UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Identidades Polinomiais $\mathbb{Z}_n$-graduadas da Álgebra $M_n(F)$

Evandro Riva

SÃO CARLOS - SP

2016

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Identidades Polinomiais $\mathbb{Z}_n$-graduadas da Álgebra $M_n(F)$

Evandro Riva

Orientador: Prof. Dr. Humberto Luiz Talpo

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do Título de Mestre em Matemática.

SÃO CARLOS - SP

2016

Ficha catalográfica elaborada pelo DePT da Biblioteca Comunitária UFSCar
Processamento Técnico
com os dados fornecidos pelo(a) autor(a)

Riva, Evandro
R616i Identidades polinomiais Zn-graduadas da álgebra Mn(F) / Evandro Riva. -- São Carlos : UFSCar, 2016.
54 p.

Dissertação (Mestrado) -- Universidade Federal de São Carlos, 2016.

1. Identidades Polinomiais. 2. G-graduação. 3. Identidades Polinomiais G- graduadas. I. Título.

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Matemática

Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Evandro Riva, realizada em 22/02/2016:

Prof. Dr. Humberto Luiz Talpo
UFSCar

Prof. Dr. Edson Ryoji Okamoto Iwaki
UFABC

Prof. Dr. Waldeck Schutzer
UFSCar

Agradecimentos

A Deus por me dar força interior para suportar as dificuldades e mostrar o caminho nas horas incertas.

A minha família, principalmente ao meu pai Sadi e minha mãe Lucia, por sempre acreditarem que eu seria capaz, sempre passarem os mais puros pensamentos e orações durante toda minha vida. A minha irmã Edina, meu cunhado Volmar e os meus sobrinhos Rafael e Isadora pelo imenso apoio, principalmente você Edina, que sempre me apoiou mesmo distante, sempre rezou e torceu por mim. Também meus avós, tios e primos.

Ao meu orientador professor Humberto, agradeço pela paciência, amizade, conselhos e por todo suporte durante o mestrado.

Aos meus amigos Carlos, Daiana e Mateus que passaram por todos esses momentos ao meu lado, que, inúmeras vezes me auxiliaram e me incentivaram, principalmente você Mateus, pelas quase infinitas horas de estudo e ajuda.

Aos meus amigos da UTFPR e do DM.

Aos meus professores da UTFPR e da UFSCar pela excelente formação que me proporcionaram.

A CAPES pelo suporte financeiro.

A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê (Arthur Schopenhauer)

Resumo

Nesta dissertação estudaremos álgebras G-graduadas e identidades polinomiais G-graduadas, onde G é um grupo aditivo. Como resultado principal descreveremos uma base finita para as identidades polinomiais $\mathbb{Z}_n$-graduadas da álgebra das matrizes $n \times n$, com entradas em um corpo F. Este estudo será subdividido em duas etapas: quando o corpo F for de característica zero e quando o corpo F for infinito. Estes resultados foram descritos por Vasilovsky [18] em 1999 e por Azevedo [2] em 2006.

Palavras Chave: *Identidades Polinomiais, G-graduação, Identidades Polinomiais G-graduadas*

Abstract

In this works we will study G-graded algebras and G-graded polynomial identities, where G is an additive group. For main result we will describe a finite basis for $\mathbb{Z}_n$-graded polynomial identities of the matrix algebra of order $n \times n$, with entries in a field F. This study will be divided into two stages: when the field F has characteristic zero and when the field F is infinite. These results were described by Vasilovsky [18] in 1999 and Azevedo [2] in 2006.

Keywords: *Polynomial Identities, G-graded, G-graded Polynomial Identities* .

Sumário

Introdução

Em matemática, uma importante área na teoria de anéis é a teoria de álgebras que satisfazem identidades polinomiais, conhecidas como PI-álgebras (do inglês *Polynomial Identities*). Esta classe de álgebras é muito ampla e engloba várias classes de álgebras. Sendo assim, existem diversas abordagens e teorias sobre PI-álgebras. Em particular, no decorrer deste trabalho, encontraremos uma base finita para as identidades polinomiais da álgebra das matrizes $n \times n$ com entradas em um corpo F, denotada por $M_n(F)$. A técnica que será utilizada para simplificar o processo de encontrar identidades polinomiais em $M_n(F)$ consiste em introduzir nessa álgebra uma $\mathbb{Z}_n$-graduação, pois, com isso, será possível exibir tal base finita para as identidades polinomiais da álgebra $M_n(F)$. Para isso precisaremos de alguns conceitos que serão apresentados ao longo do texto. Seja X um conjunto enumerável infinito. Denotemos por $F\langle X\rangle$ o F-espaço vetorial com base formada por 1 e pelas palavras $x_{i_1}x_{i_2}\cdots x_{i_n}$ com $x_{i_1}, x_{i_2}, \cdots, x_{i_n} \in X$ e $n \geq 0$. Definiremos a multiplicação entre duas palavras por concatenação, ou seja:

$$(x_{i_1}x_{i_2}\cdots x_{i_n})(x_{j_1}x_{j_2}\cdots x_{j_n}) = x_{i_1}x_{i_2}\cdots x_{i_n}x_{j_1}x_{j_2}\cdots x_{j_n},$$

o F-espaço vetorial $F\langle X\rangle$ é uma álgebra associativa com unidade (palavra vazia) gerada por X. Dizemos que um polinômio $f(x_1, ..., x_n)$ nas variáveis não comutativas $x_1, ..., x_n$ é uma **identidade polinomial** para uma álgebra A se, para quaisquer $a_1, ..., a_n \in A$, tem-se $f(a_1, ..., a_n) = 0$ em A. Se existir um polinômio não nulo com esta propriedade para uma álgebra A então diz-se que A é uma **álgebra com identidade polinomial** ou que A é uma **PI-álgebra** e f é uma identidade polinomial para A. Por exemplo, se A for uma álgebra comutativa, então $f(x_1, x_2) = x_1x_2 - x_2x_1$ é uma identidade polinomial de A e portanto A é uma PI-álgebra. O conjunto das identidades polinomiais de A é denotado por $T(A)$ e este é um ideal da álgebra associativa livre $F\langle X\rangle$ fechado por qualquer endomorfismo desta álgebra. Ideais com esta propriedade são chamados **T-ideais**. Descrever as identidades de A significa encontrar um conjunto gerador para $T(A)$ como T-ideal. Os primeiros trabalhos envolvendo PI-álgebra, apareceram, de forma implícita, por volta da década de 1930 com as pesquisas de Dëhn [3] e Wagner [19], mas somente a partir de 1948, após o artigo de Kaplansky [9] que essa teoria realmente se desenvolveu. Dentre as questões levantadas por Kaplansky, uma era sobre qual seria o menor grau de uma identidade polinomial satisfeita pela álgebra da matrizes de ordem $n \times n$, sobre um corpo. A resposta foi dada em 1950 com o celebrado resultado de Amitsur-Levitzki [1] em que o polinômio

$$St_{2n}(x_1, ..., x_n) = \sum_{\sigma \in S_{2n}} (-1)^{\sigma} x_{\sigma(1)} \cdots x_{\sigma(2n)},$$

onde S_{2n} representa o grupo simétrico de grau $2n$ e $(-1)^{\sigma}$ representa o sinal da permutação $\sigma \in S_{2n}$, chamado de **polinômio standard de grau** $2n$, é uma identidade polinomial para esta álgebra e $2n$ é o menor grau. Este resultado marcou o início de uma nova abordagem à teoria das PI-álgebras, focadas em descrever as identidades polinomiais de uma dada álgebra. As identidades polinomiais da álgebra $M_n(F)$ das matrizes $n \times n$ com entradas em um corpo F são importantes na teoria de PI-álgebras, contudo, sobre corpos infinitos, bases finitas para $T(M_n(F))$ são determinadas somente quando $n = 2$ e característica de F é diferente de 2. O caso em que $n = 3$ ainda está em aberto. Em [13] Razmyslov determinou uma base para as identidades de $M_2(F)$ com 9 elementos no caso em que a característica de F é igual a zero e em [6] Drensky melhorou este resultado dando uma base minimal com duas identidades. Uma base para $M_2(F)$ sobre corpos infinitos de característica $p > 2$ foi determinada por Koshlukov em [11]. Outro conceito importante na área de PI-álgebras é o de identidades graduadas, isto é, seja G um grupo aditivo, então uma álgebra é G-graduada se puder ser escrita como soma direta de subespaços

$$A = \sum_{g \in G} \bigoplus A^{(g)},$$

de modo que, para quaisquer $g, h \in G$ tem-se $A^{(g)} A^{(h)} \subseteq A^{(g+h)}$. Esta área permitiu que Kemer [10] desse uma resposta positiva para o famoso problema de Specht [16] que é o seguinte: "Será que toda álgebra associativa sobre um corpo de característica zero possui uma base finita para suas identidades polinomiais?". Logo após os trabalhos de Kemer, por volta de 1987, as identidades graduadas tornarem-se objeto de pesquisa muito ativa. Consideremos a álgebra associativa livre $F\langle X\rangle$ com $X = \bigcup_{\alpha\in G} X^{(\alpha)}$, em que $\{X^{(\alpha)}; \alpha \in$G$\}$ é uma familia de conjuntos não vazios, enumeráveis infinitos e disjuntos $X^{(\alpha)}$. Observemos que os monômios: $\{x_{i_1}x_{i_2}\dots x_{i_k} : k = 1, 2, ...; x_{i_1}, x_{i_2}, ..., x_{i_k} \in X\}$ formam uma base para $F\langle X\rangle$ como espaço vetorial. Dizemos que uma variável $x \in X$ possui grau homogêneo α, denotado por $\alpha(x) = \alpha$, se $x \in X^{(\alpha)}$. O grau homogêneo de um monômio $n = x_{i_1}x_{i_2}\dots x_{i_k}$ é definido por: $\alpha(n) = \alpha(x_{i_1}) + \alpha(x_{i_2}) + \ldots + \alpha(x_{i_k})$. Para $\alpha \in G$, denote por $F\langle X\rangle^{(\alpha)}$ o subespaço de $F\langle X\rangle$ gerado por todos os monômios que tem grau homogêneo α. Note que: $F\langle X\rangle^{(\alpha)}F\langle X\rangle^{(\beta)} \subseteq F\langle X\rangle^{(\alpha+\beta)}, \forall\alpha, \beta \in G$. Assim,

$$F\langle X\rangle = \sum_{\alpha\in G} \bigoplus F\langle X\rangle^{(\alpha)},$$

torna-se uma álgebra G-graduada. Os elementos da álgebra G-graduada $F\langle X\rangle$ são chamados de polinômios G-graduados ou simplesmente polinômios graduados. Dizemos que um polinômio G-graduado $f(x_1, x_2, ..., x_k)$ é uma **identidade polinomial graduada** para a álgebra G-graduada A se $f(a_1, a_2, ..., a_k) = 0$ para quaisquer $a_i \in A^{(\alpha(x_i))}$, $i = 1, 2, ..., k$. Denotaremos o conjunto das identidades G-graduadas por $T(A)^{gr}$. Aqui vale ressaltar que $T(A)^{gr}$ é um T_G-ideal, ou seja, um ideal de $F\langle X\rangle$ que é fechado para todo endomorfismo G-graduado de $F\langle X\rangle$. Neste trabalho estudaremos bases finitas para as identidades polinomiais $\mathbb{Z}_n$-graduadas da álgebra matricial $M_n(F)$ quando o corpo F tem característica zero e quando o corpo F for infinito de característica p arbitrária, tendo como referência principal os artigos [18] e [2], a dissertação está organizada da seguinte maneira: O primeiro capítulo tratará dos conceitos básicos para um melhor entendimento do restante do trabalho. Iniciaremos com a definição de álgebra e alguns exemplos importantes, logo após, definiremos o conceito de álgebra livre, identidades polinomiais, polinômios multihomogêneos e multilineares e por fim matrizes genéricas. A apresentação desses conceitos será acompanhada pelos resultados e exemplos relevantes e essenciais para uma melhor compreensão da teoria. No capítulo 2, introduziremos o conceito de álgebra G-graduada e daremos alguns exemplos. Após essa definição, descreveremos a $\mathbb{Z}_n$-graduação de $M_n(F)$ e a $\mathbb{Z}_n$-graduação de $F\langle X\rangle$, que serão o foco de atenção no decorrer do trabalho, por fim, definiremos identidades polinomiais G-graduadas, dando alguns exemplos, propriedades e resultados importantes. No terceiro e mais importante capítulo desta dissertação, descrevemos as identidades polinomiais $\mathbb{Z}_n$-graduadas da álgebra $M_n(F)$, quando o corpo F tem característica zero e quando o corpo F é infinito. Seguindo os passos dados por Vasilovsky [18] e por Azevedo [2], em cada caso, tornar-se-á evidente a diferença entre os dois trabalhos, que empregam métodos essecialmente diferentes para a obtenção do mesmo resultado.

Capítulo 1

Preliminares

Neste capítulo, descreveremos alguns conceitos, resultados e definições que usaremos no decorrer do trabalho. Ao longo deste trabalho, F denotará um corpo qualquer, exceto quando especificado o contrário.

1.1 Álgebras

Nesta seção, apresentaremos a definição de álgebra, subálgebra, ideal e homomorfismo de álgebras e relações entre estas estruturas.

Definição 1.1.1. *Seja A um espaço vetorial sobre um corpo F. Dizemos que A é uma* ***F-álgebra*** *se A é munido com uma operação binária $* : (A, A) \longrightarrow A$, chamada produto, tal que, para todos, $a, b, c \in A$ e todo $\lambda \in F$, tem-se:*

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

Usualmente denotamos $a*b = a{\cdot}b = ab$, e ao invés de escrevermos F-álgebra, escreveremos apenas álgebra deixando implícito o corpo F.

Definição 1.1.2. *Dizemos que uma Álgebra é:*

- ***Associativa*** *se o produto de A é associativo, isto é, se $(ab)c = a(bc)$, para quaisquer $a, b, c \in A$.*

- ***Comutativa*** *se o produto é comutativo, isto é, se* $ab = ba$*, para quaisquer* $a, b \in A$.

- ***Unitária (ou com unidade)*** *se* A *possui elemento neutro com relação ao produto, isto é, se existe* $1 \in A$ *tal que* $1a = a1 = a$*, para qualquer* $a \in A$.

Definição 1.1.3. *Um subespaço vetorial* S *de uma álgebra* A *é chamado de* ***subálgebra*** *se* $s_1 s_2 \in S$ *para todos* $s_1, s_2 \in S$.
Um subespaço vetorial I *de* A *é um* ***ideal bilateral*** *de* A *se* $AI \subseteq I$ *e* $IA \subseteq I$.

Exemplo 1.1.4. *Se* L *é uma extensão do corpo* F*, então* L *é uma álgebra com as operações do corpo.*
De fato, basta considerar em L *a operação induzida em* F.

