Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Programa de Pós-Graduação em Matemática

Celine Ingrid Gomes dos Santos [†]

Identidades Polinomiais Graduadas para a Álgebra de Matrizes Triangulares Superiores sobre um Corpo Finito

Campina Grande - PB

2026

[†]Este trabalho contou com apoio financeiro do Capes.

Celine Ingrid Gomes dos Santos

Identidades Polinomiais Graduadas para a Álgebra de Matrizes Triangulares Superiores sobre um Corpo Finito

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática da Universidade Federal de Campina Grande, pertencente à linha de pesquisa Álgebra e área de concentração Matemática, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Diogo Diniz Pereira da Silva e Silva

Campina Grande - PB

2026

Universidade Federal de Campina Grande - UFCG
Sistema de Bibliotecas - SISTEMOTECA
Catalogação de Publicação na Fonte. UFCG - Biblioteca Central

M357s Santos, Celine Ingrid Gomes dos.

Identidades polinomiais graduadas para a álgebra de matrizes triangulares superiores sobre um corpo finito / Celine Ingrid Gomes dos Santos. – 2026.

93 f.

Dissertação (mestrado em Matemática) – Universidade Federal de Campina Grande, Centro de Centro de Ciências e Tecnologia, 2026.

"Orientação: Prof. Dr. Diogo Diniz Pereira da Silva e Silva".

Referências.

1. PI-álgebras. 2. Álgebras graduadas. 3. Matrizes triangulares superiores. 4. Identidades polinomiais graduadas. 5. Corpos finitos. I. Silva, Diogo Diniz Pereira da Silva e. II. Título.

UFCG/BC CDU 51(043.3)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA ITAPUANA SOARES DIAS GONÇALVES CRB-15/93

Identidades Polinomiais Graduadas para a Álgebra de Matrizes Triangulares Superiores sobre um Corpo Finito

por

Celine Ingrid Gomes dos Santos

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

Área de Concentração: Álgebra

Aprovada em: 24/02/2026

gov.br Documento assinado digitalmente
JOSEFA ITAILMA DA ROCHA
Data: 05/03/2026 09:20:55-0300
Verifique em https://validar.iti.gov.br

Profª. Dra. Josefa Itailma da Rocha - UFCG

Manuela da Silva Souza

Profª. Dra. Manuela da Silva Souza - UFBA

Daniela Martinez C.

Profª. Dra. Daniela Martinez Correa - Unicamp

Diogo Diniz P.S. Silva

Prof. Dr. Diogo Diniz Pereira da Silva e Silva - UFCG

Orientador

Universidade Federal de Campina Grande

Centro de Ciências e Tecnologia

Programa de Pós-Graduação em Matemática

Curso de Mestrado em Matemática

Fevereiro - 2026

Agradecimentos

A Deus, por ser o meu alicerce e por tanto que tem feito em minha vida, ainda que imerecidamente. Obrigada, Pai, por tudo.

Aos meus pais, Rejane e Adriano. Não existem palavras que traduzam toda a minha gratidão e o amor que sinto por vocês. Vocês me apoiaram nas minhas escolhas e vibraram por cada pequena conquista ao longo do meu caminho. Se hoje chego até aqui, é porque tive o privilégio de contar com a dedicação e cuidado de vocês. Obrigada por cada incentivo. Essa conquista é tão minha quanto de vocês, e levo comigo a certeza de que tudo o que faço é, de alguma forma, reflexo do amor que recebi.

Ao meu amor, Wilton, por estar comigo em cada etapa dessa jornada, dividindo não apenas as conquistas, mas também as inseguranças e os dias difíceis. Obrigada por me apoiar com paciência, me incentivar quando pensei em desistir e celebrar comigo cada vitória. Sua presença tornou esse caminho mais leve, e cada página desta dissertação carrega um pouco do seu apoio. Eu te amo, meu amor.

Ao meu orientador, Professor Diogo, pela oportunidade e orientação que possibilitaram a realização desta dissertação.

Às professoras membras da banca examinadora, pela disponibilidade e contribuições oferecidas.

Estendo os meus agradecimentos a todos os professores que contribuíram para a minha formação acadêmica, pelo conhecimento e inspiração transmitida em sala de aula. Em especial, agradeço à Professora Itailma, cujo apoio foi fundamental. Seus conselhos, orientação desde o PET e o vínculo de amizade tornaram a minha caminhada mais leve.

Aos meus avós, Antônia e Manuel, carinhosamente chamados de Vovó Toinha e Vovô Manel, dedico a minha eterna gratidão.

Agradeço às minhas tias Graça, Rose, Nelma, Sinha e Nê, e ao meu tio Lucas, que sempre estiveram presentes de forma especial em minha vida. Aos meus primos Vittor, Davi, Laura, Thainá e Aurora, pela alegria que sempre me trouxeram.

Agradeço de coração aos meus amigos e colegas de turma Laryssa, Marisa, Pedro,

Ísis, Joice, Cleyson e Mateus, cuja companhia tornaram o mestrado mais alegre. Estendo, também, os meus agradecimentos às minhas amigas Larissa, Eduarda, Mayara, Ester e Sileia, que estão sempre presentes em minha vida. De maneira especial, agradeço à Érica, Ary, Ana Beatriz, Eduardo e ao professor José Lucas, por toda a ajuda durante o mestrado, e ao pessoal da sala da Pós-Graduação.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Dedicatória

À minha mãe, Rejane, e aos meus avós, Dona Toinha e Seu Manuel.

Resumo

Sejam $\mathbb{K}$ um corpo finito, G um grupo e UT_n a álgebra das matrizes triangulares superiores de ordem $n \times n$ sobre $\mathbb{K}$. Nesta dissertação, estudamos as graduações elementares em UT_n e suas identidades polinomiais graduadas. Classificamos todas as graduações em UT_n, mostrando que toda $G-$graduação em UT_n é isomorfa a uma graduação elementar. Além disso, demonstramos que duas graduações elementares coincidem se, e somente se, satisfazem as mesmas identidades graduadas. Finalmente, obtivemos o resultado principal do trabalho: uma descrição explícita de uma base para o T_G-ideal das identidades polinomiais graduadas de UT_n, para qualquer graduação elementar fixada. Se o grupo G é finito, então a base obtida é finita.

Palavras-chave: PI-álgebras, Álgebras graduadas, Matrizes triangulares superiores, Identidades polinomiais graduadas, Corpos finitos.

Abstract

Let $\mathbb{K}$ be a finite field, G a group, and UT_n the algebra of upper triangular matrices of order $n \times n$ over $\mathbb{K}$. In this dissertation, we study the elementary gradings on UT_n and their graded polynomial identities. We classify all the gradings on UT_n, proving that every $G-$grading on UT_n is isomorphic to an elementary grading. Furthermore, we prove that two elementary gradings coincide if and only if they satisfy the same graded identities. Finally, we obtain the main result of this work: an explicit description of a basis for the T_G-ideal of graded polynomial identities of UT_n, for any fixed elementary grading. If the group G is finite, then the obtained basis is finite.

Key Words: PI-algebras, Graded algebras, Upper triangular matrices, Graded Polynomial identities, Finite fields.

Sumário

Introdução

Dentro do campo da Álgebra, encontramos o estudo das Álgebras com Identidades Polinomiais, também denominadas simplesmente de PI-Álgebras. Essa classe é bastante extensa e inclui, por exemplo, álgebras de dimensão finita, álgebras de Grassmann, álgebras nilpotentes, além de diversas outras de significativa importância para a Matemática. A extensão desta classe é ainda atestada pelo Teorema do Produto Tensorial de Regev, que mostra como novas PI-álgebras podem ser construídas a partir de outras conhecidas, por meio do produto tensorial.

A priori, considere A um espaço vetorial sobre um corpo $\mathbb{K}$. Dizemos que A é uma $\mathbb{K}-$álgebra quando A está munido de uma multiplicação bilinear associativa. Em algumas referências, é possível encontrar o termo "álgebra associativa" nessa definição. No entanto, no contexto desta dissertação, uma $\mathbb{K}-$álgebra sempre será associativa.

Sob esse viés, se considerarmos $\mathbb{K}\langle X\rangle$, com X um conjunto infinito e enumerável, como sendo a álgebra dos polinômios em variáveis não comutativas, dizemos que o polinômio não nulo $f(x_1,\ldots,x_n)\in\mathbb{K}\langle X\rangle$ é uma identidade polinomial para A se, para qualquer substituição das variáveis de f por elementos de A, obtivermos zero como resultado. Desse modo, se existe um polinômio não nulo que é uma identidade para A, diremos que A é uma PI-álgebra, da expressão em inglês "polynomial identity". Denotaremos por $T(A)$ o conjunto de todas as identidades polinomiais de A.

Historicamente, o estudo da PI-Teoria iniciou-se por volta de 1930, ainda que de maneira implícita, com os artigos de Dëhn [10] e Wagner [49]. Nesses trabalhos, identificam-
-se as primeiras identidades polinomiais para a álgebra de matrizes de ordem 2, embora o conceito em si já pudesse ser encontrado em estudos anteriores, como os de Sylvester,

por volta de 1852.

Nesse cenário, foi a partir de 1950 que a pesquisa sobre PI-álgebras ganhou maior impulso, com contribuições de matemáticos como Jacobson [30], Kaplansky [25], Amitsur e Levitzki [30]. Nesse contexto, uma questão central para o desenvolvimento da teoria era determinar o menor grau de uma identidade polinomial válida para a álgebra matricial de ordem n sobre um corpo. A resposta para esse problema veio com o Teorema de Amitsur e Levitzki [2], que se tornou um resultado clássico e de grande importância para a consolidação da PI-Teoria, servindo de base para grande parte das pesquisas posteriores. A relevância desse teorema pode ser atestada por seu uso em trabalhos recentes como o de Breuillard, Green, Guralnick e Tao [8].

Um dos conceitos centrais na PI-Teoria é o de base para identidades polinomiais de uma álgebra, que consiste em um conjunto de identidades a partir do qual todas as demais identidades da álgebra podem ser deduzidas. Nos últimos anos, diversos autores têm contribuído para a descrição explícita de tais bases em álgebras notáveis. Contudo, tais bases são conhecidas de forma explícita apenas para um número bastante reduzido de casos.

Um dos problemas mais estudados nessa área é a determinação de uma base para a álgebra $M_n(\mathbb{K})$. Sabe-se que, até os dias atuais, não é conhecida uma base de identidades para a álgebra $M_n(\mathbb{K})$, quando $\mathbb{K}$ é infinito e $n > 3$. Já para corpos finitos e $n = 2, 3, 4$, existem bases finitas determinadas e descritas em [19], [20] e [32]. Além disso, no caso em que $n = 2$ e $\mathbb{K}$ é infinito, com $\operatorname{char}\mathbb{K} \neq 2$, bases finitas também são conhecidas. No entanto, esse caso específico permanece em aberto em característica 2.

Avançando no caso $n = 2$ e característica zero, Razmyslov [36] provou que a variedade de álgebras associativas, gerada pela álgebra de matrizes de segunda ordem, possui base finita de nove identidades. Em seguida, ele também conjecturou que, sob essas mesmas hipóteses, uma base minimal para as identidades de M_n consiste de duas identidades: $s_{2n}(x_1, x_2, \ldots, x_{2n}) = 0$ e $s_n([x_1^n, x_2], [x_1^{n-1}, x_2], \ldots, [x_1, x_2]) = 0$. A posteriori, essa conjectura teve sua veracidade confirmada por Drensky [15], para $n = 2$.

Em um contexto mais amplo, Kemer [26] provou, para o caso em que $\operatorname{char}\mathbb{K} = 0$, que, se A é uma PI-álgebra, então $T(A)$ é finitamente gerado como um $T-$ideal. Esse problema foi apresentado, em 1950, por Specht [42]. No entanto, em 1999, Belov [5], Grishin [23] e Shchigolev [40] mostraram que essa conjectura não é válida quando $\operatorname{char}\mathbb{K} =$

$p \neq 0$.

Ao longo das últimas décadas, diversas generalizações do conceito clássico de identidade polinomial têm sido investigadas na literatura. As identidades graduadas, por exemplo, ganharam relevância a partir do trabalho de Kemer [27]. Esse, em sua teoria dos ideais de identidades em álgebras associativas, fez uso essencial de identidades $\mathbb{Z}_2-$graduadas para abordar problemas fundamentais sobre identidades ordinárias.

Retomando o Problema de Specht, em 2010, Aljadeff, Belov [1] e Sviridova [46] publicaram que o Teorema de Kemer vale no contexto graduado, quando $\operatorname{char}\mathbb{K} = 0$ e G é um grupo finito.

Outras contribuições significativas sobre álgebras graduadas vieram de diferentes autores. Di Vincenzo [13] descreveu as identidades graduadas de $M_{1,1}(G)$ sobre um corpo de característica zero. Vasilovsky [48] caracterizou as identidades graduadas para a álgebra de matrizes de ordem n com $\mathbb{Z}_n-$graduação canônica. Já Di Vincenzo e Nardozza, em [11], determinaram um sistema de geradores para as identidades polinomiais graduadas das álgebras $M_{a,b}(G)$ e $M_{a,b}(G) \otimes M_{c,d}(G)$, mostrando, ainda, que este produto tensorial satisfaz as mesmas identidades graduadas que $M_{ac+bd,ad+bc}(G)$.

Considere $UT_n(\mathbb{K}) = UT_n$ a álgebra das matrizes triangulares superiores $n \times n$ sobre $\mathbb{K}$. O conjunto $T(UT_n)$, de todas as identidades polinomiais de UT_n, foi descrito por Maltsev [33] quando $\operatorname{char}(\mathbb{K}) = 0$. A posteriori, Siderov [41] obteve que $T(UT_n(\mathbb{K})) = (T(\mathbb{K}))^n$, sendo $\mathbb{K}$ um corpo qualquer.

Na PI-Teoria, a álgebra UT_n tem grande importância. Em [16] e [29], por exemplo, encontramos que se A é uma PI-álgebra finitamente gerada que satisfaz uma identidade polinomial não matricial e $\mathbb{K}$ é infinito, então existe n tal que $T(UT_n)$ está contido no conjunto de todas as identidades polinomiais de A, ou seja, $T(UT_n(\mathbb{K})) \subseteq T(A)$. Além disso, essas álgebras, em característica zero, geram variedades minimais, com respeito ao expoente da álgebra.

Nesta dissertação, focamos no estudo das identidades polinomiais graduadas da álgebra UT_n sobre um corpo finito. Um primeiro passo essencial para isso foi compreender as possíveis $G-$graduações em UT_n. Conforme demonstrado por Valenti e Zaicev [47], toda $G-$graduação em UT_n é isomorfa a uma graduação elementar. Partindo dessa classificação, investigamos o seguinte problema: como as identidades polinomiais graduadas caracterizam tais graduações? Mostramos que duas graduações elementares em UT_n co-

incidem se, e somente se, satisfazem as mesmas identidades graduadas. Nosso resultado principal consiste na descrição explícita de uma base finita para o T_G-ideal das identidades $G-$graduadas de UT_n, para qualquer graduação elementar fixada.

No primeiro capítulo desta dissertação, construímos o alicerce necessário para o entendimento desta dissertação. Nele, estão presentes os resultados preliminares da teoria de PI-álgebras, e outros temas relevantes, como espaços vetoriais quocientes, álgebras e graduações, bem como a aplicação desses conceitos na álgebra das matrizes triangulares superiores. Além disso, fizemos uma revisão dos principais conceitos sobre corpos finitos.

Como já fora dito, em 2007, Valenti e Zaicev [47] classificaram todas as graduações em UT_n, mostrando que toda $G-$graduação em UT_n é isomorfa a uma graduação elementar. Além disso, demonstraram que duas graduações elementares coincidem se, e somente se, definem as mesmas identidades graduadas. Apresentamos esses resultados no Capítulo 2 desta dissertação.

Já no Capítulo 3, apresentamos uma descrição explícita de uma base para o T_G-ideal das identidades polinomiais graduadas de UT_n, para qualquer graduação elementar fixada, feita por Riva e Gonçalves [21], para o caso em que $\mathbb{K}$ é um corpo finito. O caso em que $\mathbb{K}$ é infinito foi feito por Di Vincenzo, Koshlukov e Valenti [12]. Ademais, mostramos também os respectivos corolários que dele decorrem, os quais evidenciam consequências relevantes do teorema e complementam sua aplicação no estudo das identidades graduadas em UT_n.

Capítulo 1

Álgebras e Corpos Finitos

Para o adequado acompanhamento desta dissertação, é necessário que o leitor tenha familiaridade prévia com conceitos básicos de Álgebra Linear e de Estruturas Algébricas. Desse modo, indicamos algumas obras para esse fim na seção de referências.

Neste capítulo, serão apresentados os conceitos fundamentais que servirão como base para o desenvolvimento desta dissertação. Nosso objetivo é construir o alicerce teórico necessário, com ênfase nos espaços vetoriais quocientes, suas propriedades e aplicações, bem como nos aspectos estruturais de álgebras e corpos finitos.

Ao longo deste trabalho, $\mathbb{K}$ denotará um corpo. Todas as álgebras e espaços vetoriais considerados serão sobre $\mathbb{K}$.

1.1 Corpos Finitos

Nesta seção, reunimos os conceitos e resultados fundamentais acerca de corpos finitos que serão empregados ao longo deste trabalho. Diversas construções e argumentos apresentados nos capítulos seguintes utilizam propriedades estruturais desses corpos. Dessarte, incluímos esta exposição preliminar com o propósito de estabelecer notação, fixar resultados básicos e tornar o texto autossuficiente.

Definição 1.1.1 *Seja G é um grupo finito. O* ***expoente*** *de G, denotado por $\exp G$, é o mínimo múltiplo comum das ordens dos elementos de G.*

Observe que, se G é finito, então todo elemento tem ordem finita, e o conjunto de ordens é finito. Dessa forma, o mínimo múltiplo comum sempre existe.

Exemplo 1.1.2 *O expoente do grupo simétrico S_3 é 6.*

De fato, o grupo simétrico S_3, que consiste em todas as permutações de três elementos, possui seis elementos: a identidade, três transposições e dois 3-ciclos.

A identidade tem ordem 1. Cada transposição tem ordem 2, enquanto cada 3-ciclo tem ordem 3. Assim, as possíveis ordens de elementos em S_3 são 1, 2 e 3.

Portanto, o expoente de S_3 é dado por $\text{mmc}(1,2,3) = 6$, concluindo que o expoente de S_3 é 6.

Definição 1.1.3 *Seja $\mathbb{K}$ um conjunto não vazio, munido de uma operação de adição $+ : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K}$, e uma operação de multiplicação $\cdot : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K}$. Dizemos que $\mathbb{K}$ é um **corpo** se:*

i) $(\mathbb{K}, +)$ é um grupo abeliano;

ii) $(\mathbb{K}^*, \cdot)$ é um grupo abeliano, cujo elemento neutro é 1, e $\mathbb{K}^* = \mathbb{K} - \{0\}$;

iii) a multiplicação é distributiva em relação à adição.

