4] \dots [x_{2n-1}, x_{2n}] \rangle^T.$$

Veja [7], página 52, Teorema 5.2.1.

Definição 1.1.65. *Fixado um conjunto Y, a álgebra $F_Y(\mathcal{B})$ na variedade $\mathcal{B}$ é dita a álgebra relativamente livre de $\mathcal{B}$ (ou a álgebra $\mathcal{B}$-livre), se $F_Y(\mathcal{B})$ é livre na classe $\mathcal{B}$, livremente gerada por Y.*

O próximo teorema mostra que toda variedade tem uma álgebra livre e que a álgebra relativamente livre é determinada, a menos de isomorfismo, pela cardinalidade de Y.

Teorema 1.1.66. *Sejam $\mathcal{B}$ a variedade determinada pelo conjunto $\{f_i; i \in I\}$, Y um conjunto e J o ideal de $K\langle Y \rangle$ gerado por*

$$\{f_i(g_1, \dots, g_{n_i}); g_i \in K\langle Y \rangle, i \in I\}.$$

Então a álgebra $F = K\langle Y \rangle / J$ é relativamente livre em $\mathcal{B}$ com um conjunto de geradores livres $\overline{Y} = \{y + J | y \in Y\}$. E quaisquer duas álgebras relativamente livres em $\mathcal{B}$ de mesmo posto são isomorfas.

Demonstração. Veja a demonstração em [7], página 23, Proposição 2.2.5 por exemplo. □

Observação 1.1.67. Seja A uma PI-álgebra e $\mathcal{A}$ a variedade determinada por $T(A)$ (ou por A). Claramente $T(\mathcal{A}) = T(A)$. Assim, dado um conjunto Y, definimos $F_Y(A) = F_Y(\mathcal{A})$, a álgebra relativamente livre de posto $|Y|$ determinada por A. Mais ainda se $m = |Y| \in \mathbb{N}$, denotaremos por $F_m(A)$ a álgebra relativamente livre de posto m. Se Y for enumerável, escreveremos simplesmente $F(A)$.

Definição 1.1.68. *Seja $\mathcal{B}$ uma classe de álgebras. Denotaremos por $\mathcal{CB}$, $\mathcal{SB}$ e $\mathcal{QB}$ as classes obtidas de $\mathcal{B}$ tomando-se produtos diretos (somas Cartesianas), subálgebras e álgebras quocientes, respectivamente, de álgebras de $\mathcal{B}$.*

Teorema 1.1.69 (Teorema de Birkhoff)**.** *Uma classe de álgebras $\mathcal{B}$ é uma variedade se, e só se, $\mathcal{B}$ é fechada para produtos diretos, subálgebras e álgebras quocientes, isto é, $\mathcal{CB}$, $\mathcal{SB}$, $\mathcal{QB} \subseteq \mathcal{B}$.*

Demonstração. Para maiores detalhes, veja a demonstração em [7], página 24, Teorema 2.3.2. □

1.2 Álgebras Graduadas

1.2.1 Álgebras Graduadas: Conceitos Gerais

Nesta seção apresentaremos os conceitos de álgebras e identidades graduadas que são muito úteis no estudo de álgebras com identidades polinomiais. Essencialmente a graduação de álgebras é uma forma interessante de “quebrar a álgebra em pedaços”, com o intuito de facilitar a análise nos “pedaços”.

Definição 1.2.1. *Seja $(G, \star)$ um grupo. Uma álgebra $(A, *)$ é dita ser G-**graduada**, se $A = \bigoplus_{g \in G} A_g$, onde A_g é subespaço de A para todo $g \in G$ e $A_g * A_h \subseteq A_{g\star h}$ para todos g, $h \in G$. No decorrer do texto omitiremos as operações $\star$ e $*$, fazendo-se entender qual é a operação contextualmente. Um elemento $a \in \bigcup_{g \in G} A_g$ é chamado **homogêneo**. Se $a \in A_g$, dizemos que a é **homogêneo de grau** g e denotamos $wt(a) = g$. Se $a = \sum_{g\in G} a_g$, chamamos a_g de **componente homogênea de grau** g **em** a e dizemos que $\sum_{g\in G} a_g$ é a **decomposição de** a **como soma de elementos homogêneos** e cada elemento se decompõe de maneira única* *como soma de elementos homogêneos. Dizemos que um subespaço B de A é G-**graduado** na G-graduação de A, se*

$$B = \bigoplus_{g\in G} B_g, \text{ onde } B_g = B \cap A_g \text{ são os subespaços homogêneos de } B.$$

*Se um ideal I de A é um subespaço G-graduado, dizemos que I é um **ideal** G-**graduado** de A. Se uma subálgebra B de A é um subespaço G-graduado, dizemos que B é uma **subálgebra** G-**graduada** de A.*

Exemplo 1.2.2. Seja A uma álgebra. Então é fácil ver que a decomposição

$$\bigoplus_{g\in G} A_g,$$

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

Observação 1.2.3. É fácil ver que se a álgebra A é unitária, então $1 \in A_\varepsilon$. De fato, considere a decomposição da unidade em elementos homogêneos $1 = 1_\varepsilon + \sum_{g\neq\varepsilon} 1_g$. Para $x \in A_h$, $x - x1_\varepsilon = \sum_{g\neq\varepsilon} x1_g \in A_h \cap \bigoplus_{g\neq h} A_g$. Portanto $x - x1_\varepsilon = 0$, ou seja, $x1_\varepsilon = x$. Analogamente $1_\varepsilon x = x$ e assim $1 = 1_\varepsilon$.

Exemplo 1.2.4. A álgebra de Grassmann E possui uma $\mathbb{Z}_2$-graduação natural $E = E_0 \oplus E_1$, onde E_0 e E_1 são os subespaços definidos no Exemplo 1.1.20.

Exemplo 1.2.5. Consideremos

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

É imediato verificar que

$$E\otimes E = (E\otimes E)_0 \oplus (E\otimes E)_1, \qquad (E\otimes E)_i (E\otimes E)_j \subseteq (E\otimes E)_{i+j}$$

para todos i, $j \in \mathbb{Z}_2$. Portanto a álgebra $E\otimes E$ é $\mathbb{Z}_2$-graduada.

Exemplo 1.2.6. Consideremos a decomposição

$$M_{1,1}(E) = (M_{1,1}(E))_0 \oplus (M_{1,1}(E))_1$$

onde

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

e verificamos diretamente que

$$(M_{1,1}(E))_i (M_{1,1}(E))_j \subseteq (M_{1,1}(E))_{i+j} \text{ para todos } i, j \in \mathbb{Z}_2.$$

Assim essa decomposição é uma $\mathbb{Z}_2$-graduação para $M_{1,1}(E)$

Exemplo 1.2.7. Sejam $X = \{x\}$ e $K\langle X \rangle = K[x]$ a álgebra dos polinômios a uma variável x sobre K. Então $K[x]$ admite uma $\mathbb{Z}$-graduação: $K[x]_n$ é o espaço gerado por x^n, quando $n \geqslant 0$, e $K[x]_n = 0$ se $n < 0$.

Se X for um conjunto finito de m elementos, podemos considerar uma $\mathbb{Z}^m$-graduação usando os espaços de multigrau homogêneo. Para um conjunto X podemos considerar uma $\mathbb{Z}$-graduação levando em conta o grau total.

Exemplo 1.2.8 ((sobre a descrição de álgebras $\mathbb{Z}_2$-graduadas), veja [11] página 21.)**.** Seja A uma álgebra sobre um corpo K algebricamente fechado e de char $K \neq 2$, e $\dim_K(A) < \infty$. Um resultado clássico de C. T. C. Wall descreve as possíveis $\mathbb{Z}_2$-graduações de A supondo-se que A seja $\mathbb{Z}_2$-simples (isto é, os dois únicos ideais homogêneos são 0 e A e $A^2 \neq 0$). A menos de isomorfismo graduado (definiremos em breve), A tem de ser uma das seguintes álgebras:

1. $A = M_n(K)$ com a graduação trivial $A_0 = A$ e $A_1 = 0$;

2. $A = M_{a+b}(K)$ é dividida em 4 blocos, sendo os blocos da diagonal de tamanhos $a \times a$ e $b \times b$. Neste caso
$$A_0 = \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix}, A_1 = \begin{pmatrix} 0 & W \\ T & 0 \end{pmatrix},$$
onde $U \in M_a(K)$, $V \in M_b(K)$, $W \in M_{a\times b}(K)$ e $T \in M_{b\times a}(K)$;

3. $A = M_n(K) \oplus tM_n(k)$, onde $A_0 = M_n(K)$ e $A_1 = tM_n(K)$ e t é um elemento tal que $t^2 = 1$.

Exemplo 1.2.9. Seja $M_n(K)$ a álgebra das matrizes quadradas de ordem n sobre um corpo K. Denotemos por $E_{ij} : (k, l) \in I_n \times I_n \mapsto \delta_{ik}\delta_{jl} \in K$, as matrizes "unitárias". Para cada

$\gamma \in \mathbb{Z}_n$, definimos o subespaço $M_\gamma = span\{E_{ij}; j - i \equiv_n \gamma\}$ e para cada $k \in \mathbb{Z}$, definimos

$$M_k = \begin{cases} \{0\} & , \text{ se } |k| \geqslant n, \\ span\{E_{ij}; j - i = k\} & , \text{ se } |k| < n. \end{cases}$$

É fácil ver que

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

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

$$E_{ij}E_{kl} = \delta_{jk}E_{il},$$

donde segue que $M_{\gamma_1}M_{\gamma_2} \subseteq M_{\gamma_1+\gamma_2}$ para γ_1, $\gamma_2 \in \mathbb{Z}_n$, e $M_{k_1}M_{k_2} \subseteq M_{k_1+k_2}$ para k_1, $k_2 \in \mathbb{Z}$.

Nas graduações definidas em $M_n(K)$ no Exemplo 1.2.9 acima as matrizes elementares são homogêneas. Mais ainda, $E_{ij} \in M_{j-i}$, tanto para $i, j \in \mathbb{Z}_n$, como para $i, j \in \mathbb{Z}$.

Definição 1.2.10. *A G-graduação*

$$R = M_n(K) = \bigoplus_{g \in G} R_g$$

na álgebra das matrizes $n \times n$ sobre um corpo K é dita ***elementar*** *se existe uma n-upla $(g_1, \ldots, g_n) \in G^n$ tal que $E_{ij} \in R_{g_i^{-1}g_j}$.*

Exemplo 1.2.11. A $\mathbb{Z}_n$-graduação e a $\mathbb{Z}$-graduação definidas do Exemplo 1.2.9 são elementares.

Observação 1.2.12. Observamos que uma graduação em $M_n(K)$ é elementar se, e somente se, todas E_{ij} são homogêneas. De fato, se a graduação é elementar é óbvio que todas E_{ij} são homogêneas.

Agora se todas E_{ij} são homogêneas, $E_{ij} \in R_{h_{ij}}$ e $E_{ik} = E_{ij}E_{jk} \in R_{h_{ik}} \cap (R_{h_{ij}}R_{h_{jk}}) \subseteq R_{h_{ik}} \cap R_{h_{ij}h_{jk}}$ nos dá que $h_{ik} = h_{ij}h_{jk}$. Para $j = i$, obtemos $h_{ik} = h_{ii}h_{ik}$, donde $h_{ii} = \varepsilon$, onde ε é o elemento neutro de G. Ponha $g_1 = \varepsilon$, e defina indutivamente $g_{j+1} = g_j h_{j,j+1}$. Agora faremos indução duas vezes em j e em i. Primeiro $h_{11} = \varepsilon = g_1^{-1}g_1$. O passo indutivo de j segue de $h_{1,j+1} = h_{1j}h_{j,j+1} = g_1^{-1}g_j h_{j,j+1} = g_1^{-1}g_{j+1}$. Com isso temos que $h_{1j} = g_1^{-1}g_j$ para todo j. E finalmente, o passo indutivo de i segue de $h_{i+1,j} = h_{i,i+1}^{-1}h_{ij} = h_{i,i+1}^{-1}g_i^{-1}g_j = (g_i h_{i,i+1})^{-1}g_j = g_{i+1}^{-1}g_j$. Assim, existe uma n-upla $(g_1, \ldots, g_n)$, tal que $E_{ij} \in R_{h_{ij}} = R_{g_i^{-1}g_j}$ e a graduação é elementar.

A seguir damos uma caracterização bastante útil dos subespaços G-graduados de uma álgebra G-graduada.

Lema 1.2.13. *Sejam A uma álgebra G-graduada e B um subespaço de A. As seguintes afirmações são equivalentes:*

(1) B é subespaço G-graduado de A;

(2) As componentes homogêneas de cada elemento de B pertencem a B;

(3) B é gerado como espaço vetorial por elementos homogêneos.

Demonstração. Suponha que vale (1). Seja $b \in B$ e $b = \sum_{g\in G} b_g$, onde $b_g \in B_g$. Temos que b_g é a componente homogênea de grau g em b. Como $B_g \subseteq B$, cada b_g pertence a B

Se vale (2) então o conjunto $B \cap (\bigcup_{g\in G} A_g)$ gera B, e segue (3). De fato, seja $b \in B$ e $b = \sum_{g\in G} b_g$, onde $b_g \in A_g$, a decomposição de b como soma de elementos homogêneos, em relação a G-graduação de A. Segue de (2) que $b_g \in B$, ou seja $b_g \in B \cap (\bigcup_{g\in G} A_g)$, logo B é gerado por elementos homogêneos.

Suponha que vale (3). Seja C uma base de B, $C \subseteq (\bigcup_{g\in G} A_g)$ composta de elementos homogêneos e seja $B_g = B \cap A_g$, que é um espaço vetorial. Seja $C_g = C \cap A_g$. Agora seja o elemento $b = \sum_{i=1}^{n} \lambda_i c_i$, onde $c_i \in C$ e $\lambda_i \neq 0$. $b \in B_g$ se, e somente se, $wt(c_i) = g$, para todo $i \in I_n$. Assim $C_g = C \cap A_g$ é uma base para B_g e como $C = \bigcup_{g\in G} C_g$ segue que $B = \bigoplus_{g\in G} B_g$ e o lema está provado. $\square$

Exemplo 1.2.14. Se consideramos $M_n(K)$ com qualquer uma das graduações definidas no Exemplo 1.2.9, então é fácil ver que a álgebra $U_n(K)$ das matrizes triangulares superiores é subálgebra homogênea de $M_n(K)$, já que é gerada pelos elementos homogêneos $\{E_{ij}; i \leqslant j\}$.

Definição 1.2.15. *Uma aplicação $\Phi : A \to B$ entre álgebras G-graduadas é chamada* ***homomorfismo G-graduado****, se Φ é um homomorfismo que satisfaz $\Phi(A_g) \subseteq B_g$ para todo $g \in G$. De modo análogo, definimos* ***isomorfismo, endomorfismo*** *e* ***automorfismo G-graduado****. Agora também estamos aptos a dar outras caracterizações dos ideais e das subálgebras. I é ideal G-graduado de A se I é núcleo de algum homomorfismo G-graduado com domínio A. C é subálgebra G-graduada de B quando C é imagem de algum homomorfismo G-graduado de contradomínio B.*

Proposição 1.2.16. *Se I é um ideal G-graduado de uma álgebra G-graduada A, então A/I é uma álgebra G-graduada considerando $(A/I)_g = \{a + I; a \in A_g\}$.*

Demonstração. É claro que $A/I = \sum_{g\in G}(A/I)_g$, e que $(A/I)_g(A/I)_h \subseteq (A/I)_{gh}$. Para concluir resta mostrar que a soma é direta. Suponhamos que $\sum_{g\in G}(a_g + I) = 0$. Neste caso $\sum_{g\in G} a_g \in I$ e como I é G-graduado segue do Lema 1.2.13 que $a_g \in I$, ou seja $(a_g + I) = 0$. Assim $A/I = \bigoplus_{g\in G}(A/I)_g$ e o lema está provado. $\square$

A proposição a seguir é uma versão graduada do Teorema 1.1.28, ao longo da dissertação também iremos nos referir a ela como Teorema dos Isomorfismos.

Proposição 1.2.17. ***Teorema dos Isomorfismos*** *Sejam A e B álgebras G-graduadas e $\Phi : A \to B$ um homomorfismo G-graduado. Então, o $\ker(\Phi)$ é um ideal G-graduado de A e a álgebra quociente $A/\ker\Phi$ é isomorfa (como álgebra graduada) à $Im\Phi = \Phi(A)$.*

Demonstração. É fácil ver que $\ker(\Phi)$ é um ideal de A, vamos mostrar que ele é G-graduado. Seja $a \in \ker(\Phi)$ e $a = \sum_{g\in G} a_g$, onde $a_g \in A_g$ é a sua decomposição como soma de elementos homogêneos. Como Φ é homomorfismo graduado temos que $0 = \sum_{g\in G}(\Phi(a_g))$ e $\Phi(a_g) \in B_g$, portanto $\Phi(a_g) \in \ker(\Phi)$.

A aplicação $\Psi : A/\ker\Phi \to B$ dada por $\Psi(a + \ker(\Phi)) = \Phi(a)$ está bem definida pois se a, $b \in A$ são tais que $a + \ker(\Phi) = b + \ker(\Phi)$, então $a - b \in \ker(\Phi)$ e $\Phi(a) = \Phi(b)$, ou seja $\Psi(a + \ker(\Phi)) = \Psi(b + \ker(\Phi))$. É fácil ver que Ψ é um homomorfismo graduado, assim resta apenas mostrar que Ψ é injetor. Se $\Psi(a + \ker(\Phi)) = 0$ então $\Phi(a) = 0$ e $a \in \ker(\Phi)$, logo $a + \ker(\Phi) = 0$ e a proposição está provada. $\square$

1.2.2 Álgebras Graduadas Livres e Identidades Polinomiais Graduadas

Precisamos do conceito de álgebra associativa livre G-graduada para falar das identidades polinomiais graduadas. Consideremos uma família $\{X_g\}_{g\in G}$ de conjuntos enumeráveis e dois a dois disjuntos. Tomemos então $X = \bigcup_{g\in G} X_g$ e consideremos a álgebra associativa livre unitária $K\langle X\rangle$. Definimos agora

$$wt(1) = \varepsilon \quad \text{e} \quad wt(x_1x_2\ldots x_m) = wt(x_1)wt(x_2)\ldots wt(x_m),$$

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

$$K\langle X\rangle_g = span\{m; m \text{ é monômio de } K\langle X\rangle \ \text{ e } \ wt(m) = g\}$$

temos

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

para quaisquer g, $h \in G$, assim $K\langle X\rangle$ é uma álgebra G-graduada denominada a álgebra associativa livre (unitária) G-graduada.

Lema 1.2.18. *A álgebra G-graduada $K\langle X\rangle$ satisfaz a seguinte propriedade universal: Para toda álgebra G-graduada A, toda função $\Phi : \bigcup_{g\in G} X_g \to A$ tal que $\Phi(X_g) \subseteq A_g$, para todo $g \in G$ pode ser estendida a um único homomorfismo G-graduado de álgebras.*

Agora podemos dar a definição de identidade polinomial graduada.

Definição 1.2.19. *Seja $A = \bigoplus_{g\in G} A_g$ uma álgebra G-graduada. Dizemos que um polinômio $f(x_1, \ldots, x_n) \in K\langle X\rangle$ é uma **identidade G-graduada** de A se $f(a_1, \ldots, a_n) = 0$ para quaisquer $a_i \in A_{wt(x_i)}$ com $i \in I_n$.*

Daremos agora a definição de T_G-ideal, que é o análogo para o caso de identidades polinomiais graduadas do conceito de T-ideal.