Exemplo 1.1.5. *Considere o conjunto dos polinômios em* n *variáveis comutativas* $x_1, ..., x_n$*, denotado por* $F[x_1, ..., x_n]$*. Este conjunto é claramente um espaço vetorial com relação a soma de polinômios e o produto por escalares do corpo e, com o produto usual de polinômios, é uma álgebra.*

Exemplo 1.1.6. *Para* $n \in \mathbb{N}$*, o espaço* $M_n(F)$ *de todas as matrizes* $n \times n$ *com entradas em* F *é uma álgebra associativa com unidade, munida das operações usuais de soma e produto. Nesta álgebra destacaremos as* ***matrizes elementares*** $E_{i,j}$*, para* $1 \leq i, j \leq n$*, onde* $E_{i,j}$ *é a matriz cuja única entrada não nula é 1, na* i*-ésima linha e na* j*-ésima coluna. Essas matrizes formam uma base para* $M_n(F)$ *como espaço vetorial.*

Exemplo 1.1.7. *Considere as matrizes triangulares superior* $n \times n$ *com entradas em* F*, denotada por* $U_n(F)$*,* $U_n(F)$ *é uma subálgebra de* $M_n(F)$*, cuja base é dada pelo conjunto* $\{E_{i,j}; 1 \leq i \leq j \leq n\}$.

Definição 1.1.8. *Dizemos que o polinômio*

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

é o ***comutador*** *de* x_1 *e* x_2 *de* ***comprimento 2****. Por indução, definiremos o* ***comutador de comprimento*** n *por*

$$[x_1, x_2, ..., x_n] = [[x_1, x_2, ..., x_{n-1}], x_n].$$

Exemplo 1.1.9. *Dizemos que uma álgebra A é uma* ***Álgebra de Lie*** *se para todos $a, b, c \in A$, vale:*

$$\begin{cases} a^2 = aa = 0 \quad \textit{(anti-comutativa)} \\ (ab)c + (bc)a + (ca)b = 0 \quad \textit{(identidade de Jacobi)} \end{cases}$$

Exemplo 1.1.10. *Se A é uma álgebra associativa, o produto dado por $[a, b]$ define em A uma nova estrutura de álgebra, que denotaremos por $A^{(-)}$, e como $[a, a] = 0$ e $[a, b, c] + [b, c, a] + [c, a, b] = 0$ para quaisquer $a, b, c \in A$, segue que $A^{(-)}$ é uma álgebra de Lie.*

Definição 1.1.11. *Sejam A e B duas álgebras. Dizemos que uma transformação linear $f : A \longrightarrow B$ é um* ***homomorfismo de álgebras*** *se $f(ab) = f(a)f(b)$, para todos $a, b \in A$. Dizemos que um homomorfismo de álgebras $f : A \longrightarrow B$ é um* ***isomorfismo*** *se ele for bijetivo.*

Definição 1.1.12. *Seja I um ideal de uma álgebra A. Se $a \in A$, denote por:*

$$\overline{a} = a + I = \{a + i;\ i \in I\}.$$

Observe que $\overline{a}$ é a classe de equivalência de a segundo a relação $\sim$ definida em A por $a \sim b \Leftrightarrow (a - b) \in I$.
O conjunto $\dfrac{A}{I} = \{\overline{a};\ a \in A\}$ é o espaço quociente de A por I. Relembramos que com as operações:

$$\begin{cases} \overline{a_1} + \overline{a_2} = \overline{a_1 + a_2} \\ \alpha\overline{a} = \overline{\alpha a}, \end{cases}$$

onde $a_1, a_2 \in A$ e $\alpha \in F$, temos que $\dfrac{A}{I}$ é um F-espaço vetorial. Agora definindo

$$\overline{a_1} * \overline{a_2} = \overline{a_1 * a_2},$$

temos que $\dfrac{A}{I}$ é uma álgebra, chamada ***álgebra quociente****. Um conceito que será frequentemente usado no decorrer do capítulo 3 é o de congruência, ou seja, dados A uma álgebra e I um ideal de A se $a, b \in A$, dizemos que a é* ***congruente a*** b ***módulo I****, se $a - b \in I$, usualmente escrevemos $a \equiv b$ mod I.*

Teorema 1.1.13. *Seja $f : A_1 \longrightarrow A_2$ um homomorfismo de álgebras. O núcleo de f, denotado por $Ker(f) = \{a \in A_1; f(a) = 0\}$ é um ideal de A_1 e $\dfrac{A_1}{Ker(f)} \cong Im(f)$.*

A demonstração deste teorema é análoga ao caso de anéis.

1.2 Álgebra Livre

Neste seção, estudaremos o conceito de álgebra livre, para isto, seja A uma álgebra e $X \subseteq A$. Considere $Pal(X)$ o conjunto das palavras formadas pelos elementos de X. Se todo elemento em A é uma combinação linear dos elementos em $Pal(X)$, então dizemos que A é **gerado** por X.

Definição 1.2.1. *Definiremos o* ***comprimento*** *da palavra $x_{i_1} \cdots x_{i_n}$ como sendo n, quando $n = 0$, chamaremos essa palavra de* ***palavra vazia*** *que denotaremos por 1. Além disso, dizemos que duas palavras $x_{i_1} \cdots x_{i_n}$ e $x_{j_1} \cdots x_{j_m}$ são iguais se $n = m$ e $i_1 = j_1, ..., i_n = j_m$.*

Definição 1.2.2. *Seja V uma classe de álgebras e $A \in V$ uma álgebra gerada por um conjunto X. A álgebra A é chamada* ***livre na classe V, livremente gerada por X****, se para qualquer álgebra $R \in V$, toda função $g : X \longrightarrow R$ pode ser estendida a um homomorfismo de álgebras $G : A \longrightarrow R$.*

Definição 1.2.3. *Seja X um conjunto enumerável infinito. Denote por $F\langle X \rangle$ o F-espaço vetorial com base formada por 1 e pelas palavras*

$$x_{i_1} x_{i_2} \cdots x_{i_n},$$

onde $x_{i_1}, x_{i_2}, ..., x_{i_n} \in X$ e $n \geq 0$. Definiremos a multiplicação entre duas palavras por concatenação, ou seja:

$$(x_{i_1} x_{i_2} \cdots x_{i_n})(x_{j_1} x_{j_2} \cdots x_{j_n}) = x_{i_1} x_{i_2} \cdots x_{i_n} x_{j_1} x_{j_2} \cdots x_{j_n}.$$

Estendendo por linearidade este produto para todos os elementos de $F\langle X \rangle$, então $F\langle X \rangle$ é álgebra associativa com unidade (palavra vazia) gerada por X.

Proposição 1.2.4. *A álgebra $F\langle X \rangle$ é livre na classe de todas as álgebras associativas unitárias, livremente gerada por X.*

Demonstração: Se $p \in F\langle X\rangle$, denotamos $p = p(x_1, ..., x_n)$ se ele é formado pelos elementos $x_1, ..., x_n$. Seja $g : X \longrightarrow R$ uma função, onde R é uma álgebra associativa com unidade. Denote $g(x_i) = r_i$, para todo i e definiremos $G : F\langle X\rangle \longrightarrow R$ por $G(p(x_1, ..., x_n)) = p(r_1, ..., r_n)$.
Então G é um homomorfismo de álgebras que estende g. $\square$

Definição 1.2.5. *Seja A um espaço vetorial com base ordenada*

$$\{e_i, i \in I\} \tag{1.1}$$

onde I é um conjunto enumerável.

*A **álgebra de Grassmann** $E(A)$ é a álgebra associativa gerada pelo conjunto 1.1 que satisfaz:*

$$e_ie_j = -e_je_i,$$

para todo $i, j \in I$ e também

$$e_i^2 = 0,$$

se a característica de F é 2. Destacamos na álgebra de Grassmann os seguintes subespaços vetoriais:

- $E^{(\bar{0})}$*, gerado pelo conjunto* $\{1, e_{i_1}e_{i_2}\cdots e_{i_m}$*: m é par*$\}$
- $E^{(\bar{1})}$*, gerado pelo conjunto* $\{e_{i_1}e_{i_2}\cdots e_{i_m}$*: m é ímpar*$\}$

Temos que $E = E^{(\bar{0})} \oplus E^{(\bar{1})}$, como espaço vetorial. Veremos no próximo capítulo que a álgebra de Grassmann, com esta estrutura de soma direta, é uma álgebra graduada.

1.3 Identidades Polinomiais

Nesta seção, veremos alguns conceitos importantes sobre Identidades Polinomiais, além de exemplos para melhor compreensão desta teoria. De agora em diante, X denotará o conjunto enumerável $X = \{x_1, x_2, ...\}$ e $F\langle X\rangle$ é a álgebra associativa livre, livremente gerada por X.

Definição 1.3.1. *Seja A uma álgebra associativa e $f(x_1, ..., x_n) = f \in F\langle X\rangle$. Dizemos que f é uma* ***identidade polinomial*** *para A se $f(r_1, ..., r_n) = 0$ para todos $r_1, ..., r_n \in A$. Denotamos por $T(A)$ o conjunto das identidades polinomiais de A. Se $T(A) \neq \{0\}$ dizemos que A é uma* ***PI - álgebra****.*

Exemplo 1.3.2. *O polinômio nulo $f = 0$ é sempre uma identidade polinomial para qualquer álgebra A e é chamado* ***identidade polinomial trivial de A****.*

Exemplo 1.3.3. *Se A for uma álgebra comutativa, então A é uma PI-álgebra, a saber, $f(x_1, x_2) = [x_1, x_2] \in T(A)$.*

Definição 1.3.4. *Seja A uma álgebra, o centro de A, denotado por $\mathcal{Z}(A)$, é dado pelo conjunto:*

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

Exemplo 1.3.5. *Seja E a álgebra de Grassmann definida em 1.2.5 então:*

$$f(x_1, x_2, x_3) = [x_1, x_2, x_3] \in T(E).$$

De fato, denote por B a base de E formada por $b = e_{i_1}e_{i_2}\cdots e_{i_n}$, onde $i_1 < i_2 < \cdots < i_n$ e $n \geq 0$. Note que:

$$(e_{i_1}e_{i_2}\cdots e_{i_n})(e_{j_1}e_{j_2}\cdots e_{j_n}) = (-1)^{\sigma}(e_{j_1}e_{j_2}\cdots e_{j_n})(e_{i_1}e_{i_2}\cdots e_{i_n}),$$

onde $(-1)^{\sigma}$ é o sinal da permutação $\sigma \in S_n$ e S_n é o grupo simétrico de grau n. Assim, se n é par, então $b \in \mathcal{Z}(E)$ (centro de E).
Agora, sejam $b_1, b_2, b_3 \in B$ temos:

- $[b_1, b_2, b_3] = [[b_1, b_2], b_3] = 0$ *se o comprimento de b_1, b_2 ou b_3 é par.*
- $[b_1, b_2, b_3] = [[b_1, b_2], b_3] = [2b_1b_2, b_3] = 0$ *se os comprimentos de b_1, b_2 e b_3 são ímpares.*

Exemplo 1.3.6. *Tome a álgebra $M_2(F)$ das matrizes 2×2 com entradas no corpo F, o polinômio:*

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

chamado de ***polinômio de Hall****, é uma identidade polinomial para $M_2(F)$.*
Com efeito, seja

$$a = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

O polinômio característico de a é $p(x) = x^2 - traço(a)x + det(a)$*, agora usando o Teorema de Cayley-Hamilton, segue que* $p(a) = a^2 - traço(a)a + det(a)Id_2 = 0$.
Se b_1, b_2 *são matrizes quaisquer em* $M_2(F)$ *e* $a = [b_1, b_2]$ *então* $traço(a) = 0$ *e também* $[b_1, b_2]^2 = -det([b_1, b_2])Id_2 \in \mathcal{Z}(M_2(F))$*. Logo, para* $b_3 \in M_2(F)$ *temos* $[[b_1, b_2]^2, b_3] = 0$

Exemplo 1.3.7. *A álgebra das matrizes triangulares superior de oredem* n*,* $U_n(F)$*, satisfaz a identidade*

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

De fato, se $r_1, r_2 \in U_n(F)$*, então* $[r_1, r_2]$ *pertence a* $U_n(F)$ *e possui diagonal nula. Como o produto de* n *matrizes em* $U_n(F)$*, com diagonal nula, é a matriz nula, segue o resultado.*

Definição 1.3.8. *Fixado* n *denote por*

$$St_n(x_1, ..., x_n) = \sum_{\sigma \in S_n} (-1)^\sigma x_{\sigma(1)} \cdots x_{\sigma(n)},$$

o ***polinômio standard de grau n****, onde* S_n *é o grupo simétrico de grau* n *e* $(-1)^\sigma$ *é o sinal da permutação* σ*.*

Exemplo 1.3.9. *Toda álgebra de dimensão finita é uma PI-álgebra.*
De fato, seja A *uma álgebra de dimensão finita e* $\mathcal{B} = \{v_1, ..., v_m\}$ *uma base para* A*. Suponha* $m < n$ *e tome* $a_1, ..., a_n \in \mathcal{B}$*, escreva* $a_i = \sum_{j=1}^{m} \alpha_{ij} v_j$*. Então temos que*

$$St_n(a_1, ..., a_n) = \sum_{j_1=1}^{m} \cdots \sum_{j_n=1}^{m} (\alpha_{1j_1} \cdots \alpha_{nj_n}) St_n(v_{j_1}, ..., v_{j_n}) = 0,$$

ou seja, se uma álgebra tem dimensão finita, temos que o polinômio standard de grau n é uma identidade polinomial para esta álgebra.

Definição 1.3.10. *Dizemos que um ideal* I *de* $F\langle X \rangle$ *é um* ***T-ideal****, se* $\varphi(I) \subseteq I$ *para todo endomorfismo* φ *de* $F\langle X \rangle$*. Em outras palavras,* I *é um T-ideal se é invariante sob todos os endomorfismos de* $F\langle X \rangle$*.*

Proposição 1.3.11. *O conjunto $T(A)$ das identidades polinomiais de uma álgebra A é um T-ideal de $F\langle X\rangle$. Reciprocamente, se I é um T-ideal de $F\langle X\rangle$, então existe alguma álgebra R tal que $T(R) = I$*

Demonstração: Sejam $f(x_1, ..., x_n) \in T(A)$ e $\varphi \in \mathrm{End}(F\langle X\rangle)$, se $\psi : F\langle X\rangle \longrightarrow A$ é um homomorfismo qualquer, então $\psi(\varphi(f)) = (\psi \circ \varphi)(f) = 0$, pois $\psi \circ \varphi : F\langle X\rangle \longrightarrow A$ é um homomorfismo de álgebras e $f \in T(A)$. Logo, $\varphi(f) \in \mathrm{Ker}(\psi)$ e portanto $\varphi(f) \in T(A)$.
Reciprocamente, seja I um T-ideal de $F\langle X\rangle$. Tomemos a álgebra quociente $R = \dfrac{F\langle X\rangle}{I}$ e a projeção canônica $\pi : F\langle X\rangle \longrightarrow \dfrac{F\langle X\rangle}{I}$. Se $f \in T(R)$, então $f \in \mathrm{Ker}(\pi) = I$, assim temos, $T(R) \subseteq I$. Por outro lado, se $f(x_1, ..., x_n) \in I$ e $g_1, ..., g_n \in F\langle X\rangle$, então, $f(g_1, ..., g_n) \in I$ e daí $f(\overline{g_1}, ..., \overline{g_n}) = \overline{f(g_1, ..., g_n)} = \overline{0}$. Logo, $f \in T(R)$. □

Definição 1.3.12. *Seja $S \subseteq F\langle X\rangle$, o T-**ideal gerado por** S, denotado por $\langle S\rangle^T$, é o conjunto:*

$$\langle S\rangle^T = Span_F \ \{p_1 \ \varphi(f) \ p_2 : f \in S, \varphi \in End(F\langle X\rangle), p_1, p_2 \in F\langle X\rangle\}.$$

Exemplo 1.3.13. *Se A é uma álgebra comutativa e com unidade e F é um corpo infinito, então*

$$T(A) = \langle [x_1, x_2]\rangle^T.$$

Exemplo 1.3.14. *Em [13] Razmyslov determinou uma base para as identidades de $M_2(F)$ com 9 elementos no caso em que a característica de F é igual a zero e em [6] Drenski melhorou este resultado dando uma base minimal com duas identidades, a saber,*

$$T(M_2(F)) = \langle St_4(x_1, x_2, x_3, x_4), [[x_1, x_2]^2, x_3]\rangle^T.$$

Isto é, a base das identidades é gerado pelo polinômio standard de grau 4 e pelo polinômio de Hall.