Exemplo 1.1.4 *$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são corpos.*

Exemplo 1.1.5 *$\mathbb{Z}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$, com p primo, é um corpo e será denotado por $\mathbb{F}_p$.*

Exemplo 1.1.6 *$p(x) = x^2 + 1$ é um polinômio irredutível sobre $\mathbb{Z}_{11}$. Dessa forma, $\dfrac{\mathbb{Z}_{11}[x]}{\langle p(x) \rangle}$ é um corpo de $|\mathbb{Z}_{11}|^{\deg p(x)} = 11^2 = 121$ elementos.*

Mais geralmente, esse resultado é válido para $\mathbb{F}_p$, quando p é primo e $p(x)$ é um polinômio irredutível de grau n.

Definição 1.1.7 *Sejam $\mathbb{F}$ e $\mathbb{K}$ corpos tais que $\mathbb{F} \subseteq \mathbb{K}$. Dizemos que $\mathbb{F}$ é um **subcorpo** de $\mathbb{K}$ se $\mathbb{F}$ é um corpo em relação às operações induzidas de $\mathbb{K}$, isto é, $0, 1 \in \mathbb{F}$, $\mathbb{F}$ é fechado para as operações de adição e multiplicação de $\mathbb{K}$, e todo elemento não nulo de $\mathbb{F}$ possui inverso multiplicativo em $\mathbb{F}$.*

Definição 1.1.8 *Se $\mathbb{F}$ é um subcorpo de $\mathbb{K}$, então $\mathbb{K}$ é chamado uma **extensão** de $\mathbb{F}$. Vamos nos referir ao par $\mathbb{F} \subseteq \mathbb{K}$ como a extensão $\mathbb{K}/\mathbb{F}$ e $\mathbb{F}$ como o corpo base.*

Transformamos $\mathbb{K}$ em um $\mathbb{F}-$espaço vetorial definindo a multiplicação por escalar em $\mathbb{K}$ por $\alpha \cdot a = \alpha a$, com $\alpha \in \mathbb{F}$ e $a \in \mathbb{K}$. Escrevemos $[\mathbb{K} : \mathbb{F}]$ para nos referirmos à dimensão de $\mathbb{K}$ como um $\mathbb{F}-$espaço vetorial. Essa dimensão é chamada de grau da extensão $\mathbb{K}/\mathbb{F}$. Se $[\mathbb{K} : \mathbb{F}] < \infty$, então $\mathbb{K}$ é uma extensão finita de $\mathbb{F}$. Caso contrário, $\mathbb{K}$ é uma extensão infinita de $\mathbb{F}$.

Exemplo 1.1.9 *A extensão $\mathbb{C}/\mathbb{R}$ é finita, pois uma base de $\mathbb{C}$ como $\mathbb{R}-$espaço vetorial é $\{1, i\}$. Assim, $[\mathbb{C} : \mathbb{R}] = 2$.*

Definição 1.1.10 *Seja $\mathbb{K}$ um corpo. Se existe $n \in \mathbb{N}$ tal que $n \cdot 1 = 0$, dizemos que $\mathbb{K}$ tem caractística positiva e, nesse caso, definimos a* ***característica*** *de $\mathbb{K}$, denotada por* $\operatorname{char}\mathbb{K}$*, como sendo o menor natural que satisfaz essa igualdade. Caso não exista tal $n \in \mathbb{N}$, dizemos que $\mathbb{K}$ tem característica 0 e denotamos por* $\operatorname{char}\mathbb{K} = 0$.

Em outras palavras, a característica de um corpo é o gerador não negativo do núcleo do único homorfismo de anéis de $\mathbb{Z}$ em $\mathbb{K}$.

Exemplo 1.1.11 *$\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos de característica zero.*

Embora tenhamos definido a característica no contexto de corpos, essa noção estende-se naturalmente ao caso de anéis.

Exemplo 1.1.12 *Todo anel finito tem característica positiva, a qual deve ser menor ou igual à ordem do anel. Aqui, a ordem de um anel A significa a sua cardinalidade, isto é, o número de elementos de A. De fato, sendo A um anel de ordem n, temos que $na = 0_A$, para todo $a \in A$. Logo, $0 < \operatorname{char}(A) \leq n$.*

Exemplo 1.1.13 *Para cada inteiro primo p, $\mathbb{F}_p$ é um corpo de característica p.*

Observação 1.1.14 *Se dois corpos $\mathbb{K}$ e $\mathbb{K}'$ são isomorfos, então eles têm a mesma característica. De fato, se $\varphi : \mathbb{K} \longrightarrow \mathbb{K}'$ é um isomorfismo, então $n \cdot 1 = 0$ se, e somente se, $0 = \varphi(n \cdot 1) = n\varphi(1) = n \cdot 1$.*

Proposição 1.1.15 *Seja $\mathbb{K}$ um corpo. Então a característica de $\mathbb{K}$ é 0 ou um número primo.*

Demonstração: Suponhamos que a característica de $\mathbb{K}$ não seja 0. Então, a característica de $\mathbb{K}$ é um inteiro positivo $p > 0$. Suponha que $p = qr$, com $1 < q, r < p$. Desse modo, $0 = p \cdot 1 = (q \cdot 1)(r \cdot 1)$. Como $\mathbb{K}$ é um corpo, devemos ter $q \cdot 1 = 0$ ou $r \cdot 1 = 0$. Mas, como $q, r < p$, pela minimalidade de p, temos um absurdo. ■

Agora, apresentaremos um resultado que revela, especificamente, como deve ser a característica de um corpo finito, que é o contexto em que está inserida esta dissertação.

Proposição 1.1.16 *Se $\mathbb{K}$ é um corpo finito, então sua característica é um número inteiro primo.*

Demonstração: Veja, por exemplo, [38].

Como consequência imediata da proposição anterior, concluímos que todo corpo de característica 0 é infinito.

Agora, apresentaremos resultado fundamental sobre corpos finitos, uma vez que caracteriza totalmente quando um elemento pertence a um corpo.

Proposição 1.1.17 *Se $\mathbb{K}$ é um corpo finito com q elementos, então todo $a \in \mathbb{K}$ satisfaz $a^q = a$.*

Demonstração: A igualdade $a^q = a$ é trivial para $a = 0$. Por outro lado, $\mathbb{K}^*$ é um grupo multiplicativo de ordem $q - 1$. Assim, pelo Teorema de Lagrange,

$$a^{q-1} = 1, \text{ para todo } a \in \mathbb{K}^*.$$

Portanto,

$$a^{q-1}a = a^q = a. \ \blacksquare$$

Uma consequência do resultado anterior é que o polinômio $x^q - x$ tem exatamente q elementos de $\mathbb{F}_q$ como raízes.

Antes de avançarmos, analisaremos uma restrição importante: a hipótese de que o corpo em questão seja finito. Essa condição, embora apareça frequente em diversos resultados, impõe fortes limitações sobre a estrutura possível de tais corpos. De fato, não é possível que existam corpos finitos com cardinalidades arbitrárias.

O próximo teorema descreve precisamente quais cardinalidades podem ocorrer no caso finito, estabelecendo um vínculo direto entre a característica do corpo e sua ordem.

Teorema 1.1.18 *Seja $\mathbb{K}$ um corpo finito de característica p. Então existe um natural n tal que a ordem de $\mathbb{K}$ é exatamente p^n.*

Demonstração: Considere a aplicação

$$\begin{aligned} \varphi : \mathbb{F}_p &\longrightarrow \mathbb{K} \\ \bar{a} &\longmapsto a \cdot 1 \end{aligned} .$$

Em primeiro lugar, vejamos que φ está bem definida. Considere $a, a' \in \mathbb{Z}$ tais que $\bar{a} = \bar{a'}$. Então $p|(a - a')$. Logo, $(a - a') \cdot 1 = 0$ ou, equivalentemente, $\varphi(\bar{a}) = a \cdot 1 = a' \cdot 1 = \varphi(\bar{a'})$. Logo, φ está bem definida.

É imediato observar que φ é homomorfismo.

Além disso, sabemos que $\ker \varphi$ é um ideal de $\mathbb{F}_p$. Como todo corpo só tem dois ideais e $\ker \varphi \neq \mathbb{F}_p$, uma vez que $\varphi(1) = 1$, segue que $\ker \varphi = \{0\}$. Dessa forma, φ é injetor.

Denotemos por $\mathbb{K}'$ a imagem de φ. Como φ é injetora, $\mathbb{K}'$ tem exatamente p elementos. Além disso, a igualdade $\varphi(1) = 1$ nos diz que $1 \in \mathbb{K}'$. Também sabemos que

$0 \in \mathbb{K}'$. Das igualdades $\varphi(a+b) = \varphi(a) + \varphi(b)$ e $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, lidas da direita para a esquerda, concluímos que a adição e multiplicação de elementos de $\mathbb{K}'$ são fechadas. Finalmente, se um elemento está em $\mathbb{K}'$ então seus inversos aditivos e multiplicativos também pertencem a $\mathbb{K}'$. Logo, $\mathbb{K}'$ é um subcorpo de $\mathbb{K}$.

Consideremos $\mathfrak{B} = \{v_1, \ldots, v_n\}$ uma base de $\mathbb{K}$. Cada elemento de $\mathbb{K}$ se escreve de forma única como uma soma da forma

$$\alpha_1 v_1 + \cdots + \alpha_n v_n,$$

com $\alpha_1, \ldots, \alpha_n \in \mathbb{K}'$. Desse modo, segue que, para contar a quantidade de elementos de $\mathbb{K}$, devemos contar a quantidade de listas $(\alpha_1, \ldots, \alpha_n)$, com $\alpha_i \in \mathbb{K}'$, para cada $1 \leq i \leq n$. Como a cardinalidade de $\mathbb{K}'$ é p, segue que o número de listas deve ser exatamente p^n. ■

O próximo resultado é conhecido informalmente como Teorema do Sonho do Calouro (Freshman's Dream Theorem). Esse nome faz alusão à ideia, comumente incorreta para números reais, de que $(a+b)^n = a^n + b^n$, para todo n natural. Surpreendentemente, essa igualdade de fato ocorre, para potências da característica, em corpos de característica positiva.

Teorema 1.1.19 (Teorema do Sonho do Calouro) *Seja $\mathbb{K}$ um corpo de característica $p > 0$ e a, b elementos de $\mathbb{K}$. Então, para cada número natural n, tem-se*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Demonstração: Primeiro, faremos a prova para $n = 1$. Utilizando a expansão binomial, temos

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{r} a^{p-r}b^r + \cdots + \binom{p}{p-1} ab^{p-1} + b^p.$$

Note que, para $1 \leq r \leq p-1$, o coeficiente binomial $\binom{p}{r}$ é um número maior do que 1. Além disso, temos

$$\binom{p}{r} \cdot s! = p \cdot (p-1) \cdots (p-(p-s)+1),$$

em que $s = p - r$ ou $s = r$. Em todo caso, $s < p$. Sabemos que p divide $\binom{p}{r} \cdot s!$. Mas os fatores de $s!$ são todos menores que p. Logo, p divide $\binom{p}{r}$. Assim, como o corpo $\mathbb{K}$ tem característica p segue da igualdade que as parcelas $\binom{p}{r} a^{p-r}b^r$ são zero. Logo,

$$(a+p)^p = a^p + b^p,$$

como desejado.

Supondo, agora, que a afirmação é verdadeira para $n-1$, temos

$$(a+b)^{p^n} = \left[(a+b)^{p^{n-1}}\right]^p = \left(a^{p^{n-1}} + b^{p^{n-1}}\right)^p = \left(a^{p^{n-1}}\right)^p + \left(b^{p^{n-1}}\right)^p = a^{p^n} + b^{p^n}$$

e, portanto, concluímos a demonstração. ■

O resultado a seguir é um bastante conhecido na Teoria dos Números. Trata-se de uma conhecida consequência do Teorema de Lucas, que estabelece uma propriedade fundamental dos coeficientes binomiais módulo um primo.

Lema 1.1.20 *Se p é um número primo e $t \geq 1$, então*

$$\binom{p^t}{i} = 0 \pmod{p},$$

para todo i tal que $1 \leq i \leq p^t - 1$.

Demonstração: Faremos indução em t.

Se $t = 1$, então $\binom{p}{i} = pm$, para algum $m \in \mathbb{Z}$ tal que $p \nmid m$. De fato, $m = \dfrac{(p-1)!}{i!(p-i)!}$.

Suponha que $t \geq 2$. Na álgebra comutativa $\mathbb{Z}_p[x]$, sabemos que

$$(1+x)^{p^t} = \sum_{i=0}^{p^t} \binom{p^t}{i} x^i. \text{ (Binômio de Newton)}$$

Por hipótese de indução e utilizando o Teorema 1.1.19, valem as seguintes igualdades:

$$(1+x)^{p^t} = \left((1+x)^p\right)^{p^{t-1}} = (1+x^p)^{p^{t-1}} = \cdots = 1 + x^{p^t}.$$

Assim, de

$$\sum_{i=0}^{p^t} \binom{p^t}{i} x^i = (1+x)^{p^t} = 1 + x^{p^t},$$

concluímos que

$$\binom{p^t}{i} = 0$$

módulo p, para todo $1 \leq i \leq p^t - 1$. ■

Definição 1.1.21 *Seja $f(x) \in \mathbb{K}[x] - \mathbb{K}$ um polinômio de grau n. Um* ***corpo de decomposição*** *de $f(x)$ sobre $\mathbb{K}$ é um corpo $\mathbb{L}$ que satisfaz as seguintes propriedades:*

(i) $\mathbb{K}$ *está contido em* $\mathbb{L}$ *como subcorpo;*

(ii) $f(x)$ *se decompõe em fatores lineares sobre* $\mathbb{L}$*, isto é, existem* $a \in \mathbb{K}$ *e* $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$ *tais que*

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n);$$

(iii) $\mathbb{L}$ *é mínimo com respeito à inclusão entre os corpos que satisfazem as propriedades anteriores, ou seja, não existe subcorpo próprio de* $\mathbb{L}$ *que contenha* $\mathbb{K}$ *e todos os* α_i*.*

Teorema 1.1.22 *Sejam p, n números inteiros positivos, com p primo. Então existe um corpo $\mathbb{K}$, de característica p, com exatamente p^n elementos.*

Demonstração: Definamos $q = p^n$. Suponhamos $\mathbb{K}$ o corpo de decomposição do polinômio $f(x) = x^q - x$ sobre $\mathbb{F}_p$. Sabemos que $f(x)$ tem raízes múltiplas se, e somente se, $\text{mdc}(f, f') \neq 1$, em que f' denota a derivada formal de f. Notemos que $f'(x) = -1$ e $\text{mdc}(x^q - x, -1) = 1$. Logo, as raízes de $f(x)$ são duas a duas distintas.

Definamos, agora, $L = \{\alpha \in \mathbb{K}; f(\alpha) = 0\}$. Afirmamos que L é um subcorpo de $\mathbb{K}$. Obviamente, $f(0) = 0$ e $f(1) = 0$. Assim, $0, 1 \in L$. Agora suponhamos $\alpha, \beta \in L$. Temos

$$\begin{aligned}(\alpha + \beta)^q &= \sum_{i=0}^{q} \binom{q}{i} \alpha^{q-i} \beta^i \\ &= \alpha^q + \beta^q \\ &= \alpha + \beta.\end{aligned}$$

Assim, $\alpha + \beta \in L$.

Além disso,

$$(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta,$$

o que nos diz que $\alpha\beta \in L$.

Por último, dado $\alpha \in L$ não nulo, temos

$$(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$$

e

$$(-\alpha)^q = -\alpha,$$

ou seja, $\alpha^{-1}, -\alpha \in L$.

Como L contém $\mathbb{Z}_p$ como subcorpo e todas as raízes de $f(x)$ pertencem a L, segue que $L = \mathbb{K}$. Como L é o conjunto de todas as raízes distintas de $f(x)$ em $\mathbb{K}$, $|L| = \deg(f(x)) = q = p^n$. ■

Teorema 1.1.23 *Seja $f(x) \in \mathbb{K}[x] - \mathbb{K}$. Se $\mathbb{L}$ e $\mathbb{L}'$ são corpos de decomposição de $f(x)$ sobre $\mathbb{K}$, então $\mathbb{L} \simeq \mathbb{L}'$.*

Demonstração: Veja, por exemplo, [9].

Teorema 1.1.24 *Sejam $\mathbb{K}$ e $\mathbb{K}'$ dois corpos finitos de mesma cardinalidade. Então $\mathbb{K}$ e $\mathbb{K}'$ são isomorfos.*

Demonstração: Sabemos, pelo Teorema 1.1.18, que devem existir inteiros p e n, com p primo, tais que $|\mathbb{K}| = |\mathbb{K}'| = p^n$ e $\operatorname{char}\mathbb{K} = \operatorname{char}\mathbb{K}' = p$. Em particular, $\mathbb{F}_p$ é um subcorpo de $\mathbb{K}$ e $\mathbb{K}'$. Pela demonstração do Teorema 1.1.22, segue que $\mathbb{K}$ e $\mathbb{K}'$ são ambos corpos de decompoição do polinômio $x^{p^n} - x \in \mathbb{F}_p[x]$. Pelo Teorema 1.1.23, segue que $\mathbb{K} \simeq \mathbb{K}'$. ■

O próximo resultado será fundamental para demonstrarmos que o grupo multiplicativo de um corpo finito é cíclico.

Proposição 1.1.25 *Seja G um grupo abeliano finito. Se $n = \exp G$, então existe um elemento em G de ordem n. Desse modo, $\exp G$ é a ordem máxima de um elemento de G. Além disso, G é cíclico se, e somente se, $|G| = \exp G$.*

Demonstração: Veja, por exemplo, [35].

Teorema 1.1.26 *Se $\mathbb{K}$ é um corpo e G é um subgrupo finito de $\mathbb{K}^*$, então G é cíclico.*

Demonstração: Seja $n = |G|$ e $m = \exp G$. Então, pela Proposição 1.1.25 e pelo Teorema de Lagrange, m divide n. Se $g \in G$, então $g^m = 1$ e, assim, é raiz do polinômio $x^m - 1$. Esse polinômio tem, no máximo, m raízes no corpo $\mathbb{K}$. Entretanto, $x^m - 1$ tem, pelo menos, o número de elementos de G de raízes, ou seja, $n \leq m$. Então, $\exp G = |G|$. Portanto, pela Proposição 1.1.25, G é cíclico. ■

Corolário 1.1.27 *Se $\mathbb{K}$ é um corpo finito, então $\mathbb{K}^*$ é cíclico.*

Demonstração: Basta tomar $G = \mathbb{K}^*$ no Teorema anterior. ■

1.2 Espaços Vetoriais Quocientes

Definição 1.2.1 *Sejam V um espaço vetorial e U um subespaço de V. Se $v \in V$, então $v + U$ é o subconjunto de V definido por*

$$v + U = \{v + u;\ u \in U\}.$$

Observe que $v + U$ é subespaço se, e somente se, $v \in U$.

Exemplo 1.2.2 *Seja*

$$U = \{(x, y) \in \mathbb{R}^2;\ ax + by = 0\},$$

em que $a, b \in \mathbb{R}$ não são simultaneamente nulos. Geometricamente, U é uma reta em $\mathbb{R}^2$ que contém a origem.