Definição 1.2.20. *Seja $K\langle X\rangle$ a álgebra associativa livre G-graduada. Um ideal I de $K\langle X\rangle$ é dito ser um **T_G-ideal** se $\varphi(I) \subseteq I$ para todo endomorfismo G-graduado φ de $K\langle X\rangle$. Dado um subconjunto S qualquer de $K\langle X\rangle$, definimos o **T_G-ideal gerado por** S, que é denotado por $\langle S\rangle^{T_G}$, como sendo a interseção de todos os T_G-ideais de $K\langle X\rangle$ que contêm S. Quando $G = \mathbb{Z}_n$, o T_G-ideal também será denotado por T_n.*

É claro que $K\langle X\rangle$ é um T_G-ideal que contém S, assim na definição acima $\langle S\rangle^{T_G}$ é interseção de uma família não vazia de conjuntos, além disso não é difícil ver que a interseção de uma família qualquer de T_G-ideais é ainda um T_G-ideal, portanto $\langle S\rangle^{T_G}$ está bem definido e é o menor T_G-ideal que contém S.

O T_G-ideal gerado por S coincide com o subespaço vetorial de $K\langle X\rangle$ gerado pelo conjunto

$$\begin{aligned}\{h_1 f(g_1, \ldots, g_n) h_2 \quad ; \quad & f(x_1, \ldots, x_n) \in S \ , \ h_1, h_2, g_1, \ldots, g_n \in K\langle X\rangle, \\ & wt(g_1) = wt(x_1), \ldots, wt(g_n) = wt(x_n)\}.\end{aligned}$$

A proposição a seguir é bastante útil, sua demonstração é simples e por isso será omitida.

Proposição 1.2.21. *Sendo A uma álgebra G-graduada, temos que o conjunto $T_G(A)$ das identidades G-graduadas de A é um T_G-ideal de $K\langle X\rangle$.*

Exemplo 1.2.22. Consideremos a álgebra de Grassmann E com sua $\mathbb{Z}_2$-graduação natural (conforme definida no Exemplo 1.2.4). Como $ab = -ba$ para quaisquer elementos a, $b \in E_1$, temos que $f(x_1, x_2) = x_1x_2 + x_2x_1 \in K\langle X\rangle$, onde $K\langle X\rangle$ é a álgebra livre $\mathbb{Z}_2$-graduada, com $wt(x_1) = wt(x_2) = 1$, é identidade $\mathbb{Z}_2$-graduada de E.

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

Proposição 1.2.23. *Sejam A e B duas álgebras. Se A e B possuem G-graduações tais que $T_G(A) \subseteq T_G(B)$, então $T(A) \subseteq T(B)$. Ademais, se $T_G(A) = T_G(B)$, então $T(A) = T(B)$.*

Demonstração. Consideremos a álgebra associativa livre $K\langle X\rangle$ e seja $f(x_1, x_2, \ldots, x_n) \in T(A)$. Dados b_1, b_2, $\ldots$, $b_n \in B$, tomemos $b_{ig} \in B_g$, para $i = 1$, $\ldots$, n e uma quantidade finita de $g \in G$, tais que $b_i = \sum b_{ig}$, ou seja b_i é uma soma finita de b_{ig}. Consideremos agora, com i fixado, $\sum x_{ig}$, em que $x_{ig} \in X_g$ e o somatório é sobre o mesmo conjunto finito de índices do somatório $b_i = \sum b_{ig}$. Como $f \in T(A)$, é fácil ver que $f_1 = f(\sum x_{1g}, \ldots, \sum x_{ng}) \in T_G(A)$ Pela hipótese temos que $f_1 \in T_G(B)$, logo substituindo x_{ig} por b_{ig} temos

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

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

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

Observação 1.2.24. É importante observar que a recíproca do resultado acima é falsa. As álgebras $\mathbb{Z}_2$-graduadas $E = E_0 + E_1$ e $E = E + 0$ (graduação trivial), satisfazem identidades $\mathbb{Z}_2$-graduadas diferentes.

Definição 1.2.25. *Uma álgebra sobre K com $\operatorname{char} K \neq 2$, $\mathbb{Z}_2$-graduada A é supercomutativa, se $ab = (-1)^{wt(a)wt(b)}ba$ para todos a, $b \in A_0 \cup A_1$.*

Exemplo 1.2.26. A álgebra de Grassmann é um exemplo de álgebra supercomutativa.

Definição 1.2.27. *Seja* $K\langle X\rangle = K\langle X\rangle_0 \oplus K\langle X\rangle_1$ *a álgebra livre* $\mathbb{Z}_2$*-graduada onde* K *é um corpo com* $char\,K \neq 2$ *definida como acima. Para os monômios* $f,\, g \in K\langle X\rangle$*, consideramos as relações* $fg = (-1)^{wt(f)wt(g)}gf$ *e seja* I *o* T_2*-ideal* $\mathbb{Z}_2$*-graduado gerado por estas relações. Denotamos* $Y = X_0$ *e* $Z = X_1$*. A álgebra* $K(Y;Z) = K\langle X\rangle/I$ *é naturalmente* $\mathbb{Z}_2$*-graduada (pois herda a graduação de* $K\langle X\rangle$*) e é chamada de álgebra livre supercomutativa.*

A álgebra $K(Y;Z)$ satisfaz a seguinte propriedade universal: Para toda álgebra supercomutativa $A = A_0 \oplus A_1$, toda função $\Phi : Y \cup Z \to A$ tal que $\Phi(Y) \subseteq A_0$ e $\Phi(Z) \subseteq A_1$ pode ser estendido a um único homomorfismo de álgebras.

1.2.3 Identidades Graduadas Multilineares, Homogêneas e Próprias

Nesta seção veremos que sob determinadas condições podemos simplificar as identidades com que trabalhamos, podendo nos restringir a alguns tipos especiais de identidades.

Lema 1.2.28. *Seja* $f(x_1,\dots,x_m) = \sum_{i=0}^{n} f_i(x_1,\dots,x_m) \in K\langle X\rangle$ *onde* f_i *é a componente homogênea de* f *com grau* i *em* x_k*, fixado.*

(i) Se o corpo K *contém mais que* n *elementos, então* $f_i(x_1,x_2,\dots,x_m) \in \langle f\rangle^{T_G}$*;*

(ii) Se o corpo K *satisfaz* $char\,K = 0$ *ou maior que o grau de* f*, então* $\langle f\rangle^{T_G}$ *admite uma base composta por uma família finita de polinômios multilineares.*

Demonstração. (i) Seja $I = \langle f\rangle^{T_G}$ o T-ideal de $K\langle X\rangle$ gerado por f. Escolhemos $n+1$ elementos distintos $\alpha_0,\, \dots,\, \alpha_n$ de K. Como I é um T_G-ideal, obtemos que

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

Consideramos estas equações como um sistema linear com incógnitas $f_0, f_1, \dots, f_n$. Como o determinante do sistema

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

é o determinante de Vandermonde que é diferente de 0, temos que cada $f_i(x_1, x_2, \ldots, x_m) \in I$, isto é, as identidades $f_i = 0$ são consequências de $f = 0$.

(ii) Por (i), podemos assumir que $f(x_1, x_2, \ldots, x_m)$ é multi-homogêneo. Seja $j = \deg_{x_1} f$. Faremos indução sobre j. Escrevemos $f(y_1+y_2, x_2, \ldots, x_m) \in I = \langle f \rangle^{T_G}$ (aqui $y_1, y_2 \in X_{wt(x_1)}$) sob a forma

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

onde f_i é a componente homogênea de grau i em y_1. Logo, $f_i \in I$ para $i = 0, 1, \ldots, j$. Como $\deg_{y_k} f_i < j$; $i = 1, 2, \ldots, j-1$; $k = 1, 2$, podemos aplicar argumentos indutivos e obtemos um conjunto de consequências multilineares de f. Para ver que estas identidades multilineares são uma base para $\langle f \rangle^{T_G}$ é suficiente observarmos que

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

e que o coeficiente binomial é diferente de 0, pois temos por hipótese que $\operatorname{char} K = 0$ ou $\operatorname{char} K > \deg(f)$. □

Corolário 1.2.29. *Seja A uma álgebra. Então,*

(i) Se o corpo K é infinito, todas identidades polinomiais graduadas de A seguem de suas identidades graduadas multi-homogêneas;

(ii) Se o corpo K satisfaz $\operatorname{char} K = 0$, todas as identidades polinomiais graduadas de A seguem de suas identidades multilineares graduadas.

Neste momento podemos dar mais alguns exemplos de álgebras que não são PI-álgebras.

Exemplo 1.2.30. Seja V um espaço vetorial de base enumerável $\{v_i\}_{i \in \mathbb{N}}$ sobre um corpo K com $\operatorname{char} K = 0$. Seja $\mathcal{L}$ o espaço vetorial das transformações lineares de V em V, ou seja, os endomorfismos. Temos que $\mathcal{L}$ se torna uma álgebra quando equipada com a multiplicação dada pela composição. Ela é unitária e associativa. Considere o subespaço $\mathcal{L}' \subseteq \mathcal{L}$ dos endomorfismos de posto finito (cuja imagem tem dimensão finita). Ele também é uma álgebra com a multiplicação dada pela composição, é uma álgebra associativa embora não seja unitária. Assim, $\mathcal{L}'$ pode ser visto como uma subálgebra de $\mathcal{L}$, desde que se esqueça que $\mathcal{L}$ é unitária. Temos que tanto $\mathcal{L}'$, quanto $\mathcal{L}$ não são PI-álgebras. Caso fossem PI-álgebras, deveriam satisfazer algum polinômio multilinear de grau digamos d ($d \geqslant 1$), sem perda de generalidade podemos escrever a relação satisfeita da seguinte forma

$$x_1 \dots x_d = \sum_{\sigma \in S_d \setminus \{\varepsilon\}} x_{\sigma(1)} \dots x_{\sigma(d)}.$$

Considere $\varphi_{(i,j)}$ o endomorfismo tal que $\varphi_{(i,j)}(v_k) = \delta_{jk} v_i$ para todo i, j e $k \in \mathbb{N}$. Temos que $\varphi_{(i,j)} \in \mathcal{L}'$. No entanto,

$$0 \neq \varphi_{(1,d+1)} = \varphi_{(1,2)} \cdots \varphi_{(d,d+1)} = \sum_{\sigma \in S_d \setminus \{\varepsilon\}} \varphi_{(\sigma(1),\sigma(1)+1)} \cdots \varphi_{(\sigma(d),\sigma(d)+1)} = 0,$$

o que é absurdo. Logo nem $\mathcal{L}$, nem $\mathcal{L}'$ são PI-álgebras.

Quando a álgebra é unitária podemos restringir a nossa busca de identidades polinomiais a um determinado tipo de polinômios (polinômios próprios), conforme explicamos a seguir. No que segue, $Y = X_\varepsilon$ e $Z = \bigcup_{g \neq \varepsilon} X_g$, assim $X = Y \cup Z$. As variáveis de grau ε serão denotas por y_i, $i \in \mathbb{N}$; as variáveis de grau diferente de ε serão denotadas por z_j, $j \in \mathbb{N}$ e quando uma variável tiver grau arbitrário será denotada por x_i, $i \in \mathbb{N}$.

Definição 1.2.31. *Um polinômio $f \in K\langle X \rangle$ é chamado **polinômio próprio**, se as variáveis de grau ε aparecem em comutadores apenas, isto é,*

$$\begin{aligned} f &= f(y_1, \dots, y_m, z_1, \dots, z_k) = f(x_1, \dots, x_n) \\ &= \sum \alpha_{i,\dots,j} z_1^{a_1} z_2^{a_2} \dots z_k^{a_k} [x_{i_1}, \dots, x_{i_p}] \dots [x_{j_1}, \dots, x_{j_q}] \ ; \ \alpha_{i,\dots,j} \in K, \end{aligned}$$

onde $a_i \in \mathbb{N}$, $1 \leqslant i \leqslant k$ e assumimos que 1 é um produto de um conjunto vazio de comutadores. Denotamos por $B_G(X)$ o conjunto de todos os polinômios próprios de $K\langle X \rangle$.

O Lema 1.2.37 mais adiante mostra a importância dos polinômios próprios para encontrar uma base das identidades de uma álgebra unitária. A demonstração está baseada no Teorema de Witt e no Teorema de Poincaré-Birkhoff-Witt. Antes de enunciá-los precisamos da definição a seguir.

Definição 1.2.32. *Se A é uma álgebra associativa e a álgebra de Lie L (não precisa ser associativa e nem unitária) é isomorfa a uma subálgebra da álgebra de Lie $A^{(-)}$, definida no Exemplo 1.1.8, dizemos que A é uma **álgebra envolvente** de L. A álgebra associativa $U = U(L)$ é a **álgebra envolvente universal da álgebra de Lie** L, se L é uma subálgebra* *de $U^{(-)}$ e U satisfaz a seguinte propriedade universal: Para qualquer álgebra associativa A e qualquer homomorfismo de álgebras de Lie $\varphi : L \to A^{(-)}$ existe um único homomorfismo de álgebras associativas (que leva unidade em unidade) $\psi : U \to A$ que estende φ, ou seja, tal que $\psi(x) = \varphi(x)$ para todo $x \in L$.*

O teorema a seguir garante que toda álgebra de Lie possui uma álgebra envolvente universal, que é única a menos de isomorfismos. Recordamos que no início deste capítulo fizemos um comentário que toda álgebra de Lie L é isomorfa a uma subálgebra de alguma álgebra $A^{(-)}$, para alguma álgebra associativa.

Teorema 1.2.33. ***Teorema de Poincaré-Birkhoff-Witt*** *Toda álgebra de Lie L possui uma única (a menos de isomorfismo) álgebra envolvente universal $U(L)$. Se L tem uma base $E = \{e_i; i \in I\}$, onde I é um conjunto ordenado, então $U(L) = K\langle E\rangle/J$, onde J é o ideal de $K\langle E\rangle$ gerado pelos polinômios $[e_i, e_j] - e_i * e_j$ (símbolo $*$ denota a multiplicação em L). Além disso, os elementos*

$$\{e_{i_1} \dots e_{i_p}; i_1 \leqslant \dots \leqslant i_p, p = 1, 2, \dots\} \cup \{1\},$$

formam uma base de $U(L)$.

Demonstração. Veja a demonstração em [7], Teorema 1.3.1, página 11, por exemplo. □

Para álgebras de Jordan não temos algo desse tipo, como já comentamos.

Exemplo 1.2.34. Apenas para ilustrar, daremos um exemplo de álgebra de Jordan excepcional. Seja $\mathbb{C}$ o corpo dos complexos, que agora olhamos como $\mathbb{R}$-álgebra. Denotaremos por $\mathbb{H}$ a álgebra dos quatérnios, que é o conjunto $\mathbb{C} \times \mathbb{C}$ equipado com soma usual, coordenada a coordenada, e a multiplicação

$$(a, b) * (c, d) = (ac - \overline{d}b, da + b\overline{c}),$$

onde $\overline{x}$ denota a conjugação complexa. Claramente $\mathbb{H}$ é uma álgebra associativa unitária ($1_{\mathbb{H}} = (1_{\mathbb{C}}, 0)$), não comutativa, com divisão, isto é, para todo (a, b) existe (c, d), tal que $(a, b) * (c, d) = (1, 0) = (c, d) * (a, b)$.

Definimos a conjugação nos quatérnios por $\overline{(a, b)} = (\overline{a}, -b)$.

Denotaremos por $\mathbb{O}$ a álgebra dos octônios, que é o conjunto $\mathbb{H} \times \mathbb{H}$ equipado com soma usual, coordenada a coordenada, e a multiplicação

$$(p, q) * (r, s) = (pr - \overline{s}q, sp + q\overline{r}),$$

onde $\overline{x}$ denota a conjugação nos quatérnios definida acima. Claramente $\mathbb{O}$ é uma álgebra não associativa unitária, não comutativa, com divisão, isto é, para todo (p,q) existe (r,s), tal que $(p,q)*(r,s)=(1,0)=(r,s)*(p,q)$.

Defina a conjugação nos octônios por $\overline{(p,q)}=(\overline{p},-q)$.

Seja agora a álgebra $M_3(\mathbb{O})$. O conjunto J das matrizes auto-adjuntas de $M_3(\mathbb{O})$ é uma subálgebra de $(M_3(\mathbb{O}))^+$, que é uma álgebra de Jordan excepcional [Jordan, Neumann & Wigner] (1934).

Teorema 1.2.35. ***Teorema de Witt*** *A subálgebra de Lie $L(X)$ de $K\langle X\rangle^{(-)}$ gerada por X (isto é, $L(X)$ é a interseção de todas as álgebras de Lie que contém X), é livre na classe das álgebras de Lie. Além disso $U(L(X))=K\langle X\rangle$.*

Demonstração. Consulte a demonstração em [7], Teorema 1.3.5, página 14, por exemplo. □

Agora vamos utilizar estes dois teoremas para encontrar uma base de $K\langle X\rangle$ que será bastante útil.

Proposição 1.2.36. *Suponhamos que os elementos*

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

formam uma base ordenada de $L(X)$ onde os elementos $x_1, x_2, \ldots$ precedem os comutadores. Então

(i) O espaço vetorial $K\langle X\rangle$ tem base formada pelos elementos

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

onde $a_1\ldots,a_m,b,\ldots,c\geqslant 0$ e $[x_{i_1},x_{i_2}]<\cdots<[x_{l_1},\ldots,x_{l_p}]$, na ordenação da base de $L(X)$;

(ii) Os elementos desta base tais que $a_i=0$ sempre que $wt(x_i)=\varepsilon$, $1\leqslant i\leqslant m$, formam uma base para $B_G(X)$.

Demonstração. O item (i) segue do Teorema de Witt que garante que $U(L(X))=K\langle X\rangle$, e do Teorema de Poincaré-Brirkhoff-Witt, que nos diz como encontrar uma base para $U(L(X))$ a partir de uma base ordenada de $L(X)$. O item (ii) segue diretamente do item (i) e da definição de $B_G(X)$. □

A seguir utilizaremos a base de $K\langle X\rangle$ dada na proposição anterior para provar que quando o corpo é infinito as identidades graduadas de uma álgebra unitária seguem de suas identidades próprias. Para isto será necessário utilizar o seguinte fato: Se A é uma álgebra G-graduada, então sua unidade é homogênea de grau ε. Isto já foi observado em Observação 1.2.3.

Lema 1.2.37. *Se A é uma álgebra unitária G-graduada sobre um corpo infinito K, então todas as identidades polinomiais graduadas de A seguem das suas identidades próprias (ou seja, daquelas em $T_G(A)\cap B_G(X)$). Se $\operatorname{char} K = 0$, então todas identidades polinomiais graduadas de A seguem das suas identidades próprias multilineares.*

Demonstração. Seja $f(y_1,\ldots,y_m,z_1,\ldots,z_n)\in K\langle X\rangle$, não nulo. Pela Proposição 1.2.36 podemos escrever f como

$$f=\sum \alpha_a y_1^{a_1}\ldots y_m^{a_m} w_a(y_1,\ldots,y_m,z_1,\ldots,z_n),\quad \alpha_a\in K,$$

onde $w_a\in B_G(X)$ e a soma é feita sobre as m-uplas $a=(a_1,\ldots,a_m)$ tais que $a_i\leqslant \deg_{y_i}(f)$, $1\leqslant i\leqslant m$. Mostraremos que quando $f\in T_G(A)$, temos que

$$\sum_{a;a_1 fixado} \alpha_a y_2^{a_2}\ldots y_m^{a_m} w_a\in T_G(A).$$

O resultado seguirá indutivamente da nossa demonstração. Para cada f nessa forma, definimos o conjunto

$$\begin{aligned} M(f) &:= \{M_1,M_2,\ldots,M_l\}\\ &= \{a_1; a_1\neq 0 \text{ é o primeiro termo de uma } m\text{-upla } a=(a_1\ldots,a_m) \text{ com } \alpha_a\neq 0\},\end{aligned}$$

onde $M_1>M_2\cdots>M_l\geqslant 0$.