A demonstração dos resultados apresentados nos próximos exemplos podem ser encontradas em [5] páginas 50 e 52 respectivamente.

Exemplo 1.3.15. *Se F for um corpo infinito de característica diferente de 2, então*

$$T(E) = \langle [x_1, x_2, x_3]\rangle^T,$$

onde E é a álgebra de Grassmann infinatamente gerada por $e_1, e_2, ...$.

Exemplo 1.3.16. *Seja F um corpo de característica 0 e seja $U_n(F)$ a álgebra das matrizes triangulares superior. Então*

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

1.4 Polinômios multi-homogêneos e multilineares

Nesta seção, estudaremos polinômios multi-homogêneos e multilineares, que serão essenciais no decorrer do trabalho, pois, quando um corpo é infinito então o conjunto gerador das identidades polinomiais da álgebra sobre este corpo é formado por polinômios multi-homogêneos, e quando o corpo tem característica zero então o conjunto gerador das identidades polinomiais da álgebra é formado pelos seus polinômios multilineares, e este fato será frequentemente usado, principalmente no capítulo 3.

Definição 1.4.1. *Sejam $m \in F\langle X \rangle$ um monômio, $f \in F\langle X \rangle$ um polinômio e $x_i \in X$. Definiremos:*

a) *O grau de m em x_i ($\deg_{x_i} m$) como sendo o número de vezes que a variável x_i aparece em m.*

b) *O grau de f em x_i ($\deg_{x_i} f$) como sendo o maior grau em x_i de algum monômio de f*

Um polinômio $f \in F\langle X \rangle$ é dito **homogêneo em** x_i se todos os seus monômios têm o mesmo grau em x_i. O polinômio f é dito **multi-homogêneo** quando é homogêneo em todas as variáveis.

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

Sendo $f(x_1, \ldots, x_n) \in F\langle X\rangle$ homogêneo de grau m em x_i e $\lambda \in F$, temos

$$f(x_1, \ldots, x_{i-1}, \lambda x_i, x_{i+1}, \ldots, x_n) = \lambda^m f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n).$$

Particularmente, se f é homogêneo de grau 1 em x_i (ou **linear em** x_i), temos

$$f(x_1, \ldots, x_{i-1}, \lambda x_i, x_{i+1}, \ldots, x_n) = \lambda f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n).$$

Também não é difícil ver que se $f(x_1, \ldots, x_n)$ é linear em x_i, então

$$f(x_1, \ldots, x_{i-1}, y_1 + \ldots + y_m, x_{i+1}, \ldots, x_n) = \sum_{j=1}^{m} f(x_1, \ldots, x_{i-1}, y_j, x_{i+1}, \ldots, x_n).$$

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

$$\sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \ldots x_{\sigma(n)} \quad , \text{ com } \alpha_\sigma \in F.$$

Exemplo 1.4.2. *Seja $f(x_1, x_2, x_3) = x_1x_3 + 2x_2x_3x_2 - x_2^2x_3$. Temos que x_1x_3 e $2x_2x_3x_2 - x_2^2x_3$ são as duas componentes multi-homogêneas de f, sendo que a primeira tem multigrau $(1, 0, 1)$ enquanto a segunda tem multigrau $(0, 2, 1)$.*

Exemplo 1.4.3. *O polinômio standard de grau n, é multilinear de multigrau $\underbrace{(1, 1, \ldots, 1)}_{n}$, também chamado de **multilinear de grau** n.*

Definição 1.4.4. *Dois conjuntos de polinômios são PI-**equivalentes** ou apenas **equivalentes** se eles geram o mesmo T-ideal.*

Teorema 1.4.5. *Seja $f(x_1, ..., x_n) = \sum_{i=0}^{n} f_i(x_1, ..., x_n)$, onde f_i é a componente homogênea de f de grau i em x_1.*
(i) Se F contém mais que n elementos então

$$\langle f_0, f_1, ..., f_n\rangle^T = \langle f\rangle^T.$$

(ii) Se característica de F é igual a zero, então f é PI-equivalente a um conjunto de polinômios multilineares.

Demonstração: *Demonstração do item (i):*

A inclusão $\supseteq$ é direta.

Para provar a outra inclusão é suficiente mostrar que:

$$f_0, f_1, ..., f_n \in \langle f \rangle^T.$$

Sejam $\alpha_0, \alpha_1, ..., \alpha_n \in F$ distintos. Como $\langle f \rangle^T$ é T-ideal temos que

$$f(\alpha_j x_1, x_2, ..., x_n) = \sum_{i=0}^{n} f_i(\alpha_j x_1, x_2, ..., x_n) = \sum_{i=0}^{n} \alpha_j^i f_i(x_1, x_2, ..., x_n),$$

está em $\langle f \rangle^T$ para todo $j = 0, 1, ..., n$. Em notação matricial fica:

$$\underbrace{\begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \cdots & \alpha_0^n \\ 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^n \end{pmatrix}}_{A} \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} f(\alpha_0 x_1, x_2, ..., x_n) \\ f(\alpha_1 x_1, x_2, ..., x_n) \\ \vdots \\ f(\alpha_n x_1, x_2, ..., x_n) \end{pmatrix}$$

A matriz A, é a matriz de Vandermonde que tem determinante

$$det(A) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i) \neq 0.$$

Logo, A é invertível, assim temos que:

$$\begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_n \end{pmatrix} = \underbrace{\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n+1} \\ b_{21} & b_{22} & \cdots & b_{2n+1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n+1\ 1} & b_{n+1\ 2} & \cdots & b_{n+1n+1} \end{pmatrix}}_{A^{-1}} \begin{pmatrix} f(\alpha_0 x_1, x_2, ..., x_n) \\ f(\alpha_1 x_1, x_2, ..., x_n) \\ \vdots \\ f(\alpha_n x_1, x_2, ..., x_n) \end{pmatrix}$$

e portanto,

$$f_0, f_1, ..., f_n \in Span\{f(\alpha_0 x_1, x_2, ..., x_n), ..., f(\alpha_n x_1, x_2, ..., x_n)\} \subseteq \langle f \rangle^T.$$

Demonstração do item (ii):

Escreva

$$f(x_1, ..., x_m) = \sum_{n_1, ..., n_m \geq 0} f^{(n_1, ..., n_m)}(x_1, ..., x_m),$$

onde $f^{(n_1,...,n_m)} \in F\langle x_1, ..., x_m\rangle$ é a componente multi-homogênea de f com multigrau $(n_1, ..., n_m)$.

Aplicando algumas vezes o item (i) teremos:

$$\langle f\rangle^T = \langle f^{(n_1,...,n_m)}; n_1, ..., n_m \geq 0\rangle^T.$$

Se provarmos que $f^{(n_1,...,n_m)}$ é PI-equivalente a um conjunto de polinômios multilineares $s^{(n_1,...,n_m)}$ então

$$\langle f\rangle^T = \langle \bigcup_{n_1,...,n_m \geq 0} s^{(n_1,...,n_m)}\rangle^T.$$

Se $\{x_{ij} : i = 1, ...m \;\text{ e }\; j = 1, ..., n_i\}$ é um conjunto de variáveis distintas em X então:

$$f^{(n_1,...,n_m)}(x_{11} + \cdots + x_{1n_1}, ..., x_{m1} + \cdots + x_{mn_m}) = g,$$

está em $\langle f^{(n_1,...,n_m)}\rangle^T$.

Denotando por $h^{(n_1,...,n_m)}(x_{11}, ..., x_{1n_1}, ..., x_{m1}, ..., x_{mn_m})$ a componente multilinear de g nas variáveis x_{ij}'s, temos que, pela parte (i)

$$h^{(n_1,...,n_m)} \in \langle f^{(n_1,...,n_m)}\rangle^T.$$

Note também que

$$h^{(n_1,...,n_m)}(\underbrace{x_1, ..., x_1}_{n_1\text{fatores}}, ..., \underbrace{x_m, ..., x_m}_{n_m\text{fatores}}) = \underbrace{(n_1!) \cdots (n_m!)}_{\neq 0} f^{(n_1,...,n_m)}.$$

Logo,

$$\langle f^{(n_1,...,n_m)}\rangle^T = \langle h^{(n_1,...,n_m)}\rangle^T.$$

Este processo é chamado de **linearização** de $f^{(n_1,...,n_m)}$ $\square$

Exemplo 1.4.6. *Seja F com característica de zero, encontraremos um conjunto de identidades polinomiais multilineares que é PI-equivalente a identidade $f(x_1) = x_1^3$.*

De fato, considere o conjunto de variáveis distintas $\{y_1, y_2, y_3\}$ e fazendo:

$$\begin{aligned}
f(y_1 + y_2 + y_3) &= (y_1 + y_2 + y_3)^3 = (y_1 + y_2 + y_3)(y_1 + y_2 + y_3)(y_1 + y_2 + y_3) \\
&= (y_1 + y_2 + y_3)(y_1y_1 + y_1y_2 + y_1y_3 + y_2y_1 + y_2y_2 + y_2y_3 + y_3y_1 + y_3y_2 + y_3y_3) \\
&= \underbrace{y_1y_2y_3 + y_1y_3y_2 + y_2y_1y_3 + y_2y_3y_1 + y_3y_1y_2 + y_3y_2y_1}_{h(y_1,y_2,y_3)} + g(y_1, y_2, y_3)
\end{aligned}$$

onde $h(y_1, y_2, y_3)$ é a componente multilinear de $f(y_1+y_2+y_3)$ e $g(y_1, y_2, y_3)$ é a componete multi-homogênea de $f(y_1 + y_2 + y_3)$. Logo, f é PI-equivalente a $\{h\}$.

Proposição 1.4.7. *Toda PI-álgebra (sobre qualquer corpo) satisfaz uma identidade polinomial multilinear.*

Demonstração: Seja R uma PI-álgebra (sobre qualquer corpo) e suponha que $f(x_1, \ldots, x_n) \in F\langle X\rangle$ é uma identidade polinomial para R. Suponha que o grau de f na variável x_1 é n. Aplicaremos o processo de linearização em f. Primeiro, substituindo x_1 por $x_{11} + x_{12}$, temos

$$0 = f(x_{11} + x_{12}, x_2, \ldots, x_n) =$$

$$(f(x_{11} + x_{12}, x_2, \ldots, x_n) - f(x_{11}, x_2, \ldots, x_n) - f(x_{12}, x_2, \ldots, x_n))+$$

$$+f(x_{11}, x_2, \ldots, x_n) + f(x_{12}, x_2, \ldots, x_n).$$

Mas como f é identidade polinomial para R temos que o polinômio

$$f_1(x_{11}, x_{12}, x_2, \ldots, x_n) = f(x_{11} + x_{12}, \ldots, x_n) - f(x_{11}, x_2, \ldots, x_n) - f(x_{12}, x_2, \ldots, x_n),$$

é uma identidade polinômial para R e o grau de f_1 em x_{11} e em x_{12} é no máximo $n - 1$. Agora, aplicaremos o processo, caso seja necessário, para f_1 nas variáveis x_{11} e x_{12}. Substituindo x_{11} por $x_{11} + x_{12}$ e x_{12} por $x_{13} + x_{14}$ temos

$$0 = f_1(x_{11} + x_{12}, x_{13} + x_{14}, x_2, \ldots, x_n) =$$

$$\left(f_1(x_{11} + x_{12}, x_{13} + x_{14}, x_2, \ldots, x_n) - \sum_{\substack{i=1,2,\\ j=3,4}} f_1(x_{1i}, x_{1j}, x_2, \ldots, x_n) \right) +$$

$$+ \sum_{\substack{i=1,2,\\ j=3,4}} f_1(x_{1i}, x_{1j}, x_2, \ldots, x_n).$$

Mas como f_1 é identidade polinomial para R temos que

$$f_2(x_{11}, x_{12}, x_{13}, x_{14}, x_2, \ldots, x_n) = f_1(x_{11}+x_{12}, x_{13}+x_{14}, x_2, \ldots, x_n) - \sum_{\substack{i=1,2,\\ j=3,4}} f_1(x_{1i}, x_{1j}, x_2, \ldots, x_n),$$

é identidade polinomial para R e o grau de f_2 em x_{11}, x_{12}, x_{13} e x_{14} é no máximo $n - 2$.