Dado $v \in \mathbb{R}^2$, o conjunto

$$v + U = \{v + u;\ u \in U\}$$

é a reta que passa por v e é paralela a U.

Definição 1.2.3 *Para cada $v \in V$ e U subespaço de V, o conjunto $v + U$ é chamado* ***translação*** *de U.*

Quando U é um subespaço, $v + U$ é uma variedade afim paralela a U e passando por v.

Do ponto de vista da estrutura de grupos, considerando $(V, +)$ como um grupo abeliano e U um subgrupo, as translações $v + U$ são precisamente as classes laterais de U no grupo quociente $\frac{V}{U}$. Nesse contexto, $v + U$ representa a classe de equivalência do vetor v módulo U.

Exemplo 1.2.4 *Se U é a reta em $\mathbb{R}^2$ definida por $U = \{(x, 2x);\ x \in \mathbb{R}\}$, então todas as retas em $\mathbb{R}^2$ com inclinação 2 são translações de U.*

Mais geralmente, se U é uma reta em $\mathbb{R}^2$, então o conjunto de todas as translações de U é o conjunto de todas as retas em $\mathbb{R}^2$ que são paralelas a U.

Definição 1.2.5 *Seja U um subespaço de V. Então, o* ***espaço quociente*** *$\frac{V}{U}$ é o conjunto de todas as translações de U, ou seja,*

$$\frac{V}{U} = \{v + U; v \in V\}.$$

Exemplo 1.2.6 *Se $U = \{(x, y) \in \mathbb{R}^2;\ ax + by = 0\}$, então $\dfrac{\mathbb{R}^2}{U}$ é o conjunto de todas as retas em $\mathbb{R}^2$ paralelas a U.*

Exemplo 1.2.7 *Se U é um plano em $\mathbb{R}^3$ que contém a origem, então $\dfrac{\mathbb{R}^3}{U}$ é o conjunto de todos os planos em $\mathbb{R}^3$ paralelos a U.*

A etapa subsequente da nossa análise consiste em munir o conjunto $\dfrac{V}{U}$ de uma estrutura de espaço vetorial. Isso será realizado com base no resultado que será demonstrado a seguir.

O próximo resultado nos garantirá que duas translações de um subespaço são iguais ou disjuntas.

Proposição 1.2.8 *Suponha que U é um subespaço de V e $v, w \in V$. Então, são equivalentes:*

i) $v - w \in U$

ii) $v + U = w + U$

iii) $(v + U) \cap (w + U) \neq \emptyset$

Demonstração: Antes da demonstração, observamos que esse resultado depende apenas da estrutura de grupo abeliano de V, não sendo necessária a estrutura de espaço vetorial.

Primeiramente, vamos mostrar que $i) \Rightarrow ii)$. Suponha que $v - w \in U$. Se $u \in U$, então

$$v + u = w + ((v - w) + u) \in w + U.$$

Assim, $v + U \subseteq w + U$. De modo similar, $w + U \subseteq v + U$. Assim, $v + U = w + U$.

Agora, para provarmos que $ii) \Rightarrow iii)$, basta observar que a equação $v+U = w+U$ implica que $(v + U) \cap (w + U) \neq \emptyset$.

Por último, vejamos que $iii) \Rightarrow i)$. Suponha que $(v + U) \cap (w + U) \neq \emptyset$. Dessa forma, existem $u_1, u_2 \in U$ tais que

$$v + u_1 = w + u_2.$$

Logo,$v - w = u_2 - u_1$. Dessarte, $v - w \in U$, mostrando que $(v+U)\cap(w+U) \neq \emptyset$ implica $v - w \in U$, o que completa a demonstração. ■

Agora, podemos definir a adição e multiplicação por escalar em $\frac{V}{U}$.

Definição 1.2.9 *Seja U um subespaço de V. Então a **adição** e **multiplicação por escalar** são definidas em $\frac{V}{U}$, respectivamente, por*

$$(v + U) + (w + U) = (v + w) + U$$
$$\lambda(v + U) = (\lambda v) + U,$$

para todo $v, w \in V$ e $\lambda \in \mathbb{K}$.

Teorema 1.2.10 *Seja U um subespaço de V. Então $\frac{V}{U}$, com as operações de adição e multiplicação por escalar definidas anteriormente, é um espaço vetorial.*

Demonstração: Primeiramente, vejamos a boa definição das operações.

Como U é subespaço de V, U é, em particular, um subgrupo aditivo do grupo $(V, +)$. Assim, a boa definição da adição segue imediatamente.

Similarmente, seja $\lambda \in \mathbb{K}$. Ainda estamos supondo que $v_1 + U = v_2 + U$. Como U é um subespaço e, assim, é fechado para a multiplicação por escalar, temos $\lambda(v_1 - v_2) \in U$. Dessa forma, $\lambda v_1 - \lambda v_2 \in U$. Logo, novamente pela Proposição 1.2.8, temos

$$(\lambda v_1) + U = (\lambda v_2) + U.$$

Dessarte, a multiplicação por escalar em $\frac{V}{U}$ está bem-definida.

Por último, a verificação dos quatro axiomas de espaços vetoriais que dizem respeito à adição são imediatos, utilizando a ideia de grupo quociente. Verificaremos, então, que para todo $\lambda \in \mathbb{K}$ e para quaisquer $v + U,\ w + U \in \frac{V}{U}$, vale

$$\lambda[(v + U) + (w + U)] = \lambda(v + U) + \lambda(w + U).$$

De fato,

$$\begin{aligned}
\lambda[(v + U) + (w + U)] &= \lambda[(v + w) + U] \\
&= \lambda(v + w) + U \\
&= (\lambda v + \lambda w) + U \\
&= (\lambda v + U) + (\lambda w + U) \\
&= \lambda(v + U) + \lambda(w + U).
\end{aligned}$$

Os outros axiomas também são diretos. ■

1.3 Álgebras

Nesta seção, introduzimos formalmente o conceito de álgebra sobre um corpo $\mathbb{K}$, que constitui o objeto central de estudo na PI-Teoria.

Definição 1.3.1 *Seja A um espaço vetorial sobre um corpo $\mathbb{K}$. Definimos um par $(A, *)$ como sendo uma $\mathbb{K}$-**álgebra** (ou uma álgebra sobre $\mathbb{K}$) se $*$ é uma operação bilinear associativa em A, isto é, $* : A \times A \to A$, que satisfaz, para quaisquer $a, b, c \in A$ e $\lambda \in \mathbb{K}$:*

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

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

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

iv) $a * (b * c) = (a * b) * c$;

v) existe um elemento $1_A \in A$ *tal que*

$$1_A \cdot a = a \cdot 1_A = a, \ \forall \ a \in A.$$

A operação " $*$ *" é dita multiplicação de* A *e, por simplicidade de notação, escreveremos* $a * b = ab$*, para quaisquer* $a, b \in A$*.*

A ***dimensão*** *de uma* $\mathbb{K}$*-álgebra* A *é definida como a dimensão de* A *como espaço vetorial sobre* $\mathbb{K}$*, sendo denotada por* $\dim_{\mathbb{K}} A$ *ou* $\dim A$*. Dizemos que* A *é de dimensão finita quando* $\dim_{\mathbb{K}} A < \infty$*.*

Exemplo 1.3.2 *Fixado* $n \in \mathbb{N}$*, o espaço vetorial* $M_n(\mathbb{K})$ *das matrizes de ordem* $n \times n$ *com entradas em um corpo* $\mathbb{K}$ *é uma álgebra de dimensão* n^2*, considerando a multiplicação usual de matrizes. Além disso, a unidade é a matriz identidade* I_n*, cuja diagonal é composta inteiramente pelo elemento* 1 *e as demais entradas são nulas.*

Definição 1.3.3 *Seja* $e_{(i,j)}$ *a matriz em* $M_n(\mathbb{K})$ *tal que a* $(i, j)-$*ésima entrada é igual a* 1 *e as demais entradas são iguais a zero. Chamaremos essas matrizes de* ***matrizes elementares****. Observe que sempre que fizermos a multiplicação de duas matrizes elementares, teremos*

$$e_{(i,j)}e_{(k,l)} = \delta_{(j,k)}e_{(i,l)}, \ \textit{com} \ \delta_{(j,l)} = \begin{cases} 1, \ \textit{se} \ j = k \\ 0, \ \textit{se} \ j \neq k \end{cases} .$$

Ademais, uma base da álgebra $M_n(\mathbb{K})$ *é formada pelo conjunto de matrizes elementares* $e_{(i,j)}$*, com* $1 \leq i, j \leq n$*.*

Exemplo 1.3.4 *O espaço vetorial das matrizes triangulares superiores* $n \times n$ *com entradas em* $\mathbb{K}$*, munido da operação usual de multiplicação de matrizes, é uma álgebra, denotada por* $UT_n(\mathbb{K})$ *ou simplesmente* UT_n*. Assim,*

$$UT_n = \{(a_{ij}) \in M_n(\mathbb{K}); \ a_{ij} = 0 \ \textit{sempre que} \ i > j\}.$$

Essa notação advém da expressão em inglês "upper triangular", que significa justamente "triangular superior".

A álgebra UT_n terá um papel central nesta dissertação, sendo o foco principal dos estudos apresentados nos capítulos seguintes.

Exemplo 1.3.5 *Seja M um monóide, isto é, um conjunto munido de uma operação binária associativa que possui elemento neutro, e $\mathbb{K}[M]$ o espaço vetorial com base M. Consideremos, em $\mathbb{K}[M]$, a multiplicação que estende a operação do monóide, isto é, a multiplicação tal que $(m,n) \mapsto mn$, para quaisquer $m, n \in M$, em que mn é o produto de m e n como elementos de M. Essa álgebra é chamada álgebra de monóide de M, e sua unidade é o elemento neutro do monóide.*

Exemplo 1.3.6 *Seja $X = \{x_i;\ i \in I\}$ e seja $M\langle X\rangle$ o monóide que é o conjunto $\{x_{i_1}\cdots x_{i_n}; n \in \mathbb{N}, x_{i_k} \in X, k = 1,\ldots,n\}$, com a multiplicação sendo a justaposição de palavras, isto é, se $x_{i_1}\cdots x_{i_n}, x_{j_1}\cdots x_{j_m} \in M\langle X\rangle$, então*

$$(x_{i_1}\cdots x_{i_n})(x_{j_1}\cdots x_{j_m}) := x_{i_1}\cdots x_{i_n}x_{j_1}\cdots x_{j_m}.$$

O elemento neutro de $M\langle X\rangle$, denotado por 1, é a palavra vazia. A álgebra $\mathbb{K}\langle X\rangle$ é a álgebra de monóide de $M\langle X\rangle$, chamada álgebra livre. Os elementos de $\mathbb{K}\langle X\rangle$ são chamados polinômios.

Exemplo 1.3.7 *O espaço vetorial dos polinômios em uma indeterminada sobre um corpo $\mathbb{K}$, $\mathbb{K}[x]$, utilizando a multiplicação usual de polinômios, é uma álgebra, e sua unidade é o polinômio constante $f(x) = 1$.*

Exemplo 1.3.8 *A álgebra de Grassmann de dimensão infinita e enumerável G é tal que*

$$G = \langle 1, e_1, e_2, \ldots; e_ie_j + e_je_i = 0,\ e_i^2 = 0,\ \textit{para quaisquer } i,j \geq 1\rangle.$$

O conjunto $\beta = \{1, e_{i_1}\cdots e_{i_n},\ 1 \leq i_{i_1} < \cdots < i_k\}$ é uma base de G e $G = G_0 \oplus G_1$, em que

$$G_0 = \operatorname{span}\{e_{i_1}\cdots e_{i_{2k}};\ 1 \leq i_1 < \cdots < i_{2k},\ k \geq 0\}$$

e

$$G_1 = \operatorname{span}\{e_{i_1}\cdots e_{i_{2k+1}};\ 1 \leq i_1 < \cdots < i_{2k+1},\ k \geq 0\}.$$

Além disso, $G_iG_j \subseteq G_{i+j}$, em que a soma $i+j$ é feita módulo 2.

Definição 1.3.9 *Um subespaço S de uma álgebra A é chamado de **subálgebra** se é fechado para a multiplicação de A e se contém a unidade de A.*

Em geral, na literatura, não se exige que uma subálgebra contenha a unidade da álgebra ambiente. Nesta dissertação, adotaremos a convenção de que toda subálgebra contém a unidade.

Exemplo 1.3.10 *A álgebra UT_n é uma subálgebra de $M_n(\mathbb{K})$. De fato, UT_n é fechada para a multiplicação usual de matrizes e a unidade de $M_n(\mathbb{K})$ pertence a UT_n.*

Exemplo 1.3.11 *Seja A uma álgebra. Definimos o* ***centro*** *de A, denotado por $Z(A)$, como sendo*

$$Z(A) = \{x \in A; xa = ax, \forall a \in A\}.$$

É fácil ver que $Z(A)$ é uma subálgebra de A.

Definição 1.3.12 *Um subespaço I de A é chamado* ***ideal à esquerda*** *se $ab \in I$, para todos $a \in A$ e $b \in I$. Analogamente, quando, para quaisquer $a \in A$ e $b \in I$, obtivermos $ba \in I$, dizemos que I é um* ***ideal à direita****. Quando ocorrerem os dois casos simultaneamente, diremos que I é um* ***ideal bilateral*** *de A ou simplesmente* ***ideal*** *de A.*

Exemplo 1.3.13 *Seja UT_n a álgebra das matrizes triangulares superiores $n \times n$. Mostraremos que o conjunto*

$$I = \{a \in UT_n(\mathbb{K});\ a_{ij} = 0, se\ i = j\}$$

é um ideal de UT_n.

Primeiramente, vamos verificar que esse conjunto é um subespaço vetorial de UT_n e, logo após, um ideal.

i) Note que I é não vazio. Sejam, então, $a, b \in I$ tais que $a = (a_{ij})$ e $b = (b_{ij})$. Para $i = j$, $a_{ij} = 0$ e $b_{ij} = 0$. Logo, $a_{ij} + b_{ij} = 0$, para $i = j$. Assim, $a + b \in I$. Além disso, com $\lambda \in \mathbb{K}$, temos $\lambda a_{ij} = 0$, para $i = j$, pois $a_{ii} = 0$, então $\lambda a \in I$. Portanto, I é um subespaço vetorial de UT_n.

ii) Seja $a \in UT_n$ e $b \in I$. Mostraremos que $ab \in I$. Para tanto, façamos $ab = c = (c_{ij})$ tal que

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Para $i = j$, temos $c_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki}$. Além disso, quando $i > k$, então $a_{ik} = 0$. Logo, $a_{ik} b_{ki} = 0$. Caso $i \leq k$, então temos $b_{ki} = 0$. Assim, $a_{ik} b_{ki} = 0$. Dessa forma, $c_{ii} = 0$ e, assim, $ab \in I$. Portanto, I é um ideal à esquerda de UT_n.

Analogamente, verificamos que I é um ideal à direita.

Portanto, I é ideal de UT_n.

Proposição 1.3.14 *Sejam A uma álgebra e I um ideal de A. Como I é um subespaço vetorial, consideremos o espaço quociente $\frac{A}{I}$. Definamos a multiplicação $(\overline{a}, \overline{b}) \mapsto \overline{a}\overline{b} := \overline{ab}$ em $\frac{A}{I}$. Então essa multiplicação está bem definida e $\frac{A}{I}$, munida com essa multiplicação, é uma álgebra.*

Demonstração: Primeiramente, suponha que $\overline{a_1} = \overline{a_2}$ e $\overline{b_1} = \overline{b_2}$, com $\overline{a_1}, \overline{a_2}, \overline{b_1}, \overline{b_2} \in \frac{A}{I}$.

Como $\overline{a_1} = \overline{a_2}$, segue que $a_1 - a_2 \in I$ e, analogamente, $b_1 - b_2 \in I$. Assim,

$$(a_1 - a_2)b_1 \in I \ \text{ e } \ a_2(b_1 - b_2) \in I.$$

Logo,

$$(a_1 - a_2)b_1 + a_2(b_1 - b_2) = a_1b_1 - a_2b_2 \in I.$$

Isso significa que $\overline{a_1b_1} = \overline{a_2b_2}$ e, assim, a multiplicação está bem definida.

Além disso, a multiplicação é distributiva em relação à adição. De fato, dados $\overline{a}, \overline{b}, \overline{c} \in \frac{A}{I}$, temos

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a(b + c)} = \overline{ab + ac} = \overline{a}\overline{b} + \overline{ac}$$

e, analogamente, $(\overline{b} + \overline{c})\overline{a} = \overline{b}\overline{a} + \overline{c}\,\overline{a}$.

Por fim, dado $\lambda \in \mathbb{K}$, temos

$$\lambda\overline{a}\overline{b} = \overline{\lambda(ab)} = \overline{(\lambda a)b} = \overline{\lambda ab} = (\lambda\overline{a})\overline{b}.$$

Analogamente, $\lambda\overline{a}\overline{b} = \overline{a}(\lambda\overline{b})$.

Portanto, concluímos o resultado. ■

Definição 1.3.15 *Sejam A uma álgebra e I um ideal próprio de A. Então I é um **ideal maximal à esquerda** de A se $I \neq A$ e não existe um ideal J à esquerda de A próprio tal que I esteja contido propriamente em J, ou seja, se $I \subset J \subset A$, então ou $J = A$ ou $J = I$.*

Exemplo 1.3.16 *Seja $M_2(\mathbb{K})$ a álgebra de matrizes 2×2. O ideal à esquerda*

$$I = \{a \in M_2(\mathbb{K}); a_{ij} = 0, se\ j > 1\}$$

de $M_2(\mathbb{K})$ é um ideal maximal à esquerda de $M_2(\mathbb{K})$.

De fato, seja J um ideal à esquerda de $M_2(\mathbb{K})$ tal que $I \subsetneq J$. Consideremos $a = \begin{bmatrix} 0 & a_{12} \\ 0 & a_{22} \end{bmatrix} \in J - I$, com $a_{12} \neq 0$ ou $a_{22} \neq 0$. Note que a é uma matriz não nula. Sendo $a_{12} \neq 0$,

$$e_{(1,1)}a = \begin{bmatrix} 0 & a_{12} \\ 0 & 0 \end{bmatrix} \Longrightarrow \frac{1}{a_{12}} e_{(1,1)}a = e_{(1,2)} \in J.$$

Assim, como $e_{(2,1)} \in I$, $I \subseteq J$, então

$$(e_{(2,1)} + e_{(1,2)})^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in J.$$

Dessa forma, $J = M_2(\mathbb{K})$, o que é um absurdo.

Analogamente, sendo $a_{22} \neq 0$,

$$e_{(2,2)}a = \begin{bmatrix} 0 & 0 \\ 0 & a_{22} \end{bmatrix} \Longrightarrow \frac{1}{a_{22}} e_{(2,2)}a = e_{(2,2)} \in J.$$

Como $e_{(1,1)} \in I$, $I \subseteq J$, *então*

$$e_{(1,1)} + e_{(2,2)} \in J.$$

Novamente, $J = M_2(\mathbb{K})$, *o que é um absurdo.*
Portanto, I *é um ideal maximal à esquerda de* $M_2(\mathbb{K})$.