Afirmamos que se $f\in T_G(A)$ e f é homogêneo em y_1, então para todo $j\in I_l$,

$$g_j=\sum_{a;a_1=M_j}\alpha_a y_2^{a_2}\ldots y_m^{a_m} w_a\in T_G(A).$$

A demonstração do lema segue desta afirmação, juntamente com o Lema 1.2.28, pois se f é multi-homogêneo, então f é consequência das identidades

$$\{w_a(y_1,\ldots,y_m,z_1,\ldots,z_n);\alpha_a\neq 0\}.$$

A parte multilinear do lema segue do fato que, supondo f multilinear, temos os polinômios w_a multilineares. Agora demonstraremos a afirmação.

Se $M_1 = 0$, então não há nada a fazer, pois $f = \sum \alpha_a y_2^{a_2} \ldots y_m^{a_m} w_a \in T_G(A)$. Assim supomos $M_1 > 0$. Uma vez que em w_a as variáveis $y_1, \ldots, y_m$ aparecem apenas nos comutadores, é claro que

$$w_a(y_1 + 1, \ldots, y_m, z_1, \ldots, z_n) = w_a(y_1, \ldots, y_m, z_1, \ldots, z_n).$$

Como $wt(y_1+1) = wt(y_1) = \varepsilon$, segue que $f(y_1+1, \ldots, y_m, z_1, \ldots, z_n)$ também é identidade polinomial graduada para A e concluímos que

$$f(y_1+1, \ldots, y_m, z_1, \ldots, z_n) = \sum \alpha_a \sum_{i=0}^{a_1} \binom{a_1}{i} y_1^i y_2^{a_2} \ldots y_m^{a_m} w_a(y_1, \ldots, y_m, z_1, \ldots, z_n) \in T_G(A).$$

Observamos que no somatório acima a parcela com i fixado é a componente homogênea em relação a y_1 de grau $i + \deg_{y_1}(w_a)$.

Como f é homogêneo em y_1, $a_1 + \deg_{y_1}(w_a(y_1, \ldots, y_m, z_1, \ldots, z_n)) = \deg_{y_1}(f)$, assim a componente homogênea com menor grau em relação a y_1 é obtido das parcelas com $a_1 = M_1$ e $i = 0$ e é dada por

$$g_1 = \sum_{a; a_1 = M_1} \alpha_a y_2^{a_2} \ldots y_m^{a_m} w_a,$$

onde o sub-índice $a_1 = M_1$ no somatório significa que a soma é feita sobre os $a = (a_1 \ldots, a_m)$ tais que $a_1 = M_1$. Lembrando que o corpo K é infinito (tem mais de $\deg_{y_1}(f)$ elementos), segue do Lema 1.2.28 que o polinômio g_1 pertence a $T_G(A)$.

Suponhamos que a afirmação seja verdadeira para $1, 2, \ldots, k$, onde k é um número natural menor que l.

Tomando $g = \sum_{j=1}^{k} y_j^{M_j} g_j \in T_G(A)$ e subtraindo esta identidade de nossa identidade inicial $f(y_1, \ldots, y_m, z_1, \ldots, z_n)$ obtemos uma nova identidade

$$h(y_1, \ldots, y_m, z_1, \ldots, z_n) = \sum_{a; a_1 < M_k} \alpha_a y_1^{a_1} \ldots y_m^{a_m} w_a \in T_G(A).$$

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

$$\sum_{a; a_1 = M_{k+1}} \alpha_a y_2^{a_2} \ldots y_m^{a_m} w_a \in T_G(A),$$

e a afirmação está provada. $\square$

CAPÍTULO 2

ÁLGEBRAS FINITAMENTE GERADAS

Neste capítulo estudamos o conceito de GK-dimensão em álgebras finitamente geradas, sua relação com as PI-álgebras e a PI-equivalência (definida em Definição 1.1.35), bem como sua relação com outras dimensões algébricas. Lembramos que estamos considerando todas as álgebras associativas e neste capítulo finitamente geradas, salvo menção em contrário. Lembramos que usaremos, quando n for um número natural, I_n para denotar o subconjunto natural $\{1, 2, \ldots, n\}$.

2.1 Teorema de Shirshov

Nesta seção veremos o teorema de Shirshov que é uma ferramenta combinatória poderosa utilizada no estudo de álgebras. Consideraremos todas as álgebras arbitrárias, não precisam ser associativas e nem unitárias.

2.1.1 Teorema de Shirshov e Altura de Álgebras

Inicialmente consideremos X_m um conjunto contendo as variáveis (distintas) $x_1, \ldots, x_m$, com $m > 1$. Seja $W = \langle x_1, x_2, \ldots, x_m \rangle$ o conjunto de todos os monômios em $K\langle X_m \rangle$. W

é chamado de *semigrupo unitário livre de posto* m e é o objeto livre na classe de todos os semigrupos com unidade. Para $w = x_{i_1}x_{i_2}\dots x_{i_n} \in W$, denotaremos por $|w|$ o *comprimento* (ou grau) de w. Utilizaremos os termos palavra e monômio indistintamente.

Definição 2.1.1. *Definiremos uma ordem parcial $>$ em W:*

- *Para monômios de comprimento um, ou seja, as variáveis, $x_1 < x_2 < \cdots < x_m$;*
- *$x_{i_1}x_{i_2}\dots x_{i_p} > x_{j_1}x_{j_2}\dots x_{j_q}$ se, e só se, existe $k \geqslant 0$, tal que $i_{k+1} > j_{k+1}$ e $i_a = j_a$ para todo $a < k$.*

u e v são incomparáveis, se uma delas é o começo da outra, por exemplo, $u = v \cdot w$ com $w \neq 1$.

Um subconjunto incomparável de W é um subconjunto finito de W que contém duas palavras incomparáveis.

Definição 2.1.2. *Um monômio $w \in W$ é dito d-decomponível se ele pode ser escrito na forma*

$$w = w_0w_1\dots w_dw_{d+1},$$

(w_0 e w_{d+1} podem ser palavras vazias) e

$$w_0w_1\dots w_dw_{d+1} > w_0w_{\sigma(1)}\dots w_{\sigma(d)}w_{d+1}$$

para toda permutação não trivial, ou seja $\sigma \in S_d, \sigma \neq \varepsilon$.

Por exemplo,

$$w = (x_2x_1)(x_3x_2x_1x_2)(x_3x_1x_2)(x_4x_1) = w_0w_1w_2w_3$$

é 2-decomponível, pois

$$w_1w_2 > w_2w_1.$$

Verifica-se facilmente que esta palavra possui uma 4-decomposição

$$w = (x_2x_1)(x_3x_2x_1x_2)(x_3x_1)(x_2x_4)(x_1)().$$

Lema 2.1.3. *Se $w \in W$ é tal que $w = pq = rp$ para certas palavras não vazias p, q e r, então $w = a^n$ ou $w = (ab)^{n-1}a = abab\dots aba$ para certos $a \neq 1$ $b \neq 1$ e $n > 1$.*

Demonstração. (1) Se $|p| < |r|$, então $r = pb$ e já obtemos que $w = rp = pbp$, ou seja $w = aba$ com $a = p$.

(2) Se $|r| \leqslant |p|$, então $p = rp_1$ e $|p_1| < |p|$, pois $|r| \geqslant 1$. De $w = rp_1q = rrp_1$, obtemos $p_1q = rp_1$. Se $|r| \leqslant |p_1|$, então $p_1 = rp_2$ e $p_2q = rp_2$, com $|p_2| < |p_1|$. Continuamos esse processo até que $|p_{k+1}| < |r|$. Temos assim, $p_k = rp_{k+1}$ e $p_{k+1}q = rp_{k+1}$. Deste modo, consideremos as duas possibilidades:

- Se $p_{k+1} = 1$, então $p = r^{k+1}$ e $w = r^{k+2} = a^{k+2}$ para $a = r$;
- Se $p_{k+1} \neq 1$, então $p_{k+1}q = rp_{k+1}$ e $|p_{k+1}| < |r|$. Pelo argumento já usado em (1), para $a = p_{k+1}$, $r = ab$ obtemos $p = r^{k+1}p_{k+1}$ e assim

$$w = r^{k+2}p_{k+1} = (ab)^{k+2}a.$$

E assim concluímos a demonstração. □

Lema 2.1.4. *Seja $v = w_0ww_1ww_2 \dots w_{d-1}ww_d$ uma palavra em que a subpalavra w possui d subpalavras distintas e comparáveis. Então v é d-decomponível.*

Demonstração. Seja $w = a_iv_ib_i$, $i \in I_d$ e $v_1 > v_2 > \cdots > v_d$. Então v tem a seguinte d-decomposição

$$v = (w_0a_1)(v_1b_1w_1a_2)(v_2b_2w_2a_3)\dots(v_{d-1}b_{d-1}w_{d-1}a_d)(v_db_d)w_d$$

pois $t_1 > t_2 > \cdots > t_d$, em que $t_i = v_ib_iw_ia_{i+1}$ para $i \in I_{d-1}$ e $t_d = v_db_d$. □

Exemplo 2.1.5. Se p e q são palavras comparáveis, então a palavra $w = p^{d-1}q$ contém d subpalavras distintas e comparáveis.

Se $p > q$, então

$$p^{d-1}q > p^{d-2}q > \cdots > pq > q.$$

Se $p < q$, então

$$p^{d-1}q < p^{d-2}q < \cdots < pq < q.$$

Definição 2.1.6. *Seja uma palavra w com $|w| \geqslant d$. Escrevamos*

$$w = w_1 = e_2w_2 = \cdots = e_dw_d,$$

onde $|e_i| = i - 1$, $|w_i| = |w| + 1 - i$.

Chamaremos de $w_1, w_2, \dots, w_d$ os d-finais *de w.*

Lema 2.1.7. *Seja uma palavra w, com $|w| \geqslant d$ tal que os d-finais de w são incomparáveis, então $w = ab^tc$, onde $|a| + |b| < d$, $t \geqslant 1$ e $c = 1$ ou c é início de b.*

Se $|w| \geqslant dk$, então $t \geqslant k$ e, em particular, w possui subpalavra b^k com $|b| < d$.

Demonstração. Sejam w_i, w_j dois d-finais de w incomparáveis, com $i < j$. Assim $w = aw_i = abw_j$, logo $w_i = bw_j$. Como w_i e w_j são incomparáveis, $w_i = w_ju$ e pelo Lema 2.1.3 (já que $bw_j = w_i = w_ju$) obtemos $w_i = b^tc$, onde $c = 1$ ou c é um começo de b e logo $w = aw_i = ab^tc$. Claramente $|a| + |b| = j - 1 < d$.

Continuando, $dk \leqslant |w| = |a|+|b|+(t-1)|b|+|c| < d+(t-1)|b|+|c| < d+t|b| < (t+1)d$, donde $k < t + 1$ e assim $k \leqslant t$. □

Lema 2.1.8. *Seja $w \in W$ com $|w| = kd$ e w não contém subpalavra b^k com $|b| < d$. Então $w = vu$, os d-finais de v são comparáveis e v pertence a um subconjunto S de W que tem no máximo $s(d, k) = \binom{d}{2}(k - 1)m^d$ elementos, ou seja, $|S| \geqslant s(d, k)$.*

Demonstração. Se os d-finais de w não são comparáveis, então, pelo Lema anterior, w possui uma subpalavra b^k, com $|b| < d$, absurdo. Logo os d-finais de w são comparáveis. Seja v o início de w de menor comprimento tal que os d-finais(donde $|v| \geqslant d$) de v são comparáveis. Mas $v = qx$, com $|x| = 1$, e assim ou $|q| < d$, ou os d-finais de q são incomparáveis (pela condição minimal de v).

Logo os d-finais de q são incomparáveis e $|q| \geqslant d$ (pois $|q| < d$ e os d-finais de q serem comparáveis são condições incompatíveis), pelo Lema anterior $q = a(cb')^tc$, onde $c \neq 1 \neq b'$, $|a| + |b'| + |c| < d$ e $t \geqslant 1$ ou $q = ab^t$, onde $b \neq 1$ e $|a| + |b| < d$. Portanto w contém b^t (ou $(cb')^t$), $|b| < d$ ($|cb'| < d$), donde $t < k$, pela hipótese.

Denotemos por S o conjunto de todas as palavras escritas de uma das seguintes formas:

(i) $v = a(cb')^tcx$, onde $c \neq 1 \neq b'$, $t \in I_{k-1}$, $|a| + |b'| + |c| \leqslant d - 1$, $|x| = 1$ e x não é início de b;

(ii) $v = ab^tx$, onde $b \neq 1$, $t \in I_{k-1}$, $|a| + |b| \leqslant d - 1$, $|x| = 1$ e x não é início de b.

Vamos agora estimar a quantidade de elementos de S. Para os elementos do tipo (i), seja $l = |a| + |b'| + |c|$ fixado. Sabemos que $2 \leqslant l \leqslant d - 1$. Também os inteiros $|a|$ e $|a| + |c|$ determinam $|a|$, $|b'|$ e $|c|$. Deste modo, $|a|$ e $|a| + |c|$ devem ser elementos distintos entre $0, 1, \ldots, l - 1$, donde temos $\binom{l}{2}$ possibilidades para os inteiros $|a|$,$|b'|$ e $|c|$. Como $ab'c$ é palavra em W e determina a, b' e c, temos m^l possibilidades para a, b' e c. Temos $(k - 1)$

possibilidades para o t e $(m-1)$ possibilidades para que a letra x seja distinta da primeira letra de b. Assim, com l fixado temos

$$\binom{l}{2} m^l (k-1)(m-1)$$

possibilidades para v. Somando em $l = 2$ até $d-1$ obtemos que o número de elementos do tipo (i) é limitado por

$$\sum_{l=2}^{d-1} \binom{l}{2} m^l (k-1)(m-1).$$

Com uma análise análoga para os elementos do tipo (ii), obtemos que o número de elementos do tipo (ii) é limitado por

$$\sum_{l=1}^{d-1} l m^l (k-1)(m-1).$$

Assim,

$$|S| \leqslant \sum_{l=2}^{d-1} \binom{l}{2} m^l (k-1)(m-1) + \sum_{l=1}^{d-1} l m^l (k-1)(m-1) =$$

$$(k-1)(m-1) \sum_{l=1}^{d-1} \binom{l+1}{2} m^l \leqslant (k-1)\binom{d}{2}(m-1) \sum_{l=0}^{d-1} m^l \leqslant (k-1)\binom{d}{2} m^d.$$

□

Observação 2.1.9. Agora, motivados pelo Lema anterior, definimos o número $s(d,k) = \binom{d}{2}(k-1)m^d$.

O próximo teorema é a versão combinatória do teorema de Shirshov, demonstrado por Belov, o qual será o resultado chave em nossa abordagem às PI-Álgebras finitamente geradas.

Teorema 2.1.10. *Seja $w \in W = \langle x_1, \ldots, x_m \rangle$, $m > 1$, e sejam k e d inteiros tais que $k \geqslant d > 1$ e w não é d-decomponível. Então*

$$w = c_0 v_1^{k_1} c_1 v_2^{k_2} \ldots v_r^{k_r} c_r,$$

onde $|v_i| < d$, $k_i \geqslant k$, $r < dm^d$ e

$$\sum_{i=0}^{r} |c_i| \leqslant d^2 k s(d,k) + dk(r+1) \leqslant \frac{d^4 k^2 m^d}{2},$$

as palavras v_i e c_i não possuem início comum e quando $c_i = 1$, v_i e v_{i+1} não possuem início comum.

Demonstração. Podemos assumir $|w| > d^2ks(d,k)$, caso contrário ponha $c_0 = w$ e o resultado está mostrado. Assim podemos escrever

$$w = a_1b_1a_2b_2\ldots a_tb_ta_{t+1},$$

onde $t = ds(d,k)$, $|b_i| = kd$ e os a_i são arbitrários. Caso nenhum b_i contenha uma subpalavra b^k, $|b| < d$, então, pelo lema anterior, $b_i = v_iu_i$, onde $v_i \in S$ e v_i tem d subpalavras comparáveis. Mas como $t = ds(d,k) \geqslant |S|$ temos que algum v_i se repete d vezes em w. Pelo Lema 2.1.4, w é d-decomponível, absurdo.

Assim, existe b_i que possui uma subpalavra b^k com $|b| < d$. Logo w também contém b^k. Seja c_0 o menor início de w tal que $w = c_0v_1^{k_1}w_1$, onde $|v_1| < d$, $k_1 \geqslant k$ e v_1 e w_1 não possuem início comum. Podemos supor que eles não possuem início comum, pois, caso contrário, poderíamos escrever $v_1 = pr$, $w_1 = pq$ com q e r sem início comum, e então $w = c_0p(qp)^{k_1}r$, onde qp e r não possuem início em comum. Caso w_1 contenha uma subpalavra b^k, $|b| < d$, escolhemos o menor c_1 tal que $w_1 = c_1v_2^{k_2}w_2$, onde $|v_2| < d$, $k_2 \geqslant k$ e v_2 e w_2 não possuem início comum (da mesma forma com que fizemos anteriormente). Procedendo desta maneira obtemos o seguinte

$$w = c_0v_1^{k_1}c_1v_2^{k_2}\ldots v_r^{k_r}c_r,$$

onde $|v_i| < d$, $k_i \geqslant k$, os c_i não contém palavra da forma b^k, $|b| < d$ e as palavras v_i e c_i não possuem início comum e quando $c_i = 1$, v_i e v_{i+1} não possuem início comum.

Agora w possui $r-1$ subpalavras disjuntas, a saber $v_i^{d-1}x_i$ com $i \in I_{r-1}$, onde x_i é uma letra diferente da primeira letra de v_i. (Aqui usamos que $k \geqslant d$ e possivelmente $c_r = 1$). O número de palavras da forma $v^{d-1}x$, $|x| = 1$ e x não é a primeira letra de v é

$$\sum_{l=1}^{d-1} m^l(m-1) = m^d - m < m^d.$$

Se $r \geqslant dm^d$, então alguma palavra da forma $v^{d-1}x$, $|x| = 1$ e x não é a primeira letra de v se repete pelo menos d vezes em w:

$$w = q_0(v^{d-1}x)q_1(v^{d-1}x)q_2\ldots q_{d-1}(v^{d-1}x)q_d,$$

pelo Exemplo 2.1.5, $v^{d-1}x$ possui d subpalavras comparáveis, e pelo Lema 2.1.4 w é d-decomponível, absurdo. Logo $r < dm^d$ (e $r+1 \leqslant dm^d$).