Repetindo esse processo, após alguns passos, caso sejam necessários, encontraremos uma identidade

$$f_{n-1}(x_{11}, x_{12}, \ldots, x_{1,2^{n-1}}, x_2 \ldots, x_n)$$

para R tal que o grau de f_{n-1} nas variáveis $x_{11}, x_{12}, \ldots, x_{1,2^{n-1}}$ é no máximo 1.
Agora, repetindo o argumento para as variáveis $x_2, \ldots, x_n$ encontraremos uma identidade polinomial multilinear para R. $\square$

1.5 O Teorema de Amitsur-Levitzki

Nesta seção, apresentaremos a demonstração de Teorema de Amitsur-Levitzki feita por Rosset [15] em 1976, além desta demonstração existem outras, a demonstração original de Amitsur e Levitzki [1], B. Kostant [12], R. Swan [17] e Yu. Razmyslov [14], todas usando diferentes ferramentas para sua demonstração.
Iniciamos com o seguinte lema:

Lema 1.5.1. *A álgebra $M_n(F)$ não satisfaz identidades polinomiais de grau menor que $2n$.*

Demonstração: Suponha o contrário, ou seja, existe $f(x_1, x_2, ..., x_m) \in F\langle X\rangle$ uma identidade polinomial não nula para $M_n(F)$, com $m < 2n$. Pela proposição 1.4.7, podemos supor $f(x_1, x_2, ..., x_m)$ uma identidade polinomial multilinear.
Agora fazendo:

$$f(x_1, x_2, ..., x_m)x_{m+1} \cdots x_{2n-1} = g(x_1, ..., x_{2n-1})$$

e escrevendo

$$g(x_1, ..., x_{2n-1}) = \sum_{\sigma \in S_{2n-1}} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(2n-1)},$$

podemos supor $\alpha_{id} \neq 0$ e assim temos

$$0 = g(E_{1,1}, E_{1,2}, E_{2,2}, E_{2,3}, ..., E_{n-1,n-1}, E_{n-1,n}, E_{n,n}) = \alpha_{id} E_{1,n} \Rightarrow \alpha_{id} = 0.$$

Absurdo. $\square$

Lema 1.5.2. *Se o polinômio standard de grau $2n$ é uma identidade para $M_n(\mathbb{Q})$, então é também para $M_n(F)$.*

Demonstração: Definiremos:
$\varphi : M_n(\mathbb{Z}) \longrightarrow M_n(F)$, com $\varphi((a_{ij})_{ij}) = (a_{ij} \cdot 1_F)_{ij}$, onde, 1_F é o elemento neutro do corpo F com relação ao produto. Note que φ é homomorfismo de anéis.
Se $E_1, ..., E_{2n}$ são matrizes elementares em $M_n(\mathbb{Z})$ então $\varphi(E_1), ..., \varphi(E_{2n})$ são matrizes elementares em $M_n(F)$. Assim

$$St_{2n}(\varphi(E_1), ..., \varphi(E_{2n})) = \varphi(St_{2n}(E_1, ..., E_{2n})) = \varphi(0) = 0.$$

□

Lema 1.5.3. *Seja C uma álgebra comutativa sobre $\mathbb{Q}$. Se $a \in M_n(C)$ e*

$$\textit{traço}(a) = \textit{traço}(a^2) = \cdots = \textit{traço}(a^n) = 0.$$

então $a^n = 0$.

A prova deste resultado pode ser vista em [5] página 82.
O próximo resultado é o famoso Teorema de Amitsur e Levitzki.

Teorema 1.5.4. *O polinômio standard de grau $2n$ é uma identidade polinomial para a álgebra $M_n(F)$.*

Demonstração: Pelo lema 1.5.2 é suficiente considerar o caso $F = \mathbb{Q}$.
Decomponha a $\mathbb{Q}$-álgebra de Grassmann E em $E^{(\bar{0})} \oplus E^{(\bar{1})}$ como em 1.2.5.
Dados $a_1, ..., a_{2n} \in M_n(\mathbb{Q})$ definiremos $b \in M_n(E)$ por:

$$b = a_1e_1 + a_2e_2 + \cdots a_{2n}e_{2n}.$$

Temos

$$a = b^2 = \sum_{1 \leq i < j \leq 2n} (a_ia_j - a_ja_i)e_ie_j.$$

Note que $a \in M_n(E^{(\bar{0})})$ onde $E^{(\bar{0})}$ é $\mathbb{Q}$-álgebra comutativa. Além disso,

$$\text{traço}(a) = \text{traço}(a^2) = \cdots = \text{traço}(a^n) = 0.$$

De fato,

$$\text{traço}(a) = \text{traço}(b^{2j}) = \text{traço}(b^{2j-1} \cdot b) =$$

$$-\text{traço}(b \cdot b^{2j-1}) = -\text{traço}(b^{2j}) = -\text{traço}(a^j) \Rightarrow \text{traço}(a^j) = 0.$$

Segue do lema 1.5 que $a^n = 0$. Então:

$$\begin{aligned} 0 = a^n = b^{2n} &= \sum_{\sigma \in S_{2n}} (a_{\sigma(1)} e_{\sigma(1)}) \cdots (a_{\sigma(2n)} e_{\sigma(2n)}) \\ &= \sum_{\sigma \in S_{2n}} (a_{\sigma(1)} \cdots a_{\sigma(2n)}) e_{\sigma(1)} \cdots e_{\sigma(2n)} \\ &= St_{2n}(a_1, ..., a_{2n})(e_1 \cdots e_{2n}) \end{aligned}$$

Portanto, $St_{2n}(a_1, ..., a_n) = 0$ □

Observação 1.5.5. *Mesmo conhecendo-se o grau mínimo para as identidades polinomiais da álgebra $M_n(F)$ não se conhece uma base no caso geral.*

1.6 Matrizes Genéricas

Outro conceito importante para o trabalho é o de matrizes genéricas, esta teoria é uma importante ferramenta para a caracterização das identidades $\mathbb{Z}_n$-graduadas de $M_n(F)$, que veremos no capítulo 3. Aqui daremos uma breve introdução sobre este assunto, para isso denote por Ω_n a álgebra comutativa livre

$$\Omega_n = F[y_{pq}^{(i)} : p, q = 1, ..., n \text{ e } i \in \mathbb{N}],$$

livremente gerada pelas variáveis $y_{pq}^{(i)}$.

Definição 1.6.1. *As matrizes $y_i = \sum_{p,q=1}^{n} y_{pq}^{(i)} E_{pq}$ onde $i \in \mathbb{N}$ são chamadas de **matrizes genéricas**. A subálgebra R_n de $M_n(\Omega_n)$ gerada por $y_1, y_2, ..., y_i, ...$ é chamada de **álgebra das matrizes genéricas** $n \times n$.*

Exemplo 1.6.2. *Tomando R_2 a subálgebra de $M_2(\Omega_2)$ temos que ela é gerada por:*

$$y_1 = \begin{pmatrix} y_{11}^{(1)} & y_{12}^{(1)} \\ y_{21}^{(1)} & y_{22}^{(1)} \end{pmatrix}, \ y_2 = \begin{pmatrix} y_{11}^{(2)} & y_{12}^{(2)} \\ y_{21}^{(2)} & y_{22}^{(2)} \end{pmatrix}, \ldots$$

Teorema 1.6.3. *Se F é infinito então* $\dfrac{F\langle X\rangle}{T(M_n(F))} \cong R_n$.

Demonstração: Considere o homomorfismo $\varphi : F\langle X\rangle \longrightarrow R_n$ tal que $\varphi(x_i) = y_i$, para todo $i \in \mathbb{N}$. Como φ é sobrejetora, segue que

$$\frac{F\langle X\rangle}{Ker\ \varphi} \cong R_n.$$

Mostremos que $Ker\ \varphi = T(M_n(F))$.

Seja $f(x_1, ..., x_n) \in Ker\ \varphi$. Dados $a_1, ..., a_m \in M_n(F)$, devemos mostrar que $f(a_1, ..., a_m) = 0$. Escreva

$$a_i = \sum_{p,q=1}^{n} a_{pq}^{(i)} E_{pq}.$$

Considere $\psi : \Omega_n \longrightarrow F$ homomorfismo tal que $\psi(y_{pq}^{(i)}) = a_{pq}^{(i)}$, para todos i, p, q. A função $\overline{\psi} : M_n(\Omega_n) \longrightarrow M_n(F)$ definida por $\overline{\psi}((b_{pq})_{pq}) = (\psi(b_{pq}))_{pq}$ é um homomorfismo.

Observe que $\overline{\psi}(y_i) = a_i$, para todo i. Temos:

$$f(a_1, ..., a_m) = f(\overline{\psi}(y_1), ..., \overline{\psi}(y_m)) = \overline{\psi}(f(y_1, ..., y_m)) = \overline{\psi}(0) = 0,$$

pois, $f \in Ker\ \varphi$ e $0 = \varphi(f(x_1, ..., x_m)) = f(y_1, ..., y_m)$.

Por outro lado, seja $f(x_1, ..., x_m) \in T(M_n(F))$. Suponha $f \notin Ker\ \varphi$. Escreva

$$\varphi(f(x_1, ..., x_m)) = f(y_1, ..., y_m) = \sum_{p,q=1}^{n} f_{pq} E_{pq},$$

onde $f_{pq} \in \Omega_n$, para todo p, q. Suponha, sem perda de generalidade, que $f_{11} \neq 0$. Note que f_{11} é um polinômio nas variáveis comutativas $y_{pq}^{(i)}$, onde $p, q = 1, ..., n$ e $i = 1, .., m$. Como F é infinito, existem $a_{pq}^{(i)} \in F$, onde $p, q = 1, ..., n$ e $i = 1, ..., m$, tais que

$$f_{11}(a_{11}^{(1)}, a_{12}^{(1)}, ..., a_{nm}^{(m)}) \neq 0.$$

Agora, considere ψ e $\overline{\psi}$ construídos como anteriormente. Temos:

$$0 = f(a_1, ..., a_m) = f(\overline{\psi}(y_1), ..., \overline{\psi}(y_m)) = \overline{\psi}(f(y_1, ..., y_m) = \overline{\psi}((f_{pq})_{pq}) = (\psi(f_{pq}))_{pq}.$$

Absurdo, pois $\psi(f_{11}) = f_{11}(a_{11}^{(1)}, ..., a_{nm}^{(m)}) \neq 0$. □

Capítulo 2

Graduações

Neste capítulo, estudaremos o conceito de álgebra G-graduada por um grupo aditivo G, trabalharemos com algumas definições, exemplos e resultados, dando um enfoque maior para o caso em que $G = \mathbb{Z}_n$.

2.1 G-graduação

Definição 2.1.1. *Seja A uma álgebra sobre um corpo F, considere a família $\{A^{(\alpha)}, \alpha \in G\}$ de subespaços de A, onde G é um grupo aditivo, dizemos que A é uma **álgebra G-graduada** se puder ser escrita como soma direta de subespaços*

$$A = \sum_{\alpha \in G} \bigoplus A^{(\alpha)},$$

e além disso, para quaisquer α, $\beta \in G$, deve valer

$$A^{(\alpha)} A^{(\beta)} \subseteq A^{(\alpha+\beta)}.$$

Exemplo 2.1.2. *Qualquer álgebra A pode ser graduada por qualquer grupo G, definindo $A^{(e)} = A$ e $A^{(g)} = 0$ para qualquer $g \neq e$. Essa graduação é chamada **trivial**, onde e é o elemento identidade de G.*

Exemplo 2.1.3. *Sejam $A = M_2(F)$ e $G = \mathbb{Z}_2$, definiremos:*

$$M_2(F)^{(\bar{0})} = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in F \right\}$$

$$M_2(F)^{(\bar{1})} = \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} : b, c \in F \right\}$$

Temos que $M_2(F)$ possui a seguinte $\mathbb{Z}_2$-graduação: $M_2(F) = M_2(F)^{(\bar{0})} \oplus M_2(F)^{(\bar{1})}$.

Exemplo 2.1.4. *A álgebra de Grassmann E definida em 1.2.5 possui uma $\mathbb{Z}_2$-Graduação natural, $E = E^{(\bar{0})} \oplus E^{(\bar{1})}$.*

Definição 2.1.5. *Sejam $A = \sum_{g \in G} \bigoplus A^{(g)}$ e $B = \sum_{g \in G} \bigoplus B^{(g)}$ duas álgebras G-graduadas. Dizemos que uma aplicação $\varphi : A \longrightarrow B$ é um **homomorfismo G-graduado**, se φ é um homomorfismo de álgebras que satisfaz $\varphi(A^{(g)}) \subseteq B^{(g)}$, para todo $g \in G$. Dizemos que φ é um **isomorfismo G-graduado**, se φ é um homomorfismo G-graduado bijetivo.*

2.1.1 A $\mathbb{Z}_n$-graduação de $M_n(F)$

Definição 2.1.6. *Para $t \in \mathbb{Z}$, denote por $\bar{t}$ a classe residual em $\mathbb{Z}_n$ contendo t. Para $\alpha \in \mathbb{Z}_n$, seja $M_n^{(\alpha)}$ o subespaço de $M_n(F)$ gerado por todas as matrizes elementares $E_{i,j}$, tais que $\overline{j-i} = \alpha$.*

De modo que, $M_n^{(\bar{0})}$ consiste das matrizes da forma

$$\begin{pmatrix} a_{1,1} & 0 & \dots & 0 \\ 0 & a_{2,2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{n,n} \end{pmatrix}, a_{1,1}, a_{2,2}, ..., a_{n,n} \in F$$

e, para $0 < t \leq n-1$, temos que $M_n^{(\bar{t})}$ consiste das matrizes da forma

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

onde, $a_{1,t+1}, a_{2,t+2}, ..., a_{n-t+1,1}, a_{n-t+2,2}, ..., a_{n,t} \in F$. Então $M_n(F)$ é a soma direta de subespaços $M_n^{(\alpha)}$'s:

$$M_n(F) = \sum_{\alpha \in \mathbb{Z}_n} \bigoplus M_n^{(\alpha)}.$$

Além disso, para p, $q \in \{0, 1, ..., n-1\}$, temos:

$$M_n(F)^{(\overline{p})} M_n(F)^{(\overline{q})} \subseteq M_n(F)^{(\overline{p+q})}.$$

Portanto a decomposição define uma $\mathbb{Z}_n$-graduação da álgebra $M_n(F)$.

Observação 2.1.7. *Ao longo do texto usaremos a $\mathbb{Z}_n$-graduação construída acima para a álgebra $M_n(F)$.*

2.1.2 A $\mathbb{Z}_n$-graduação de $F\langle X \rangle$

Seja $\{X^{(\alpha)}, \alpha \in \mathbb{Z}_n\}$ uma família de conjuntos enumeráveis infinitos, disjuntos e não vazios $X^{(\alpha)}$. Coloquemos $X = \bigcup_{\alpha \in \mathbb{Z}_n} X^{(\alpha)}$ e denote por $F\langle X \rangle$ a álgebra associativa livre, livremente gerada pelo conjunto X. Observe que os monômios

$$\{x_{i_1} x_{i_2} \dots x_{i_k} : k = 1, 2, ...; x_{i_1}, x_{i_2}, ..., x_{i_k} \in X\},$$

formam uma base para $F\langle X \rangle$ como espaço vetorial.

Definição 2.1.8. *Uma variável $x \in X$ diz-se ser de* ***grau homogêneo*** *α, denotado por, $\alpha(x) = \alpha$, se $x \in X^{(\alpha)}$. O grau homogêneo de um monômio $n = x_{i_1} x_{i_2} \dots x_{i_k}$ é definido por:*

$$\alpha(n) = \alpha(x_{i_1}) + \alpha(x_{i_2}) + \dots + \alpha(x_{i_k}).$$

Para $\alpha \in \mathbb{Z}_n$, denote por $F\langle X \rangle^{(\alpha)}$ o subespaço de $F\langle X \rangle$ gerado por todos os monômios que tem grau homogêneo α. Note que:

$$F\langle X \rangle^{(\alpha)} F\langle X \rangle^{(\beta)} \subseteq F\langle X \rangle^{(\alpha+\beta)}, \forall \alpha, \beta \in \mathbb{Z}_n.$$

Assim,

$$F\langle X \rangle = \sum_{\alpha \in \mathbb{Z}_n} \bigoplus F\langle X \rangle^{(\alpha)},$$

revela-se uma álgebra $\mathbb{Z}_n$-graduada.