Para garantir a existência de ideais maximais, utilizaremos uma ferramenta clássica da Teoria dos Conjuntos, a saber, o Lema de Zorn.

Lema 1.3.17 (Lema de Zorn) *Seja* S *um conjunto não vazio parcialmente ordenado. Se toda cadeia em* S *tem uma cota superior em* S, *então* S *tem pelo menos um elemento maximal.*

Teorema 1.3.18 *Seja* A *uma álgebra. Então* A *tem pelo menos um ideal maximal à esquerda.*

Demonstração: Seja Γ o conjunto de todos os ideais à esquerda diferentes de A. Ordenemos Γ pela inclusão de conjuntos. Note que Γ é diferente do vazio, pois $0 \in \Gamma$.

Para aplicar o Lema de Zorn. devemos mostrar que toda cadeia em Γ tem uma cota superior em Γ. Seja, então, (I_α) uma cadeia de ideais em Γ. Dessa forma, para cada par de índices α, β, temos $I_\alpha \subseteq I_\beta$ ou $I_\beta \subseteq I_\alpha$.

Seja $I = \bigcup_\alpha I_\alpha$. Então I é um ideal à esquerda de A e $1 \notin I$, já que $1 \notin I_\alpha$, para todo α. Logo, $I \in \Gamma$ e I é uma cota superior da cadeia. Assim, pelo Lema de Zorn, Γ tem um elemento maximal e, portanto, A tem um ideal maximal à esquerda. ■

Na demonstração acima utilizamos de maneira essencial o fato de que A possui unidade. Sem essa hipótese, o resultado pode não valer e existem contraexemplos.

Definição 1.3.19 *Definimos o* ***radical de Jacobson*** *de uma álgebra* A, $J(A)$, *como a interseção de todos os ideais maximais à esquerda de* A.

Lema 1.3.20 *Seja* A *uma álgebra. Se* $y \in A$, *então as seguintes afirmações são equivalentes:*

i) $y \in J(A)$;

ii) $1 - xy$ *é invertível à esquerda, isto é, existe* $z \in A$ *tal que* $z(1 - xy) = 1$, *para todo* $x \in A$.

Demonstração: $(i) \Rightarrow (ii)$: Suponhamos que $y \in J(A)$. Se para algum x, o elemento $1 - xy$ não for invertível à esquerda, então $A(1 - xy) \subsetneq A$ é um ideal à esquerda de A. Logo, está contido em algum ideal maximal J à esquerda de A. Mas $1 - xy \in J$ e, como $y \in J(A)$, então $y \in J$. Logo, $xy \in J$. Assim, como J é um subespaço vetorial, temos

$$1 - xy + xy = 1 \in J,$$

o que é uma contradição.

$(ii) \Rightarrow (i)$: Seja M um ideal maximal à esquerda de A. Para provar que $y \in J(A)$, basta mostrar que $y \in M$.

Suponha, por contradição, que $y \notin M$. Então, o ideal à esquerda gerado por M e y, $M + Ay$, é todo o A, ou seja, $M + Ay = A$. Assim, existem $m \in M$ e $a \in A$ tais que

$$m + ay = 1 \Rightarrow 1 - ay = m \in M.$$

Desse modo, por (ii), para $x = a$, segue que $1 - ay$ é invertível à esquerda. Assim, existe $b \in A$ tal que

$$b(1 - ay) = 1.$$

Como $1 - ay \in M$ e M é ideal à esquerda, $b(1 - ay) \in M$. Logo, $1 \in M$, o que é um absurdo. Assim, $y \in M$ e, portanto, $y \in J(A)$. ■

Exemplo 1.3.21 *O radical de Jacobson de UT_n é o conjunto das matrizes estritamente triangulares superiores de UT_n, ou seja,*

$$J(UT_n) = \{a \in UT_n;\ a \text{ tem diagonal nula}\}.$$

De fato, sejam $I = \{b \in UT_n;\ b \text{ tem a diagonal nula}\}$, $b \in I$ e $a \in UT_n$. Do Exemplo 1.3.13, temos que ab tem a diagonal nula. Assim, $det(Id - ab) = 1$. Desse modo, $Id - ab$ é uma matriz invertível para qualquer matriz $a \in UT_n$. Logo, pelo Lema 1.3.20, $b \in J(UT_n)$. Logo, $I \subset J(UT_n)$.

Agora, suponha que $J(UT_n) \not\subseteq I$ e $c \in J(UT_n)$, mas $c \notin I$. Então, para algum $i \in \{1, \ldots, n\}$, temos $c_{ii} \neq 0$. Seja b a matriz diagonal tal que as entradas não nulas são os elementos c_{ii}^{-1}, sempre que $c_{ii} \neq 0$. Assim, $det(Id - ab) = 0$. Logo, $Id - ab$ não será invertível à esquerda, o que contraria o Lema 1.3.20. Portanto, $J(UT_n) \subset I$ e concluímos que $J(UT_n) = I$.

Definição 1.3.22 *Sejam A uma álgebra e I um ideal de A. Dizemos que I é um **ideal nilpotente** se existe n natural tal que $a_1 \cdots a_n = 0_A$, para quaisquer $a_1, \ldots, a_n \in I$. Diremos que n é o **índice de nilpotência** de I quando n é o menor natural que satisfaz isso. Utilizamos a notação $I^n = 0$ para indicar que o produto de quaisquer n elementos de I é zero.*

1.4 Graduações

Nesta seção introduzimos o conceito de graduação por um grupo em uma álgebra, ferramenta fundamental para o desenvolvimento dos resultados posteriores.

Definição 1.4.1 *Sejam G um grupo e A uma álgebra. Uma $G-$graduação da álgebra A é uma decomposição do espaço vetorial A, dada por uma coleção de subespaços $\{A_g\}_{g\in G}$ de A*

$$A = \bigoplus_{g\in G} A_g$$

tal que, para quaisquer $g, h \in G$, temos $A_g A_h \subseteq A_{gh}$. Nesse caso, dizemos que A é $G-$graduada.

Observação 1.4.2 *Destacamos que:*

i) A partir da definição, todo $a \in A$ pode ser escrito unicamente como uma soma finita

$$a = \sum_{g\in G} a_g, \text{ com } a_g \in A_g.$$

ii) Os subespaços A_g são chamados de componentes homogêneas de A e diremos que o elemento a é homogêneo se $a \in A_g$. Quando a for diferente do elemento nulo de A, existe um único $g \in G$ tal que $a \in A_g$, pois a soma da graduação é direta. Assim, podemos definir o conceito de grau como $\deg(a) = g$, se $a \in A_g$.

Definição 1.4.3 *Dizemos que*

i) Uma subálgebra $B \subseteq A$ é $G-$graduada (ou homogênea) se $B = \bigoplus_{g\in G}(B \cap A_g)$.

ii) Um ideal I de A é $G-$graduado se $I = \bigoplus_{g\in G}(I \cap A_g)$. Em outras palavras, I é graduado se, para qualquer $a \in I$, $a = \sum_{g\in G} a_g$, temos $a_g \in I$, para todo $g \in G$.

Exemplo 1.4.4 *Uma álgebra A pode ser graduada por um grupo arbitrário G com as componentes $A_e = A$ e $A_g = 0$, se $g \neq e$. Essa graduação é chamada graduação trivial.*

Proposição 1.4.5 *Se A é uma álgebra $G-$graduada e H é um subgrupo de G, então $A' = \bigoplus_{h\in H} A_h$ é uma subálgebra graduada de A.*

Definição 1.4.6 *Dado $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in G^n$, escrevemos*

$$UT_n = \bigoplus_{g\in G} (UT_n)_g, \tag{1.1}$$

em que $(UT_n)_g = \text{span}\{e_{(i,j)};\ \varepsilon_i^{-1}\varepsilon_j = g\}$. Então UT_n é uma álgebra $G-$graduada, e dizemos que (1.1) é uma $G-$graduação elementar em UT_n.

Nessa graduação, cada matriz elementar $e_{(i,j)}$ é homogênea, com grau dado por $\deg(e_{(i,j)}) = \varepsilon_i^{-1}\varepsilon_j$.

Exemplo 1.4.7 *Seja* $G = \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$. *Considere a sequência* $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon_3) = (\bar{0}, \bar{1}, \bar{0}) \in G^3$. *Vamos definir a* $G-$*graduação elementar de* UT_3. *Para tanto, sabemos que cada entrada* $e_{(i,j)}$, *com* $i \leq j$, *receberá um grau dado por*

$$\deg(e_{(i,j)}) = -\varepsilon_i + \varepsilon_j \text{ (em } \mathbb{Z}_2).$$

Assim,

$$\begin{aligned}
\deg(e_{(1,1)}) &= \bar{0} - \bar{0} = \bar{0} \\
\deg(e_{(1,2)}) &= \bar{1} - \bar{0} = \bar{1} \\
\deg(e_{(1,3)}) &= \bar{0} - \bar{0} = \bar{0} \\
\deg(e_{(2,2)}) &= \bar{1} - \bar{1} = \bar{0} \\
\deg(e_{(2,3)}) &= \bar{1} - \bar{0} = \bar{1} \\
\deg(e_{(3,3)}) &= \bar{0} - \bar{0} = \bar{0}.
\end{aligned}$$

Com isso, a álgebra UT_3 *se decompõe como:*

$$UT_3 = (UT_3)^{\bar{0}} \oplus (UT_3)^{\bar{1}},$$

em que

$$\begin{aligned}
(UT_3)^{\bar{0}} &= \text{span}\{e_{(1,1)}, e_{(1,3)}, e_{(2,2)}, e_{(3,3)}\} \\
(UT_3)^{\bar{1}} &= \text{span}\{e_{(1,2)}, e_{(2,3)}\}.
\end{aligned}$$

Definição 1.4.8 *Sejam* A *e* B *álgebras. Uma transformação linear* $f : A \longrightarrow B$ *é dita um* ***homomorfismo de álgebras*** *se* $f(a_1a_2) = f(a_1)f(a_2)$, *para quaisquer* $a_1, a_2 \in A$, *e* $f(1) = 1$.

Observação 1.4.9 *De maneira totalmente análoga às definições de grupos e anéis, temos:*

i) Um homomorfismo injetor é chamado ***monomorfismo****;*

ii) Um homomorfismo sobrejetor é chamado ***epimorfismo****;*

iii) Um homomorfismo bijetor é chamado ***isomorfismo****;*

iv) Um homomorfismo de A *em* A *é chamado* ***endomorfismo****;*

v) Um homomorfismo de A *em* A *bijetor é chamado* ***automorfismo****.*

Exemplo 1.4.10 *Sejam* A *uma álgebra e* I *um ideal de* A. *A aplicação*

$$\begin{aligned}
\varphi : A &\longrightarrow \frac{A}{I} \\
a &\longmapsto a + I
\end{aligned}$$

é um epimorfismo de álgebras, chamado projeção canônica.

De fato, veja que, dados $a, b \in A$, *temos:*

$$\varphi(ab) = (ab) + I = (a + I)(b + I) = \varphi(a)\varphi(b).$$

Além disso, como $1_A + I$ *é a unidade de* $\frac{A}{I}$ *e*

$$\varphi(1_A) = 1_A + I.$$

Dessa forma, φ *é um homomorfismo de álgebras.*

Veja, ainda, que, dado $b + I \in \frac{A}{I}$, *então* $b + I = \varphi(b)$, *em que* $b \in A$. *Assim, concluímos que* φ *é um epimorfismo de álgebras.*

Definição 1.4.11 *Sejam* A *e* B *álgebras e* $\varphi : A \longrightarrow B$ *um homomorfismo de álgebras. Dizemos que o conjunto* $\ker(\varphi) = \{a \in A; \varphi(a) = 0_B\}$ *é o núcleo do homomorfismo* φ *e que* $\mathrm{Im}(\varphi) = \{\varphi(a) \in B; a \in A\}$ *é a imagem de* φ.

Verifica-se que $\ker(\varphi)$ é um ideal de A e que $\mathrm{Im}(\varphi)$ é uma subálgebra de B.

Exemplo 1.4.12 *Sendo* φ *o homomorfismo*

$$\begin{aligned} \varphi : A &\longrightarrow \frac{A}{I} \\ a &\longmapsto a + I \ , \end{aligned}$$

temos $\ker(\varphi) = I$.

Definição 1.4.13 *Sejam* $A = \bigoplus_{g \in G} A_g$ *e* $B = \bigoplus_{g \in G} B_g$ *álgebras* $G-$*graduadas. Dizemos que uma aplicação* $f : A \longrightarrow B$ *é um homomorfismo de álgebras* $G-$*graduadas se* f *for um homomorfismo de álgebras tal que* $f(A_g) \subseteq B_g$.

Exemplo 1.4.14 *Se* B *é uma subálgebra* $G-$*graduada de* A, *então a inclusão* $i : B \hookrightarrow A$ *é um homomorfismo de álgebras graduadas.*

Exemplo 1.4.15 *Vamos mostrar que*

$$R_l = \mathrm{span}\{e_{(i,j)}; 1 \leq i \leq j \leq n, i \neq l \ e \ j \neq l\}$$

e

$$UT_{n-1} = \mathrm{span}\{e_{(i,j)}; 1 \leq i \leq j \leq n-1\}$$

são isomorfas como álgebras graduadas.

Consideramos em UT_n *a graduação elementar determinada pela* n*-upla* $(g_1, \ldots, g_n) \in G^n$, *isto é, aquela para a qual*

$$\deg(e_{(i,j)}) = g_i g_j^{-1}.$$

Em R_l, consideramos a graduação induzida por essa graduação de UT_n e, em UT_{n-1}, a graduação elementar induzida pela $(n-1)-$upla $(g_1, \ldots, g_{l-1}, g_{l+1}, \ldots, g_n)$.

A priori, note que R_l é uma subálgebra graduada de UT_n. De fato, cada gerador $e_{(i,j)}$ de R_l é um elemento homogêneo na graduação UT_n, R_l é fechada para as operações da álgebra e contém a unidade de UT_n.

Além disso, sabemos que $\dim UT_n = \frac{n(n+1)}{2}$. *Além disso, para sabermos a dimensão de R_l, devemos retirar os $e_{(i,j)}$ de UT_n cujos índices envolvem l, ou seja,*

$$\dim(R_l) = \frac{n(n+1)}{2} - n = \frac{(n-1)n}{2} = \dim(UT_{n-1}).$$

Agora, defina $\varphi : R_l \longrightarrow UT_{n-1}$ como a única transformação linear tal que

$$\varphi(e_{(i,j)}) = e_{(\tilde{i},\tilde{j})}$$

em que

$$\tilde{i} = \begin{cases} i, & se\ i < l \\ i-1, & se\ i > l \end{cases}, \quad \tilde{j} = \begin{cases} j, & se\ j < l \\ j-1, & se\ j > l \end{cases}.$$

Note que,

$$\varphi(e_{(i,j)}e_{(j,k)}) = \varphi(e_{(i,k)}) = e_{(\tilde{i},\tilde{k})}$$

e

$$\varphi(e_{(i,j)})\varphi(e_{(j,k)}) = e_{(\tilde{i},\tilde{j})} \cdot e_{(\tilde{j},\tilde{k})} = e_{(\tilde{i},\tilde{k})},$$

ou seja, essa aplicação também é compatível com o produto e, dessa forma, é um homomorfismo de álgebras.

Além disso, como essa transformação linear leva base em base, segue que φ é bijetiva. Logo, $R_l \simeq UT_{n-1}$.

Por fim, para verificar que φ é um isomorfismo de álgebras $G-$graduadas, precisamos mostrar que φ preserva a graduação. Seja $e_{(i,j)} \in R_l$ um elemento homogêneo da base. Assim,

$$\deg(\varphi(e_{(i,j)})) = \deg(e_{(\tilde{i},\tilde{j})}) = \deg(e_{(i,j)}).$$

Uma vez que φ é linear e leva base em base, segue que φ preserva o grau de todos os elementos homogêneos.

Portanto, φ é um isomorfismo de $G-$álgebras graduadas.

Proposição 1.4.16 *Se $f : A \to B$ é um homomorfismo de álgebras, então $F : M_n(A) \to M_n(B)$, dado por $F\Big((a_{ij})\Big) = \Big(f(a_{ij})\Big)$, é um homomorfismo de álgebras.*

Demonstração: Sejam $(a_{ij}), (b_{ij}) \in M_n(A)$ e $\lambda \in \mathbb{K}$. Temos:

$$\begin{aligned}(i)\ F\Big((a_{ij}) + (b_{ij})\Big) &= F\Big((a_{ij} + b_{ij})\Big) \\ &= \Big(f(a_{ij} + b_{ij})\Big) \\ &= \Big(f(a_{ij}) + f(b_{ij})\Big) \\ &= \Big(f(a_{ij})\Big) + \Big(f(b_{ij})\Big) \\ &= F\Big((a_{ij})\Big) + F\Big((b_{ij})\Big).\end{aligned}$$

$$\begin{aligned}(ii)\ F\Big(\lambda(a_{ij})\Big) &= F\Big((\lambda a_{ij})\Big) \\ &= \Big(f(\lambda a_{ij})\Big) \\ &= \Big(\lambda f(a_{ij})\Big) \\ &= \lambda\Big(f(a_{ij})\Big) \\ &= \lambda F\Big((a_{ij})\Big).\end{aligned}$$

$$(iii)\ F\left(\begin{pmatrix} 1_A & 0 & \cdots & 0 \\ 0 & 1_A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1_A \end{pmatrix}\right) = \begin{pmatrix} f(1_A) & 0 & \cdots & 0 \\ 0 & f(1_A) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f(1_A) \end{pmatrix} = \begin{pmatrix} 1_B & 0 & \cdots & 0 \\ 0 & 1_B & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1_B \end{pmatrix}.$$

$$\begin{aligned}(iv)\ F\Big((a_{ij})(b_{ij})\Big) &= F\Big(\Big(\sum_{k=1}^{n} a_{ik}b_{kj}\Big)_{i,j}\Big) \\ &= \Big(f\Big(\sum_{k=1}^{n} a_{ik}b_{kj}\Big)\Big)_{i,j} \\ &= \Big(\sum_{k=1}^{n} f(a_{ik})f(b_{kj})\Big)_{i,j} \\ &= (f(a_{ij}))_{i,j}(f(b_{ij}))_{i,j} \\ &= F((a_{ij}))F((b_{ij})).\end{aligned}$$

Dessa forma, temos o resultado. ■

Em particular, o resultado anterior também é válido para UT_n, e a sua verificação é análoga.