Para provar a desigualdade do $\sum_{i=0}^{r} |c_i|$, dividimos os c_i em subpalavras de comprimento dk, mais uma palavra de comprimento menor que dk. Assim

$$p = \sum_{i=0}^{r} \left\lfloor \frac{|c_i|}{dk} \right\rfloor,$$

temos p segmentos de comprimento dk ($\lfloor \alpha \rfloor$ denota a parte inteira de $\alpha \in \mathbb{R}$). Como c_i não possui subpalavras da forma b^k, $|b| < d$, pelo Lema anterior, cada um desses p segmentos começa por um elemento de S com d subpalavras comparáveis. Se $p \geqslant ds(d,k)$, então algum elemento de S repete d vezes em w, que já sabemos, pelo Lema 2.1.3, torna w d-decomponível, absurdo. Logo $p < ds(d,k)$. Além disso, usando as propriedades de parte inteira,

$$p > \frac{1}{dk} \sum_{i=0}^{r} |c_i| - (r+1),$$

donde

$$\sum_{i=0}^{r} |c_i| < dk(p + (r+1)) \leqslant d^2ks(d,k) + dk(r+1) \leqslant d^2km^d \left(\frac{(k-1)(d-1)(d))}{2} + 1 \right) \leqslant$$

$$\leqslant d^2km^d \left(\frac{(k-1)(d-1)(d))}{2} + 1 \right) \leqslant \frac{1}{2} d^4k^2m^d.$$

□

Definição 2.1.11. *Seja A uma álgebra gerada por $V = \{r_i\}_{i \in I_m}$. Seja H um subconjunto finito das palavras com letras em V ($H \subseteq \langle r_1, r_2, \cdots, r_m \rangle$ na nossa notação). Diremos que* A tem altura h com respeito a H *se h é o menor número natural x tal que*

$$A = span\{u_{i_1}^{k_1} u_{i_2}^{k_2} \dots u_{i_t}^{k_t};\ para\ todo\ j \in I_t, u_{i_j} \in H, t \leqslant x\}.$$

Exemplo 2.1.12. Seja $A = K[X]$, onde $X = \{x_1, \dots, x_m\}$, a álgebra unitária dos polinômios sobre um número finito de variáveis comutativas. Então A tem altura m com respeito a X, pois $A = span\{x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}; k_i \geqslant 0\}$ e $x_1 x_2 \dots x_m$ não pode ser escrito com menos do que m fatores distintos.

Teorema 2.1.13 (Shirshov)**.** *Seja A uma PI-Álgebra, satisfazendo uma identidade de grau $d > 1$, gerada (como álgebra) por $V = \{r_i\}_{i \in I_m}$. Então A tem altura finita com respeito a $H = \{r_{i_1} r_{i_2} \dots r_{i_s}; s < d, i_j \in I_m\}$.*

Demonstração. Podemos supor que a identidade polinomial é multilinear, digamos f tal que

$$f(x_1, \dots, x_d) + x_1 x_2 \dots x_d = \sum_{\sigma \in S_d \setminus \varepsilon} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(d)}.$$

(somamos sob todas as permutações não triviais)

Considere um produto $w = r_{i_1} r_{i_2} \dots r_{i_p} \in A$. Se a palavra w é d-decomponível, então

$$w = w_0 w_1 \dots w_d w_{d+1} > w_0 w_{\sigma(1)} \dots w_{\sigma(d)} w_{d+1}$$

para toda permutação não trivial $\sigma \in S_d$. Utilizando a identidade polinomial

$$w_0(w_1 w_2 \dots w_d) w_{d+1} = \sum_{\sigma \in S_d \setminus \varepsilon} \alpha_\sigma w_0 w_{\sigma(1)} w_{\sigma(2)} \dots w_{\sigma(d)} w_{d+1}.$$

Assim w é combinação linear de palavras de tamanho p, e menores em relação a ordenação definida (em Definição 2.1.1). Podemos continuar o processo nas parcelas, até w ser combinação de palavras não d-decomponíveis. Seja w' uma dessas parcelas não d-decomponíveis. Fixamos $k = d$. Pelo teorema anterior,

$$w' = c_0 v_1^{k_1} c_1 v_2^{k_2} \dots v_r^{k_r} c_r,$$

onde $|v_i| < d$, $k_i \geqslant k$, $r < dm^d$ e

$$\sum_{i=0}^{r} |c_i| \leqslant d^2 ks(d,k) + dk(r+1) \leqslant \frac{d^4 k^2 m^d}{2},$$

as palavras v_i e c_i não possuem início comum e quando $c_i = 1$, v_i e v_{i+1} não possuem início comum. Considerando a palavra $c_i \neq 1$ como produto $c_i = u_{j_1} \dots u_{j_q}$ com $u_{j_v} \in V$, obtemos que

$$A = span\{w; w = u_1 \dots u_{p_0} v_1^{k_1} u_{p_0+1} \dots u_{p_1} v_2^{k_2} \dots v_t^{k_t} u_{p_{t-1}+1} \dots u_{p_t}\}.$$

Portanto a altura h de A satisfaz

$$h \leqslant t + \sum_{i=0}^{t} |c_i| \leqslant dm^d + \frac{d^6 m^d}{2}.$$

□

Teorema 2.1.14 (Levitzki)**.** *Seja A uma PI-Álgebra, satisfazendo uma identidade de grau $d > 1$, gerada (como álgebra) por $V = \{r_i\}_{i \in I_m}$. Seja P o conjunto de todos os produtos $r_{i_1} \cdots r_{i_k}$, $k < d$.*

Se todo elemento de P é nil, então a álgebra A é nilpotente. Em particular, $\dim_K A < \infty$.

Demonstração. Pelo Teorema de Shirshov 2.1.13, A é gerado pelos produtos

$$w = u_{i_1}^{k_1} \cdots u_{i_t}^{k_t},$$

onde $t \leqslant h$ (h é a altura) e os u_{i_j} são palavras de comprimento $< d$ com letras em V. Como as possíveis palavras u_{i_j} são em número finito, existe uma cota superior n para a classe de nilpotência delas. Portanto, se todos u_{i_j} são nil e a soma $k_1 + \ldots + k_t$ é suficientemente grande (maior que $h(n-1)$), então algum u_{i_j} aparece com grau maior que $n-1$ e a palavra é igual a 0. □

2.2 Dimensão de Gelfand-Kirillov

Nesta seção apresentaremos conceitos básicos e propriedades da teoria de GK-dimensão necessárias para uma boa compreensão do próximo capítulo (tais conceitos e propriedades não aparecem no Capítulo 1). Após, vamos relacionar PI-equivalência com a Dimensão de Gelfand-Kirillov. Nesta seção vamos considerar $\mathbb{N}_0$ o conjunto dos números naturais com o zero e $\mathbb{N}$ o conjunto dos naturais sem o zero. Aqui estaremos considerando todas as álgebras associativas, não necessariamente unitárias.

2.2.1 Conceitos Básicos e Propriedades

Iniciamos com a definição do nosso principal objeto de estudos, a dimensão de Gelfand-Kirillov.

Definição 2.2.1. *Seja A uma K-álgebra, gerada (algebricamente) por $V = \{r_i\}_{i \in I_m}$*

$$V^0 := \begin{cases} K & \text{, se } A \text{ é unitária} \\ 0 & \text{, c.c.} \end{cases}$$

Para todo $n \in \mathbb{N}, V^n := span\{r_{i_1} \cdot \ldots \cdot r_{i_n};\ i : j \in I_n \mapsto i_j \in I_m\} \subseteq A$.

Definimos

$$\begin{array}{rccc} g_V : & \mathbb{N}_0 & \longrightarrow & \mathbb{N}_0 \\ & n & \longmapsto & \dim_K(\sum_{i=0}^n V^i) \end{array}.$$

(chamada de função crescimento de A, *com respeito a V)*

A dimensão de Gelfand-Kirillov de A é definida por:

$$GK\dim(A) := \limsup \log_n g_V(n).$$

Observação 2.2.2. A dimensão de Gelfand-Kirillov de uma álgebra A pode não existir, não ser um número real. Neste caso, por abuso, ainda diremos que existe a dimensão de Gelfand-Kirillov e escrevemos $\mathrm{GKdim}\,(A) = \infty$ e, caso seja necessário, consideraremos a aritmética real estendida sem menções explícitas, uma vez que o comportamento é natural.

Observação 2.2.3. Na verdade, o conceito de dimensão de Gelfand-Kirillov é mais geral e esta é uma versão particular. Para maiores detalhes veja [12].

Proposição 2.2.4. *$GK\mathrm{dim}\,(A)$ não depende da escolha de V, conjunto finito que gera (algebricamente) A.*

Demonstração. De fato, sejam $V = \{r_i\}_{i \in I_m}$ e $W = \{s_i\}_{i \in I_{m'}}$ conjuntos que geram (algebricamente) A .

Como V gera A como álgebra, $s_j \in W \subseteq R$, existe $p_j \in \mathbb{N}$ tal que $s_j \in \sum_{i=0}^{p_j} V^i$.

Assim existe $p = \max\{p_j; j \in I_{m'}\}$ tal que $W \subseteq \sum_{i=0}^{p} V^i$. Logo $W^1 \subseteq \sum_{i=0}^{p} V^i$, donde concluímos que $W^n \subseteq \sum_{i=0}^{pn} V^i$ e também que $\sum_{i=0}^{n} W^i \subseteq \sum_{i=0}^{pn} V^i$.

Agora temos $g_W(n) \leqslant g_V(pn)$, donde tiramos

$$\log_n g_W(n) \leqslant \log_n g_V(pn) = \log_n pn \cdot \log_{pn} g_V(pn) = (1 + \log_n p) \log_{pn} g_V(pn) =: c_n.$$

Sejam $c := \limsup c_n$, $d_n := \log_{pn} g_V(pn)$ e $d := \limsup d_n$. Mostremos que $c = d$.

Primeiro vamos mostrar que $d \leqslant c$. Para todo $n \in \mathbb{N}, 1 \leqslant p$ implica $0 = \log_n 1 \leqslant \log_n p$, donde $1 \leqslant 1 + \log_n p$, e assim $d_n = \log_{pn} g_V(pn) \leqslant (1 + \log_n p)d_n = c_n$.

Portanto $d \leqslant c$.

Agora mostremos que $c \leqslant d$. Existe sequência $n : j \in \mathbb{N} \hookrightarrow n_j \in \mathbb{N}$ crescente tal que $\lim\limits_j c_{n_j} = c$ (mesmo que c seja ∞).

Existe $\lim\limits_n (1 + \log_n p) = 1$, logo existe $\lim\limits_j (1 + \log_{n_j} p) = 1$.

Agora $\lim\limits_j d_{n_j} = \lim\limits_j \dfrac{c_{n_j}}{(1 + \log_{n_j} p)} = \dfrac{\lim_j c_{n_j}}{\lim_j (1 + \log_{n_j} p)} = c.$

Portanto $c \leqslant d$.

Assim $\limsup \log_n g_W(n) \leqslant d = \limsup\limits_n \log_{pn} g_V(pn) \leqslant \limsup\limits_k \log_k g_V(k)$.

Finalmente, $\mathrm{GKdim}_W(A) \leqslant \mathrm{GKdim}_V(A)$.

Analogamente mostra-se que $\mathrm{GKdim}_V(A) \leqslant \mathrm{GKdim}_W(A)$. □

Exemplo 2.2.5. Para $A = K[X]$, onde $X = \{x_1, \ldots, x_m\}$, a álgebra unitária dos polinômios em m variáveis comutativas. Então, $\mathrm{GKdim}\,(A) = m$.

De fato, com relação ao conjunto usual que gera (algebricamente) os polinômios, $V = \{x_i\}_{i \in I_m}$,

$$\begin{aligned} g_V(n) &= \#\{\text{monômios de grau } \leqslant n \text{ em } m \text{ variáveis comutativas}\} \\ &= \#\{\text{monômios de grau } n \text{ em } m+1 \text{ variáveis comutativas}\} \\ &= \#\{\text{sequências de } n \bullet \text{ e } m \,|\} \\ &= \frac{(m+n)!}{m!n!} \end{aligned}$$

Basta observar que,

$$\begin{aligned} x_1^{a_1} \cdot \ldots \cdot x_m^{a_m} &\xrightarrow{\sim} y_0^{a_0} \cdot y_1^{a_1} \cdot \ldots \cdot y_m^{a_m} \\ &\xrightarrow{\sim} a_0 \bullet | \ldots | a_m \bullet \end{aligned}$$

Portanto $g_V(n) = \dfrac{(m+n)!}{m!n!} = \dfrac{(m+n)\cdot \ldots \cdot (n+1)}{m!}$, que é uma função polinomial de grau m. Logo $\text{GKdim}\,(A) = \limsup \log_n g_V(n) = m$.

Para deixar mais claro, no exemplo anterior identificamos, no caso particular $m = 2$ e $n = 6$, $x_1^2 x_2$ com $y_0^3 y_1^2 y_2$, com $3 \bullet |2 \bullet |1 \bullet$ que pode ser vista como a sequência de símbolos $\bullet \bullet \bullet | \bullet \bullet | \bullet$.

Exemplo 2.2.6. Para $A = K\langle X \rangle$, onde $X = \{x_1, \ldots, x_m\}$ e $m > 1$, $\text{GKdim}\,(A) = \infty$. De fato, suponha que $\text{GKdim}\,(A) = t$. Com relação ao conjunto usual que gera (algebricamente) os polinômios, $V = \{x_i\}_{i \in I_m}$, temos $g_V(n) = \sum_{i=0}^{n} m^i$.

Mas é fácil ver que g_V cresce mais que qualquer função polinomial, isto é, para todo $k \in \mathbb{N}$, $k \leqslant \log_n g_V(kn)$, pois se $n \in \mathbb{N}_0$, então $2^n - n \geqslant 0$ e como $m \geqslant 2$ temos

$m^n \geqslant 2^n \geqslant n \rightarrow (m^n)^k \geqslant n^k \rightarrow n^k \leqslant m^{kn} \leqslant \sum_{i=0}^{kn} m^i = g_V(kn)$.

Portanto $k \leqslant \log_n g_V(kn)$ que nos dá que $k \leqslant \text{GKdim}\,(A)$, absurdo visto que k é arbitrário.

Proposição 2.2.7. *Seja A uma álgebra associativa finitamente gerada como álgebra. Então $\dim_K A < \infty$ se, e somente se, $GK\dim(A) = 0$. Mais ainda, se $\dim_K A = \infty$, então $GK\dim(A) \geqslant 1$.*

Demonstração. Seja $V = \{r_i\}_{i \in I_m}$ conjunto que gera (algebricamente) A.

Sabemos que para álgebras associativas $V^{n+1} = span\{V^n \cdot V\}$. Temos dois casos a considerar.

• Existe $n_0 \in \mathbb{N}_0$ tal que $V^{n_0+1} \subseteq \sum_{i=0}^{n_0} V^i$. Neste caso, $p \in \mathbb{N}$ implica que $V^{n_0+p} \subseteq \sum_{i=0}^{n_0} V^i$, e assim $g_V(n_0+p) = g_V(n_0) < \infty$.

Logo $n \geqslant n_0$ implica $g_V(n) = g_V(n_0) < \infty$, o que nos dá que $\mathrm{GKdim}\,(A) = 0$.

Isto ocorre se $\dim_K A < \infty$ (basta tomar $V = \{r_i\}_{i \in I_m}$ base de A $(A = V^1)$).

• Para todo $n \in \mathbb{N}_0, V^{n+1} \nsubseteq \sum_{i=0}^{n} V^i$.

Neste caso, $\sum_{i=0}^{n} V^i \subsetneq \sum_{i=0}^{n+1} V^i$, donde $g_V(n) < g_V(n+1)$.

Mostremos que $g_V(n) \geqslant n$ por indução.

i)$g_V(0) \geqslant 0$ trivialmente;

ii)$g_V(n+1) > g_V(n) \overset{HI}{\geqslant} n$, logo $g_V(n+1) > n$ donde $g_V(n+1) \geqslant n+1$ como queríamos.

Enfim, $\log_n g_V(n) \geqslant 1$, implicando $\mathrm{GKdim}\,(A) = \limsup \log_n g_V(n) \geqslant 1$. Isto ocorre se $\dim_K R = \infty$. □

Proposição 2.2.8. *Seja A uma álgebra, e $S = h(A)$ imagem homomórfica de A pelo homomorfismo h. Então $GK\mathrm{dim}\,(S) \leqslant GK\mathrm{dim}\,(A)$.*

Demonstração. Sejam $h : A \to h(A) = S$ homomorfismo de K-álgebras e $V = \{r_i\}_{i \in I_m}$ conjunto que gera (algebricamente) A . Claramente temos que $W = \{h(r_i)\}_{i \in I_m}$ é conjunto que gera (algebricamente) S.

Agora, para todo $n \in \mathbb{N}$,

$$\sum_{i=0}^{n} W^i \subseteq \sum_{i=0}^{n} h(V^i) = h(\sum_{i=0}^{n} V^i).$$

Assim

$$g_W(n) = \dim_K \sum_{i=0}^{n} W^i \leqslant \dim_K h(\sum_{i=0}^{n} V^i) \leqslant \dim_K \sum_{i=0}^{n} V^i = g_V(n).$$

Portanto $\mathrm{GKdim}\,(S) \leqslant \mathrm{GKdim}\,(A)$. □

Proposição 2.2.9. *Sejam A uma álgebra finitamente gerada como álgebra, e S uma subálgebra de R, finitamente gerada como álgebra.*

Então $GK\mathrm{dim}\,(S) \leqslant GK\mathrm{dim}\,(A)$.

Demonstração. Sejam $W = \{s_i\}_{i \in I_{m'}}$ conjunto que gera (algebricamente) S, e $U = \{r_i\}_{i \in I_m}$ conjunto que gera (algebricamente) A.

Como $V = W \cup U$ gera (algebricamente) R e para todo $n \in \mathbb{N}$ temos $W^n \subseteq V^n$, donde $g_W(n) \leqslant g_V(n)$

Finalmente $\mathrm{GKdim}\,(S) \leqslant \mathrm{GKdim}\,(A)$. □

Proposição 2.2.10. *Seja A uma álgebra comutativa, S uma subálgebra de A, finitamente gerada como álgebra, tal que A é finitamente gerado como S-módulo. Então* $GK\mathrm{dim}\,(S) = GK\mathrm{dim}\,(A)$.

Demonstração. Seja $U = \{r_i\}_{i\in I_m}$ conjunto gerador de A como S-módulo.

Temos $r_i r_j = \sum_{k=0}^{m} s_{ij}^{(k)} r_k$, onde $s_{ij}^{(k)} \in S$.

Seja $T = \{s_i\}_{i\in I_p}$ conjunto que gera (algebricamente) S.

Temos que $W = T \cup \{s_{ij}^{(k)}; (i,j,k) \in I_m \times I_m \times I_m\}$ é conjunto que gera (algebricamente) S.

Logo $V = W \cup U$ gera (algebricamente) R.

Mostremos que $\sum_{t=0}^{n} V^t \subseteq \sum_{t=0}^{n} W^t + \sum_{k=1}^{m}\sum_{t=0}^{n-1} W^t r_k$.

Primeiro vamos provar por indução em t que $V^t \subseteq W^t + \sum_{i=1}^{m} W^{t-1} r_i$.

i)$V^0 = W^0$ claramente;

ii)$V^t \cdot V^1 \subseteq (W^t + \sum_{i=1}^{m} W^{t-1} r_i)\,(W^1 + U^1) \subseteq W^{t+1} + \sum_{i=1}^{m} W^t r_i + \sum_{i,j=1}^{m} W^{t-1} r_i r_j$
$\subseteq W^{t+1} + \sum_{i=1}^{m} W^t r_i + \sum_{i,j,k=1}^{m} W^{t-1} s_{ij}^{(k)} r_k \subseteq W^{t+1} + \sum_{i=1}^{m} W^t r_i$, o que prova o passo indutivo.

Somando em t, obtemos $\sum_{t=0}^{n} V^t \subseteq W^0 + \sum_{t=1}^{n} (W^t + \sum_{i=1}^{m} W^{t-1} r_i) \subseteq \sum_{t=0}^{n} W^t + \sum_{i=1}^{m}\sum_{t=1}^{n} W^{t-1} r_i = \sum_{t=0}^{n} W^t + \sum_{i=1}^{m}\sum_{t=0}^{n-1} W^t r_i$.