Os elementos da álgebra $\mathbb{Z}_n$-graduada $F\langle X \rangle$ são chamados de **polinômios $\mathbb{Z}_n$-graduados** ou, simplesmente, **polinômios graduados**.

Observação 2.1.9. *A $\mathbb{Z}_n$-graduação de $F\langle X\rangle$ pode ser generalizada para uma G-graduação, onde G é um grupo aditivo. Para isto basta fazer um processo análogo ao anterior.*

Exemplo 2.1.10. *Se denotarmos por $\overline{0}$ o conjunto dos monômios em $F\langle X\rangle$ com grau homogêneo par, e por $\overline{1}$ o conjunto dos monômios em $F\langle X\rangle$ com grau homogêneo ímpar, então teremos que $F\langle X\rangle$ possui a seguinte $\mathbb{Z}_2$-graduação:*

$$F\langle X\rangle = F\langle X\rangle^{(\overline{0})} \oplus F\langle X\rangle^{(\overline{1})}$$

2.2 Identidades G-graduadas

Nesta seção, apresentaremos o conceito de identidades polinomiais G-graduadas que serão objeto central de estudo no restante do texto. De agora em diante denotaremos por $F\langle X\rangle$ a álgebra associativa livre G-graduada.

Definição 2.2.1. *Seja $A = \sum_{\alpha\in G} \bigoplus A^{(\alpha)}$ uma álgebra G-graduada. Um polinônimio G-graduado $f(x_1, x_2, ..., x_k) \in F\langle X\rangle$ é dito ser uma* ***identidade polinomial graduada*** *para a álgebra G-graduada A se $f(a_1, a_2, ..., a_k) = 0$ para quaisquer $a_i \in A^{(\alpha(x_i))}$, $i = 1, 2, ..., k$. Denotaremos o conjunto das identidades polinomiais G-graduadas por $T(A)^{gr}$, ou seja:*

$$T(A)^{gr} = \{f \in F\langle X\rangle : f \equiv 0 \ em \ A\}.$$

Exemplo 2.2.2. *Seja $A = \sum_{g\in G} \bigoplus A^{(g)}$ uma álgebra G-graduada com a graduação trivial definida no exemplo (2.1.2). Se $\alpha(x_1) \in G - \{e\}$, então o polinômio $x_1 \in F\langle X\rangle$ é uma identidade G-graduada de A.*

Exemplo 2.2.3. *Tome a álgebra de Grassmann E com sua $\mathbb{Z}_2$-graduação natural definida em (2.1.4), temos que $f(x_1, x_2) = [x_1, x_2] = x_1x_2 - x_2x_1 \in F\langle X\rangle$, com $\alpha(x_1) = 0 = \alpha(x_2)$ é uma identidade $\mathbb{Z}_2$-graduada de E.*
Com efeito, basta observar que $\mathcal{Z}(E) = E^{(\overline{0})}$.

Definição 2.2.4. *Um ideal I de $F\langle X\rangle$ é dito ser um T_G-**ideal** se $\varphi(I) \subseteq I$ para todo endomorfismo G-graduado φ de $F\langle X\rangle$, ou seja, um ideal I é um T_G-ideal se é fechado sob todos os endomorfismos G-graduados $\varphi : F\langle X\rangle \longrightarrow F\langle X\rangle$.*

Observação 2.2.5. *Quando $G = \mathbb{Z}_n$ o T_G-ideal será denotado por T_n.*

Definição 2.2.6. *Seja $S \subseteq F\langle X\rangle$. O T_G**-ideal gerado por S** é a interseção de todos os T_G-ideais de $F\langle X\rangle$ que contém S, denotaremos esse conjunto por $\langle S\rangle^{T_G}$, ou seja,*

$$\langle S\rangle^{T_G} = Span_F \ \{p_1 \ \varphi(f) \ p_2 : f \in S, \varphi \in End(F\langle X\rangle)^{gr}, p_1, p_2 \in F\langle X\rangle\}.$$

Definição 2.2.7. *Um polinômio G-graduado $f \in F\langle X\rangle$ é dito **homogêneo na variável** $x_i \in X$, se x_i aparece o mesmo número de vezes em todos os monômios de f. Se f é homogêneo em todas as variáveis, então diremos que f e **multi-homogêneo**.*

Definição 2.2.8. *Um polinômio G-graduado $f \in F\langle X\rangle$ é **linear na variável** $x_i \in X$, se x_i aparece apenas uma vez em cada monômio de f. Se f é linear em todas as suas variáveis, diremos que f é **multilinear G-graduado**.*

Observação 2.2.9. *Não é dificil ver que I é um T_G-ideal se, e somente se, $f(g_1, ..., g_n) \in I$, para quaisquer $f(x_1, ..., x_n) \in I$ e $g_i \in F\langle X\rangle^{\alpha(x_i)}$.*
Se A é uma álgebra G-graduada, então o conjunto $T(A)^{gr}$ é um T_G-ideal de $F\langle X\rangle$ e os resultados do Teorema 1.4.5 ainda são válidos no caso de um T_G-ideal, isto é:

Teorema 2.2.10. *Seja $f(x_1, ..., x_n) = \sum_{i=0}^{n} f_i(x_1, ..., x_n)$, onde f_i é a componente homogênea de f de grau i em x_1.*
(i) Se F contém mais que n elementos então

$$\langle f_0, f_1, ..., f_n\rangle^{T_G} = \langle f\rangle^{T_G}.$$

(ii) Se característica de F é igual a zero, então f é PI-equivalente a um conjunto de polinômios multilineares G-graduados.

Exemplo 2.2.11. *Seja $M_2(F)$ munida da $\mathbb{Z}_2$-graduação definida no exemplo 2.1.3, Di Vincenzo [4] provou que para um corpo de característica zero*

$$T(M_2(F))^{gr} = \langle y_1y_2 - y_2y_1, z_1z_2z_3 - z_3z_2z_1\rangle^{T_2}.$$

Exemplo 2.2.12. *Seja F um corpo finito de característica $p > 2$ e E a álgebra de Grassmann unitária de dimensão infinita, Fonseca em [7] determinou uma base para as identidades polinomiais $\mathbb{Z}_2$-graduadas para qualquer $\mathbb{Z}_2$-graduação não trivial da álgebra E.*

A seguir veremos um resultado que relaciona os conceitos de identidades polinomiais ordinárias (as identidades definidas no capítulo 1) e identidades polinomiais graduadas.

Proposição 2.2.13. *Sejam A e B duas álgebras. Se A e B possuem G-graduações tais que $T(A)^{gr} \subseteq T(B)^{gr}$, então $T(A) \subseteq T(B)$. Além disso, se $T(A)^{gr} = T(B)^{gr}$ então $T(A) = T(B)$.*

Demonstração: Consideremos a álgebra associativa livre $F\langle Y\rangle$, onde $Y = \{y_1, y_2, ...\}$ é um conjunto não vazio enumerável de variáveis não comutativas e seja $f = f(y_1, ..., y_n) \in T(A)$. Dados $b_1, ..., b_n \in B$, tomemos $b_{i_g} \in B^{(g)}$ tal que, para $1 \leq i \leq n$ e $g \in G$, temos

$$b_i = \sum_{g\in G} b_{i_g}.$$

Para cada $b_{i_g} \neq 0$, podemos associar uma variável $x_{i_g} \in X^{(g)}$. Consideramos o polinômio

$$g = g(x_{1_e}, ..., x_{1_g}, ..., x_{2_e}, ...) = f\left(\sum_{g\in G} x_{1_g}, ..., \sum_{g\in G} x_{n_g}\right) \in F\langle Y\rangle.$$

Como $f \in T(A)$, então $g \in T(A)^{gr}$, e assim, por hipótese temos que $g \in T(B)^{gr}$. Fazendo as substituições $x_{i_g} = b_{i_g}$, para $1 \leq i \leq n$ e $g \in G$, temos

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

$\square$

Observação 2.2.14. *A recíproca do resultado acima é falsa. De fato, considere na álgebra de Grassmann E a $\mathbb{Z}_2$-graduação natural $E = E^{(\bar{0})} \oplus E^{(\bar{1})}$ e a $\mathbb{Z}_2$-graduação trivial $E = E \oplus \{0\}$. Temos que $f(x_1, x_2) = [x_1, x_2]$, com $\alpha(x_1) = \alpha(x_2) = 0$, é identidade polinomial $\mathbb{Z}_2$-graduada de E com respeito à primeira graduação, mas não é identidade polinomial graduada com respeito à graduação trivial.*

Capítulo 3

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

Neste capítulo estudaremos os resultados obtidos por Vasilovsky [18] e por Azevedo [2]. Ambos descreveram uma base finita para as identidades polinomiais $\mathbb{Z}_n$-graduadas de $M_n(F)$, [18] quando F for um corpo de característica zero e [2] quando F for um corpo infinito de característica qualquer. Vale ressaltar que a base para as identidades polinomiais $\mathbb{Z}_n$-graduadas de $M_n(F)$ é a mesma, a fundamental diferença entre os artigos está na técnica utilizada para se obter o resultado, fato que exploraremos aqui.

3.1 Corpo com Característica Zero

Teorema 3.1.1. *Seja F um corpo de característica 0. Todas as identidades polinomiais graduadas da álgebra $\mathbb{Z}_n$-graduada $M_n(F)$ seguem de:*

$$x_1x_2 - x_2x_1 = 0, \quad \alpha(x_1) = \alpha(x_2) = \overline{0} \tag{3.1}$$

e

$$x_1xx_2 - x_2xx_1 = 0, \quad \alpha(x_1) = \alpha(x_2) = -\alpha(x) \tag{3.2}$$

Antes de demonstrar esse Teorema precisaremos de alguns resultados que faremos a seguir:

Lema 3.1.2. *A álgebra graduada $M_n(F)$ satisfaz as identidades 3.1 e 3.2.*

Demonstração: Como os elementos de $M_n^{(\overline{0})}$ consistem apenas de matrizes diagonais, e nós temos que duas matrizes diagonais quaisquer comutam, segue que $M_n(F)$ satisfaz a identidade graduada 3.1. Uma vez que a identidade 3.2 é multilinear, basta demonstrar apenas para os elementos da base (no sentido de geradores), isto é, mostrar que essa identidade vale quando

$$x_1 = E_{i_1,j_1}, \quad x_2 = E_{i_2,j_2}, \quad x = E_{r,s}.$$

Para E_{i_1,j_1}, $E_{i_2,j_2} \in M_n^{(\bar{t})}$ e $E_{r,s} \in M_n^{(\overline{n-t})}$, onde $0 \leq t \leq n-1$, de modo que:

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

$$i_2 = \begin{cases} j_2 - t & \text{se} \;\; j_2 - t \geq 1 \\ j_2 - t + n & \text{se} \;\; j_2 - t < 1 \end{cases}$$

$$r = \begin{cases} s + t & \text{se} \;\; s + t \leq n \\ s + t - n & \text{se} \;\; s + t > n \end{cases}$$

Note que $E_{i_1,j_1}E_{r,s}E_{i_2,j_2} \neq 0$ somente se $j_1 = r$ e $s = i_2$.

Afirmação 3.1.3. *Neste caso $i_1 = s = i_2$ e $j_1 = r = j_2$.*

De fato, se $j_1 = i_1 + t$ e $r = s + t - n$, então, de $j_1 = r$, temos que, $r = i_1 + t$ então, $i_1 + t = s + t - n$ e assim $n = s - i_1$, que é impossível, pois $1 \leq s, i_1 \leq n$. Assim, as igualdades $j_1 = i_1 + t$ e $r + s = t$ não podem ocorrer simultaneamente. O mesmo se aplica para as igualdades $s = r - t$ e $i_2 = j_2 - t + n$. Assim, quando $j_1 = i_1 + t$, temos $r = s + t$ e $i_2 = j_2 - t$, de modo que

$$i_2 = s = r - t = j_1 - t = i_1$$

e

$$r = j_1 = i_1 + t = i_2 + t = j_2.$$

Analogamente, quando $j_1 = i_1 + t - n$, temos $r = s + t - n$ e $i_2 = j_2 - t + n$, de onde

$$i_2 = s = r - t + n = j_1 - t + n = i_1$$

e

$$r = j_1 = i_1 + t - n = i_2 + t - n = j_2.$$

Provando a afirmação acima.

Isso nos permite concluir que $E_{i_1,j_1}E_{r,s}E_{i_2,j_2} \neq 0$ se, e somente se, $i_1 = s = i_2$ e $j_1 = r = j_2$, e se, e somente se, $E_{i_2,j_2}E_{r,s}E_{i_1,j_1} \neq 0$. Neste caso,

$$E_{i_1,j_1}E_{r,s}E_{i_2,j_2} = E_{i_1,j_2} = E_{i_2,j_2}E_{r,s}E_{i_1,j_1}.$$

Caso contrário,

$$E_{i_1,j_1}E_{r,s}E_{i_2,j_2} = 0 = E_{i_2,j_2}E_{r,s}E_{i_1,j_1}.$$

Provando que $M_n(F)$ satisfaz a identidade 3.2

□

A partir de agora denotaremos por I_n o T_n-ideal gerado pelos polinômios descritos nas identidades 3.1 e 3.2.

Definição 3.1.4. *Para um inteiro k, denotamos por S_k o conjunto de todas as permutações do conjunto $\{1, 2, ..., k\}$. Para $x_1, x_2, ..., x_k \in X$ e $\sigma \in S_k$, seja*

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

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

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

Observação 3.1.5. *Qualquer identidade graduada multilinear pode ser expressa por*

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

onde $a_\sigma \in F$.

Definição 3.1.6. *Por uma **substituição standard** em um polinômio f em $F\langle X\rangle$, entenderemos uma substituição $\mathcal{S}$ da forma*

$$x_1 = E_{i_1,j_1}, x_2 = E_{i_2,j_2}, ..., x_k = E_{i_k,j_k} \tag{3.3}$$

onde

$$\overline{j_s - i_s} = \alpha(x_s) \tag{3.4}$$

De modo que $E_{i_s,j_s} \in M_n^{(\alpha(x_s))}$, $s = 1, 2, ..., k$.

Para o polinômio graduado $f(x_1, x_2, ..., x_k)$ e a substituição $\mathcal{S}$, denotaremos por $f|_{\mathcal{S}}$ o valor de f correspondente à substituição $\mathcal{S}$.