Lema 1.4.17 *Sejam $A = \bigoplus_{g\in GA_g}$ e $B = \bigoplus_{g\in G} B_g$ $\mathbb{K}-$álgebras graduadas por um grupo G. Se $\varphi : A \longrightarrow B$ é um homomorfismo de álgebras $G-$graduadas, então* $\ker(\varphi)$ *é um ideal graduado de A.*

Demonstração: Dado $x = x_{g_1} + \cdots + x_{g_n} \in \ker(\varphi)$, com $x_{g_i} \in A_{g_i}$, então

$$0 = \varphi(x) = \varphi(x_{g_1} + \cdots + x_{g_n}) = \varphi(x_{g_1}) + \cdots + \varphi(x_{g_n}),$$

com $\varphi(x_{g_i}) \in B_{g_i}$. Como cada $\varphi(x_{g_i})$ está em um subespaço diferente B_g e a soma é direta, segue que

$$\varphi(x_{g_i}) = 0, \forall i.$$

De onde, $x_{g_i} \in \ker(\varphi)$, para todo i e, portanto, $\ker(\varphi)$ é um ideal graduado. ■

Lema 1.4.18 *Sejam $A = \bigoplus_{g\in GA_g}$ e $B = \bigoplus_{g\in G} B_g$ $\mathbb{K}-$álgebras graduadas por um grupo G. Se $\varphi : A \longrightarrow B$ é um homomorfismo de álgebras $G-$graduadas, então* $\mathrm{Im}(\varphi)$ *é uma subálgebra graduada de B.*

Demonstração: Análoga à anterior.

Recordamos que o Teorema Fundamental dos Homomorfismos é um resultado clássico e amplamente conhecido no estudo de Álgebra. A seguir, apresentaremos uma versão graduada desse teorema, adequada ao contexto de álgebras graduadas por um grupo G.

Teorema 1.4.19 (Teorema Fundamental dos Homomorfismos Graduados) *Sejam $A = \bigoplus_{g\in G} A_g$ e $B = \bigoplus_{g\in G} B_g$ álgebras graduadas por um grupo G sobre um corpo $\mathbb{K}$. Seja $\varphi : A \longrightarrow B$ um homomorfismo de $\mathbb{K}-$álgebras compatível com a graduação. Então existe um isomorfismo*

$$\frac{A}{\ker(\varphi)} \simeq \mathrm{Im}(\varphi)$$

e o quociente herda a graduação, ou seja, para cada $g \in G$, $\left(\frac{A}{\ker(\varphi)}\right)_g = \frac{A_g + \ker(\varphi)}{\ker(\varphi)}$.

Demonstração: Como φ é homomorfismo de álgebras, já sabemos que $\ker(\varphi)$ é um ideal graduado de A e também verifica-se que $\mathrm{Im}(\varphi)$ é subálgebra graduada de B.

Defina

$$\begin{aligned} \psi : \ \frac{A}{\ker(\varphi)} &\longrightarrow \mathrm{Im}(\varphi) \\ a + \ker(\varphi) &\longmapsto \varphi(a) \ . \end{aligned}$$

Primeiramente, note que, se $a+\ker(\varphi) = a'+\ker(\varphi)$, então $a-a' \in \ker(\varphi)$. Logo, $\varphi(a-a') = 0$, ou seja, $\varphi(a) = \varphi(a')$. Logo, ψ está bem-definida.

Além disso, verifica-se facilmente que ψ é um homomorfismo de álgebras.

Agora, veja que, como $\ker(\varphi)$ é um ideal graduado, o quociente $\dfrac{A}{\ker(\varphi)}$ herda a graduação, ou seja, para cada $g \in G$,

$$\Big(\frac{A}{\ker(\varphi)}\Big)_g = \frac{A_g + \ker(\varphi)}{\ker(\varphi)}.$$

Desse modo, ψ satisfaz

$$\psi(a_g + \ker(\varphi)) = \varphi(a_g) \in B_g, \text{ para todo } a_g \in A_g.$$

Observe, também, que ψ é sobrejetora. De fato, dado $y \in \mathrm{Im}(\varphi)$, existe $a \in A$ tal que $y = \varphi(a)$. Tomando $x = a + \ker(\varphi) \in \frac{A}{\ker(\varphi)}$, temos

$$\psi(x) = \psi(a + \ker(\varphi)) = \varphi(a) = y.$$

Ademais, ψ é injetora. Com efeito,

$$\begin{aligned}
\ker(\psi) &= \{a + \ker(\varphi) \in \frac{A}{\ker(\varphi)}; \psi(a + \ker(\varphi)) = 0\} \\
&= \{a + \ker(\varphi) \in \frac{A}{\ker(\varphi)}; \varphi(a) = 0\} \\
&= \{a + \ker(\varphi) \in \frac{A}{\ker(\varphi)}; a \in \ker(\varphi)\} \\
&= \bar{0},
\end{aligned}$$

como queríamos demonstrar.

Portanto, ψ é um isomorfismo de álgebras graduadas. ■

Exemplo 1.4.20 *Seja $\mathbb{K}$ um corpo e considere a álgebra das matrizes triangulares superiores*

$$UT_2(\mathbb{K}) = \left\{ \begin{bmatrix} a & c \\ 0 & b \end{bmatrix} : a, b, c \in \mathbb{K} \right\}.$$

Graduamos $UT_2(\mathbb{K})$ pelo grupo $\mathbb{Z}_2$ definindo

$$A_0 = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a, b \in \mathbb{K} \right\} \quad e \quad A_1 = \left\{ \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix} : c \in \mathbb{K} \right\},$$

de modo que $UT_2(\mathbb{K}) = A_0 \oplus A_1$.

Definimos o homomorfismo de $\mathbb{K}-$álgebras

$$\varphi : UT_2(K) \longrightarrow \mathbb{K},$$
$$\begin{bmatrix} a & c \\ 0 & b \end{bmatrix} \longmapsto a.$$

Note que φ é compatível com a graduação, pois $\varphi(A_0) = \mathbb{K}$ e $\varphi(A_1) = \{0\}$. Assim, $\varphi(A_g) \subseteq B_g$ para todo $g \in \mathbb{Z}_2$, em que $B_0 = \mathbb{K}$ e $B_1 = \{0\}$.

Pelo Teorema do Homomorfismo para Álgebras Graduadas, temos um isomorfismo de álgebras graduadas

$$\frac{UT_2(\mathbb{K})}{\ker(\varphi)} \cong \mathrm{Im}(\varphi) = \mathbb{K}.$$

De fato,

$$\ker(\varphi) = \left\{ \begin{bmatrix} 0 & c \\ 0 & b \end{bmatrix} : b, c \in \mathbb{K} \right\},$$

e o quociente $\dfrac{UT_2(\mathbb{K})}{\ker(\varphi)}$ é isomorfo ao corpo $\mathbb{K}$, identificado com os elementos da posição $(1,1)$.

1.5 Identidades Polinomiais

Introduziremos, agora, o conceito de identidade polinomial, que será central ao longo deste trabalho.

Para formalizar a noção de substituição de elementos de uma álgebra em polinômios não comutativos, utilizamos a álgebra livre e sua propriedade universal. Essa abordagem permite definir de maneira precisa quando um polinômio se anula sob todas as avaliações em uma álgebra dada, conduzindo ao conceito de PI-álgebra.

Teorema 1.5.1 (Propriedade Universal da Álgebra Livre) *Seja $X = \{x_i;\ i \in I\}$ um conjunto não vazio e $\mathbb{K}\langle X\rangle$ a álgebra livre. Se A é uma álgebra, então qualquer aplicação $X \longrightarrow A$ pode ser estendida a um único homomorfismo $\mathbb{K}\langle X\rangle \longrightarrow A$.*

Demonstração: Seja $X \longrightarrow A$ uma aplicação e $a_i \in A$ a imagem de x_i por essa aplicação. Para cada monômio $x_{i_1} \cdots x_{i_n}$, consideremos o produto $a_{i_1} \cdots a_{i_n}$ em A. Existe uma única transformação linear $f : \mathbb{K}\langle X\rangle \longrightarrow A$ tal que $f(x_{i_1} \cdots x_{i_n}) = a_{i_1} \cdots a_{i_n}$. Dados dois monômios $x_{i_1} \cdots x_{i_n},\ x_{j_1} \cdots x_{j_m}$, temos

$$f((x_{i_1} \cdots x_{i_n})(x_{j_1} \cdots x_{j_m})) = a_{i_1} \cdots a_{i_n} a_{j_1} \cdots a_{j_m} = f(x_{i_1} \cdots x_{i_n}) f(x_{j_1} \cdots x_{j_m}).$$

Assim, segue que f é um homomorfismo de álgebras.

Seja $g : \mathbb{K}\langle X\rangle \longrightarrow A$ um homomorfismo de álgebras que estende $X \longrightarrow A$. Então $g(x_i) = f(x_i)$, para todo $i \in I$. Dessa forma, $g(x_{i_1} \cdots x_{i_n}) = f(x_{i_1} \cdots x_{i_n})$, para todo monômio $x_{i_1} \cdots x_{i_n}$. Portanto, $g = f$. ■

Seja $x_i \mapsto a_i$ uma aplicação de X em A. A imagem $f(x_{i_1}, \ldots, x_{i_n}) \in \mathbb{K}\langle X\rangle$ pelo homomorfismo que estende a aplicação é denotada por $f(a_{i_1}, \ldots, a_{i_n})$.

Observação 1.5.2 *Dado $f \in \mathbb{K}\langle X\rangle$, temos $f(x_1, \ldots, x_n) = \alpha_1 w_1 + \cdots + \alpha_m w_m$, em que $\alpha_i \in \mathbb{K}$ e $w_i = x_{i_1} \cdots x_{i_l}$. Assim, ao considerarmos ϕ um homomorfismo de $\mathbb{K}\langle X\rangle \longrightarrow A$, obtemos*

$$\begin{aligned}\phi(f(x_1, \ldots, x_n)) &= \phi(\alpha_1 x_{11} \cdots x_{1l_1} + \cdots + \alpha_m x_{m1} \cdots x_{ml_2}) \\ &= \alpha_1 \phi(x_{11}) \cdots \phi(x_{1l_1}) + \cdots + \alpha_m \phi(x_{m1}) \cdots \phi(x_{ml_2}) \\ &= f(\phi(x_1), \ldots, \phi(x_n)).\end{aligned}$$

Dessa forma,

$$\phi(f(x_1, \ldots, x_n)) = f(\phi(x_1), \ldots, \phi(x_n)).$$

Definição 1.5.3 *Seja $f = f(x_1, \cdots, x_n) \in \mathbb{K}\langle X\rangle$ e seja A uma álgebra. Dizemos que f é uma **identidade polinomial** para A se $f(a_1, \ldots, a_n) = 0$, para quaisquer $a_1, \ldots, a_n \in A$. Denotaremos por $T(A)$ o conjunto das identidades polinomiais de A.*

Se existe um polinômio não nulo que é uma identidade para A, diremos que A é uma PI-álgebra, da expressão em inglês "polynomial identity".

Definiremos os comutadores normados à esquerda como sendo:

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

e

$$[x_1, \cdots, x_n] = [[x_1, \cdots, x_{n-1}], x_n],\ n \geq 3.$$

Exemplo 1.5.4 *A álgebra A é comutativa se, e somente se, $[x, y]$ é uma identidade polinomial para A.*

Exemplo 1.5.5 *A álgebra $\mathbb{K}\langle X\rangle$ não é uma PI-álgebra.*

Com efeito, suponha, por absurdo, que $f(x_1, \ldots, x_n)$ seja uma identidade não nula de $\mathbb{K}\langle X\rangle$. Então, dados quaisquer $f_1, \ldots, f_n$ elementos de $\mathbb{K}\langle X\rangle$, devemos obter

$$f(f_1, \ldots, f_n) = 0.$$

Em particular, podemos escolher $f_1 = x_1, \ldots, f_n = x_n$. Logo, teremos

$$f(x_1, \ldots, x_n) = 0,$$

ou seja, f seria igual ao polinômio nulo, o que contraria a hipótese.

Exemplo 1.5.6 *A álgebra UT_n satisfaz a identidade*

$$[x_1, x_2] \cdots [x_{2n-1}, x_{2n}] \equiv 0.$$

Primeiramente, analisaremos o comutador de forma geral. Seja $[x_l, x_r] = x_l x_r - x_r x_l$. Mostraremos que, sendo a_l e a_r matrizes triangulares superiores, teremos que a diagonal principal de $a_l a_r$ é igual a diagonal principal de $a_r a_l$.

De fato, sejam $a_l = (a_{ij})$, $a_r = (b_{ij})$, $a_l a_r = (c_{ij})$ e $a_r a_l = (d_{ij})$. Para a diagonal principal de $a_l a_r$, temos

$$c_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki}, \ com \begin{cases} a_{ik} = 0, \ se \ i > k \\ b_{ik} = 0, \ se \ k > i \end{cases},$$

ou seja, para $i > k$, temos que $a_{ik} b_{ki} = 0$ e, para $k > i$, temos $a_{ik} b_{ki} = 0$. Assim,

$$c_{ii} = \sum_{k=1}^{n} a_{ik} b_{ki} = a_{ii} b_{ii}.$$

Para a diagonal principal de $a_r a_l$, temos

$$d_{ii} = \sum_{k=1}^{n} b_{ik} a_{ki}, \ com \begin{cases} b_{ik} = 0, \ se \ i > k \\ a_{ki} = 0, \ se \ k > i \end{cases},$$

ou seja, para $i > k$, temos $b_{ik} a_{ki} = 0$ e,para $k > i$, temos $b_{ik} a_{ki} = 0$. Logo,

$$d_{ii} = \sum_{k=1}^{n} b_{ik} a_{ki} = b_{ii} a_{ii}.$$

Como b_{ii} e a_{ii} são elementos de $\mathbb{K}$, então $b_{ii} a_{ii} = a_{ii} b_{ii}$. Dessa forma, as matrizes $a_l a_r$ e $a_r a_l$ têm as mesmas diagonais principais. Consequentemente, $[a_l, a_r] = a_l a_r - a_r a_l$ é uma matriz triangular estritamente superior, isto é, para $i \geq j$, o elemento da linha i e da coluna j de $[a_l, a_r]$ será igual a zero.

Agora, veremos que o produto de n matrizes triangulares estritamente superiores de ordem n dá zero. Utilizaremos indução em n.

Primeiramente, vemos que, para $n = 1$, isso é imediato.

Agora, suponha que seja válido para $n-1$ e mostremos que é válido para n. Observe o produto de n matrizes de ordem n cada uma

$$\begin{bmatrix} 0 & a_{12} & \cdots & a_{1\,n-1} & a_{1n} \\ 0 & 0 & \cdots & a_{2\,n-1} & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_{n-1\,n} \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}_{n \times n} \cdots \begin{bmatrix} 0 & b_{12} & \cdots & b_{1\,n-1} & b_{1n} \\ 0 & 0 & \cdots & b_{2\,n-1} & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & b_{n-1\,n} \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}_{n \times n},$$

e note que, em cada matriz de ordem $n \times n$, podemos considerar o bloco $(n-1) \times (n-1)$, que consiste das $n-1$ primeiras entradas de cada uma das $n-1$ primeiras linhas e que cada matriz consiste desse bloco incluindo a última linha igualmente nula, pois as matrizes são triangulares estritamente superiores e uma coluna com $n-1$ elementos possivelmente diferentes de zero. Consequentemente, ao realizarmos o produto acima até a penúltima matriz, teremos que pelo menos o bloco $(n-1) \times (n-1)$ do resultado desse produto terá todos os elementos nulos. Desse modo, obtemos

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & c_{1n} \\ 0 & 0 & \cdots & 0 & c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & c_{n-1\,n} \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}_{n\times n} \cdot \begin{bmatrix} 0 & b_{12} & \cdots & b_{1\,n-1} & b_{1n} \\ 0 & 0 & \cdots & b_{2\,n-1} & b_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & b_{n-1\,n} \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}_{n\times n},$$

em que $c_{1n}, c_{2n}, \ldots, c_{n-1,n}$ são escalares. O produto das duas matrizes acima é zero e, dessa forma, fica demonstrado o que queríamos.

Dessarte, a álgebra UT_n satisfaz a identidade $[x_1, x_2] \cdots [x_{2n-1}, x_{2n}]$.

Para cada $g \in G$, seja $X^g = \{x_1^g, x_2^g, \cdots\}$ um conjunto infinito e seja

$$X = \bigcup_{g\in G} X^g$$

uma união disjunta.

Definição 1.5.7 *Sejam $A = \bigoplus_{g\in G} A_g$ uma álgebra graduada e $f(x_1^{g_1}, \ldots, x_n^{g_n}) \in \mathbb{K}\langle X^g \rangle$, com $X^G = \bigcup_{g\in G} X^g$. Dizemos que o polinômio $f(x_1^{g_1}, \ldots, x_n^{g_n})$ é uma **identidade polinomial graduada** para A se $f(a_1, \ldots, a_n) = 0$, para quaisquer $a_1 \in A_{g_1}, \ldots, a_n \in A_{g_n}$.*

Denotaremos por $T_G(A)$ o conjunto das identidades $G-$graduadas de A.

No caso específico em que $A = UT_n$ está munida de uma graduação elementar determinada por uma $n-$upla $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in G^n$, denotaremos o conjunto de todas as identidades $G-$graduadas de A por $T_G(UT_n, \varepsilon)$.

Exemplo 1.5.8 *Seja $A = M_n(K)$ com a G-graduação elementar determinada por uma n-upla $(g_1, \ldots, g_n)$ tal que $g_i \neq g_j$ para quaisquer $i \neq j$. Então $[x_1^e, x_2^e] = 0$ é uma identidade polinomial graduada para A. Com efeito, basta observar que A_e é o subespaço das matrizes diagonais, ou seja, $A_e = \text{span}\{e_{(i,i)};\ i = 1, \ldots, n\}$.*

De fato, nesse caso, a graduação elementar implica que cada matriz $e_{(i,j)}$ tem grau $g_i^{-1}g_j$. Assim, $g_i^{-1}g_j = e$ ocorre apenas quando $i = j$. Desse modo, a componente homogênea de grau neutro A_e consiste exatamente das matrizes diagonais.

Como toda matriz diagonal comuta com qualquer outra matriz diagonal, o comutador entre quaisquer dois elementos de A_e é nulo. Logo, o polinômio $[x_1^e, x_2^e]$ é uma identidade polinomial graduada para A.

A Propriedade Universal da Álgebra Livre é um resultado bastante importante na PI-Teoria. Abaixo, apresentaremos, também, uma versão estendida dessa propriedade para álgebras graduadas.

Teorema 1.5.9 (Propriedade Universal - caso graduado) *Sendo $A = \bigoplus_{g\in G} A_g$ uma álgebra $G-$graduada sobre $\mathbb{K}$ e $h : X \longrightarrow A$ uma aplicação, com $h(x_i^g) \in A_g$, para todo $x_i^g \in X^g$ e $g \in G$, então existe um único homomorfismo de álgebras $G-$graduadas $\varphi : \mathbb{K}\langle X^G\rangle \longrightarrow A$ que estende h, isto é, $\varphi(x_i^g) = h(x_i^g)$, para todo $x_i^g \in X^g$.*

Demonstração: Uma vez que já demonstramos o caso geral da propriedade, precisamos mostrar apenas a compatibilidade da graduação.