Portanto $g_V(n) \leqslant (m+1) g_W(n)$ e $\mathrm{GKdim}\,(A) \leqslant \mathrm{GKdim}\,(S)$.

Pela Proposição anterior, $\mathrm{GKdim}\,(S) \leqslant \mathrm{GKdim}\,(A)$.

Assim, $\mathrm{GKdim}\,(S) = \mathrm{GKdim}\,(A)$. □

Proposição 2.2.11. *Seja A uma álgebra comutativa.*

Então $GK\mathrm{dim}\,(A)$ *é igual a dimensão de Krull de A.*

Demonstração. Usando o Teorema de Normalização de Noether, que nos diz que A contém uma subálgebra polinomial S, ou seja $S \simeq K[y_1, \ldots, y_d]$, onde d é a *Dimensão de Krull* de A (comprimento da maximal cadeia de ideais primos de A), tal que A é um S-módulo finitamente gerado (A é integral sobre S).

Assim de $S \simeq \mathbb{K}[y_1, \ldots, y_d]$ temos que $\mathrm{GKdim}\,(S) = d$ (Lema 2.2.8 e Exemplo 2.2.5).

Pela Proposição anterior $\mathrm{GKdim}\,(A) = \mathrm{GKdim}\,(S) = d$. □

Observação 2.2.12. Este resultado é interessante pois, em suma, diz que a dimensão de Gelfand-Kirillov é uma boa generalização do conceito de dimensão de Krull, pelo menos para álgebras comutativas. Já é conhecido que a dimensão de Gelfand-Kirillov coincide com a dimensão de Krull clássica para PI-algebras semiprimas e finitamente geradas, num resultado de Malliavin-Bremeret [14]. Mais interessante ainda é observar que, a princípio a dimensão de Gelfand-Kirillov assumiria qualquer valor real, no entanto em álgebras comutativas ela assume apenas valores inteiros (positivos).

Vejamos agora mais alguns resultados que facilitam o cálculo da dimensão de Gelfand-Kirillov.

Proposição 2.2.13. *Seja A uma álgebra*

- *Se I é um ideal de A, então $GK\dim(A/I) \leqslant GK\dim(A)$;*
- *Já vimos que $GK\dim(A) = 0$ se, e só se $\dim_K A < \infty$. Se $\dim_K A = \infty$ e A é associativa, então $GK\dim(A) = 1$ ou $GK\dim(A) \geqslant 2$;*
- *Se $B = A[x_1, \ldots, x_m]$, então*
$$GK\dim(B) = GK\dim(A) + m;$$
- *Se B é uma álgebra, então*
$$GK\dim(A \oplus B) = \max\{GK\dim(A), GK\dim(B)\};$$
- *Se B é uma álgebra, então*
$$\max\{GK\dim(A), GK\dim(B)\} \leqslant GK\dim(A \otimes B) \leqslant GK\dim(A) + GK\dim(B);$$
- *Para todo $\alpha \in \mathbb{R}$, $\alpha \geqslant 2$, existe uma álgebra associativa B com $GK\dim(B) = \alpha$.*

Demonstração. Para maiores detalhes, veja [12]. □

Teorema 2.2.14. *(*Berele*, [6]) Toda PI-Álgebra finitamente gerada como álgebra possui GK-dimensão finita.*

Demonstração. A demonstração seguirá a prova dada em [7], Teorema 9.4.1. Seja A uma PI-Álgebra finitamente gerada como álgebra por $V = \{r_i\}_{i \in I_m}$ que satisfaça uma identidade polinomial de grau d. Pelo Teorema de Shirshov 2.1.13, A possui altura h finita com respeito a $H = \{r_{i_1} r_{i_2} \ldots r_{i_s}; s < d\}$, as palavras com letras em V de tamanho menor que d. Ou seja,

$$A = span\{u_{i_1}^{k_1} u_{i_2}^{k_2} \ldots u_{i_t}^{k_t};\ \text{para todo } j \in I_t, u_{i_j} \in H, k_j > 0, t \leqslant h\}.$$

Assim,

$$V^n = span\{u_{i_1}^{k_1} u_{i_2}^{k_2} \dots u_{i_h}^{k_h};\ \text{para todo } j \in I_h, u_{i_j} \in H, k_j \geqslant 0, \sum_{j=1}^{h} k_{i_j}|u_{i_j}| = n\},$$

e temos

$$\sum_{r=0}^{n} V^r = span\{u_{i_1}^{k_1} u_{i_2}^{k_2} \dots u_{i_h}^{k_h};\ \text{para todo } j \in I_h, u_{i_j} \in H, k_j \geqslant 0, \sum_{j=1}^{h} k_{i_j}|u_{i_j}| \leqslant n\}.$$

Seja p o número de palavras em H ($p = \sum_{i=0}^{d-1} m^i$). A quantidade de índices $(i_1, \dots, i_h)$ é limitado por p^h. A quantidade de monômios de grau $\leqslant n$ em h variáveis é $\binom{n+h}{h}$, como visto em Exemplo 2.2.5, pois os u_{i_j} são variáveis e como não estão determinados podemos tomar como comutativos. Assim $g_V(n) = \dim \sum_{r=0}^{n} V^r$ é limitado pelo produto da quantidade de índices $(i_1, \dots, i_h)$ com a quantidade de monômios de grau $\leqslant n$ em h variáveis,

$$g_V(n) \leqslant p^h \binom{n+h}{h}.$$

Portanto $\operatorname{GKdim}(A) \leqslant h$, pois o lado direito da desigualdade é um polinômio de grau h (em n). □

Corolário 2.2.15. *A GK-dimensão de uma PI-álgebra finitamente gerada A é limitada pela altura de A, com respeito a qualquer conjunto finito que gera A.*

2.2.2 Relação entre PI-Equivalência e GK-Dimensão

Nesta seção pretendemos mostrar resultados que permitem relacionar os conceitos de GK-dimensão e de PI-equivalência.

Definição 2.2.16. *A álgebra relativamente livre (também chamada de universal) de posto m na variedade gerada pela álgebra A é definida por*

$$F_m(A) = K\langle x_1, \dots, x_m\rangle / (T(A) \cap K\langle x_1, \dots, x_m\rangle).$$

Lema 2.2.17. *Se A e B são duas álgebras PI-equivalentes, então*

$$F_m(A) = F_m(B) \text{ e } GK\dim F_m(A) = GK\dim F_m(B).$$

Demonstração. Sendo A e B álgebras PI-equivalentes, temos que $T(A) = T(B)$. Daí, vem que $T_m(A) = T(A) \cap K\langle X\rangle = T(B) \cap K\langle X\rangle = T_m(B)$ e

$$F_m(A) = K\langle x_1, \ldots, x_m\rangle/T_m(A) = K\langle x_1, \ldots, x_m\rangle/T_m(B) = F_m(B).$$

Portanto, $\mathrm{GKdim}\, F_m(A) = \mathrm{GKdim}\, F_m(B)$. □

Observação 2.2.18. Podemos extrair uma relação extremamente útil deste lema. Podemos utilizar a contra-positiva do Lema 2.2.17 para concluir a não PI-equivalência de álgebras, pois essa contra-positiva diz que PI-álgebras que possuem álgebras universais com dimensões de Gelfand-Kirillov diferentes não são PI-equivalentes.

Lema 2.2.19. *Se $T(A) \subseteq T(B)$, então $GK\mathrm{dim}\, F_m(A) \geqslant GK\mathrm{dim}\, F_m(B)$.*

Demonstração. Sendo $T(A) \subseteq T(B)$ obtemos que $T_m(A) \subseteq T_m(B)$. A partir disso obtemos o seguinte homomorfismo sobrejetor:

$$\begin{array}{rccc} \Psi : & F_m(A) & \longrightarrow & F_m(B) \\ & f + T_m(A) & \longmapsto & f + T_m(B). \end{array}$$

Daí, $F_m(B)$ é imagem homomórfica de $F_m(A)$ e da Proposição 2.2.8, obtemos que

$$\mathrm{GKdim}\, F_m(A) \geqslant \mathrm{GKdim}\, F_m(B)$$

como queríamos. □

Lema 2.2.20. *Se $B \subseteq A$, então $GK\mathrm{dim}\, F_m(B) \leqslant GK\mathrm{dim}\, F_m(A)$.*

Demonstração. Como $B \subseteq A$, temos $T(B) \supseteq T(A)$ e em seguida usamos o Lema 2.2.19. □

Teorema 2.2.21. *$GK\mathrm{dim}\, F_m(A \oplus B) = \max\{GK\mathrm{dim}\, F_m(A), GK\mathrm{dim}\, F_m(B)\}$.*

Demonstração. Inicialmente, observamos que

(1) $T(A \oplus B) = T(A) \cap T(B)$ e $T_m(A \oplus B) = T_m(A) \cap T_m(B)$;

(2) $F_m(A \oplus B) = K\langle x_1, \ldots, x_m\rangle/T_m(A \oplus B) = K\langle x_1, \ldots, x_m\rangle/T_m(A) \cap T_m(B)$.

Agora, sendo $A, B \subseteq A \oplus B$, usamos o Lema 2.2.20, para obter que

$$\operatorname{GKdim} F_m(A), \operatorname{GKdim} F_m(B) \leqslant \operatorname{GKdim} F_m(A \oplus B).$$

Daí, vem que

$$\operatorname{GKdim} F_m(A \oplus B) \geqslant \max\{\operatorname{GKdim} F_m(A), \operatorname{GKdim} F_m(B)\}. \tag{2.1}$$

Consideramos agora a imersão natural

$$K\langle x_1, \ldots, x_m\rangle/T_m(A \oplus B) \hookrightarrow K\langle x_1, \ldots, x_m\rangle/T_m(A) \oplus K\langle x_1, \ldots, x_m\rangle/T_m(B),$$

ou seja,

$$F_m(A \oplus B) \hookrightarrow F_m(A) \oplus F_m(B).$$

Utilizando (1) e a Proposição 2.2.9 (juntamente com Proposição 2.2.8), obtemos que

$$\operatorname{GKdim} F_m(A \oplus B) \leqslant \max\{\operatorname{GKdim} F_m(A), \operatorname{GKdim} F_m(B)\}. \tag{2.2}$$

A partir de 2.1 e 2.2, obtemos que

$$\operatorname{GKdim} F_m(A \oplus B) = \max\{\operatorname{GKdim} F_m(A), \operatorname{GKdim} F_m(B)\} = \operatorname{GKdim} [F_m(A) \oplus F_m(B)]$$

como desejado. □

Com isto, já possuímos as ferramentas necessárias para concluir a não PI-equivalência de $M_{1,1}(E)$ e $E \otimes E$ sobre K infinito e $\operatorname{char} K \neq 2$ usando GK-dimensão.

CAPÍTULO 3

TEOREMA SOBRE O PRODUTO TENSORIAL EM CARACTERÍSTICA COSITIVA

3.1 Teorema sobre o Produto Tensorial

Uma consequência da teoria de Kemer sobre a estrutura dos T-ideais é conhecida como o Teorema sobre o Produto Tensorial (TPT):

Teorema 3.1.1 (Kemer)**.** *Seja K um corpo e $\operatorname{char} K = 0$ e a, b, c, $d \in \mathbb{N}$. Então:*

(1) $T(M_{a,b}(E) \otimes E) = T(M_{a+b}(E))$;

(2) $T(M_{a,b}(E) \otimes M_{c,d}(E)) = T(M_{ac+bd,ad+bc}(E))$;

(3) $T(M_{1,1}(E)) = T(E \otimes E)$.

Este resultado foi também demonstrado por Regev em [19], sem o uso da teoria citada acima. A demonstração de Regev é mais simples, pois usa argumentos combinatórios e (implicitamente) identidades graduadas. A ideia central do artigo citado acima é construir uma aplicação linear que, embora não possua propriedades como ser homomorfismo, injetividade e sobrejetividade, ainda garanta a igualdade dos respectivos T-ideais. Uma importante ideia deste estudo foi olhar para as matrizes em questão como uma álgebra de funções. A princípio, esta atitude pode não parecer interessante, no entanto goza de boas propriedades, além de facilitar a notação.

No artigo [3] foi indicada uma demonstração, quando K é um corpo infinito e char $K \neq 2$, para a versão multilinear do TPT. Isto é, quando nos restringimos aos T-ideais gerados apenas pelos polinômios multilineares. Nas próximas, seções desenvolveremos as ideias de Regev ([19]), com as devidas modificações, para demonstrarmos o TPT multilinear como foi sugerido no artigo citado no início do parágrafo. Na última seção, mostraremos que o TPT (geral) não é válido em característica positiva.

3.1.1 Álgebras de Matrizes

Definição 3.1.2. *Seja J um conjunto finito e $v : J \to \mathbb{Z}_2$ uma função. O par (J, v) é chamado* conjunto a valores em $\mathbb{Z}_2$. *Escreveremos $J = J_0 \cup J_1$, onde $J_g = v^{-1}(g)$, para $g \in \mathbb{Z}_2$. Dado um segundo conjunto (J', v'), $v' : J' \to \mathbb{Z}_2$, definimos:*

$$\begin{array}{rccc} \tilde{v} = (v, v') : & J \times J' & \longrightarrow & \mathbb{Z}_2 \times \mathbb{Z}_2 \\ & (i,j) & \longmapsto & (v(i), v'(j)) \end{array}$$

e também

$$\begin{array}{rccc} v_+ : & J \times J' & \longrightarrow & \mathbb{Z}_2 \\ & (i,i') & \longmapsto & v(i) + v'(i'). \end{array}$$

Observação 3.1.3. A definição acima nos permite escrever $M_{a,b}(E)$ (lembre que E é a álgebra de Grassmann) de outro modo muito interessante. A saber, seja $n = a + b$, J um conjunto com n elementos, como I_n por exemplo, com $v : J \to \mathbb{Z}_2$ tal que $J_0 = v^{-1}(0)$ como acima e com a elementos, como I_a por exemplo, $v' = v$ e considere $v_+ : J \times J \to \mathbb{Z}_2$. Assim, podemos escrever $M_{a,b}(E) = \{(a_{i,j})_{i,j \in I_n}; a_{i,j} \in E_{v_+(i,j)}\} = M_J(E_{v_+(i,j)}; i, j \in J)$.

Nesta seção, denotaremos por simplicidade $E_{i,j} := E_{v_+(i,j)}$. Desta forma, escreveremos $M_J(E_{i,j}) = M_J(E_{v_+(i,j)}; i, j \in J)$. Recordemos que na Álgebra de Grassmann $E_g E_h \subseteq E_{g+h}$ se g, $h \in \mathbb{Z}_2$ e a soma $g + h$ é a soma em $\mathbb{Z}_2$. Logo, $E_{i_1,i_2} E_{i_2,i_3} \subseteq E_{i_1,i_3}$, para todo i_1, i_2, $i_3 \in J$.

Note que, como espaços vetoriais, $M_J(E_{i,j})$ e $\bigoplus_{i,j\in J} E_{i,j}$ são isomorfos. Consideremos

$$\pi_{r,s} : E_{r,s} \to \bigoplus_{i,j\in J} E_{i,j}$$

as inclusões canônicas. Para termos a igualdade acima no nível de álgebras, definimos a multiplicação em $\bigoplus_{i,j\in J} E_{i,j}$ como sendo distributiva e satisfazendo:

$$\pi_{i,j}(a_{i,j})\,\pi_{r,s}(a_{r,s}) = \begin{cases} 0 & \text{, se } j \neq r \\ \pi_{i,s}(a_{i,j}\,a_{j,s}) & \text{, se } j = r. \end{cases}$$

A próxima observação ilustra o bom comportamento dos conjuntos a valores em $\mathbb{Z}_2$ com o produto tensorial.

Observação 3.1.4. Para (J, v) e (J', v') conjuntos a valores em $\mathbb{Z}_2$, considere $M_J(E_{i,j})$ e $M_{J'}(E_{r,s})$. Então $M_J(E_{i,j}) \otimes M_{J'}(E_{r,s}) \cong M_{J\times J'}(E_{i,j} \otimes E_{r,s})$ (veja Definição 3.1.2). Com efeito, temos que $M_J(E_{i,j}) \otimes M_{J'}(E_{r,s}) \cong (\bigoplus_{i,j\in J} E_{i,j}) \otimes (\bigoplus_{r,s\in J'} E_{r,s}) \cong \bigoplus_{i,j\in J} \bigoplus_{r,s\in J'} (E_{i,j} \otimes E_{r,s})$, como espaços vetoriais. Além disso, este isomorfismo é dado por $\pi_{i,j}(a_{i,j}) \otimes \pi_{r,s}(a_{r,s}) \mapsto \pi_{(i,r),(j,s)}(a_{i,j} \otimes a_{r,s})$, o que faz dele um isomorfismo de álgebras.

Por outro lado, se $M_{a,b}(E) = M_J(E_{i,j})$ e $M_{c,d}(E) = M_{J'}(E_{r,s})$, então segue da Observação 3.1.3 que $M_{ac+bd,ad+bc}(E) = M_{J\times J'}(E_{(i,j),(r,s)})$.

3.1.2 Equivalência Multilinear

Nesta seção, enunciaremos o resultado principal deste capítulo: o TPT multilinear. Faremos algumas simplificações na notação e, logo após, definiremos uma aplicação μ^*, estudaremos suas propriedades e apresentaremos alguns resultados essenciais para a demonstração do TPT multilinear.

Para uma álgebra A, denotamos por $P(A) = \{f \in T(A); f \text{ é multilinear}\}$ as identidades polinomiais multilineares satisfeitas por A.

Definição 3.1.5. *Duas PI-álgebras A e B são ditas* PI-equivalentes *se $T(A) = T(B)$. Quando $P(A) = P(B)$, dizemos que A e B estão em* equivalência multilinear.

Observemos que, quando consideramos álgebras sobre corpos com característica zero, a PI-equivalência é consequência da equivalência multilinear. Veremos no final deste capítulo que, para álgebras sobre corpos infinitos com característica positiva, isto não é verdade.

O resultado principal deste capítulo é o TPT multilinear, ou seja, a "versão multilinear" do Teorema do Produto Tensorial:

Teorema (TPT multilinear) *Seja K um corpo infinito com $\operatorname{char} K \neq 2$ e a, b, c, $d \in \mathbb{N}$. Então:*

(1) $P(M_{a,b}(E) \otimes E) = P(M_{a+b}(E))$;

(2) $P(M_{a,b}(E) \otimes M_{c,d}(E)) = P(M_{ac+bd,ad+bc}(E))$;

(3) $P(M_{1,1}(E)) = P(E \otimes E)$.

No restante desta seção desenvolveremos grande parte da técnica necessária para demonstrarmos o teorema acima. Vale notar que, de acordo com a Observação 3.1.3, para demonstrarmos a segunda afirmação do TPT multilinear é suficiente mostrarmos que:

$$P(M_{I\times I'}(E_{i,j} \otimes E_{r,s})) = P(M_{I\times I'}(E_{(i,j),(r,s)})).$$

Definição 3.1.6. *Seja $\mu : E \otimes E \to E$ a multiplicação $\mu(x \otimes y) = xy$.*

Observação 3.1.7. De acordo com a definição acima, para g, h, $g + h \in \mathbb{Z}_2$, temos que $\mu(E_g \otimes E_h) \subseteq E_{g+h}$. Assim, sejam $D(0) = \{1\}$, $D(l) = \{e_{i_1} \dots e_{i_l}; 1 \leqslant i_1 < \cdots < i_l\}$ para $l \geqslant 1$, $E^{(n)}$ o subespaço de E gerado pela união $\bigcup_{l\geqslant n} D(l)$ e seja também $E_g^{(n)} = E_g \cap E^{(n)}$. Então, temos que $\mu(E_0 \otimes E_g) = \mu(E_g \otimes E_0) = E_g$, pois $1 \in E_0$ e $\mu(E_1 \otimes E_1) = E_0^{(2)}$. Deste modo, denotaremos $\mu(E_g \otimes E_h) = E_{g+h}^{(g,h)}$.