Observação 3.1.7. *Se f é multilinear e se $f|_{\mathcal{S}} = 0$ para toda substituição standard $\mathcal{S}$, então f é uma identidade graduada de $M_n(F)$.*

Observação 3.1.8. *Quando uma substituição standard $\mathcal{S}$ é feita, o valor do monômio $m_\sigma(x_1, x_2, ..., x_k)$ é diferente de zero se, e somente se,*

$$j_{\sigma(1)} = i_{\sigma(2)}, j_{\sigma(2)} = i_{\sigma(3)}, ..., j_{\sigma(k-1)} = i_{\sigma(k)}, \tag{3.5}$$

e neste caso,

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

Definição 3.1.9. *Para um monômio $m_\sigma(x_1, x_2, ..., x_k)$, $\sigma \in S_k$, e dois inteiros $1 \leq p \leq q \leq k$, denote por $m_\sigma^{[p,q]}$ a subpalavra obtida a partir de m_σ descartando os primeiros $p-1$ e os últimos $k-q$ fatores:*

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

Lema 3.1.10. *Para qualquer $\sigma \in S_k$, existe uma substituição standard $\mathcal{S}$ tal que*

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

Demonstração: Usaremos indução em k para demonstrar esse fato.
Para $k = 1$, temos

$$m_\sigma(x_1) = x_1.$$

Assim, basta tomar S tal que $x_1 = E_{i,n}$ com $\overline{n-i} = \alpha(x_1)$. Portanto teremos

$$m_\sigma(x_1) = E_{i,n} \neq 0.$$

Sejam $k > 1$ e $\alpha(x_k) = \bar{t}$, para algum inteiro $0 \leq t < n$, suponha por hipótese de indução o enunciado para $k-1$. Assim, existe uma substituição standard $\mathcal{S}$, satisfazendo

$$x_{\sigma(1)} = E_{i_1, j_1}, x_{\sigma(2)} = E_{i_2, j_2}, ..., x_{\sigma(k-1)} = E_{i_{k-1}, j_{k-1}} \tag{3.6}$$

tal que

$$m_\sigma(x_1, x_2, ..., x_{k-1}) = E_{i_1, j_{k-1}} \neq 0.$$

Então, definindo além de 3.6, $x_{\sigma(k)} = E_{j_{k-1}, j_k}$, onde

$$j_k = \begin{cases} j_{k-1} + t & \text{se } \ j_{k-1} + t \leq n \\ j_{k-1} + t - n & \text{se } \ j_{k-1} + t > n \end{cases}$$

Temos

$$m_\sigma(x_1, x_2, ..., x_k) = E_{i_1,j_{k-1}} E_{j_{k-1},j_k} = E_{i_1,j_k} \neq 0.$$

□

Lema 3.1.11. *Se $m_\sigma|_{\mathcal{S}} \neq 0$ então, para qualquer $1 \leq p \leq q \leq k$,*

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

Demonstração: Temos que

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

Assim, usando 3.4 e 3.5, temos

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

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

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

□

Lema 3.1.12. *Se, para uma permutação $\sigma \in S_k$, existe uma substituição standard $\mathcal{S}$ tal que*

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

então,

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

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

Demonstração: Se $\sigma(1) = 1$, temos o resultado.

Suponha $\sigma(1) \neq 1$, note que:

$$1 = \sigma^{-1}(\sigma(1)) < \sigma^{-1}(1).$$

Seja t o menor inteiro positivo tal que $\sigma^{-1}(t+1) < \sigma^{-1}(1)$

Temos

$$1 \leq \sigma^{-1}(t+1) < \sigma^{-1}(1) \leq \sigma^{-1}(t).$$

Uma vez que, por hipótese,

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

segue que, $i_1 = i_{\sigma(1)}$, $j_t = i_{t+1}$ e, para $s > 1$, $j_{\sigma(s-1)} = i_{\sigma(s)}$. Então definindo

$$p = \sigma^{-1}(t+1), \quad q = \sigma^{-1}(1), \quad r = \sigma^{-1}(t),$$

temos $1 \leq p < q \leq r$ com $j_{\sigma(q-1)} = i_{\sigma(q)} = i_{\sigma^{-1}(\sigma(1))} = i_1 = i_{\sigma(1)}$, $j_{\sigma(r)} = i_{\sigma(p)}$ e, quando $p > 1$, $j_{\sigma(p-1)} = i_{\sigma(p)}$.

Primeiramente consideremos o caso em que $p > 1$, e neste caso temos:

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

o que implica que

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

para algum $t_0 \in \mathbb{Z}$. Logo, pelo lema 3.1.11, temos

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

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

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

Agora como o polinômio $x_1xx_2 - x_2xx_1$ está em I_n, temos

$$\begin{aligned}
m_\sigma &= m_\sigma^{[1,p-1]} \cdot m_\sigma^{[p,q-1]} \cdot m_\sigma^{[q,r]} \cdot m_\sigma^{[r+1,k]} \\
&\equiv m_\sigma^{[q,r]} \cdot m_\sigma^{[p,q-1]} \cdot m_\sigma^{[1,p-1]} \cdot m_\sigma^{[r+1,k]} \\
&= x_{\sigma(q)} m_\sigma^{[q+1,r]} \cdot m_\sigma^{[p,q-1]} \cdot m_\sigma^{[1,p-1]} \cdot m_\sigma^{[r+1,k]} \\
&= x_{\sigma(q)} x_{l_2} \cdots x_{l_k} \\
&= x_1 x_{l_2} \cdots x_{l_k} (mod\ I_n)
\end{aligned}$$

Se $p = 1$, temos

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

usando novamente 3.1.11, temos que

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

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

Como o polinômio $x_1x_2 - x_2x_1$ está em I_n, segue que

$$\begin{aligned} m_\sigma &= m_\sigma^{[1,q-1]} \cdot m_\sigma^{[q,r]} \cdot m_\sigma^{[r+1,k]} \\ &\equiv m_\sigma^{[q,r]} \cdot m_\sigma^{[1,q-1]} \cdot m_\sigma^{[r+1,k]} \\ &= x_{\sigma(q)} x_{l_2} \cdots x_{l_k} \\ &= x_1 x_{l_2} \cdots x_{l_k} (mod\ I_n) \end{aligned}$$

□

Lema 3.1.13. *Se, para uma permutação $\sigma \in S_k$, existir uma substituição standard $\mathcal{S}$ tal que*

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

então

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

Demonstração: Seja r o maior inteiro positivo tal que

$$m_\sigma(x_1, x_2, ..., x_k) \equiv x_1 x_2 \cdots x_r \cdot n(x_{r+1}, ..., x_k)(mod\ I_n),$$

para algum monômio multilinear $n(x_{r+1}, x_{r+2}, ..., x_k)$. Precisamos mostrar que $r = k$ para termos

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

Por contradição, suponhamos $r < k$. Então $r \leq k - 2$.

Como $m_\sigma(x_1, x_2, ..., x_k) \equiv x_1 x_2 \cdots x_r \cdot n(x_{r+1}, ..., x_k)(mod\ I_n)$ e $I_n \subseteq T(M_n(F))^{gr}$, então

$$m_\sigma(x_1, x_2, ..., x_k) - x_1 x_2 \cdots x_r \cdot n(x_{r+1}, ..., x_k) \in I_n \subseteq T(M_n(F))^{gr}.$$

Logo,

$$(m_\sigma(x_1, x_2, ..., x_k) - x_1x_2\cdots x_r \cdot n(x_{r+1}, ..., x_k))|_{\mathcal{S}} = 0 \Rightarrow$$

$$m_\sigma(x_1, x_2, ..., x_k)|_{\mathcal{S}} = x_1x_2\cdots x_r \cdot n(x_{r+1}, ..., x_k)|_{\mathcal{S}}.$$

Portanto,

$$x_1x_2\cdots x_r \cdot n(x_{r+1}, x_{r+2}, ..., x_k)|_{\mathcal{S}} = m_\sigma(x_1, x_2, ..., x_k)|_{\mathcal{S}} = m(x_1, x_2, ..., x_k)|_{\mathcal{S}} \neq 0.$$

Além disso,

$$x_1x_2\cdots x_r \cdot n(x_{r+1}, x_{r+2}, ..., x_k)|_{\mathcal{S}} = E_{i_1,j_1}E_{i_2,j_2}\cdots E_{i_r,j_r} \cdot n(x_{r+1}, ..., x_k)|_{\mathcal{S}} =$$

$$= E_{i_1,j_r} \cdot n(x_{r+1}, ..., x_k)|_{\mathcal{S}}$$

e

$$m(x_1, ..., x_k)|_{\mathcal{S}} = E_{i_1,j_1}\cdots E_{i_r,j_r}\{x_{r+1}, ..., x_k\}|_{\mathcal{S}} = E_{i_1,j_r}\{x_{r+1}, ..., x_k\}|_{\mathcal{S}}.$$

Assim, temos que

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

Pelo lema 3.1.12, existe um monômio multilinear $n'(x_{r+2}, x_{r+3}, ..., x_k)$ tal que

$$n(x_{r+1}, x_{r+2}, ..., x_k) \equiv x_{r+1} \cdot n'(x_{r+2}, x_{r+3}, ..., x_k)(mod\ I_n).$$

Assim,

$$\begin{aligned} m_\sigma(x_1, x_2, ..., x_k) &\equiv x_1\cdots x_r \cdot n(x_{r+1}, ..., x_k)(mod\ I_n) \\ &\equiv x_1\cdots x_r x_{r+1} \cdot n'(x_{r+2}, ..., x_k)(mod\ I_n) \end{aligned}$$

O que contradiz a escolha do número r. □

Corolário 3.1.14. *Se, para duas permutações $\sigma, \tau \in S_k$, existe uma substituição standard $\mathcal{S}$ tal que*

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

então

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

Demonstração:

Note primeiramente que,

$$\begin{aligned} m_\sigma(x_1, x_2, ..., x_k) &= x_{\sigma(1)}x_{\sigma(2)} \cdots x_{\sigma(k)} \\ &= x_{\tau(\tau^{-1}(\sigma(1)))}x_{\tau(\tau^{-1}(\sigma(2)))} \cdots x_{\tau(\tau^{-1}(\sigma(k)))} \\ &= y_{\tau^{-1}(\sigma(1))}y_{\tau^{-1}(\sigma(2))} \cdots y_{\tau^{-1}(\sigma(k))} \end{aligned}$$

onde $y_i = x_{\tau(i)}$, $i = 1, 2, ..., k$. Além disso,

$$\begin{aligned} m(y_1, y_2, ..., y_k) &= y_1 y_2 \cdots y_k \\ &= x_{\tau(1)}x_{\tau(2)} \cdots x_{\tau(k)} \\ &= m_\tau(x_1, x_2, ..., x_k) \end{aligned}$$

Como por hipótese

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

temos que,

$$m_{\tau^{-1}\sigma}(y_1, y_2, ..., y_k)|_{\mathcal{S}} = m(y_1, y_2, ..., y_k)|_{\mathcal{S}} \neq 0.$$

Portanto, pelo Lema anterior

$$m_{\tau^{-1}\sigma}(y_1, y_2, ..., y_k) \equiv m(y_1, y_2, ..., y_k)(mod\ I_n).$$

Logo,

$$m_\sigma(x_1, x_2, ..., x_k)|_{\mathcal{S}} \equiv m_\tau(x_1, x_2, ..., x_k)(mod\ I_n).$$

□

Agora fazeremos a demonstração do Teorema 3.1.1, que é o resultado principal desta seção.

Demonstração:[Teorema 3.1.1] Já mostramos no lema 3.1.2 que $I_n \subseteq T(M_n)^{gr}$, agora mostraremos que $T(M_n)^{gr} \subseteq I_n$. Com efeito, seja $f(x_1, x_2, ..., x_k) \neq 0$ uma identidade polinomial graduada de $M_n(F)$, uma vez que a característica de F é zero, podemos supor f multilinear.

Seja r o menor inteiro não negativo tal que o polinômio f pode ser expresso, módulo I_n, como combinação linear de monômios

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

com $0 \neq a_{\sigma_q} \in F$, $\sigma_q \in S_k$. Mostraremos que $r = 0$, para termos $f \equiv 0(mod\ I_n)$.
Suponha o contrário, ou seja, $r > 0$, pelo lema 3.1.10, existe uma substituição standard $\mathcal{S}$, tal que $m_{\sigma_1}|_{\mathcal{S}} \neq 0$, agora como $f|_{\mathcal{S}} = 0$, então

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

Além disso,

$$m_{\sigma_q}|_{\mathcal{S}} \in \{E_{i,j} : i, j = 1, 2, ..., n\} \cup \{0\}, \quad q = 1, 2, ..., r,$$

segue que existe pelo menos um inteiro $p \in \{2, 3, ..., r\}$ tal que

$$m_{\sigma_p}|_{\mathcal{S}} = m_{\sigma_1}|_{\mathcal{S}} \neq 0.$$

Pelo corolário 3.1.14,

$$m_{\sigma_p} \equiv m_{\sigma_1} (mod\ I_n).$$

Logo,

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

Assim, f pode ser expressa, módulo I_n, como combinação linear de não mais que $r - 1$ monômios multilineares, o que contradiz a escolha do r.
Portanto $f \equiv 0\ (mod\ I_n)$, ou seja, $f \in I_n$ □

3.2 Corpo Infinito

Na seção anterior, estudamos as identidades polinomiais $\mathbb{Z}_n$-graduadas da álgebra $\mathbb{Z}_n$-graduada $M_n(F)$ quando F é um corpo de característica zero. Nesta seção, trataremos as identidades polinomiais $\mathbb{Z}_n$-graduadas da álgebra $\mathbb{Z}_n$-graduada $M_n(F)$ no caso mais geral em que F é um corpo infinito de característica qualquer. No entanto, vale ressaltar que, ao estudarmos sobre um corpo de característica zero, poderíamos assumir que os polinômios eram multilineares e, com isso, conseguimos o resultado. Nesta seção, como o corpo é infinito, não podemos, em geral, utilizar este fato, sendo assim, as ferramentas utilizadas por Azevedo em [2] para mostrar o resultado foram polinômios multi-homogêneos e matrizes genéricas.

Teorema 3.2.1. *Seja F um corpo infinito. Todas as identidades polinomiais $\mathbb{Z}_n$-graduadas da álgebra $\mathbb{Z}_n$-graduada $M_n(F)$ seguem de*

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

$$x_1xx_2 - x_2xx_1 = 0, \quad \alpha(x_1) = \alpha(x_2) = -\alpha(x).$$

Antes de demonstrar este teorema precisaremos de algumas definições e resultados que faremos a seguir:

Definição 3.2.2. *Seja $\Omega = F[y_i^{(k)} : 1 \leq k \leq n, i \geq 1]$ a álgebra dos polinômios comutativos gerados pelas variáveis $y_i^{(k)}$. Para $i \in \{0, 1, ..., n-1\}$, denotaremos $M_n(\Omega)_{\bar{i}}$ o subespaço de $M_n(\Omega)$ que consiste de matrizes da forma:*

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

onde $f_1, f_2, ..., f_n \in \Omega$.

Lema 3.2.3. *A álgebra $\mathbb{Z}_n$-graduada $M_n(F)$ satisfaz as identidades 3.1 e 3.2.*

Demonstração: A demonstração deste lema é análoga a demonstração do lema 3.1.2. □

O próximo lema vai mostrar que a decomposição dada na definição 3.2.2 define uma $\mathbb{Z}_n$-graduação para a álgebra $M_n(\Omega)$.