Se $x_i^g \in X^g$, então $h(x_i^g) \in A_g$. Além disso, sejam $x_{i_1}^{g_1} \in X^{g_1}, \ldots, x_{i_m}^{g_m} \in X^{g_m}$. Então,

$$\varphi(x_{i_1}^{g_1} \cdots x_{i_m}^{g_m}) = h(x_{i_1}^{g_1}) \cdots h(x_{i_m}^{g_m}) \in A_{g_1} \cdots A_{g_m} \subseteq A_{g_1 \cdots g_m}.$$

Portanto, H preserva a graduação. ■

Definição 1.5.10 *Um ideal I de $\mathbb{K}\langle X^G\rangle$ é dito um T_G-ideal se $\varphi(I) \subseteq I$, para todo endomorfismo de álgebras $G-$graduadas φ de $\mathbb{K}\langle X^G\rangle$.*

Proposição 1.5.11 *O polinômio $f \in \mathbb{K}\langle X^G\rangle$ é uma identidade polinomial $G-$graduada para A se, e somente se, f está no núcleo de todo homomorfismo de álgebras $G-$graduadas $\phi : \mathbb{K}\langle X^G\rangle \longrightarrow A$. Em particular, $T_G(A)$ é a interseção de todos os núcleos dos homomorfismos graduados, ou seja,*

$$T_G(A) = \bigcap_{\phi\ G-graduado} \ker(\phi).$$

Demonstração: Suponha que f seja uma identidade $G-$graduada para a álgebra A. Seja $\phi : \mathbb{K}\langle X^G\rangle \longrightarrow A$ um homomorfismo de álgebras $G-$graduadas. Devemos mostrar que $\phi(f) = 0$. Da Observação 1.5.2, temos

$$\phi(f) = f(\phi(x_1^{g_1}), \ldots, \phi(x_n^{g_n})).$$

Como $\phi(x_i^{g_i}) \in A_{g_i}$ e f é uma identidade polinomial de A, então

$$\phi(f) = f(\phi(x_1^{g_1}), \ldots, \phi(x_n^{g_n})) = 0.$$

Logo, $\phi(f) = 0$ e, assim, $f \in \ker(\phi)$. Como ϕ é um homomorfismo de álgebras $G-$graduadas qualquer, temos a primeira implicação do resultado.

Reciprocamente, suponha que $f \in \ker(\phi)$, para todo homomorfismo de álgebras $G-$graduadas $\phi : \mathbb{K}\langle X^G\rangle \longrightarrow A$. Dados $a_i \in A_{g_i}$, com $i = 1, \ldots, n$, defina $\alpha : X^G \longrightarrow A$ por $\alpha(x_i^{g_i}) = a_i \in A_{g_i}$. Agora, tomemos $\phi : \mathbb{K}\langle X^G\rangle \longrightarrow A$ o homomorfismo que estende α. Por hipótese, $\phi(f) = 0$. Mas $\phi(f) = 0$. Então,

$$0 = \phi(f) = f(\phi(x_1^{g_1}), \ldots, \phi(x_n^{g_n})) = f(a_1, \ldots, a_n).$$

Logo, $f(a_1, \ldots, a_n) = 0$, para todo $a_i \in A_{g_i}$. Desse modo, f é uma identidade $G-$graduada para A.

Por fim,

$$f \in T_G(A) \Longleftrightarrow f \in \bigcap_{\phi\ G-\text{graduado}} \ker(\phi).$$

Portanto,

$$T_G(A) = \bigcap_{\phi\ G-\text{graduado}} \ker(\phi). \ \blacksquare$$

Corolário 1.5.12 *Seja A uma álgebra $G-$graduada. O conjunto $T_G(A)$, de todas as identidades polinomiais $G-$graduadas de A, é um T_G-ideal de $\mathbb{K}\langle X^G\rangle$.*

Demonstração: Sejam $\varphi : \mathbb{K}\langle X^G\rangle \longrightarrow \mathbb{K}\langle X^G\rangle$ um endomorfismo de álgebras graduadas e $h \in \varphi(T_G(A))$. Basta mostrarmos que $\psi(h) = 0$, para todo homomorfismo de álgebras $G-$graduadas $\psi : \mathbb{K}\langle X^G\rangle \longrightarrow A$. Com efeito, como $h \in \varphi(T_G(A))$, existe $f \in T_G(A)$ tal que $h = \varphi(f)$.

Dado $\psi : \mathbb{K}\langle X^G\rangle \longrightarrow A$ um homomorfismo graduado, então $\psi \circ \varphi : \mathbb{K}\langle X^G\rangle \longrightarrow A$ é também um homomorfismo graduado. Assim, $\psi \circ \varphi(f) = 0$, pois $f \in T_G(A)$. Portanto, $\psi(h) = \psi(\varphi(f)) = 0$. $\blacksquare$

Sabemos que isomorfismos preservam propriedades algébricas. O resultado a seguir mostrará que, no contexto de identidades polinomiais, não é diferente. Em outras palavras, será provado que álgebras isomorfas satisfazem as mesmas identidades. Destacamos, também, que, em geral, a recíproca desse fato não é válida.

Lema 1.5.13 *Sejam $A = \bigoplus_{g\in G} A_G$ e $B = \bigoplus_{g\in G} B_g$ álgebras $G-$graduadas. Se existir $\varphi : A \longrightarrow B$ um monomorfismo de álgebras $G-$graduadas, então $T_G(B) \subseteq T_G(A)$.*

Demonstração: Suponha que $\varphi : A \longrightarrow B$ um monomorfismo de álgebras $G-$graduadas. Tomemos $f = f(x_{i_1}^{g_1}, \ldots, x_{i_m}^{g_m}) \in T_G(B)$. Dados $a_1, \ldots, a_m \in A_{g_i}$, como φ é graduado, temos $\varphi(a_i) \in B_{g_i}$. Assim,

$$0 = f(\varphi(a_1), \ldots, \varphi(a_m)) = \varphi(f(a_1, \ldots, a_m)).$$

Assim, $f(a_1, \ldots, a_m) \in \ker(\varphi)$. Como φ é injetor, temos $\ker(\varphi) = \{0\}$. Dessa forma, $f(a_1, \ldots, a_m) = 0$.

Portanto, segue que $f \in T_G(A)$. ■

Lema 1.5.14 *Sejam $A = \bigoplus_{g\in G} A_g$ e $B = \bigoplus_{g\in G}$ álgebras $G-$graduadas. Se existir $\varphi : A \longrightarrow B$ um epimorfismo de álgebras $G-$graduadas, então $T_G(A) \subseteq T_G(B)$.*

Demonstração: Seja $\varphi : A \longrightarrow B$ um epimorfismo de álgebras $G-$graduadas. Tomemos $f = f(x_{i_1}^{g_1}, \ldots, x_{i_m}^{g_m}) \in T_G(A)$. Dados $b_1, \ldots, b_m \in B$ tais que $b_i \in B_{g_i}$, como φ é sobrejetor e preserva a graduação, existem $a_i \in A_{g_i}$ tais que $\varphi(a_i) = b_i$. Assim,

$$f(b_1, \ldots, b_m) = f(\varphi(a_1), \ldots, \varphi(a_m)) = \varphi(f(a_1, \ldots, a_m)) = \varphi(0) = 0.$$

Portanto, $f \in T_G(B)$. ■

Teorema 1.5.15 *Sejam $A = \bigoplus_{g\in G} A_g$ e $B = \bigoplus_{g\in G} B_g$ álgebras $G-$graduadas. Se existir $\varphi : A \longrightarrow B$ um isomorfismo graduado, então $T_G(A) = T_G(B)$*

Demonstração: Pelos Lemas 1.5.13 e 1.5.14, esse resultado segue imediatamente. ■

Proposição 1.5.16 *Sendo I um T_G-ideal de $\mathbb{K}\langle X\rangle$, então $I = T_G\left(\frac{\mathbb{K}\langle X\rangle}{I}\right)$.*

Demonstração: Vejamos, primeiramente, que $I \subset T_G\left(\frac{\mathbb{K}\langle X\rangle}{I}\right)$. Seja $f(x_1^{g_1}, \ldots, x_n^{g_n}) \in I$. Dados $g_1 + I \ldots, g_n + I \in \frac{\mathbb{K}\langle X\rangle}{I}$ quaisquer, temos

$$f(g_1 + I, \ldots, g_n + I) = f(g_1, \ldots, g_n) + I.$$

Como I é um T_G-ideal e $f \in I$, segue que $f(g_1, \ldots, g_n) \in I$. Logo,

$$f(g_1 + I, \ldots, g_n + I) = 0 + I, \text{ em } \frac{\mathbb{K}\langle X\rangle.}{I}$$

Assim, $f \in T_G\left(\frac{\mathbb{K}\langle X\rangle}{I}\right)$.

Agora, vejamos que $T_G\left(\frac{\mathbb{K}\langle X\rangle}{I}\right) \subset I$. Com efeito, seja $f(x_1^{g_1}, \ldots, x_n^{g_n}) \in T_G\left(\frac{\mathbb{K}\langle X\rangle}{I}\right)$. Então

$$0 + I = f(x_1^{g_1} + I, \ldots, x_n^{g_n} + I) = f(x_1^{g_1}, \ldots, x_n^{g_n}) + I.$$

Dessa forma, $f(x_1^{g_1}, \ldots, x_n^{g_n}) \in I$, ou seja, $f \in I$. ■

1.6 Matrizes genéricas

Nesta seção introduzimos a álgebra de matrizes genéricas, que desempenhará um papel fundamental na demonstração do Teorema Principal, que será apresentada no capítulo final.

Definição 1.6.1 *Fixe um inteiro $n \geq 2$ e denote por*

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

a $\mathbb{K}-$álgebra de polinômios em infinitas variáveis comutativas. As $n \times n$ matrizes com entradas em Ω_n

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

*são chamadas **matrizes genéricas** $n \times n$. A álgebra R_n, gerada pelas matrizes genéricas $n \times n$, é a álgebra de matrizes genéricas $n \times n$. Denotamos por $R_{n,d}$ a subálgebra de R_n gerada pelas d primeiras matrizes $y_1, \ldots, y_d$.*

Por exemplo, para $n = d = 2$, mudando a notação para $x = y_1$, $y = y_2$, e $x_{pq} = y_{(p,q)}^{(i)}$, $y_{pq} = y_{(p,q)}^{(2)}$, a álgebra R_{22} é gerada por

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

Para qualquer $\mathbb{K}-$álgebra comutativa C, as matrizes $n \times n$ com entradas em C podem ser obtidas por especializações das matrizes genéricas, por exemplo,

$$a = \sum_{p,q=1}^{n} \gamma_{(p,q)} e_{(p,q)},\ \gamma_{(p,q)} \in C,$$

é obtida a partir de

$$y_1 = \sum_{p,q=1}^{n} y_{(p,q)}^{(i)} e_{(p,q)}$$

substituindo as variáveis $y_{(p,q)}^{(1)}$ por $\gamma_{(p,q)}$. Essa substituição é um caso particular da Proposição 1.4.16, em que $A = \Omega_n$, $B = C$, o homomorfismo $f : \Omega_n \longrightarrow C$ é dado por $f(y_{(p,q)}^{(1)}) = \gamma_{(p,q)}$, e a aplicação induzida $F : M_n(\Omega_n) \longrightarrow M_n(C)$ leva a matriz genérica y_1 na matriz $a = \sum_{p,q=1}^{n} \gamma_{(p,q)} e_{(p,q)} \in M_n(C)$.

Proposição 1.6.2 *Se o corpo base $\mathbb{K}$ é infinito, então a álgebra de matrizes genéricas R_n é isomorfa à álgebra relativamente livre $\frac{\mathbb{K}\langle X\rangle}{T(M_n(\mathbb{K}))}$. Se $\mathbb{K}$ é um corpo finito e P é qualquer extensão infinita de $\mathbb{K}$, então $R_n \simeq \frac{\mathbb{K}\langle X\rangle}{T(M_n(P))}$, em que $M_n(P)$ é considerada como $\mathbb{K}-$álgebra.*

Demonstração: Seja P um corpo infinito qualquer que contém $\mathbb{K}$ e consideremos o homomorfismo

$$\begin{aligned} \rho : \mathbb{K}\langle X\rangle &\longrightarrow R_n \\ x_i &\longmapsto y_i \quad . \end{aligned}$$

Mostraremos que $\ker\rho = T(M_n(P))$.

Claramente, se $f(x_1,\ldots,x_m) \in \ker\rho$, então $f(y_1,\ldots,y_m) = 0$, pois

$$0 = \rho(f(x_1,\ldots,x_m)) = f(y_1,\ldots,y_m).$$

Sendo $r_i = (\tau^{(i)}_{(j,k)}) \in \Omega_n$ e considerando o homomorfismo

$$\begin{aligned} \Omega_n &\longrightarrow \mathbb{K} \\ \tau^{(i)}_{(j,k)} &\longmapsto \begin{cases} \tau^{(i)}_{(j,k)}, \text{ se } i \leq m \\ 0, \text{ se } i > m \end{cases} , \end{aligned}$$

temos, pela Proposição 1.4.16, um homomorfismo

$$\varphi : R_n \longrightarrow M_n(P)$$

tal que $y_i \mapsto r_i$, para $i = 1,\ldots,m$, e $y_i \mapsto 0$, para $i > m$. Logo, $f(r_1,\ldots,r_m) = 0$, pois

$$f(r_1,\ldots,r_m) = f(\varphi(y_1),\ldots,\varphi(y_m)) = \varphi(f(y_1,\ldots,y_m)) = \varphi(0) = 0,$$

e $f(x_1,\ldots,x_m) = 0$ é uma identidade polinomial para $M_n(P)$.

Agora, seja $f(x_1,\ldots,x_m) \in T(M_n(P))$ e suponha que $f(y_1,\ldots,y_m) \neq 0$ em R_n. As entradas f_{pq} de $f(y_1,\ldots,y_m)$ são polinômios nas variáveis comutativas $y^{(i)}_{pq}$. Como P é um corpo infinito contendo $\mathbb{K}$ e algum $f_{p_0q_0} = f_{p_0q_0}(y^{(i)}_{pq})$ é um polinômio não nulo nos $y^{(i)}_{pq}$, podemos encontrar elementos $\xi^{(i)}_{pq} \in P$ tais que

$$f_{p_0q_0}(\xi^{(i)}_{pq}) \neq 0.$$

Isso significa que, para as matrizes

$$r_i = \sum_{p,q=1}^{n} \xi^{(i)}_{(p,q)} e_{(p,q)}, \ i = 1,\ldots,m,$$

a expressão $f(r_1,\ldots,r_m)$ é diferente de zero, o que é uma contradição, pois $f \in T(M_n(P))$.

Portanto, $\ker\rho = T(M_n(P))$.

Por fim, pelo Teorema Fundamental dos Homomorfismos,

$$\frac{\mathbb{K}\langle X\rangle}{\ker\rho} \longrightarrow R_n$$

$$f(\bar{x}_1,\ldots,\bar{x}_m) \longmapsto f(y_1,\ldots,y_m) \ . \qquad \blacksquare$$

1.7 Polinômios Multihomogêneos e Multilineares

A estrutura do conjunto $T(A)$, das identidades polinomiais de uma álgebra, é melhor compreendida por meio da teoria de T-ideais e da análise de polinômios homogêneos e multilineares. A decomposição em componentes homogêneas e a redução ao caso multilinear constituem ferramentas fundamentais na teoria de PI-álgebras.

Definição 1.7.1 *Dado $S \subseteq \mathbb{K}\langle X\rangle$, definimos o $T-$ideal de $\mathbb{K}\langle X\rangle$ gerado por S, e denotamos por $\langle S\rangle^T$, como sendo a interseção dos $T-$ideais de $\mathbb{K}\langle X\rangle$ que contém S.*

Seja A uma álgebra. Se $S \subset T(A)$ é tal que $T(A) = \langle S\rangle$, dizemos que S é uma base das identidades polinomiais de A. Além disso, os elementos de $T(A)$ são chamados consequências das identidades polinomiais de S.

Definição 1.7.2 *Seja*

$$f(x_1,\ldots,x_n) = \sum \alpha_i x_{i_1}\cdots x_{i_{d_i}} \in \mathbb{K}\langle X\rangle.$$

Dizemos que f é homogêneo de grau d se $d_i = d$, para todo i tal que $\alpha_i \neq 0$. Além disso, f é multihomogêneo de multigrau $(d_1,\ldots,d_n)$ se, em cada monômio que aparece com coeficiente não nulo, a variável x_k aparece exatamente d_k vezes, para $k = 1,\ldots,n$. Se $f(x_1,\ldots,x_n)$ é multihomogêneo de multigrau $(1,\ldots,1)$, dizemos que f é multilinear. Nesse último caso, podemos escrever f na seguinte forma:

$$f(x_1,\ldots,x_n) = \sum_{\sigma\in Sym(n)} \alpha_\sigma x_{\sigma(1)}\cdots x_{\sigma(n)}, \text{ com } \alpha_\sigma \in \mathbb{K}.$$

Note que, dado um polinômio qualquer $f(x_1,\ldots,x_n) \in \mathbb{K}\langle X\rangle$, fixamos uma variável x_t, com $1 \leq t \leq n$ que aparece em f e seja d o maior número de vezes que x_t aparece em um monômio de f com coeficiente não nulo. Podemos escrever f de modo único da seguinte forma: $f = \sum_{i=0}^{d} f_i$, onde f_i é homogêneo de grau i em x_t, isto é, x_t aparece exatamente i vezes em cada monômio de f_i com coeficiente não nulo. Iremos nos referir a f_i como a componente homogênea de grau i em x_t.

Proposição 1.7.3 *Seja*

$$f(x_1,\ldots,x_m) = \sum_{i=0}^{n} f_i \in \mathbb{K}\langle X\rangle,$$

em que f_i é a componente homogênea de f de grau i em x_1.

i) Se o corpo base $\mathbb{K}$ *possui mais do que* n *elementos, então as identidades polinomiais* $f_i = 0, i = 0, 1, \cdots, n$*, são consequência de* $f = 0$*.*

ii) Se o corpo base tem característica 0 *(ou se* $\operatorname{char}\mathbb{K} > \deg f$*), então* $f = 0$ *é equivalente a um conjunto de identidades polinomiais multilineares.*

Demonstração: *i*) Seja $V = \langle f \rangle^T$ o T-ideal gerado por f. Podemos escolher $n+1$ elementos distintos $\alpha_0, \alpha_1, \ldots, \alpha_n$ de $\mathbb{K}$. Como V é um $T-$ideal,

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

Considere essas equações como um sistema linear com incógnitas $f_i, i = 0, \ldots, n$. Sendo o determinante

$$\begin{vmatrix} 1 & \alpha_0 & \alpha_0^2 & \cdots & \alpha_0^n \\ 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^n \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^n \end{vmatrix} = \prod_{i<j} (\alpha_j - \alpha_i)$$

o determinante de Vandermonde que é diferente de 0, obtemos que cada $f_i(x_1, \ldots, x_m)$ também pertence a V, isto é, as identidades polinomiais $f_i = 0$ são consequência de $f = 0$. *ii*) Usaremos o processo de linearização.