Neste momento, usando a observação acima, faremos algumas simplificações nas notações que serão usadas nesta e em outras seções.

Notação 3.1.8. *Dados (J, v), (J', v') conjuntos a valores em $\mathbb{Z}_2$, denotaremos:*

- $E[i, j, r, s] := E_{v_+(i,j)+v'_+(r,s)}^{(v_+(i,j),v'_+(r,s))}$;
- $M_1 := M_{J\times J'}(E[i, j, r, s])$;
- $M := M_{J\times J'}(E_{v_+(i,j)+v'_+(r,s)})$;
- $N := M_{J\times J'}(E_{v_+(i,j)} \otimes E_{v'_+(r,s)})$.

A ação de μ nas entradas de N induz uma aplicação sobrejetora $\mu^* : N \to M_1 \subseteq M$. Mais precisamente, se $(x_{k,l})_{k,l \in J \times J'} \in N$, então $\mu^*((x_{k,l})) = (\mu(x_{k,l}))$. É imediato que a aplicação μ^* é linear.

Teorema 3.1.9. *Sejam M_1, M como descrito em Notação 3.1.8. Então $P(M) = P(M_1)$.*

Para demonstrarmos este teorema faremos uso do seguinte resultado:

Lema 3.1.10. *Sejam $A \supseteq B$ duas PI-álgebras satisfazendo a seguinte condição: para quaisquer $a_1, a_2, \ldots, a_n \in A$, existem $a_1', a_2', \ldots, a_n' \in Z(A)$ tais que:*

(1) $a_i' \, a_i \in B$ para $i = 1, \ldots, n$;

(2) Para qualquer $a \in K(a_1, \ldots, a_n)$ temos $a_1' \, a_2' \cdots a_n' \cdot a = 0$ se, e somente se, $a = 0$.

Então $P(A) = P(B)$.

Demonstração. Como $A \supseteq B$, basta mostrarmos que toda identidade multilinear de B é também uma identidade de A. Para tanto, sejam $f(x_1, \ldots, x_n)$ uma identidade multilinear de B e $a_1, \ldots, a_n \in A$. Chame $a = f(a_1, \ldots, a_n)$ e sejam $a_1', \ldots, a_n' \in Z(A)$ satisfazendo *(1)* e *(2)*. Logo, segue de *(1)* que:

$$0 = f(a_1' \, a_1, \ldots, a_n' \, a_n) = a_1' \cdots a_n' \, f(a_1, \ldots, a_n) = a_1' \cdots a_n' \, a$$

e, por *(2)*, temos que $a = f(a_1, \ldots, a_n) = 0$, como queríamos. □

Agora estamos em condições de demonstrar o teorema.

Demonstração. (**Teorema 3.1.9**) Basta mostrarmos que M_1 e M satisfazem as hipóteses do Lema 3.1.10. Com efeito, desde que $E[i,j,r,s] = E_{v_+(i,j)+v_+'(r,s)}^{(v_+(i,j), v_+'(r,s))} \subseteq E_{v_+(i,j)+v_+'(r,s)}$, temos que $M_1 \subseteq M$.

Sabemos que $M = M_{k,l}(E)$, para k, l convenientes (veja Observação 3.1.4). Assim, dados $u_1, \ldots, u_t \in M$, seja $n = n(u_1, \ldots, u_t)$, tal que $u_1, \ldots, u_t \in M_{k,l}(E(V_n))$ (veja Exemplo 1.1.20). Tome $u_1' = e_{n+1} \, e_{n+2} \, 1_M, \ldots, u_t' = e_{n+2t-1} \, e_{n+2t} \, 1_M$, e disto seguem *(1)* e *(2)* do Lema 3.1.10, implicando no resultado desejado. □

Notação 3.1.11. *Seja $W = J \times J'$. Dados $u, w \in W$, considere $e_{u,w} \in M_{J\times J'}(E)$ a "matriz unidade" correspondente à posição u, w. Isto é, $e_{u,w} : W \times W \to E$ é definida por:*

$$e_{u,w}(r,s) = \begin{cases} 1 & , \ se\ (r,s) = (u,w) \\ 0 & , \ se\ (r,s) \neq (u,w). \end{cases}$$

Observe que, dependendo de u e w, podemos ter $e_{u,w} \notin N$ ou $e_{u,w} \notin M_1$. Seguindo a notação da Definição 3.1.2, para $u, w \in W$, escreveremos em $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$$\tilde{v}(u) + \tilde{v}(w) = (g,h), \ \ g, h \in \mathbb{Z}_2,$$

e denotaremos:

$$E(\tilde{v}(u) + \tilde{v}(w)) = E_g \otimes E_h.$$

Recordemos que $D = D_0 \cup D_1$ é uma base de E, onde $D_0 = \{1\} \cup \{e_{i_1} \ldots e_{i_r}; 1 \leqslant i_1 < \cdots < i_r,\ r = 2, 4, 6, \ldots\}$, $D_1 = \{e_{i_1} \cdots e_{i_r}; 1 \leqslant i_1 < \cdots < i_r,\ r = 1, 3, 5, \ldots\}$ e . Assim, escreveremos $S = \{(c \otimes d)\, e_{u,w}; u, w \in W,\ c \in D_g,\ e\ d \in D_h,\ onde\ \tilde{v}(u) + \tilde{v}(w) = (g,h)\}$.

Observação 3.1.12. No que foi feito acima, considere $u = (i,r)$, $w = (j,s) \in W = J \times J'$. Então $\tilde{v}(u) + \tilde{v}(w) = (v(i) + v(j), v'(r) + v'(s)) = (v_+(i,j), v'_+(r,s)) = (g,h)$. Logo, se $c \in D_g$ e $d \in D_h$, temos que $c \otimes d \in E_{v_+(i,j)} \otimes E_{v_+(r,s)}$ e estes elementos $c \otimes d$ geram linearmente $E_{v_+(i,j)} \otimes E_{v_+(r,s)}$. Disto segue que o conjunto S, definido em Notação 3.1.11, gera linearmente a álgebra N.

Definição 3.1.13. *Sejam A e B duas PI-álgebras. Uma aplicação linear sobrejetora $\varphi : A \to B$ é dita* cancelável *se, para todo polinômio multilinear $f(x)$, temos que $\varphi \circ f(x)$ é identidade em B se, e somente se, $f(x)$ é identidade em A.*

Queremos mostrar que μ^* é cancelável, e para tanto precisaremos do seguinte resultado:

Lema 3.1.14. *Sejam $a_1, a_2, \ldots, a_n \in D$, a base de E. Então existem um homomorfismo (de álgebras) $\varphi : E \to E$ e elementos $a'_1, a'_2, \ldots, a'_n \in D$, tais que $\varphi(a'_i) = a_i$, para $1 \leqslant i \leqslant n$ e $a'_1\, a'_2 \cdots a'_n \neq 0$.*

Demonstração. Desde que $\dim E = \infty$, podemos encontrar elementos $a'_1, a'_2, \ldots, a'_n \in D$ tais que $a'_1\, a'_2 \cdots a'_n \neq 0$, e $a'_i \in D_0$ se, e somente se, $a_i \in D_0$, $1 \leqslant i \leqslant n$. Primeiramente, definamos $\varphi(a'_1) = a_1$ e seja $K(a'_1, \ldots, a'_n) \subseteq E$ a subálgebra gerada por $a'_1, \ldots, a'_n$. Como

$a'_i\, a'_j = (-1)^{wt(a'_i)wt(a'_j)} a'_j\, a'_i$ para todo $1 \leqslant i, j \leqslant n$, segue que $H = \{a'_{i_1}\, a'_{i_2} \cdots a'_{i_r}; 1 \leqslant i_1 < \cdots < i_r \leqslant n\}$ é uma base linear de $K(a'_1, \ldots, a'_n)$. Para os elementos da base H definiremos $\varphi(a'_{i_1} \cdots a'_{i_r}) = a_{i_1} \cdots a_{i_r} = \varphi(a'_{i_1}) \cdots \varphi(a'_{i_r})$. Desta forma, podemos estender φ linearmente para $K\langle a'_1, \ldots, a'_n\rangle$ e, pela escolha dos elementos a'_i, φ é um homomorfismo de álgebras.

Como espaços vetoriais, temos $E = K(a'_1, \ldots, a'_n) \oplus A$, para algum subespaço $A \subseteq E$. Logo, estendendo φ trivialmente para E, isto é, impondo $\varphi(A) = 0$, obtemos o resultado desejado. □

Teorema 3.1.15. *A aplicação $\mu^* : N \to M_1$ é cancelável.*

Demonstração. Seja $f(x) = f(x_1, \ldots, x_n)$ um polinômio multilinear. Primeiramente, suponha que $f(x)$ é uma identidade para N. Então, temos imediatamente que $\mu^* \circ f(x)$ é uma identidade para M_1, pois μ^* é sobrejetora e linear.

Reciprocamente, suponha que $\mu^* \circ f(x)$ é uma identidade para M_1. Sejam $S \subseteq N$ e $\overline{x}_l = (c_l \otimes d_l)e_{u_l,w_l} \in S$, para $1 \leqslant l \leqslant n$ (como em Notação 3.1.11 e Observação 3.1.12). Desde que S gera linearmente N, é suficiente mostrarmos que $f(\overline{x}) = f(\overline{x}_1, \ldots, \overline{x}_n) = 0$. O restante da demonstração será dividido em dois casos:

Caso 1: Assuma que $c_1\, c_2 \cdots c_n \cdot d_1\, d_2 \cdots d_n \neq 0$, e sejam $u, w \in W = J \times J'$. Então a entrada u, w de $f(\overline{x})$ (isto é, os coeficientes de $e_{u,w}$ em $f(\overline{x})$) é $\alpha_{u,w}\; c_1 \cdots c_n \otimes d_1 \cdots d_n$, para algum $\alpha_{u,w} \in K$. Logo, $\alpha_{u,w}\; c_1 \cdots c_n \cdot d_1 \cdots d_n$ é a entrada u, w em $0 = \mu^* \circ f(\overline{x})$. Como $c_1 \cdots c_n \cdot d_1 \cdots d_n \neq 0$, segue que $\alpha_{u,w} = 0$, e disto obtemos $f(\overline{x}) = 0$.

Caso 2: Sejam $c_1, \ldots, c_n, d_1, \ldots, d_n$ quaisquer. Aplicando o Lema 3.1.14 para $c_1, \ldots, c_n$, $d_1, \ldots, d_n$, temos que existem $\varphi : E \to E$ homomorfismo de álgebras e $c'_1, \ldots, c'_n$, $d'_1, \ldots, d'_n \in D$ tais que:

$$\varphi(c'_l) = c_l, \text{ onde } c'_l \in D_0 \text{ se, e somente se, } c_l \in D_0$$

e

$$\varphi(d'_l) = d_l, \text{ onde } d'_l \in D_0 \text{ se, e somente se, } d_l \in D_0,$$

com $c'_1 \cdots c'_n \cdot d'_1 \cdots d'_n \neq 0$. Definindo $\overline{x}'_l = (c'_l \otimes d'_l)e_{u_l,w_l}$, tem-se $\overline{x}'_l \in S$, para todo $1 \leqslant l \leqslant n$. Agora, estendendo φ para o homomorfismo de álgebras $\varphi^* : N \to N$ pela ação de $\varphi \otimes \varphi$ nas entradas, temos:

$$\varphi^*((c' \otimes d')e_{u,w}) = (\varphi(c') \otimes \varphi(d'))e_{u,w}.$$

Logo, $\varphi^*(\overline{x}'_l) = \overline{x}_l$, para todo $1 \leqslant l \leqslant n$, e desde que $f(\overline{x}'_l) = 0$, segue do *Caso 1* que:

$$0 = \varphi^*(0) = \varphi^*(f(\overline{x}'_1, \overline{x}'_2, \ldots, \overline{x}'_n)) = f(\varphi^*(\overline{x}'_1), \varphi^*(\overline{x}'_2), \ldots, \varphi^*(\overline{x}'_n)) = f(\overline{x}),$$

como queríamos demonstrar. $\square$

Notação 3.1.16. *Fixemos* $\overline{x}_l = (c_l \otimes d_l)e_{u_l,w_l} \in S$, $1 \leqslant l \leqslant n$ *(como no Teorema 3.1.15). Denotemos* $e_\sigma = \prod_{l=1}^{n} e_{u_{\sigma(l)},w_{\sigma(l)}}$, $\overline{x}_\sigma = \prod_{l=1}^{n} \overline{x}_{\sigma(l)}$, *onde* $\sigma \in S_n$, *o grupo das permutações de* n *elementos. Se* $e_\sigma = 0$, *então* $\overline{x}_\sigma = 0$. *Assuma que* $e_\sigma \neq 0$, *para algum* $\sigma \in S_n$. *Por simplicidade, assuma que* $e_\varepsilon \neq 0$, *onde* ε *é o elemento neutro do grupo* S_n. *Logo,* $w_l = u_{l+1}$, $1 \leqslant l \leqslant n-1$. *Denotemos* $w_n = u_{n+1}$ *e* $(\underline{u}) = (u_1, \ldots, u_{n+1})$. *Chamaremos a permutação* $\sigma \in S_n$ *de* $(u_1, \ldots, u_{n+1})$-permissível *se* $e_\sigma \neq 0$. *Isto é,* $u_{\sigma(l+1)} = w_{\sigma(l)}$, $1 \leqslant l \leqslant n-1$. *Notemos que o símbolo* $u_{\sigma(n+1)}$ *não está definido, uma vez que* $\sigma \in S_n$, *ou seja, não há sentido para* $\sigma(n+1)$. *Aproveitamos isso para definir* $u_{\sigma(n+1)} := w_{\sigma(n)}$. *Para este* σ *denotaremos* $(\underline{u})\sigma = (u_{\sigma(1)}, \ldots, u_{\sigma(n+1)})$. *Observemos que se* $\eta \in S_n$ *é* $(\underline{u})\sigma$*-permissível, então* $((\underline{u})\sigma)\eta = (\underline{u})(\sigma\eta)$, *ou seja,* $\sigma\eta$ *é* $(\underline{u})$*-permissível.*

Observação 3.1.17. Sejam $\overline{x}_1$, $\overline{x}_2 \in S$, como nas notações acima. Naturalmente tem-se $d_1c_2 = \rho c_2 d_1$, onde $\rho = \pm 1$ e daí $\mu^*(\overline{x}_1 \cdot \overline{x}_2) = \rho\mu^*(\overline{x}_1) \cdot \mu^*(\overline{x}_2)$. Se ambos os lados são não nulos, ρ é unicamente determinado e depende apenas da paridade de d_1 e c_2. Logo, ρ é determinado por (u_1, u_2, u_3). Analogamente, podemos estender estas considerações para qualquer produto de elementos $\overline{x}_l$ e, em particular, para o produto $\overline{x}_1 \cdots \overline{x}_n$. Observe que, neste caso, $\rho = \pm 1$ é determinado por $(\underline{u}) = (u_1, \ldots, u_{n+1})$.

Definição 3.1.18.

(1) Sejam $\overline{x}_1, \ldots, \overline{x}_n \in S$ *e* $(\underline{u}) = (u_1, \ldots, u_{n+1})$ *como em Notação 3.1.16. Então definimos* $\rho(\underline{u}) = \rho(u_1, \ldots, u_{n+1})$ *via:*

$$\mu^*(\overline{x}_1 \cdots \overline{x}_n) = \rho(u_1, \ldots, u_{n+1})\, \mu^*(\overline{x}_1) \cdots \mu^*(\overline{x}_n).$$

(2) Se $\sigma \in S_n$ *é* $(\underline{u})$*-permissível, então* $\rho((\underline{u})\sigma)$ *é dado por:*

$$\mu^*(\overline{x}_{\sigma(1)} \cdots \overline{x}_{\sigma(n)}) = \rho((\underline{u})\sigma)\, \mu^*(\overline{x}_{\sigma(1)}) \cdots \mu^*(\overline{x}_{\sigma(n)}).$$

Observação 3.1.19. Recordemos de Notação 3.1.11 que $E(g,h) = E_g \otimes E_h$, para g, $h \in \mathbb{Z}_2$, e a soma $g+h$ é a soma de $\mathbb{Z}_2$, e também $\overline{x}_l = (c_l \otimes d_l)e_{u_l,w_l}$, onde $c_l \otimes d_l \in E(\tilde{v}(u_l) + \tilde{v}(w_l))$, para $1 \leqslant l \leqslant n$. Desde que $w_l = u_{l+1}$, para $1 \leqslant l \leqslant n$, e $z + z = 0$ em $\mathbb{Z}_2 \times \mathbb{Z}_2$, segue que para quaisquer $1 \leqslant a \leqslant b \leqslant n$, temos:

$$\prod_{l=a}^{b} (c_l \otimes d_l) \in E(\tilde{v}(u_a) + \tilde{v}(u_{b+1})).$$

Lema 3.1.20. *Sejam $\rho(\underline{u})$ como na Definição 3.1.18 e $1 \leqslant a \leqslant n-1$. Então:*

$$\rho(u_1, \ldots, u_{n+1}) = \rho(u_1, \ldots, u_{a+1})\ \rho(u_{a+1}, \ldots, u_{n+1})\ \rho(u_1, u_{a+1}, u_{n+1}).$$

Demonstração. Sejam $\overline{x}_1, \ldots, \overline{x}_n$ como em Notação 3.1.16. Pela Observação 3.1.19:

$$\prod_{l=1}^{a} \overline{x}_l = (c' \otimes d')e_{u_1, u_{a+1}}, \text{ em que } c' \otimes d' \in E(\tilde{v}(u_1) + \tilde{v}(u_{a+1}))$$

e

$$\prod_{l=a+1}^{n} \overline{x}_l = (c'' \otimes d'')e_{u_{a+1}, u_{n+1}}, \text{ em que } c'' \otimes d'' \in E(\tilde{v}(u_{a+1}) + \tilde{v}(u_{n+1})).$$

A demonstração segue da comparação das ações de μ^* em ambos os lados da equação:

$$\prod_{l=1}^{n} \overline{x}_l = \left(\prod_{l=1}^{a} \overline{x}_l \right) \left(\prod_{l=a+1}^{n} \overline{x}_l \right).$$

Do lado esquerdo:

$$\mu^*(\prod_{l=1}^{n} \overline{x}_l) = \rho(u_1, \ldots, u_{n+1}) \prod_{l=1}^{n} \mu^*(\overline{x}_l).$$

Do lado direito, usando que $\left(\prod_{l=1}^{a} \overline{x}_l \right) \left(\prod_{l=a+1}^{n} \overline{x}_l \right) = c'c'' \otimes d'd'' e_{u_1, u_{n+1}}$:

$$\mu^* \left(\left(\prod_{l=1}^{a} \overline{x}_l \right) \left(\prod_{l=a+1}^{n} \overline{x}_l \right) \right) = c'c''d'd''e_{u_1, u_{n+1}}.$$

Mas $c''d' = \rho(u_1, u_{a+1}, u_{n+1})d'c''$, $\mu^* \left(\prod_{l=1}^{a} \overline{x}_l \right) = c'd'e_{u_1, u_{a+1}}$ e também $\mu^* \left(\prod_{l=a+1}^{n} \overline{x}_l \right) = c''d''e_{u_{a+1}, u_{n+1}}$. Assim:

$$\mu^* \left(\left(\prod_{l=1}^{a} \overline{x}_l \right) \left(\prod_{l=a+1}^{n} \overline{x}_l \right) \right) = \rho(u_1, u_{a+1}, u_{n+1)} \mu^* \left(\prod_{l=1}^{a} \overline{x}_l \right) \mu^* \left(\prod_{l=a+1}^{n} \overline{x}_l \right).$$

Deste modo obtemos, do lado direito:

$$\mu^* \left(\left(\prod_{l=1}^{a} \overline{x}_l \right) \left(\prod_{l=a+1}^{n} \overline{x}_l \right) \right) = \rho(u_1, u_{a+1}, u_{n+1)} \rho((u_1, \ldots, u_{a+1}) \rho(u_{a+1}, \ldots, u_{n+1}) \prod_{l=1}^{n} \mu^*(\overline{x}_l).$$

□

Para demonstrarmos o resultado principal desta seção, como no capítulo anterior, precisaremos de uma definição e um resultado de caráter combinatório, devido a Regev ([20]). Optamos por omitir a demonstração deste resultado.