Lema 3.2.4. *Seja $f_1, f_2, ..., f_n, g_1, g_2, ..., g_n$ polinômios de Ω, e denote*

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

e

$$B = \begin{pmatrix} 0 & \cdots & 0 & g_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & g_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & g_{n-j} \\ g_{n-j+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & g_n & 0 & 0 & \cdots & 0 \end{pmatrix},$$

com $0 \leq i, j \leq n-1$. Então,

$$AB = \begin{pmatrix} 0 & \cdots & 0 & f_1 g_{i_1} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & f_2 g_{i_2} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & f_x g_{i_x} \\ f_{x+1} g_{i_{x+1}} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & f_n g_{i_n} & 0 & 0 & \cdots & 0 \end{pmatrix},$$

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

Demonstração: O elemento f_1 está na posição $(1, i+1)$ da matriz A. Portanto quando $k = 1$, $i_1 = i + 1 = (i+k-1) mod \ n+1$.

Para $k \geq 2$, a posição do elemento f_k é $(k, i+k)$ se $i+k \leq n$ e $(k, i+k-n)$ se $i+k > n$. Logo, a posição de f_k é $(k, (i+k-1) mod \ n+1)$. Portanto,

$$i_k = (i+k-1) mod \ n + 1 \tag{3.7}$$

Agora determinaremos x, de tal modo que $f_x g_{i_x}$ apareça na última coluna da matriz AB, para isso observamos que g_{n-j} está na última coluna da matriz B e nós sabemos que o índice i_x de $f_x g_{i_x}$ da matriz AB acompanha o índice $n-j$ da matriz B, assim,

$$n - j = i_x \tag{3.8}$$

Portanto, usando as equações 3.7 e 3.8, temos que

$$i_x = n - j = (i + x - 1) mod\ n + 1.$$

Analisaremos dois possíveis casos:

Caso 1: $0 \leq i + x - 1 < n$

Neste caso, $n - j = i + x$, assim, $x = n - (i + j)$. Como $1 \leq x \leq n$, nós temos $0 \leq i + j \leq n - 1$. Logo $x = n - (i + j) mod\ n$.

Caso 2: $n \leq i + x - 1 \leq 2n - 2$

Aqui, $n - j = i + x - n$, assim, $x = n - (i + j - n)$. Como $1 \leq x \leq n$, nós temos, $0 \leq i + j - n \leq n - 1$. Assim, $x = n - (i + j - n) mod\ n = n - (i + j) mod\ n$ □

Definição 3.2.5. *Denote por R a subálgebra $\mathbb{Z}_n$-graduada de $M_n(\Omega)$ gerada pelas matrizes*

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

Lema 3.2.6. *A álgebra relativamente livre $\mathbb{Z}_n$-graduada $\dfrac{F\langle X\rangle}{T(M_n(F))^{gr}}$ é isomorfa a álgebra R.*

Demonstração: A prova é análoga ao caso para matrizes genéricas (teorema 1.6.3). A aplicação $\varphi : F\langle X\rangle \longrightarrow R$ definida por $\varphi(f(x_1, ..., x_k)) = f(A_1, ..., A_k)$ é um homomorfismo $\mathbb{Z}_n$-graduado. Claramente φ é sobrejetora. Além disso, $\text{Ker}\varphi = T(M_n(F))^{gr}$. □

Lema 3.2.7. *Para todo monômio* $0 \neq m(x_1, x_2, ..., x_k) \in F\langle X\rangle$ *de comprimento* q*, existem inteiros* $1 \leq i_1 \leq ... \leq i_q \leq k$ *e* $\{k_1, ..., k_q, x\} \subseteq \{1, ..., n\}$ *tais que*

$$m(A_1, ..., A_k) = \begin{pmatrix} 0 & \cdots & 0 & y_{i_1}^{(k_1)} \cdots y_{i_q}^{(k_q)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_x \\ \omega_{x+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_n & 0 & 0 & \cdots & 0 \end{pmatrix},$$

onde $\omega_i = y_{i_1}^{((k_1+i-2)mod\ n+1)} \cdots y_{i_q}^{((k_q+i-2)mod\ n+1)},\ i = 2, ..., n$

Demonstração: Usaremos indução sobre o comprimento q.

Para $q = 1$, temos

$$m(x_1) = x_1.$$

Logo,

$$m(A_1) = A_1 = \begin{pmatrix} 0 & \cdots & 0 & y_i^{(1)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & y_i^{(2)} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & y_i^{(n-\alpha(x_1))} \\ y_i^{(n-\alpha(x_1)+1)} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & y_i^{(n)} & 0 & 0 & \cdots & 0 \end{pmatrix}$$

e aqui temos, $i_1 = 1,\ k_1 = 1,\ x = n - \alpha(x_1)$, e $\omega_r = y_1^{(r-1)mod\ n+1}$.

Se $q > 1$, então existe um monômio $n(x_1, ..., x_k) \in F\langle X\rangle$, tal que $m(x_1, ..., x_k) = n(x_1, ..., x_k)x_p$, onde $1 \leq i \leq k$. Por hipótese de indução o resultado é válido para o monômio $n(x_1, ..., x_k)$, pois o seu comprimento é $q - 1$, assim existem inteiros $1 \leq i_1 \leq$

$... \leq i_{q-1} \leq k$ e $\{k_1, ..., k_{q-1}, t\} \subseteq \{1, 2, ..., n\}$ tais que

$$n(A_1, ..., A_k) = \begin{pmatrix} 0 & \cdots & 0 & y_{i_1}^{(k_1)} \cdots y_{i_{q-1}}^{(k_{q-1})} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \delta_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \delta_t \\ \delta_{t+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \delta_n & 0 & 0 & \cdots & 0 \end{pmatrix}, \tag{3.9}$$

onde $\delta_r = y_{i_1}^{((k_1+r-2)mod\ n+1)} \cdots y_{i_{q-1}}^{((k_{q-1}+r-2)mod\ n+1)},\ r = 2, ..., n.$

Assim, usando o lema 3.2.4, temos que $n(A_1, ..., A_k) \cdot A_p$ é

$$\begin{pmatrix} 0 & \cdots & 0 & y_{i_1}^{(k_1)} \cdots y_{i_{q-1}}^{(k_{q-1})} y_p^{(j_1)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \delta_2 y_p^{(j_2)} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \delta_x y_p^{(j_x)} \\ \delta_{x+1} y_p^{(j_{x+1})} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \delta_n y_p^{(j_n)} & 0 & 0 & \cdots & 0 \end{pmatrix},$$

onde $n(A_1, ..., A_k)$ é dada por 3.9 e

$$A_p = \begin{pmatrix} 0 & \cdots & 0 & y_p^{(1)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & y_p^{(2)} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & y_p^{(n-\alpha(x_p))} \\ y_p^{(n-\alpha(x_p)+1)} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & y_p^{(n)} & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Além disso,

$$j_r = (n - t + r - 1) mod\ n\ + 1 \quad \text{e} \quad x\ = n - (n - t + \alpha(x_p)) mod\ n \tag{3.10}$$

Logo, tomando $i_q = p$ e $k_q = j_1$, temos que

$$n(A_1,...,A_k)\cdot A_p = \begin{pmatrix} 0 & \cdots & 0 & y_{i_1}^{(k_1)}\cdots y_{i_{q-1}}^{(k_{q-1})}y_{i_q}^{(k_q)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_x \\ \omega_{x+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_n & 0 & 0 & \cdots & 0 \end{pmatrix} = m(A_1,...,A_k),$$

onde $\omega_r = \delta_r y_{i_q}^{(j_r)} = y_{i_1}^{((k_1+r-2)mod\ n+1)}\cdots y_{i_{q-1}}^{((k_{q-1}+r-2)mod\ n+1)}y_{i_q}^{(j_r)}$, $r = 2,...,n$. Agora analisaremos j_r, usando 3.10, temos

$$j_1 \equiv (n-t)mod\ n\ +1 \Rightarrow j_1 - n + t = c_1 n + 1 \Rightarrow j_1 - c_1 n = n - t + 1,\ c_1 \in \mathbb{Z}.$$

Assim,

$$\begin{aligned} j_r = (n-t+r-1)mod\ n\ +1 \quad &\Rightarrow \quad j_r = ((n-t+1)+r-2)mod\ n\ +1 \\ &\Rightarrow \quad j_r - n + t - r + 2 = c_2 n + 1 \\ &\Rightarrow \quad j_r - (n-t+1) - r + 2 = c_2 n + 1 \\ &\Rightarrow \quad j_r - (j_1 - c_1 n) - r + 2 = c_2 n + 1 \\ &\Rightarrow \quad j_r - j_1 - r + 2 = c_3 n + 1 \\ &\Rightarrow \quad j_r = (j_1 + r - 2)mod\ n\ +1, \end{aligned}$$

onde $c_2, c_3 \in \mathbb{Z}$.

Logo

$$\omega_r = \delta_r y_{i_q}^{(j_r)} = y_{i_1}^{((k_1+r-2)mod\ n+1)}\cdots y_{i_{q-1}}^{((k_{q-1}+r-2)mod\ n+1)}y_{i_q}^{((k_q+r-2)mod\ n+1)},$$

com $r = 2,...,n$. Como queríamos. $\square$

Lema 3.2.8. *Sejam $m(x_1,...,x_k)$ e $n(x_1,...,x_k)$ dois monômios de $F\langle X\rangle$. Se as matrizes $m(A_1,...,A_k)$ e $n(A_1,...,A_k)$, têm na primeira linha, a mesma entrada não nula, então $m(A_1,...,A_k) = n(A_1,...,A_k)$*

Demonstração:

Pelo Lema anterior temos que existem $1 \leq i_1 \leq \cdots \leq i_q \leq k$ e $\{k_1, ..., k_q, x\} \subseteq \{1, ..., n\}$ tal que

$$m(A_1, ..., A_k) = \begin{pmatrix} 0 & \cdots & 0 & y_{i_1}^{(k_1)} \cdots y_{i_q}^{(k_q)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_x \\ \omega_{x+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_n & 0 & 0 & \cdots & 0 \end{pmatrix},$$

onde $\omega_i = y_{i_1}^{((k_1+i-2) mod\ n+1)} \cdots y_{i_q}^{((k_q+i-2) mod\ n+1)},\ i = 2, ..., n.$

Analogamente existem $1 \leq j_1 \leq \cdots \leq j_p \leq k$ e $\{r_1, ..., r_p, t\} \subseteq \{1, ..., n\}$ tal que

$$n(A_1, ..., A_k) = \begin{pmatrix} 0 & \cdots & 0 & y_{j_1}^{(r_1)} \cdots y_{j_p}^{(r_p)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \delta_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \delta_t \\ \delta_{t+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \delta_n & 0 & 0 & \cdots & 0 \end{pmatrix},$$

onde $\delta_i = y_{j_1}^{((r_1+i-2) mod\ n+1)} \cdots y_{j_p}^{((r_p+i-2) mod\ n+1)},\ j = 2, ..., n.$

Por hipótese, temos que $y_{i_1}^{(k_1)} \cdots y_{i_q}^{(k_q)} = y_{j_1}^{(r_1)} \cdots y_{j_p}^{(r_p)}$ então,

$$p = q,\ x = t \ \text{ e } \ i_1 = j_1, ..., i_q = j_q.$$

Assim, reordenando se necessário, temos que

$$k_1 = r_1, ..., k_q = r_q.$$

Portanto,

$$\omega_2 = \delta_2, ..., \omega_n = \delta_n.$$

□

Lema 3.2.9. *Sejam $m(x_1, ..., x_k)$ e $n(x_1, ..., x_k)$ dois monômios de $F\langle X\rangle$. Se $m(A_1, ..., A_k) = n(A_1, ..., A_k)$ então $m(x_1, ..., x_k) \equiv n(x_1, ..., x_k) mod\ I_n$*

Demonstração: Seja q o comprimento do monômio m. Usaremos indução em q.

Se $q = 1$ temos o resultado.

Suponha agora $q > 1$.

Suponha que x_p é uma indeterminada de $m(x_1, ..., x_k)$ e m_1 e m_2 dois monômios de $F\langle X\rangle$ tais que $m = m_1 x_p m_2$. Pelo lema 3.2.7, temos que existem monômios $\omega_1, ..., \omega_n, \delta_1, ..., \delta_n$ em Ω e inteiros $0 \leq i, j \leq n - 1$ tais que

$$m_1(A_1, ..., A_k) = \begin{pmatrix} 0 & \cdots & 0 & \omega_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_{n-i} \\ \omega_{n-i+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_n & 0 & 0 & \cdots & 0 \end{pmatrix}$$

e

$$m_2(A_1, ..., A_k) = \begin{pmatrix} 0 & \cdots & 0 & \delta_1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \delta_2 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \delta_{n-j} \\ \delta_{n-j+1} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \delta_n & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Observe que o grau de $m_1(A_1, ..., A_k)$ e $m_2(A_1, ..., A_k)$ em R são respectivamente $\bar{i}$ e $\bar{j}$.

Pelo lema 3.2.4, temos que $m_1(A_1, ..., A_k) \cdot A_p$ é igual a

$$\begin{pmatrix} 0 & \cdots & 0 & \omega_1 y_p^{(i_1)} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_2 y_p^{(i_2)} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_x y_p^{(i_x)} \\ \omega_{x+1} y_p^{(i_{x+1})} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_n y_p^{(i_x)} & 0 & 0 & \cdots & 0 \end{pmatrix},$$

onde $i_r = (i + r - 1) mod\ n\ + 1$ e $x = n - (i + \alpha(x_p)) mod\ n$.

Assim, a matriz $m(A_1, ..., A_k) = m_1(A_1, ..., A_k) \cdot A_p \cdot m_2(A_1, ..., A_k)$ é igual a

$$\begin{pmatrix} 0 & \cdots & 0 & \omega_1 y_p^{(i_1)} \delta_{j_1} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \omega_2 y_p^{(i_2)} \delta_{j_2} & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \omega_x y_p^{(i_x)} \delta_{j_y} \\ \omega_{x+1} y_p^{(i_{x+1})} \delta_{j_{y+1}} & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \omega_n y_p^{(i_x)} \delta_{j_n} & 0 & 0 & \cdots & 0 \end{pmatrix},$$

onde $j_s = (n - x + s - 1) mod\ n + 1$ e $y = n - (n - x + j) mod\ n$.

Assim a variável $y_p^{(i_1)}$ deve aparecer pelo menos uma vez na primeira linha de $n(A_1, ..., A_k)$, pois, $m(A_1, ..., A_k) = n(A_1, ..., A_k)$. Aplicando o mesmo raciocínio para n, existem dois monômios n_1 e n_2 em $F\langle X\rangle$ tais que $n = n_1 x_p n_2$ e o grau de $n_1(A_1, ..., A_k)$ é $\bar{i}$ em R, pois caso contrário a variável $y_p^{(i_1)}$ não apareceria na primeira linha de $n(A_1, ..., A_k)$. Assim, $m_1(A_1, ..., A_k)$ e $n_1(A_1, ..., A_k)$ tem o mesmo grau homogêneo em R, logo, $\alpha(m_1) = \alpha(n_1)$. Portanto, podemos concluir que se x_p é uma indeterminada de $m(x_1, ..., x_k)$ e $m_1, ..., m_l$ monômios em $F\langle X\rangle$ tal que $m = m_1 x_p m_2 x_p m_3 \cdots m_{l-1} x_p m_l$, então existem monômios $n_1, ..., n_l$ em $F\langle X\rangle$ e uma correspondência biunívoca $\varphi : \{1, ..., l\} \longrightarrow \{1, ..., l\}$ tal que $n = n_1 x_p n_2 x_p n_3 \cdots n_{l-1} x_p n_l$ e $\alpha(m_1 x_p m_2 \cdots m_t) = \alpha(n_1 x_p n_2 \cdots n_{\varphi(t)})$, $t = 1, ..., l$.