Por *i*), podemos assumir que $f(x_1, \ldots, x_m)$ é homogêneo em cada variável. Seja $\deg_{x_1} f = d$. Escrevemos $f(y_1 + y_2, x_2, \ldots, x_m) \in V$ na forma

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

em que f_i é a componente homogênea de grau i em y_1. Assim, por (i), $f_i \in V, i = 1, \ldots, d$. Como $\deg_{y_1} f_i < d, i = 1, \ldots, d-1, j = 1, 2$, aplicamos um argumento indutivo e obtemos um conjunto de consequências multilineares de $f = 0$. Para ver que essas identidades multilineares são equivalentes a $f \equiv 0$, é suficiente ver que

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

e o coeficiente binomial é diferente de zero, pois $\operatorname{char}\mathbb{K} = 0$ ou $\operatorname{char}\mathbb{K} = p > d$. ■

Capítulo 2

Graduações Elementares de UT_n

Neste capítulo, trataremos de graduações elementares na álgebra das matrizes triangulares superiores, UT_n, e sua relação com identidades polinomiais graduadas. Classificamos todas as graduações em UT_n, mostrando que toda $G-$graduação em UT_n é isomorfa a uma graduação elementar. Além disso, demonstramos que duas graduações elementares coincidem se, e somente se, induzem as mesmas identidades graduadas.

Os nossos esforços convergirão para demonstrar o Teorema 2.0.7, que se encontra em [47], o qual estabelece que, se UT_n é uma álgebra $G-$graduada, então é isomorfa a UT_n com alguma $G-$graduação elementar. Para tanto, serão necessários alguns lemas da mesma referência.

Lema 2.0.1 *Qualquer idempotente em UT_n, isto é, $e^2 = e$, é conjugado a um idempotente diagonal da forma $e_{(i_1,i_1)} + \cdots + e_{(i_k,i_k)}$, para certos $1 \leq i_i < \cdots < i_k \leq n$.*

Demonstração: Considere V um espaço vetorial de dimensão n sobre um corpo $\mathbb{K}$ e uma cadeia

$$V_1 \subseteq V_2 \subseteq \cdots \subseteq V_n \tag{2.1}$$

de subespaços de V com $\dim V_k = k,\ k = 1, \ldots, n$. Então, UT_n pode ser visto como a álgebra de todas as transformações lineares de V que preservam a cadeia (2.1).

Seja $e \in UT_n$ um idempotente. Para provar o lema, é suficiente encontrar uma base $v_1, \ldots, v_n$ de V tal que $V_k = \text{span}\{v_1, \ldots, v_k\}$ e $e(v_i) = \varepsilon_i v_i$ para todo i, em que $\varepsilon_i = 0$ ou 1.

Vamos fazer indução sobre n. Para $n = 1$, assuma que existe $v_1 \in V_1$ tal que V_1 é gerado por v_1. Logo,

$$\varepsilon_1 v_1 = e(v_1) = e^2(v_1) = e(e(v_1)) = e(\varepsilon_1 v_1) = \varepsilon_1 e(v_1) = \varepsilon_1\varepsilon_1 v_1 = \varepsilon_1^2 v_1$$
$$\Rightarrow \varepsilon_1 = \varepsilon_1^2 \Rightarrow \varepsilon_1 = 0 \text{ ou } 1$$

Agora, vamos assumir que existem $v_1, \ldots, v_n \in V$ com $e(v_j) = \varepsilon_j v_j$, para todo $j = 1, \ldots, n-1$. Se $e(v_n) \notin V_{n-1}$, então $e^2(v_n) = e(v_n)$ implica que $\{v_1, \ldots, v_{n-1}, e(v_n)\}$ é a base procurada. Por outro lado, se $e(v_n) \in V_{n-1}$, então $v_n' = v_n - e(v_n)$ é tal que $e(v_n') = 0$ e $\{v_1, \ldots, v_{n-1}, v_n'\}$ é a base procurada. ■

Lema 2.0.2 *Seja e um idempotente de UT_n. Então a subálgebra eAe é isomorfa a $UT_k(\mathbb{K})$, em que $k = tr(e)$ é o traço da matriz e.*

Demonstração: Sem perda de generalidade, pelo Lema 2.0.1, $e = e_{(i_1,i_1)} + \cdots + e_{(i_k,i_k)}$, $1 \leq i_1 < \cdots < i_k \leq n$. Além disso, sendo $UT_n = A$, temos, em eAe,

$$e\Big(\sum_{i\leq j} \lambda_{(i,j)} e_{(i,j)}\Big)e = \sum_{i\leq j} \lambda_{(i,j)} e e_{(i,j)} e \neq 0 \Rightarrow i, j \in \{i_1, \ldots, i_k\}.$$

Logo,

$$eAe = \text{span}\{e_{(i,j)}; i \leq j,\ i, j \in \{i_1, \ldots, i_k\}\}.$$

Considere, agora, a transformação linear bijetora

$$\varphi : eAe \longrightarrow UT_k$$
$$e_{(i_r,i_s)} \longmapsto e_{(r,s)} \ .$$

Devemos mostrar, ainda, que essa aplicação é compatível com o produto, ou seja,

$$\varphi(xy) = \varphi(x)\varphi(y), \forall x, y \in eAe.$$

Note que,

$$\varphi(e_{(i_r,i_s)} e_{(i_t,i_u)}) = \varphi(\delta_{(s,t)} e_{(i_r,i_u)}) = \delta_{(s,t)} e_{(r,u)} \text{ e}$$
$$\varphi(e_{(i_r,i_s)})\varphi(e_{(i_t,i_u)}) = e_{(r,s)} e_{(t,u)} = \delta_{(s,t)} e_{(r,u)}.$$

Logo, como a igualdade nos garante que vale com elementos base, concluímos que vale para elementos quaisquer. Consequentemente, a aplicação é compatível com o produto. ■

Lema 2.0.3 *Qualquer conjunto $\{a_1, \cdots, a_n\}$ de n idempotentes ortogonais, isto é, tais que $a_i^2 = a_i$ para todo i e $a_i a_j = 0$ sempre que $i \neq j$, de UT_n é conjugado a $\{e_{(1,1)}, \ldots, e_{(n,n)}\}$, no sentido de que existe $u \in UT_n(\mathbb{K})$ invertível tal que $u a_i u^{-1} = e_{(i,i)}$ para todo i.*

Demonstração: Considere A como sendo a álgebra de todas as transformações lineares de um espaço vetorial V de dimensão n que preservam a cadeia (2.1). Então é suficiente encontrar uma base $v_1, \ldots, v_n$ de V tal que $V_k = \text{span}\{v_1, \ldots, v_k\}, k = 1, \ldots, n$, e $a_i(v_j) = \delta_{ij} v_j$, em que δ_{ij} é o delta de Kronecker, para todo i, j.

Primeiro, escolhemos uma base arbitrária $u_1, \ldots, u_n$ de V, com $V_k = \text{span}\{u_1, \ldots, u_k\}$, para todo $k = 1, \ldots, n$. Então $a_1, \ldots, a_n$, vistos como transformações lineares, têm matrizes triangulares superiores associadas nessa base e denote por $(a_k)_{ij}$ a $(i, j)-$ésima entrada da matriz associada a a_k, $k = 1, \ldots, n$. Note que, como $a_k^2 = a_k$, então $(a_k)_{ii} = 0$ ou 1, para todo $i = 1, \ldots, n$. Além disso, como $a_1, \ldots, a_n$ são ortogonais e são n, segue que cada a_k tem, precisamente, uma entrada diagonal diferente de zero em posições distintas. Reordenando, eventualmente, os $a_i's$, podemos assumir que $(a_1)_{11} = \cdots = (a_n)_{nn} = 1$ e $(a_i)_{jj} = 0$, para todo $i \neq j$. Se definirmos $e = a_1 + \cdots + a_{n-1}$, então, pelo Lema 2.0.2, eAe é a subálgebra de $\text{End}\, V_{n-1}$ isomorfa a UT_{n-1}. Mas, então, por indução em n, existe uma base $\{v_1, \ldots, v_{n-1}\}$ de V_{n-1} tal que $a_i(v_j) = \delta_{ij}$, para todo $1 \leq i, j \leq n-1$. Se definirmos, agora, $v_n = a_n(u_n) \notin V_{n-1}$, então obtemos a base desejada de V. ■

Lema 2.0.4 *Seja $UT_n(\mathbb{K}) = \bigoplus_{g \in G} A_g$ uma álgebra de matrizes triangulares superiores sobre um corpo $\mathbb{K}$ graduada por um grupo G, com elemento neutro $1 \in G$. Então A_1 contém n idempotentes ortogonais.*

Demonstração: Denotaremos por I_n a matriz identidade de $UT_n(\mathbb{K})$. Procederemos por indução em n. Para $n = 1$, a afirmação do lema é óbvia, pois a álgebra UT_1 é composta apenas de matrizes 1×1.

Seja $n > 1$. Como $I_n \in A_1$, existe uma subálgebra semissimples (isto é, com radical de Jacobson nulo) maximal B de A_1 (veja, por exemplo, [50]). Seja C um somando simples de B (isto é, um ideal simples que aparece na decomposição $B = C_1 \oplus \cdots \oplus C_r$) e seja e a unidade de C. Pelo Lema 2.0.1, e é conjugado a um idempotente diagonal. Logo, e e $I_n - e$ são dois idempotentes ortogonais ou $e = I_n$ e $C = B = \text{span}\{I_n\}$.

No primeiro caso, pelo Lema 2.0.2, $P = eAe \simeq UT_k$ e $Q = (I_n - e)A(I_n - e) \simeq UT_{n-k}$, em que $k \neq 0, n$. Como e, $I_n - e \in A_1$, as álgebras P e Q são homogêneas na $G-$graduação. Mas, pela hipótese de indução, podemos encontrar n idempotentes ortogonais $a_1, \ldots, a_k \in P_1$, $a_{k+1}, \ldots, a_n \in Q_1$ e concluímos.

Suponha, agora, que $\dim B = 1$. Vamos provar que isso leva a uma contradição.

Procederemos por indução na ordem de G. Se $|G| = 1$, então $A_1 = A = UT_n$ é uma subálgebra maximal semissimples de A_1 tem dimensão $n > 1$, isto é, uma subálgebra $S \subseteq A_1$ tal que S é semissimples (ou seja, possui radical de Jacobson nulo) e é maximal com respeito a essa propriedade, tem dimensão $n > 1$.

Suponha que, para qualquer $H-$graduação em UT_n, em que H é um grupo finito com $|H| < |G|$, tenhamos mostrado que a igualdade $\dim B = 1$ é impossível.

Primeiro afirmamos que qualquer elemento homogêneo de A é ou nilpotente ou invertível.

De fato, suponha que $a \in A_g$ não seja nilpotente. Para m suficientemente grande, os elementos $a, a^2, \ldots, a^m$ são linearmente dependentes e homogêneos. Segue que g deve ter ordem finita k e $a^k \in A_1$. Além disso, não sendo nilpotente, o elemento a^k não está no radical de Jacobson $J(A_1)$ de A_1. Desde que $\frac{A_1}{J(A_1)} \simeq \mathbb{K}I_n$, segue que $a^k - \lambda I_n$ é nilpotente para algum $\lambda \in \mathbb{K}, \lambda \neq 0$. Isso significa que a^k e, consequentemente, a são invertíveis e a afirmação está provada.

Provaremos, agora, que o radical de Jacobson $J(A)$ de A não contém elementos homogêneos diferentes de zero.

De fato, suponha, por contradição, que $0 \neq a \in A_g$ é nilpotente. Seu anulador à esquerda

$$L = \{x \in A;\ xa = 0\}$$

é um subespaço graduado de A. Como foi mostrado anteriormente, todo elemento homogêneo $x \in A$ é nilpotente ou invertível. Logo, desde que um elemento invertível não é divisor de zero, L consiste de matrizes triangulares estritamente superiores. Mas a matriz diagonal unitária $e_{(n,n)}$ anula à esquerda qualquer matriz estritamente triangular superior, isto é, $e_{(n,n)} \in L$, o que é uma contradição.

Nós provamos que $J(A)$ não contém elementos homogêneos não nulos. Mas, em particular, $J(A_1) \subseteq J(A)$ deve ser zero e $A_1 = B = \{\lambda I_n; \lambda \in \mathbb{K}\}$ consiste em matrizes escalares. Segue-se, também, que o suporte de A,

$$\operatorname{supp} A = \{g \in G; A_g \neq 0\}$$

é um subgrupo finito de G. Podemos supor que $\operatorname{supp} A = G$ e, caso contrário, aplicamos indução em $|G|$.

Afirmamos que $\dim A_g = 1$, para qualquer $g \in G$. De fato, se $x, y \in A_g$ são linearmente independentes, então, lembrando que todo elemento não nulo é invertível,

temos que $x^{-1} \in A_{g^{-1}}$ e, então, $yx^{-1} = \lambda I_n$, para algum $\lambda \in \mathbb{K}$. Então $(x - \lambda^{-1}y)x^{-1} = 0$, e isso contradiz a invertibilidade de $0 \neq x - \lambda^{-1}y \in A_g$.

Note que G não pode ser um grupo abeliano. De fato, nesse caso, como $g, h \in G, [a_g, a_h] \subseteq A_{gh} + A_{hg} \subseteq A_{gh}$, segue que a subálgebra gerada pelos comutadores $[A, A]$ é um ideal graduado nilpotente não nulo de A e isso não é permitido em nossa situação, porque $J(A)$ não tem elementos homogêneos não nulos.

Logo, G não é abeliano e, se G' é o subgrupo comutador de G, consideremos a graduação quociente $A = \bigoplus_{t \in \frac{G}{G'}} A_t$. Como $\frac{G}{G'}$ é abeliano, a conclusão do nosso lema se aplica a essa graduação $\frac{G}{G'}$, isto é, existem n idempotentes ortogonais $e_1, \ldots, e_n$ em

$$D = A_1 = \bigoplus_{h \in G'} A_h.$$

Por outro lado, G' é gerado pelos comutadores de grupo $a^{-1}b^{-1}ab, a, b \in G$. Se $h = a^{-1}b^{-1}ab$ e $0 \neq x \in A_a,\ 0 \neq y \in A_b$, então $z = x^{-1}y^{-1}xy$ é um elemento não nulo de A_h. Como $\dim A_h = 1$, temos $A_h = \text{span}\{z\}$. Em particular, $D = A_1$, como uma álgebra, é gerado por todos os $x^{-1}y^{-1}xy$, com x, y homogêneos. Qualquer $x^{-1}y^{-1}xy$ é uma matriz da forma $I_n + a$, em que $a \in J(A)$. Logo, todo elemento de D é múltiplo escalar de um elemento dessa forma. Em particular, para os idempotentes ortogonais $e_1, \ldots, e_n \in D$ anteriores, devemos ter $e_i = \lambda_i I_n + a_i, 1 \leq i \leq n$, para escalares não nulos $\lambda_1, \ldots, \lambda_n$. Mas, então, para qualquer $i \neq j$, o produto $e_i e_j$ não pode ser zero, contrariando a ortogonalidade dos $e_i's$. Essa contradição mostra que $\dim B \neq 1$ e concluímos a demonstração. ■

Lema 2.0.5 *Seja $A = \bigoplus_{g \in G} A_g$ um $G-$graduação em UT_n. Então a graduação é elementar se, e somente se, toda matriz unitária $e_{(i,j)}, 1 \leq i \leq j \leq n$, é homogênea.*

Demonstração: $\Rightarrow$) Se a graduação G é elementar, então todos os $e_{(i,j)}$ são homogêneos por definição.

$\Leftarrow$) Suponha, agora que todas as matrizes elementares são homogêneas. Primeiro, provaremos que existem $g_1, \ldots, g_n \in G$ tais que

$$\deg(e_{(i,i+1)}) = g_i^{-1} g_{i+1}, \tag{2.2}$$

para todo $i = 1, \ldots, n-1$.

Se $g_1 = 1$ e $g_2 = \deg(e_{(1,2)})$, então (2.2) é válida para $i = 1$. Assuma que (2.2) vale para $i = 1, \ldots, k-1$. Se $h = \deg(e_{(k,k+1)})$, então tome $g_{k+1} = g_k h$. Obviamente $\deg(e_{(k,k+1)}) = g_k^{-1} g_{k+1}$ e (2.2) vale para se $i = k$.

Finalmente, o grau de $e_{(i,j)}$, para quaisquer $1 \leq i < j \leq n$, é igual a

$$\begin{aligned}\deg(e_{(i,j)}) &= \deg(e_{(i,i+1)}) \deg_(e_{(i+1,i+2)}) \cdots \deg(e_{(j-1,j)}) \\ &= g_i^{-1} g_{i+1} g_{i+1}^{-1} g_{i+2} \cdots g_{j-1}^{-1} g_j = g_i^{-1} g_j. \ \blacksquare\end{aligned}$$

Lema 2.0.6 *Seja $UT_n(\mathbb{K}) = \bigoplus_{g \in G} A_g$ graduada por um grupo G, com $1 \in G$. Então a graduação é elementar se, e somente se, toda matriz elementar $e_{(i,i)}$ pertence a A_1.*

Demonstração: Se a graduação G é elementar, então $e_{(i,i)} \in A_1$, para todo $1 \leq i \leq n$, já que qualquer idempotente graduado pertence a componente neutra A_1.

Reciprocamente, seja $e_{(i,i)} \in A_1$. Então $A_{ij} = e_{(i,i)} A e_{(j,j)}$ é um subespaço graduado, para todo $1 \leq i < j \leq n$. Como $e_{(i,j)} \in A_{ij}$ e $\dim A_{ij} = 1$, todas as matrizes elementares $e_{(i,j)}$ são homogêneas e usamos a recíproca do Lema 2.0.5. $\blacksquare$

Teorema 2.0.7 *Se UT_n é uma álgebra G-graduada, então é isomorfa a UT_n com alguma G-graduação elementar.*

Demonstração: Pelo Lema 2.0.4, $A = UT_n$ contém n idempotentes ortogonais em A_1. Então, pelo Lema 2.0.3, como UT_n é uma álgebra G-graduada, então é isomorfa a $UT_n(\mathbb{K}) = UT_n' = A'$ com a G-graduação em que todas as matrizes elementares $e_{(1,1)}, \cdots, e_{(n,n)}$ são homogêneas e pertencem a A_1'. Assim, pelo Lema 2.0.6, A' tem uma G-graduação elementar. $\blacksquare$

Note que

$$(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n)$$

e

$$(1, \varepsilon_1^{-1}\varepsilon_2, \cdots, \varepsilon_1^{-1}\varepsilon_n)$$

definem a mesma $G-$graduação em UT_n. De fato, na graduação elementar, o grau de $e_{(i,j)}$ é dado por

$$\deg(e_{(i,j)}) = \varepsilon_i^{-1}\varepsilon_j.$$

Se tomarmos uma nova sequência $(1, \varepsilon_1^{-1}\varepsilon_2, \ldots, \varepsilon_1^{-1}\varepsilon_2)$ e denotarmos por $\deg'$ o grau na graduação definida pela nova sequência, temos:

- se $i = 1$, então $\varepsilon_1' = 1$ e

$$\deg'(e_{(i,j)}) = (\varepsilon_1')^{-1}\varepsilon_j' = 1^{-1}(\varepsilon_1^{-1}\varepsilon_j) = \varepsilon_1^{-1}\varepsilon_j.$$

- se $i > 1$, então $\varepsilon_i' = \varepsilon_1^{-1}\varepsilon_i$ e

$$\deg'(e_{(i,j)}) = (\varepsilon_i')^{-1}\varepsilon_j' = (\varepsilon_1^{-1}\varepsilon_i)^{-1} \cdot (\varepsilon_1^{-1}\varepsilon_j) = \varepsilon_i^{-1}\varepsilon_1 \cdot \varepsilon_1^{-1}\varepsilon_j = \varepsilon_i^{-1}\varepsilon_j.$$

Então,

$$\deg'(e_{(i,j)}) = \varepsilon_i^{-1}\varepsilon_j = \deg(e_{(i,j)}),$$

para todos i, j. Isso mostra que as duas sequências definem a mesma graduação.