Definição 3.1.21. *([20]) Um elemento* $\eta \in S_n$ *é dito ser uma* transposição de blocos *se podemos escrever* $x_1 \cdots x_n = ABCDE$ *e* $x_{\eta(1)} \cdots x_{\eta(n)} = ADCBE$*, onde* B *e* D *são blocos de comprimento maior que 1.*

Teorema 3.1.22. *([20]) Sejam* $e_{u_l,w_l} = e_{u_l,u_{l+1}}$, $1 \leqslant l \leqslant n$*, como em Notação 3.1.16. Então* $\prod_{l=1}^{n} e_{u_l,u_{l+1}} = e_{u_1,u_{n+1}}$*. Seja também* $\sigma \in S_n$*, tal que* $e_\sigma = e_{u_1,u_{n+1}}$*. Então existem transposições de blocos* $\eta^{(1)}, \ldots, \eta^{(s)} \in S_n$ *tais que, se escrevermos* $\eta^{(1)} \cdots \eta^{(i)} = \sigma^{(i)}$*, (onde* $1 \leqslant i \leqslant s$*), temos:*

(1) $\sigma = \sigma^{(s)}$ *e*

(2) $e_{\sigma^{(i)}} = e_{u_1,u_{n+1}}$*, para cada* $1 \leqslant i \leqslant s$*.*

Com o resultado acima, podemos demonstrar o próximo Lema, que será usado na demonstração do teorema principal desta seção.

Lema 3.1.23. *Sejam* $\overline{x}_l$, $1 \leqslant l \leqslant n$ *(como em Notação 3.1.16 e* $(\underline{u}) = (u_1, \ldots, u_{n+1})$ *correspondente),* σ *uma permutação* $(\underline{u})$*-permissível de* S_n *tal que* $u_1 = u_{\sigma(1)}$, $u_{n+1} = u_{\sigma(n+1)}$ *e* ρ *como na Definição 3.1.18. Então* $\rho(\underline{u}) = \rho((\underline{u})\sigma)$*.*

Demonstração. Segue da Notação 3.1.16 e do Teorema 3.1.22 que é suficiente mostrarmos o Lema 3.1.23 no caso em que σ é uma transposição de blocos $(\underline{u})$-permissível.

Assumiremos que $\overline{x}_1 \cdots \overline{x}_n = ABCDE$ e $\overline{x}_{\sigma(1)} \cdots \overline{x}_{\sigma(n)} = ADCBE$. Mais ainda, $u_{\sigma(1)} = u_1$ e $u_{\sigma(n+1)} = u_{n+1}$. Sem perda de generalidade, podemos assumir que $A = E = 1$, $\overline{x}_1 \cdots \overline{x}_n = BCD$ e $\overline{x}_{\sigma(1)} \cdots \overline{x}_{\sigma(n)} = DCB$. Estes blocos correspondem às sequências

$$B \leftrightarrow (u_1, \ldots, u_{a+1}),$$

$$C \leftrightarrow (u_{a+1}, \ldots, u_{b+1})$$

e

$$D \leftrightarrow (u_{b+1}, \ldots, u_{n+1}).$$

Desde que σ é $(\underline{u})$-permissível, temos:

$$u_1 = u_{b+1} \text{ e } u_{a+1} = u_{n+1}. \tag{3.1}$$

Além disso,

$$DCB \quad \leftrightarrow \quad (\overbrace{u_{b+1}, u_{b+2}, \ldots,}^{D}\underset{\substack{\| \\ u_{a+1}}}{u_{n+1}}\overbrace{, u_{a+2}, \ldots,}^{C}\underset{\substack{\| \\ u_1}}{u_{b+1}}\overbrace{, u_2, \ldots,}^{B}u_{a+1}) \tag{3.2}$$

Aplicando o Lema 3.1.20 duas vezes, temos que $\rho(\underline{u}) = \rho_1\,\rho_2\,\rho_3\,\rho_4\,\rho_5$, onde cada ρ_i é dado por $\rho_1 = \rho(u_1, \ldots, u_{a+1})$, $\rho_2 = \rho(u_{a+1}, \ldots, u_{b+1})$, $\rho_3 = \rho(u_{b+1}, \ldots, u_{n+1})$, $\rho_4 = \rho(u_1, u_{a+1}, u_{b+1})$ e $\rho_5 = \rho(u_1, u_{b+1}, u_{n+1})$. Com um argumento similar, segue de (3.2) acima que $\rho((\underline{u})\sigma) = \rho_3\,\rho_2\,\rho_1\,\delta_4\,\delta_5$, onde $\delta_4 = \rho(u_{b+1}, u_{n+1}, u_{b+1})$ e $\delta_5 = \rho(u_{b+1}, u_{b+1}, u_{a+1})$. De (3.1) segue que $\rho_4 = \delta_4$ e $\rho_5 = \delta_5$, implicando no resultado. $\square$

Teorema 3.1.24. *A aplicação $\mu^* : N \to M_1$ da Definição 3.1.6 satisfaz:*

(1) Existe $S \subseteq N$ tal que S gera linearmente N.

(2) Dados $\overline{x}_1, \ldots, \overline{x}_n \in S$ e u, $w \in W$, existe $\rho = \rho(u, w, \overline{x}_1, \ldots, \overline{x}_n) \neq 0$ tal que, para todo $\sigma \in S_n$, a entrada u, w satisfaz:

$$\left(\mu^*(\overline{x}_{\sigma(1)} \cdots \overline{x}_{\sigma(n)})\right)_{u,w} = \rho\left(\mu^*(\overline{x}_{\sigma(1)}) \cdots \mu^*(\overline{x}_{\sigma(n)})\right)_{u,w}$$

(independente de $\sigma \in S_n$).

Demonstração. Para demonstrarmos *(1)*, basta tomarmos S como em Notação 3.1.11. Na Observação 3.1.12 foi visto que S gera linearmente N.

Para a afirmação *(2)*, sejam $\overline{x}_l = (c_l \otimes d_l)e_{u_l,w_l} \in S$ $(1 \leqslant l \leqslant n)$, $\sigma \in S_n$ e u, $w \in W$. Denotemos:

$$L(\sigma) = \left(\mu^*\left(\prod_{l=1}^{n} \overline{x}_{\sigma(l)}\right)\right)_{u,w}$$

e

$$R(\sigma) = \left(\prod_{l=1}^{n} \mu^*(\overline{x}_{\sigma(l)})\right)_{u,w}.$$

Da Definição 3.1.18 sabemos que $L(\sigma) = \rho(\sigma, u, v, \overline{x}_1, \ldots, \overline{x}_n)R(\sigma)$. A fim de completarmos a demonstração é suficiente mostrarmos que este ρ não depende de σ. Podemos assumir, sem perda de generalidade que, para algum $\sigma \in S_n$, temos $L(\sigma)$, $R(\sigma) \neq 0$. Por simplicidade, assumiremos que $L(\varepsilon)$, $R(\varepsilon) \neq 0$, onde ε é o elemento neutro de S_n, como de costume. Logo $w_l = u_{l+1}$, $1 \leqslant l \leqslant n$, e desta forma $(\underline{u}) = (u_1, \ldots, u_{n+1})$ foi determinado. Escreva $L(\varepsilon) = \rho R(\varepsilon)$, com $\rho = \pm 1$. Mostremos que para este ρ temos $L(\sigma) = \rho R(\sigma)$, para qualquer $\sigma \in S_n$.

Claramente temos $L(\sigma) = 0$ se, e somente se, $R(\sigma) = 0$. Dessa forma, podemos assumir que ambos são não nulos. Segue que σ é $(\underline{u})$-permissível e $u_1 = u_{\sigma(1)} = u$, $u_{\sigma(n+1)} = u_{n+1} = w$. Pelo Lema 3.1.23, temos:

$$\mu^* \left(\prod_{l=1}^{n} \overline{x}_{\sigma(l)} \right) = \rho(\underline{u}) \prod_{l=1}^{n} \mu^*(\overline{x}_{\sigma(l)}),$$

onde $\rho = \rho(\underline{u}) = \rho((\underline{u})\sigma)$. E isto vale para cada entrada u, $w \in W$, implicando na afirmação *(2)*, como queríamos. $\square$

Corolário 3.1.25. *Sejam N e M_1 como em Notação 3.1.8. Então $P(N) = P(M_1)$.*

Demonstração. Seja $f(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(n)}$ uma identidade multilinear de N. $\mu^*(S)$ gera M_1, já que pela Observação 3.1.12 foi visto que S gera linearmente N. Assim, basta mostrarmos que para quaisquer u, $w \in W$ e $\overline{x}_1, \ldots, \overline{x}_n \in S$, é satisfeita a equação $\left(f(\mu^*(\overline{x}_1), \ldots, \mu^*(\overline{x}_n))\right)_{u,w} = 0$. Seja $\rho = \rho(u, w, \overline{x}_1, \ldots, \overline{x}_n)$ como no Teorema 3.1.24, satisfazendo

$$\left(\mu^*(\overline{x}_{\sigma(1)} \cdots \overline{x}_{\sigma(n)})\right) = \rho \left(\mu^*(\overline{x}_{\sigma(1)}) \cdots \mu^*(\overline{x}_{\sigma(n)})\right).$$

Então

$$\begin{aligned} 0 = \left(\mu^*(f(\overline{x}_1, \ldots, \overline{x}_n))\right)_{u,w} &= \textstyle\sum_{\sigma \in S_n} \alpha_\sigma \mu^* \left(\overline{x}_{\sigma(1)} \cdots \overline{x}_{\sigma(n)}\right)_{u,w} = \\ &= \textstyle\sum_{\sigma \in S_n} \alpha_\sigma \rho \left(\mu^*(\overline{x}_{\sigma(1)}) \cdots \mu^*(\overline{x}_{\sigma(n)})\right)_{u,w} = \\ &= \rho \left(\textstyle\sum_{\sigma \in S_n} \alpha_\sigma \mu^*(\overline{x}_{\sigma(1)}) \cdots \mu^*(\overline{x}_{\sigma(n)})\right)_{u,w} = \\ &= \rho \left(f(\mu^*(\overline{x}_1), \ldots, \mu^*(\overline{x}_n))\right)_{u,w}. \end{aligned}$$

Logo, $f(x)$ é uma identidade em M_1.

Como μ^* é cancelável, (via Teorema 3.1.15) segue que $P(N) = P(M_1)$, como queríamos. $\square$

3.1.3 A Demonstração do TPT Multilinear

Nesta seção, estamos em condições de demonstrar o TPT multilinear. Como a demonstração de cada afirmação usa técnicas distintas, demonstraremos cada afirmação como um novo teorema.

Teorema 3.1.26. [TPT multilinear (2)] *Sejam $a, b, c, d \in \mathbb{N}$, $p = ac + bd$ e $q = ad + bc$. Então as álgebras $N_1 = M_{a,b}(E) \otimes M_{c,d}(E)$ e $M = M_{p,q}(E)$ satisfazem as mesmas identidades polinomiais multilineares.*

Demonstração. A álgebra N_1 é isomorfa à álgebra N, conforme a Observação 3.1.4 (veja também Notação 3.1.8). Segue da mesma observação que $M = M_{J \times J'}(E_{v_+(i,j)+v'_+(r,s)})$. O Teorema 3.1.9 diz que $P(M) = P(M_1)$. Agora, segue dos Teoremas 3.1.24, 3.1.15 e do Corolário 3.1.25 que $P(N_1) = P(M)$, como queríamos. □

Antes da demonstração da primeira afirmação do TPT, precisaremos de algumas definições.

Definição 3.1.27.

(1) Seja $a = a_0 + a_1 \in E$, onde $a_0 \in E_0$, $a_1 \in E_1$, e defina g_0, $g_1 : E \to M_2(E)$ por:

$$g_0(a_0 + a_1) = \begin{pmatrix} a_0 & a_1 \\ a_1 & a_0 \end{pmatrix} \text{ e } g_1(a_0 + a_1) = \begin{pmatrix} a_1 & a_0 \\ a_0 & a_1 \end{pmatrix}.$$

Denote $g_i(E) = \Omega_i$, para $i = 1, 2$, e $\Omega = \Omega_0 \oplus \Omega_1 \subseteq M_2(E)$. Observe que Ω_0 é uma subálgebra de $M_{1,1}(E)$, $\Omega_0 \cong E$ e Ω_1 é um Ω_0-módulo. Claramente temos que

$$\Omega = \left\{ \begin{pmatrix} x & y \\ y & x \end{pmatrix}; x, y \in E \right\}$$

é uma álgebra.

(2) Defina $f : \Omega \to E$ por:

$$f \begin{pmatrix} x & y \\ y & x \end{pmatrix} = x + y.$$

É imediato que f é um homomorfismo de álgebras. Além disso, $f \circ g_0 = f \circ g_1 = id_E$. Logo, $f|_{\Omega_i}$ é injetora, para $i = 1, 2$.

(3) Seja (J, v) um conjunto a valores em $\mathbb{Z}_2$, com $|J_0| = a$ e $|J_1| = b$. Defina a álgebra $U \subseteq M_{2(a+b)}(E)$ por:

$$U = \{g_{v_+(i,j)}(x_{i,j}); i, j \in I \text{ e } x_{i,j} \in E\}.$$

Assim, para $J' = J \times \mathbb{Z}_2$ e $v'(i, z) = v(i) + z \in \mathbb{Z}_2$, temos $U \subseteq M_{J'}(E_{v_+(r,s)}; r, s \in J')$.

Lema 3.1.28. *Com as notações e definições da Definição 3.1.27, temos que* $U \cong M_{a+b}(E) = M_J(E)$.

Demonstração. Defina $f^* : U \to M_J(E)$ por $f^*(g_{v+(i,j)}(x_{i,j})) = (f \circ g_{v+(i,j)}(x_{i,j})) = x_{i,j}$, para todo i, $j \in I$. Observe que f^* é um homomorfismo de álgebras, pois herda de f esta propriedade. Além disso, f^* é claramente sobrejetora, e desde que $f|_{\Omega_0}$, $f|_{\Omega_1}$ são injetoras, segue que f^* é injetora. Portanto, f^* é um isomorfismo de álgebras, como queríamos. □

Observação 3.1.29. Seja $E' = E^{(1)}$ a álgebra de Grassmann sem unidade (veja Observação 3.1.7), e seja U como na Definição 3.1.27 (3). Considere $U' = \{g_{v+(i,j)}(x_{i,j}); i, j \in I \text{ e } x_{i,j} \in E'\} \subseteq U$. Com um argumento similar ao do Teorema 3.1.9, temos que $P(U) = P(U')$. Logo, para qualquer U'' tal que $U' \subseteq U'' \subseteq U$, temos que $P(U'') = P(U)$.

Teorema 3.1.30. [TPT multilinear (2)] *Sejam* a, $b, \in \mathbb{N}$. *Então as álgebras* $M_{a,b}(E) \otimes E$ *e* $M_{a+b}(E)$ *satisfazem as mesmas identidades multilineares.*

Demonstração. Sejam $M_{a,b}(E) = M_J(E_{v+(i,j)})$, $M_{1,1}(E) = M_{\mathbb{Z}_2}(E_{z_1+z_2}; z_1, z_2 \in \mathbb{Z}_2)$ e denote $U_1 = M_J(E_{v+(i,j)}) \otimes E$. O mergulho $g_0 : E \hookrightarrow M_{1,1}(E)$ induz o mergulho $\overline{g}_0 = (id, g_0) : U_1 \hookrightarrow M_J(E_{v+(i,j)}) \otimes M_{\mathbb{Z}_2}(E_{z_1+z_2}) = M_{J\times\mathbb{Z}_2}(E_{v+(i,j)} \otimes E_{z_1+z_2}) = G$. Denote $\overline{U} = \overline{g}_0(U_1) \subseteq G$. Aplicando μ^*, temos:

$$\mu^* : G \to M_{I\times\mathbb{Z}_2}(E_{v+(i,j)+z_1+z_2}).$$

Sejam $\mu^*(\overline{U}) = \mu^*(\overline{g}_0(U_1)) = U''$ e U, U' como na Definição 3.1.27 (3) e Observação 3.1.29. Verifica-se diretamente que $U' \subseteq U'' \subseteq U$, e pela mesma observação citada acima, temos que $P(U'') = P(U) = P(U')$.

A mesma demonstração de que μ^* é cancelável e satisfaz as propriedades do Teorema 3.1.24 se aplica para a restrição de μ^* à subálgebra $\overline{U} \subseteq G$, com o subconjunto gerador sendo $\overline{U} \cap S$. Logo, pelo Teorema 3.1.25 temos:

$$P(\overline{U}) = P(\mu^*(\overline{U})) = P(U'') = P(U).$$

Como $\overline{g}_0$ é um mergulho, segue que $U_1 \cong \overline{U}$. Logo, $P(U_1) = P(\overline{U})$, e da igualdade acima temos que $P(U_1) = P(U)$. Como $U \cong M_J(E) = M_{a+b}(E)$ (Lema 3.1.28), segue que $P(M_{a+b}(E)) = P(U) = P(U_1) = P(M_{a,b}(E) \otimes E)$, como queríamos. □

Como nos casos anteriores, precisamos explorar algumas propriedades antes de demonstrarmos a última afirmação do TPT.

Recordemos do Exemplo 1.1.26 que E^{op} denota a álgebra oposta de E. A multiplicação em E^{op} é denotada aqui por $*$, e é dada por $a * b = ba$, para a, $b \in E^{op}$, e $E \cong E^{op}$. Assim, de acordo com os resultados de [13], temos que $T(E \otimes E) = T(E \otimes E^{op})$ e, em particular, temos que $P(E \otimes E) = P(E \otimes E^{op})$.

Definição 3.1.31.

(a) Sejam $\underline{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\underline{i} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\underline{j} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\underline{k} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. *Observe que* $\underline{i}\,\underline{j} = \underline{k} = -\underline{j}\,\underline{i}$, $\underline{i}^2 = \underline{k}^2 = \underline{1}$ *e* $\underline{j}^2 = -\underline{1}$.

(b) Defina $g : E \to M_{1,1}(E)$, $h : E^{op} \to M_{1,1}(E)$ *por:*

$$g(a) = g(a_0 + a_1) = a_0\underline{1} + a_1\underline{i}, \text{ onde } a = a_0 + a_1 \in E = E_0 \oplus E_1,$$

$$h(b) = h(b_0 + b_1) = b_0\underline{1} + b_1\underline{j}, \text{ onde } b = b_0 + b_1 \in E^{op} = E_0^{op} \oplus E_1^{op}.$$

Observação 3.1.32. As aplicações g e h possuem as seguintes propriedades (de verificação imediata):

(1) $g : E \to M_{1,1}(E)$ e $h : E^{op} \to M_{1,1}(E)$ são mergulhos de álgebras.