Seja x_i a primeira indeterminada de m. Assim, existem dois monômios n_1 e n_2 em $F\langle X\rangle$ tais que $n = n_1 x_i n_2$ e $\alpha(n_1) = 0$. Analisaremos os três possíveis casos:

Caso 1: Existem dois monômios m_1, m_2 em $F\langle X\rangle$ tais que $m = x_i m_1 x_i m_2$ e $\alpha(x_i m_1) = 0$. Denotando $m_0 = 1$, temos $m = m_0 x_i m_1 x_i m_2$, com $\alpha(m_0) = \overline{0}, \alpha(m_0 x_i m_1) = \overline{0}$ e

$\alpha(m_0x_im_1x_im_2) = \alpha(m)$. Então existem 3 monômios n_3, n_4, n_5 em $F\langle X\rangle$ tais que

$$n = n_3x_in_4x_in_5.$$

Portanto, como $\alpha(n) = \alpha(m)$, pois $n(A_1, ..., A_k) = m(A_1, ..., A_k)$, temos que

$$\alpha(n_3) = \overline{0} \text{ e } \alpha(n_3x_in_4) = \overline{0}.$$

Caso 2: Existem duas indeterminadas x_a e x_b e seis monômios $m_1, m_2, n_3, n_4, n_5, n_6$ em $F\langle X\rangle$ tais que $m = m_1x_ax_bm_2$ e $n = n_3x_an_4x_in_5x_bn_6, n_1 = n_3x_an_4, \alpha(m_1) = \alpha(n_3)$ e $\alpha(m_1x_a) = \alpha(n_3x_an_4x_in_5)$.

Como $\alpha(m_1) = \alpha(n_3)$, temos que, $\alpha(m_1x_a) = \alpha(n_3x_a)$. Assim, $\alpha(n_3x_a) = \alpha(m_1x_a) = \alpha(n_3x_an_4x_in_5)$. Logo, $\alpha(n_4x_in_5) = \overline{0}$.

Caso 3: Nenhum dos casos anteriores ocorre.

Considere $m = x_{i_1} \cdots x_{i_q}$. Seja $r \in \{1, ..., q\}$ e sejam $n_3, n_4, n_5, n_6 \in F\langle X\rangle$ tais que $n_1 = n_3x_{i_r}n_4$, $\alpha(n_3) = \alpha(x_{i_1} \cdots x_{i_{r-1}})$, $n = n_5x_{i_{r+1}}n_6$, $\alpha(n_5) = \alpha(x_{i_1} \cdots x_{i_r})$.

Afirmação: *Como não ocorre nenhum dos casos anteriores, temos que o comprimento de $n_5x_{i_{r+1}}$ é menor que o comprimento de n_1x_i.*

De fato, se o comprimento de $n_5x_{i_{r+1}}$ é igual ao comprimento de n_1x_i, então $n_5 = n_1$ e $x_{i_{r+1}} = x_i$. Assim, como x_i é a primeira indeterminada de m então $x_i = x_{i_1}$, logo,

$$m = x_{i_1}x_{i_2} \cdots x_{i_r}x_{i_{r+1}}x_{i_{r+2}} \cdots x_{i_q} = x_i \underbrace{x_{i_2} \cdots x_{i_r}}_{m_1} x_i \underbrace{x_{i_{r+2}} \cdots x_{i_q}}_{m_2},$$

com $\alpha(x_im_1) = \alpha(x_i \cdots x_{i_r}) = \alpha(n_5) = \alpha(n_1) = \overline{0}$, ocorrendo o caso 1.

Agora se o comprimento de $n_5x_{i_{r+1}}$ é maior que o comprimento de n_1x_i, temos que

$$\left\{ \begin{array}{l} n = n_5x_{i_{r+1}}n_6 \\ n = n_1x_in_2 = n_3x_{i_r}n_4x_in_2 \end{array} \right\},$$

então $x_{i_{r+1}}$ aparece em n_2, assim existe um monômio $n_y \in F\langle X\rangle$ tal que $n_2 = n_yx_{i_{r+1}}n_6$. Logo,

$$n = \overbrace{n_3 \underbrace{x_{i_r}}_{x_a} n_4x_in_y}^{n_5} \underbrace{x_{i_{r+1}}}_{x_b} n_6$$

e

$$m = x_{i_1}x_{i_2} \cdots x_{i_r}x_{i_{r+1}}x_{i_{r+2}} \cdots x_{i_q} = \underbrace{x_{i_1}x_{i_2} \cdots x_{i_{r-1}}}_{m_1'} x_ax_b \underbrace{x_{i_{r+2}} \cdots x_{i_q}}_{m_2'},$$

além disso, $\alpha(m_1') = \alpha(x_i \cdots x_{i_{r-1}}) = \alpha(n_3)$ e $\alpha(m_1'x_a) = \alpha(x_1 \cdots x_r) = \alpha(n_5) = \alpha(n_3x_an_4x_in_y)$, ocorrendo o caso 2. O que prova a afirmação.

Logo o comprimento de $n_5x_{i_{r+1}}$ não é maior que o comprimento de n_1. Aplicando a mesma ideia para $r+1, r+2, \ldots$ concluímos que existe $r_0 \in \{1, \ldots, q\}$ tal que para $r \geq r_0$, todo x_{i_r} aparace em n_1 o mesmo número de vezes que em $x_{i_{r_0}}x_{i_{r_0+1}} \cdots x_{i_q}$ e, toda indeterminada de n_1 está em $x_{i_{r_0}}x_{i_{r_0+1}} \cdots x_{i_q}$. Assim n_1 e $x_{i_{r_0}}x_{i_{r_0+1}} \cdots x_{i_q}$ tem o mesmo grau homogêneo. Ou seja,

$$\alpha(x_{i_{r_0}}x_{i_{r_0+1}} \cdots x_{i_q}) = \alpha(n_1) = \overline{0}.$$

Sejam m_3, m_4, m_5 monômios de $F\langle X\rangle$ tais que $m = m_3m_4x_jm_5$, onde x_j é a primeira indeterminada de n, $\alpha(m_3m_4) = \overline{0}$ e $m_4x_jm_5 = x_{i_{r_0}}x_{i_{r_0+1}} \cdots x_{i_q}$, portanto, $\alpha(m_4x_jm_5) = \alpha(x_{i_{r_0}}x_{i_{r_0+1}} \cdots x_{i_q}) = \alpha(n_1) = \overline{0}$.

Trocando as letras m por n temos o caso 3, e podemos concluir que existem quatro monômios n_7, n_8, n_9, n_{10} em $F\langle X\rangle$ tais que $n = n_7n_8x_in_9n_{10}$ e $\alpha(n_7n_8) = \overline{0}$ e $\alpha(n_8x_in_9) = \overline{0}$. Defininiremos

$$w(x_1, \ldots, x_k) = \begin{cases} x_in_9n_7n_8n_{10}, & \text{se } \alpha(n_8) = \overline{0} \\ x_in_9n_8n_7n_{10}, & \text{se } \alpha(n_8) \neq \overline{0} \end{cases}$$

Se $\alpha(n_8) = \overline{0}$, como $\alpha(n_8x_in_9) = \overline{0}$, então $\alpha(x_in_9) = \overline{0}$, agora como $\alpha(n_7n_8) = \overline{0}$ usando a identidade $x_1x_2 - x_2x_1 = \overline{0}$ com $\alpha(x_1) = \alpha(x_2) = \overline{0}$, temos que

$$(x_in_9)(n_7n_8)n_{10} \equiv (n_7n_8)(x_in_9)n_{10} \bmod I_n,$$

ou seja:

$$w(x_1, \ldots, x_k) \equiv n(x_1, \ldots, x_k) \bmod I_n.$$

Se $\alpha(n_8) \neq \overline{0}$, como $\alpha(n_7n_8) = \overline{0}$ e $\alpha(n_8x_in_9) = \overline{0}$ então $\alpha(n_7) = \alpha(x_in_9) = -\alpha(n_8)$, assim usando a identidade, $x_1xx_2 - x_2xx_1 = \overline{0}$ com $\alpha(x_1) = \alpha(x_2) = -\alpha(x)$, temos que

$$(x_in_9)n_8(n_7)n_{10} \equiv (n_7)n_8(x_in_9)n_{10} \bmod I_n,$$

ou seja:

$$w(x_1, \ldots, x_k) \equiv n(x_1, \ldots, x_k) \bmod I_n.$$

Assim, $w(x_1, \ldots, x_k) - n(x_1, \ldots, x_k) \in I_n$, agora usando os resultados 3.2.6 e 3.2.3, temos que $I_n \subseteq T(M_n(F))^{gr} = T(\frac{F\langle X\rangle}{T(M_n(F)^{gr}})^{gr} = T(R)^{gr}$, assim,

$$w(x_1, \ldots, x_k) - n(x_1, \ldots, x_k) \in T(R)^{gr}.$$

Logo,

$$w(A_1, ..., A_k) = n(A_1, ..., A_k).$$

Mas por hipótese $n(A_1, ..., A_k) = m(A_1, ..., A_k)$, assim

$$m(A_1, ..., A_k) = w(A_1, ..., A_k).$$

Se w_0 e m_0 são monômios de $F\langle X\rangle$ tais que $w = x_i w_0$ e $m = x_i m_0$, segue do lema 3.2.4 que

$$w_0(A_1, ..., A_k) = m_0(A_1, ..., A_k).$$

Como tanto o comprimento de w_0 quanto o comprimento de m_0 é $q-1$, temos por hipótese de indução que,

$$w_0(x_1, ..., x_k) \equiv m_0(x_1, ..., x_k) \bmod I_n.$$

Assim,

$$x_i w_0(x_1, ..., x_k) \equiv x_i m_0(x_1, ..., x_k) \bmod I_n,$$

e, portanto,

$$w(x_1, ..., x_k) \equiv m(x_1, ..., x_k) \bmod I_n.$$

□

Agora faremos a demonstração do Teorema 3.2.1, que é o resultado principal desta seção.

Demonstração:[Teorema 3.2.1] Já mostramos no lema 3.2.3 que $I_n \subseteq T(M_n(F))^{gr}$, agora mostraremos que $T(M_n)^{gr} \subseteq I_n$. Com efeito, seja $f(x_1, x_2, ..., x_k) \neq 0$ uma identidade polinomial graduada de $M_n(F)$, uma vez que o corpo F é infinito, podemos supor que f é multi-homogênea.

Seja r o menor inteiro não negativo tal que f pode ser expresso, módulo I_n, como uma combinação linear de r monômios multi-homogêneos, ou seja,

$$f \equiv \sum_{q=1}^{r} a_q m_q \bmod I_n,$$

onde $0 \neq a_q \in F$ e $m_1, ..., m_r \in F\langle X\rangle$. Mostraremos que $r = 0$ para termos $f \equiv 0 \bmod I_n$.

Suponha $r > 0$, como f é uma identidade polinomial graduada de $M_n(F)$ e $T(M_n(F))^{gr} = T(\frac{F\langle X\rangle}{T(M_n(F)^{gr}})^{gr} = T(R)^{gr}$, então, $f(A_1, ..., A_k) = 0$, logo,

$$a_1 m_1(A_1, ..., A_k) = -\sum_{q=2}^{r} a_q m_q(A_1, ..., A_k).$$

Segue que existe um inteiro $p \in \{2, 3, ..., r\}$ tal que $m_1(A_1, ..., A_k)$ e $m_p(A_1, ..., A_k)$ tem, na primeira linha, a mesma entrada não nula.

Pelo lema 3.2.8, segue que, $m_1(A_1, ..., A_k) = m_p(A_1, ..., A_k)$, logo, pelo lema 3.2.9,

$$m_1 \equiv m_p \text{ mod } I_n.$$

Assim,

$$f \equiv \sum_{q=1}^{r} a_q m_q \equiv (a_1 + a_p)m_1 + \sum_{q=2}^{p-1} a_q m_q + \sum_{q=p+1}^{r} a_q m_q \ (\text{mod } I_n).$$

Portanto f pode ser expressa como a soma de não mais que $r - 1$ monômios multi-homogêneos, uma contradição pela escolha do número r. Logo,

$$f \equiv 0 \text{ mod } I_n.$$

Isso completa a prova do Teorema. □

Referências Bibliográficas

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

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

[3] Dehn, M. *Uber die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme*, (German) Math. Ann. **85**, 184-194, (1922).

[4] Di Vincenzo, O. M. *On The Graded Identities of* $M_{1,1}(E)$, Israel Journal of Mathematics, **80**(1992), 323-335.

[5] Drensky, V. *Free algebras and PI-algebras*, Graduate Course in Algebra, Springer, Singapore, 1999.

[6] Drensky, V. *A minimal basis of identities for a second-order matrix algebra over a field of characteristic 0 .* Algebra and Logic. **20(3)**, (1981), 188-194.

[7] Fonseca, L. F. G. $\mathbb{Z}_2$*-graded identities of the Grassmann algebra over a finite field.* arXiv preprint arXiv:1403.0888 (2014).

[8] Giambruno, A.; Zaicev, M. *Polynomial Identities and Asymptotic Methods*, Mathematical Surveys and Monographs, vol.122, American Mathematical Society, Providence, RI, 2005.

[9] Kaplansky, I. *Rings with a polynomial identity.*Bull. Amer. Math. Soc. **54**(1948), 496-500.

[10] Kemer, A. R. *Finite basis property of identities of associative algebra.* Algebra and Logic. **26**, (1987), 362-397.

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

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

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

[14] Razmyslov P.Yu., *Trace identities of full matrix algebras over a field of characteristic zero.* (Russian) Izv. Akad. Nauk SSSR, Ser. Mat. **38,** 723-756, (1974). Translation: Math. USSR, Izv. **8**, 727-760, (1974).

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

[16] Specht, W. *Gesetze in ringen.* Math. Zeitschrift. **52**, (1950), 557-589.

[17] Swan, R. G. *A new proof of the Amitsur-Levitzki identity,* Israel J. Math., **23**, (1976), 187-188.

[18] Vasilovsky, S.Yu. $\mathbb{Z}_n$*-graded Polynomial Identities of the Full Matrix of order* n, Proceedings of the American Mathematical Society, **127(12)**(1999), 3517-3524.

[19] Wagner, W. *Uber die Grundlagen der projektiven Geometrie und allgemeine Zahlensysteme*, (German) Math. Ann. **113**, 528-567, (1936).