(2) $g(a)\,h(b) = h(b)\,g(a)$, para todo $a \in E$, $b \in E^{op}$.

Definição 3.1.33. *Com g e h como na Definição 3.1.31, definimos* $\varphi : E \otimes E^{op} \to M_{1,1}(E)$ *por* $\varphi(a \otimes b) = g(a)\,h(b)$.

Lema 3.1.34. *A aplicação φ definida acima satisfaz as seguintes propriedades:*

(1) φ é homomorfismo de álgebras;

(2) $\varphi(E \otimes E^{op}) \supseteq \begin{pmatrix} E_0^{(2)} & E_1 \\ E_1 & E_0^{(2)} \end{pmatrix}$.

Demonstração. A afirmação *(1)* é imediata.

Para demonstrarmos *(2)*, note que se $a_1 \in E_1$, então $\begin{pmatrix} 0 & 0 \\ a_1 & 0 \end{pmatrix} \in \varphi(E \otimes E^{op})$, pois $\frac{1}{2}[\varphi(a_1 \otimes 1) + \varphi(1 \otimes a_1)] = \begin{pmatrix} 0 & 0 \\ a_1 & 0 \end{pmatrix}$ (lembremos que $\operatorname{char} K \neq 2$). Analogamente para

$\begin{pmatrix} 0 & a_1 \\ 0 & 0 \end{pmatrix}$. Logo, $\begin{pmatrix} a_1b_1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a_1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ b_1 & 0 \end{pmatrix}$ e igualmente para $\begin{pmatrix} 0 & 0 \\ 0 & a_1b_1 \end{pmatrix}$. Assim, ambos estão em $\varphi(E \otimes E^{op})$ e a afirmação *(2)* segue. □

Finalmente estamos em condições de demonstrar a última afirmação do TPT.

Teorema 3.1.35. [TPT multilinear (3)] *As álgebras $E \otimes E$ e $M_{1,1}(E)$ satisfazem as mesmas identidades multilineares.*

Demonstração. Seja $A = E \otimes E^{op}$. Seguiremos a técnica do Teorema 3.1.9. Dados $y_1, \ldots, y_n \in M_{1,1}(E)$, existe um natural k, tal que $\{y_i\}_{i \in I_n} \subseteq M_{1,1}(E(V_k))$, isto é, os elementos y_i envolvem no máximo os k primeiros vetores da base de V. Consideremos $y'_i = e_{(k+2i-1)}\, e_{(k+2i)}\underline{1}$. É fácil ver que $y'_i \in Z(M_{1,1}(E)$. Assim temos que $y'_i y_i \in \begin{pmatrix} E'_0 & E_1 \\ E_1 & E'_0 \end{pmatrix} \subseteq \varphi(A)$, pelo Lema 3.1.34. Além disso, dado $Y \in K(y_1, \ldots, y_n)$, temos que $y'_1 \cdots y'_n Y = 0$ implica $Y = 0$. Assim pelo Lema 3.1.10 temos que $P(\varphi(A)) = P(M_{1,1}(E))$. Portanto, para completarmos a demonstração, basta mostrarmos que $P(A) = P(\varphi(A))$. Desde que φ é um homomorfismo, temos que $P(A) \subseteq P(\varphi(A))$. Logo, para obter a igualdade desejada, devemos mostrar a inclusão $P(\varphi(A)) \subseteq P(A)$. Com efeito, seja $f = \sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(n)} \in P(\varphi(A))$. Para mostrarmos que a identidade $f \in P(A)$, é suficiente fazê-lo para os elementos da base de A, isto é, basta que $f(u_1, \ldots, u_n) = 0$, onde $u_i = a_i \otimes a_{n+i}$, e os elementos a_i, com $i \in I_{2n}$ estão em D. Mas como os elementos u_i e u_j comutam entre si ou anticomutam entre si, podemos escrever

$$f(u_1, \ldots, u_n) = \sum_{\sigma \in S_n} \alpha_\sigma u_{\sigma(1)} \cdots u_{\sigma(n)} = \beta u_1 \cdots u_n.$$

Aplicando o Lema 3.1.14, existem $a'_1, \ldots, a_2n' \in E$, um homomorfismo $\psi : E \to E$, tal que $\psi(a'_i) = a_i$, satisfazendo $a'_1 \cdots a'_{2n} \neq 0$ e $a'_i \in D_{wt(a_i)}$. Sejam $\psi^* = \psi \otimes \psi$ e $u'_i = a'_i \otimes a'_{n+i}$. Agora temos que

$$f(u'_1, \ldots, u'_n) = \beta u'_1 \cdots u'_n \text{ e } \psi^*(f(u'_1, \ldots, u'_n)) = f(u_1, \ldots, u_n).$$

Com isso podemos concluir que $\beta = 0$, já que $\underline{i}^r \underline{j}^s \neq 0$ e

$$0 = \varphi f(u'_1, \ldots, u'_n) = \beta g(a'_1) \cdots g(a'_n) h(a'_{n+1}) \cdots h(a'_{2n}) = \beta a'_1 \cdots a'_{2n} \underline{i}^r \underline{j}^s,$$

onde na primeira igualdade usamos que $f \in P(\varphi(A))$ e na última usamos que $g(a'_i) = a'_i\underline{1}$ ou $g(a'_i) = a'_i\underline{i}$ e que $h(a'_{n+i}) = a'_{n+i}\underline{1}$ ou $h(a'_{n+i}) = a'_{n+i}\underline{j}$, pois os elementos a'_i com $i \in I_{2n}$

estão na base de E. Com isto mostramos que f é uma identidade de A e assim $P(A) = P(\varphi(A))$. $\square$

Teorema 3.1.36. *Se* $\operatorname{char} K = 0$*,* $M_{1,1}(E)$ *e* $E \otimes E$ *são PI-equivalentes.*

Demonstração. Como já observamos, se $\operatorname{char} K = 0$ todas as identidades seguem das identidades multilineares (Corolário 1.2.29 *(ii)*). E pelo *[TPT multilinear (3)]*, $P(M_{1,1}(E)) = P(E \otimes E)$, donde $T(M_{1,1}(E)) = T(E \otimes E)$, logo $M_{1,1}(E)$ e $E \otimes E$ são PI-equivalentes. $\square$

3.2 O TPT é falso para $M_{1,1}(E)$ e $E \otimes E$ em característica positiva

3.2.1 Calculando Algumas GK-Dimensões

Com o objetivo de demonstar a não PI-equivalência de $M_{1,1}(E)$ e $E \otimes E$, nesta seção encontraremos as GK-dimensões (que definimos no Capítulo 2) de $\operatorname{GKdim} F_m(E \otimes E)$ e $\operatorname{GKdim} F_m(M_{1,1}(E))$, sobre corpos infinitos com $\operatorname{char} K = p > 2$.

Para $\operatorname{char} K = p > 2$; Azevedo, Fidélis e Koshlukov em ([2], [3]), usando identidades graduadas mostraram os seguintes resultados

(1) Se $\mathcal{A} = K \oplus M_{1,1}(E')$, então $T(\mathcal{A}) = T(K \oplus M_{1,1}(E')) = T(E \otimes E)$;

(2) As álgebras $\mathcal{A}$ e $M_{1,1}(E)$ não são PI-equivalentes. Mais ainda,

$$T(\mathcal{A}) = T(E \otimes E) \supsetneq T(M_{1,1}(E)).$$

Com isto nosso objetivo será apresentar uma prova da não PI-equivalência das álgebras $E \otimes E$ e $M_{1,1}(E)$, independente de identidades graduadas, utilizando a Observação 2.2.18.

Para isto mostraremos que

$$\operatorname{GKdim} F_m(E \otimes E) = m.$$

O próximo resultado é devido a Procesi e Berele, para mais detalhes e demonstrações sugerimos uma leitura de ([5],[17]). Nestes artigos são calculadas as GK-dimensões de álgebras relativamente livres de posto finito de algumas álgebras de matrizes.

Teorema 3.2.1. *(Procesi (i) e Berele ((ii),(iii))) Seja K um corpo infinito de característica arbitrária e $m \geqslant 2$. Então:*

(i) $GK\dim F_m(M_n(K)) = (m-1)n^2 + 1$;

(ii) $GK\dim F_m(M_n(E)) = (m-1)n^2 + 1$;

(iii) $GK\dim F_m(M_{a,b}(E)) = (m-1)(a^2+b^2) + 2$.

Para nós será útil o seguinte corolário:

Corolário 3.2.2. *Seja K um corpo infinito de característica arbitrária e $m \geqslant 2$. Então $GK\dim F_m(M_{1,1}(E)) = 2m$.*

Notamos ainda que $\mathrm{GKdim}\, F_m(K) = m$, aplicando $n = 1$ no item (i). Também podíamos ter usado que $F_m(K)$ é isomorfo a $K[x_1, \ldots, x_m]$ e $\mathrm{GKdim}\, K[x_1, \ldots, x_m] = m$, pelo Exemplo 2.2.5.

Lema 3.2.3 (Regev [18])**.** *E', a álgebra de Grassmann sem unidade, sobre um corpo com $\operatorname{char} K = p > 2$ satisfaz $x^p = 0$.*

Corolário 3.2.4. *Sobre um corpo com $\operatorname{char} K = p > 2$, $GK\dim F_m(E') = 0$.*

Demonstração. Como E' é nil de índice limitado, $F_m(E')$ é álgebra finitamente gerada e nil de índice limitado. Logo, pelo Teorema 2.1.14 de Levitzki $\dim_K F_m(E') < \infty$, donde $\mathrm{GKdim}\, F_m(E') = 0$, pela Proposição 2.2.7. □

Lema 3.2.5. *$E' \otimes E'$, sobre um corpo com $\operatorname{char} K = p > 2$ satisfaz $x^{2p} = 0$.*

Demonstração. Começamos mostrando que, $u_p(x_1, \ldots, x_p) = \sum_{\sigma \in S_p} x_{\sigma(1)} \cdots x_{\sigma(p)} \in T(E'_r \otimes E'_s)$, com $r, s \in \{0, 1\}$ fixos, isto é, $u_p(b_1, \ldots, b_p) = 0$ para $b_1, \ldots, b_p \in E'_r \otimes E'_s$. Como u_p é um polinômio multilinear, basta mostrarmos para elementos da base, ou seja, vamos considerar $b_i = a_i \otimes a_{p+i}$, onde $\{a_i\}_{i \in I_n} \subseteq D'_r$ e $\{a_{p+i}\}_{i \in I_n} \subseteq D'_s$. Se $r = s$, temos que $b_i b_j = b_j b_i$. Se $r = 0$ e $s = 1$ (o outro caso é análogo), temos que $b_i b_j = -b_j b_i$ para todo i e j. Assim, seja $c = b_{\sigma(i+1)} \cdots b_{\sigma(j-1)}$, onde $i < j$, $\sigma \in S_p$, $\sigma(i) = 1$ e $\sigma(j) = 2$. Tendo isto em vista, é fácil ver que

$$b_1 c b_2 = -b_2 c b_1.$$

Para $\sigma, \rho \in S_p$, definamos a relação

$$\sigma R \rho \Leftrightarrow \sigma = \rho \text{ ou } \sigma = (12)\rho.$$

Nota-se facilmente que R é relação de equivalência. Deste modo,

$$u_p(b_1, \ldots, b_p) = \begin{cases} p! b_1 \cdots b_p, & \text{se } r = s \\ \displaystyle\sum_{[\sigma] \in S_p/R} \left(b_{\sigma(1)} \cdots b_{\sigma(p)} + b_{(12)\sigma(1)} \cdots b_{(12)\sigma(p)} \right), & \text{se } r \neq s \end{cases} = 0.$$

Nesta segunda etapa, mostramos que $x^p \in T(E'_r \otimes E'_s)$, com $r, s \in \{0, 1\}$ fixos. Seja $b \in E'_r \otimes E'_s$, escrevemos $b = \sum_{i \in I_k} \alpha_i b_i$, onde b_i são elementos da base de $E' \otimes E'$ que estão em $E'_r \otimes E'_s$.

Para $j, l \in I = \{h : I_p \longrightarrow I_k ; h \text{ é injetiva}\}$, definamos a relação

$$jTl \Leftrightarrow \text{Existe } \sigma \in S_p, \text{ tal que } j = l\sigma.$$

Nota-se facilmente que T é relação de equivalência. Deste modo,

$$\begin{aligned} b^p &= \sum_{j : I_p \to I_k} \alpha_{j(1)} \cdots \alpha_{j(p)} b_{j(1)} \cdots b_{j(p)} \\ &= \sum_{j \in I} \alpha_{j(1)} \cdots \alpha_{j(p)} b_{j(1)} \cdots b_{j(p)} \\ &= \sum_{[j] \in I/T} \alpha_{j(1)} \cdots \alpha_{j(p)} \left(\sum_{\sigma \in S_p} b_{j(\sigma(1))} \cdots b_{j(\sigma(p))} \right) \\ &= \sum_{[j] \in I/T} \alpha_{j(1)} \cdots \alpha_{j(p)} \left(u_p(b_{j(1)}, \ldots, b_{j(p)}) \right) \\ &= 0 \end{aligned}$$

Agora finalmente mostraremos que $x^{2p} \in T(E' \otimes E')$. Seja $b \in E' \otimes E'$, escrevemos de forma única $b = b_{00} + b_{11} + b_{10} + b_{01}$, com $b_{rs} \in E'_r \otimes E'_s$.

$$\begin{aligned}
b^{2p} &= ((b_{00} + (b_{11} + b_{10} + b_{01}))^p)^2 \\
&= (b_{00}^p + (b_{11} + b_{10} + b_{01})^p)^2 \\
&= (b_{11} + (b_{10} + b_{01}))^2)^p \\
&= (b_{11}^2 + (b_{10} + b_{01})^2)^p \\
&= b_{11}^{2p} + (b_{10} + b_{01})^{2p} \\
&= ((b_{10} + b_{01})^p)^2 \\
&= (b_{10}^p + b_{01}^p)^2 \\
&= 0
\end{aligned}$$

□

Corolário 3.2.6. *Sobre um corpo com* $\operatorname{char} K = p > 2$, $GK\dim F_m(E' \otimes E') = 0$.

Demonstração. Como $E' \otimes E'$ é nil de índice limitado, $F_m(E' \otimes E')$ é álgebra finitamente gerada e nil de índice limitado. Logo, pelo Teorema 2.1.14 de Levitzki $\dim_K F_m(E' \otimes E') < \infty$, donde $\operatorname{GKdim} F_m(E' \otimes E') = 0$, pela Proposição 2.2.7. □

Teorema 3.2.7. *Se* $\operatorname{char} K = p > 2$, *então* $GK\dim F_m(E \otimes E) = m$.

Demonstração. Pelo Teorema 2.2.21 temos que

$$\begin{aligned}
\operatorname{GKdim} F_m(E \otimes E) &= \max\{\operatorname{GKdim} F_m(K \otimes K), \operatorname{GKdim} F_m(E' \otimes K), \\
&\quad \operatorname{GKdim} F_m(K \otimes E'), \operatorname{GKdim} F_m(E' \otimes E')\} \\
&= \max\{\operatorname{GKdim} F_m(K), \operatorname{GKdim} F_m(E'), \\
&\quad \operatorname{GKdim} F_m(E'),\ \operatorname{GKdim} F_m(E' \otimes E')\} \\
&= m.
\end{aligned}$$

□

Teorema 3.2.8. *Sobre um corpo K infinito de char $= p > 2$, $M_{1,1}(E)$ e $E \otimes E$ não são PI-equivalentes.*

Demonstração. Temos que $\operatorname{GKdim} F_m(M_{1,1}(E)) = 2m$, pelo Corolário 3.2.2. Como $\mathcal{A}$ e $E \otimes E$ são PI-equivalentes, $\operatorname{GKdim} F_m(E \otimes E) = \operatorname{GKdim} F_m(\mathcal{A}) = m$. Assim temos que $\operatorname{GKdim} F_m(E \otimes E) \neq \operatorname{GKdim} F_m(M_{1,1}(E))$ e logo $M_{1,1}(E)$ e $E \otimes E$ não podem ser PI-equivalentes, tendo em vista a Observação 2.2.18. □

BIBLIOGRAFIA

[1] S. M. Alves, *PI equivalência e não equivalência de Álgebras*, Tese de Doutorado - Unicamp (2006).

[2] S. Azevedo, M. Fidellis, P. Koshlukov, *Graded identities and PI equivalence of algebras in positive characteristic*, Commun. Algebra, **33(4)**, 1011–1022, (2005).

[3] S. Azevedo, M. Fidelis, P. Koshlukov, *Tensor products theorems in positive characteristic*, Journal of Algebra **276**, no. 2, 836–845, (2004).

[4] S. Azevedo, P. Koshlukov, *Graded identities for T-prime algebras over fields of positive characteristic*, Israel J. Math., **81(3)**, 343–355, (2002).

[5] A. Berele, *Generic Verbally Prime Algebras and their GK-dimensions*, Commun. Algebra, **21(5)**, 1487–1504, (1993).

[6] A. Berele, *Homogeneous polynomial identities*, Israel J. Math. **42**, 258–272, (1982).

[7] V. Drensky, *Free algebras and PI algebras. Graduate Course in Algebra*, Springer, Singapore, (1999).

[8] V. Drensky, *Gelfand-Kirillov dimension of PI algebras*, Lecture Notes in Pure and Appl. Math. **198**, Denker, New York, 97–113, (1998).

[9] M. Fidélis, *Identidades Polinomiais em Álgebras T-primas*, Tese de Doutorado - Unicamp (2005).

[10] A. Giambruno, M. Zaicev, *Polynomial identities and asymptotic methods*, Math. Surveys Monographs **122**, Amer. Math. Soc., Providence, RI, (2005).

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

[12] G.R. Krause, T.H. Lenagan, *Growth of Algebras and Gelfand-Kirillov Dimension*, Pitman Publ., London, (1985).

[13] U. Leron, A. Vapne, *Polynomial identities of related rings*, Israel Journal of Mathematics **8**, 127–136, (1970).

[14] M.-P. Malliavin-Brameret , *Dimension de Gelfand-Kirillov des algèbres à identités polynomiales*, C.R. Acad. Sci. Paris **282**, 679–681, (1976).

[15] V. Nardozza, O. M. Di Vincenzo, *Graded polynomial identities for tensor products by the Grassmann algebra*, Commun. Algebra, **31 (3)**, 1453–1474, (2003).

[16] V. Nardozza, O. M. Di Vincenzo, $\mathbb{Z}_{k+l} \times \mathbb{Z}_2$*-graded polynomial identities for* $M_{k,l}(E) \otimes E$, Rend. Sem. Mat. Univ. Padova, **108**, 27–39, (2000).

[17] C. Procesi, *Non-comutative Affine Rings*, Atti Accad. Naz. Lincei menh. Cl. Sci. Fis. Mat. Natur. Sez I, **8(8)**, 239–255, (1967).

[18] A. Regev, *Grasmann algebras over finite fields*, Commun. Algebra, **19**, 1829–1849, (1991).

[19] A. Regev, *Tensor products of matrix algebras over the Grassmann algebra*, Journal of Algebra **133**, no. **2**, 512–526, (1990).

[20] A. Regev, *A transposition factorization of walk-permutations in graphs*, Journal of Combinatorial Theory, Series A, **56**, no. **1**, 160–165, (1991).

[21] D. D. P. Silva, *Álgebras Graduadas e Identidades Polinomiais Graduadas* Dissertação de Mestrado - Unicamp (2007).

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