Definição 2.0.8 *Seja $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in G^n$ e $\eta = (\eta_1, \ldots, \eta_m) \in G^m$. Considere a $G-$graduação elementar em UT_n induzida por ε. Dizemos que η é uma sequência $\varepsilon-$boa se existe uma sequência de m matrizes elementares $(r_1, \ldots, r_m)$ no radical de Jacobson de UT_n tal que*

$$r_1 r_2 \cdots r_m \neq 0 \text{ e } \deg_G(r_i) = \eta_i,$$

para todo $i = 1, \ldots, m$. Caso contrário, η é chamada de sequência $\varepsilon-$ruim.

Agora, recorde que, para cada $g \in G$, $X^g = \{x_1^g, x_2^g, \cdots\}$ é um conjunto infinito e

$$X = \bigcup_{g \in G} X^g$$

é uma união disjunta. Considere, em $\mathbb{K}\langle X\rangle$, a $G-$graduação tal que $\mathbb{K}\langle X\rangle$ é a álgebra $G-$graduada livre, livremente gerada por X. Às vezes, denotaremos por y_i as variáveis em $Y = X^1$, e por z_i uma variável x_i^g em $Z = \bigcup_{g \neq 1} X^g$, omitindo o grau, para simplificar a notação. Igualmente iremos omitir o grau nas variáveis de X.

Vamos considerar $\mathbb{K}$ um corpo finito com q elementos e G um grupo com elemento neutro 1.

Definição 2.0.9 *Seja $\eta = (\eta_1, \ldots, \eta_m) \in G^m$. Para cada $j = 1, \ldots, m$, defina o conjunto C_j como segue*

$$C_j = \begin{cases} \{x_j^{\eta_j}\}, & \text{se } \eta_j \neq 1; \\ \{[y_{2j}, y_{2j+1}], y_{2j}^q - y_{2j}\}, & \text{se } \eta_j = 1. \end{cases}$$

Se $c_1 \in C_1, c_2 \in C_2, \ldots, c_m \in C_m$, dizemos que

$$f_\eta = c_1 c_2 \cdots c_m$$

é um $\eta-$polinômio.

Lema 2.0.10 *Seja $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in G^n$ e $\eta = (\eta_1, \ldots, \eta_m) \in G^m$. Então η é $\varepsilon-$ruim se, e somente se, cada $\eta-$polinômio está em $T_G(UT_n, \varepsilon)$.*

Demonstração: Denote por J o radical de Jacobson de UT_n. Note que

$$\sum_{g\in G, g\neq 1} (UT_n)^g \subseteq J,$$

pois, se $e_{(i,j)}$ tem grau diferente de 1, então $i \neq j$.

Além disso, se $a_1, a_2 \in (UT_n)^g$, com $g = 1$, então

$$[a_1, a_2] \in J \text{ e } a_1^q - a_1 \in J.$$

$\Rightarrow$) Como η é $\varepsilon-$ruim, segue que $f_n \in T_G(UT_n, \varepsilon)$.

$\Leftarrow$) Seja $\tilde{\eta}$ uma sequência ε-boa. Então existe uma sequência de m matrizes elementares $(e_{(a_1,a_2)}, e_{(a_2,a_3)}, \ldots, e_{(a_{m-1},a_m)}, e_{(a_m,a_{m+1})})$ no radical de Jacobson de UT_n tal que o grau homogêneo $\varepsilon_{a_i}^{-1}\varepsilon_{a_{i+1}}$ de $e_{(a_i,a_{i+1})}$ é η_i para todo $i = 1, \ldots, m$. Note que se $\eta_i = 1$ então $e_{(a_i,a_{i+1})}$ é de $G-$grau 1 e podemos avaliar os polinômios $f_{\tilde{\eta},i} = [y_{2i-1}, y_{2i}]$ nas matrizes $e_{(a_i,a_{i+1})}$ e $e_{(a_{i+1},a_{i+1})}$ que são elementos elementos de grau 1 de UT_n. Claro que se $\eta_j \neq 1$ então $f_{\tilde{\eta},j} = x_j^{\eta_j}$ e a matriz $e_{(a_j,a_{j+1})}$ é um elemento homogêneo de UT_n de G-grau η_j. Segue-se que a avaliação de $f_{\tilde{\eta}} = f_{\tilde{\eta},1} \cdots f_{\tilde{\eta},m}$ nesses elementos homogêneos não se anula e terminamos. ■

Proposição 2.0.11 *Toda $G-$graduação elementar em UT_n é unicamente determinada pelos graus homogêneos das matrizes elementares $e_{(1,i)}$, com $i = 1, \ldots, n$.*

Demonstração: Sejam $UT_n = \bigoplus_{g\in G} A_g$ e $e_{(1,r)} \in A_{g_r}$. Todo $e_{(i,i)}$ pertence a A_1, a componente neutra. Suponha que $e_{(i,j)} \in A_g$, para algum $g \in G$ e $i < j$. Então, como $e_{(1,i)}e_{(i,j)} = e_{(1,j)}$, obtemos que $g_i g = g_j$ e, então, $g = g_i^{-1}g_j$ é unicamente determinado. ■

Proposição 2.0.12 *Toda $G-$graduação elementar em UT_n é unicamente determinada pelos graus homogêneos dos elementos $e_{(i,i+1)}$ ou seja, os elementos imediatamente acima da diagonal principal de uma matriz no radical de Jacobson.*

Demonstração: É suficiente descrever os graus homogêneos dos elementos $e_{(1,j)}$ na primeira linha. Sejam $UT_n = \bigoplus_{g\in G} A_g$ e $e_{(r,r+1)} \in A_g$. Temos que $e_{(1,1)}$ pertence a A_1, a componente neutra. Suponha que $e_{(1,j)} \in A_g$, para algum $g \in G$ e $1 < j$. Então, como $e_{(1,j)} = e_{(1,2)}e_{(2,3)} \cdots e_{(j-1,j)}$, obtemos que $g = g_1 g_2 \cdots g_j$ e, portanto, g é unicamente determinado. ■

Teorema 2.0.13 *Sejam $\varepsilon = (1, \varepsilon_2, \ldots, \varepsilon_n) \in G^n$ e $\varepsilon' = (1, \varepsilon_2', \ldots, \varepsilon_n') \in G^n$.*

a) $\varepsilon = \varepsilon'$ *se, e somente se, os* T_G*-ideais das identidades polinomiais* $G-$*graduadas de* UT_n *são iguais.*

b) $\varepsilon = \varepsilon'$ *se, e somente se, as* $G-$*graduações elementares correspondentes em* UT_n *são isomorfas.*

Demonstração: *a)* $\Rightarrow$) Imediato.

$\Leftarrow$) Primeiramente, observe que, no radical de Jacobson de UT_n, existe uma única sequência de $n-1$ matrizes elementares $(r_1, \ldots, r_{n-1})$ tal que o produto não é zero, a saber, $(e_{(1,2)}, e_{(2,3)}, e_{(3,4)}, \ldots, e_{(n-1,n)})$. Dessa forma, se $\varepsilon = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ determina alguma graduação fixada, então a sequência $d(\varepsilon) = (\varepsilon_1^{-1}\varepsilon_2, \ldots, \varepsilon_{n-1}^{-1}\varepsilon_n)$ é a única sequência $\varepsilon-$boa de tamanho $n-1$. Na verdade, essa sequência descreve os $G-$graus dos elementos $e_{(i,i+1)}$, com $i = 1, \ldots, n-1$, que estão no radical de Jacobson de UT_n.

Pela Proposição 2.0.12, os graus dos elementos $e_{(i,i+1)}$ determinam unicamente a graduação elementar. Como $\varepsilon_1 = \varepsilon_1' = 1$, se $\varepsilon \neq \varepsilon'$, então existe algum $i \geq 2$ tal que $\varepsilon_i \neq \varepsilon_i'$. Isso implica que as sequências $d(\varepsilon)$ e $d(\varepsilon')$ são diferentes. Dessa forma, o polinômio multilinear $f_{d(\varepsilon)}$ é uma identidade polinomial graduada de UT_n com respeito a graduação elementar ε', mas não é uma identidade com respeito a graduação determinada por ε. Logo, graduações elementares diferentes satisfazem identidades polinomiais diferentes e, portanto, $T_G(UT_n, \varepsilon) \neq T_G(UT_n, \varepsilon')$.

b) $\Rightarrow$) Imediato.

$\Leftarrow$) Sejam $\varepsilon, \varepsilon' \in G^n$. Denote por $T_G(UT_n, \varepsilon)$ o T_G-ideal de $\mathbb{K}\langle X\rangle$ formado por todas as identidades polinomiais $G-$graduadas de UT_n, quando UT_n tem a $G-$graduação determinada por ε. Suponha que as $G-$graduações elementares correspondentes em UT_n sejam isomorfas, ou seja,

$$(UT_n, \varepsilon) \simeq (UT_n, \varepsilon').$$

Então, $T_G(UT_n, \varepsilon) = T_G(UT_n, \varepsilon')$. Logo, pela letra (a), $\varepsilon = \varepsilon'$.■

Em suma, no contexto da álgebra UT_n munida de graduações elementares por um grupo G, a estrutura da graduação está diretamente ligada ao conjunto de identidades polinomiais graduadas que ela determina.

Corolário 2.0.14 *Seja* G *um grupo finito. Então existem* $|G|^{n-1}$ *graduações elementares na álgebra* UT_n *pelo grupo* G*. Duas graduações elementares diferentes satisfazem identidades polinomiais graduadas diferentes.*

Demonstração: Seja G um grupo finito. Já vimos que toda $G-$graduação elementar em UT_n é determinada por uma $n-$upla

$$\varepsilon = (1, \varepsilon_2, \ldots, \varepsilon_n) \in G^n.$$

Como a primeira entrada é fixada igual a 1, as demaus entradas podem ser escolhidas arbitrariamente em G. Como G possui $|G|$ elementos, pelo Princípio Fundamental da Contagem, temos $|G|^{n-1}$ $n-$uplas distintas.

Agora, pelo Teorema 2.0.13, se $\varepsilon \neq \varepsilon'$, então $T_G(UT_n, \varepsilon) \neq T_G(UT_n, \varepsilon')$. Isso mostra que $n-$uplas diferentes determinam graduações elementares distintas.

Assim, existem $|G|^{n-1}$ graduações elementares distintas em UT_n e duas graduações elementares diferentes satisfazem identidades polinomiais graduadas diferentes. ■

Capítulo 3

Identidades polinomiais $G-$graduadas para UT_n

Este capítulo se divide em duas partes. Inicialmente, estabelecemos os fundamentos teóricos, com a demonstração de lemas e proposições técnicas. Esses serão cruciais para a prova do teorema principal: uma descrição explícita de uma base para o T_G-ideal das identidades polinomiais graduadas de UT_n, para qualquer graduação elementar fixada.

A principal referência utilizada para a construção deste capítulo foi o artigo [21].

3.1 Alguns resultados técnicos

Seja $X = \{x_1, x_2, \ldots\}$ um conjunto infinito enumerável. Denotaremos por $\mathbb{K}[X]$ a álgebra comutativa livre, livremente gerada por X, e lembramos que $\mathbb{K}\langle X\rangle$ é a álgebra associativa livre, livremente gerada por X.

Considere a ordem lexicográfica à direita nos monômios da álgebra comutativa $\mathbb{K}[X]$. Assim, se $a_1, \ldots, a_m, b_1, \ldots, b_m \geq 0$, então

$$x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} < x_1^{b_1} x_2^{b_2} \cdots x_m^{b_m}$$

se, e somente se, existe $1 \leq j \leq m$ tal que $a_j < b_j, a_{j+1} = b_{j+1}, a_{j+2} = b_{j+2}, \ldots, a_m = b_m$.

Exemplo 3.1.1 *Considere, em* $\mathbb{K}[x, y, z]$*, os monômios*

$$x^7y^2z^2 \text{ e } x^2y^3z^2.$$

Comparando os expoentes de z, vemos que eles são iguais. Logo, temos de analisar os de y. Note que, no segundo monômio, o expoente de y é 3, enquanto no primeiro é 2. Assim,

$$x^7y^2z^2 < x^2y^3z^2.$$

Lema 3.1.2 *Sejam $<$ a ordem lexicográfica à direita e*

$$f(x_1, \cdots, x_m) = \sum_{a \in A} \alpha_a x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} \in T(\mathbb{K}),$$

em que $a = (a_1, \cdots, a_m), \alpha_a \in \mathbb{K}$, A é um conjunto finito e $T(\mathbb{K})$ é o $T-$ideal de $\mathbb{K}$ que está contido em $\mathbb{K}[X]$. Denote por $b = (b_1, \cdots, b_m)$ a m-upla tal que

$$x_1^{b_1} x_2^{b_2} \cdots x_m^{b_m} = \max\{x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}; a = (a_1, \cdots, a_m) \in A\}.$$

Se $0 \leq b_1, b_2, \cdots, b_m < q$, então $\alpha_b = 0$.

Demonstração: Escreva

$$f(x_1, \ldots, x_m) = \sum_{j=0}^{q-1} f_j(x_1, \ldots, x_{m-1}) x_m^j.$$

Como $|\mathbb{K}| = q$ e $\partial_{x_m} f < q$, pela Proposição 1.7.3, segue que

$$f_j(x_1, \ldots, x_m) x_m^j \in T(\mathbb{K}),\ \forall j.$$

Em particular,

$$f_{b_m}(x_1, \ldots, x_{m-1}) = f_{b_m}(x_1, \ldots, x_{m-1})(1)^{b_m} \in T(\mathbb{K}).$$

Como $x_1^{b_1} x_2^{b_2} \cdots x_{m-1}^{b_{m-1}}$ é o monômio máximo de $f_{b_m}(x_1, \ldots, x_{m-1})$ e seu coeficiente é α_b, por indução, temos $\alpha_b = 0$. ■

Definição 3.1.3 *Dado $m \geq 1$, seja D_m o subespaço vetorial de $\mathbb{K}\langle X\rangle$ gerado pelo conjunto de todos os polinômios*

$$c_1 c_2 \cdots c_m,$$

em que $c_i \in \mathbb{K}\langle X\rangle$ é um comutador de grau ≥ 2, para todo i. Denote

$$D'_m = \sum_{t=m}^{\infty} D_t$$

e $D_o = \mathbb{K}$.

Usando a igualdade

$$ab = ba + [a, b]$$

(ou o Teorema de Poincaré-Birkhoff-Witt), temos o seguinte lema:

Lema 3.1.4 *O espaço vetorial $\mathbb{K}\langle X\rangle$ é gerado pelo conjunto de todos os polinômios*

$$y_1^{a_1}\cdots y_s^{a_s}z_1^{b_1}\cdots z_s^{b_s}f_m,$$

em que $a_1,\cdots,a_s,b_1,\cdots,b_s\geq 0, s\geq 0, f_m\in D_m$ e $m\geq 0$.

Definição 3.1.5 *Um polinômio $f\in\mathbb{K}\langle X\rangle$ é chamado polinômio normal se uma das três alternativas abaixo ocorre:*

1) $f=[z_i,y_{i_1},\ldots,y_{i_s}]$, para alguns $z_i\in Z, y_{i_1},\ldots,y_{i_s}\in Y, s\geq 0$;

2) $f=[y_{i_1},\ldots,y_{i_s}]$, para alguns $y_{i_1},\ldots,y_{i_s}\in Y, s\geq 2$;

3) $f=[y_{i_1}^q-y_{i_1},\ldots,y_{i_s}]$, para alguns $y_{i_1},\ldots,y_{i_s}\in Y, s\geq 1$.

Note que, se $s=0$, então $[z_i,y_{i_1},\cdots,y_{i_s}]=z_i$ é um polinômio normal. Além disso, se $s=1$, então

$$[y_{i_1}^q-y_{i_1},\cdots,y_{i_s}]=y_{i_1}^q-y_{i_1}$$

é também um polinômio normal.

Definição 3.1.6 *Dado $m\geq 1$, seja N_m o subespaço vetorial de $\mathbb{K}\langle X\rangle$ gerado pelo conjunto de todos os polinômios*

$$c_1c_2\cdots c_m,$$

em que $c_i\in\mathbb{K}\langle X\rangle$ é um polinômio normal de grau ≥ 1, para todo i. Denote

$$N'_m=\sum_{t=m}^{\infty}N_t$$

e $N_0=\mathbb{K}$.

Lema 3.1.7 *O espaço vetorial $\mathbb{K}\langle X\rangle$ é gerado pelo conjunto de todos os polinômios*

$$y_1^{a_1}\cdots y_s^{a_s}f_m,$$

em que $0\leq a_1,\ldots,a_s<q,\ s\geq 0,\ f_m\in N_m$ e $m\geq 0$.

Demonstração: A prova será dividida em três afirmações.

Afirmação 1: Se $g\in N_m$, então $[g,x]\in N'_m$, para todo $x\in X$.

Suponha $g=c_1c_2\cdots c_m$, em que cada c_i é um polinômio normal. Pela igualdade $[uv,w]=u[v,w]+[u,w]v$, válida para qualquer álgebra associativa, temos

$$[g,x]=\sum_{i=1}^{m}c_1\cdots c_{i-1}[c_i,x]c_{i+1}\cdots c_m. \tag{3.1}$$

De fato, o caso $m = 1$ é trivial.

Suponha, agora, que

$$[c_1 \cdots c_{m-1}, x] = \sum_{i=1}^{m-1} c_1 \cdots c_{i-1}[c_i, x]c_{i+1} \cdots c_{m-1}, \ \forall x \in X, \ \forall c_1, \ldots, c_m \in N_1.$$

Dessa forma,

$$\begin{aligned}
[c_1 c_2 \cdots c_m, x] &= c_1[c_2 \cdots c_m, x] + [c_1, x]c_2 \cdots c_m \\
&= c_1\Big(\sum_{i=2}^{m} c_2 \cdots c_{i-1}[c_i, x]c_{i+1} \cdots c_m\Big) + [c_1, x]c_2 \cdots c_m \\
&= \sum_{i=2}^{m} c_1 c_2 \cdots c_{i-1}[c_i, x]c_{i+1} \cdots c_m + [c_1, x]c_2 \cdots c_m \\
&= \sum_{i=1}^{m} c_1 \cdots c_{i-1}[c_i, x]c_{i+1} \cdots c_m.
\end{aligned}$$

Utilizando a igualdade (3.1), temos:

i) Se $x \in Y$, então $c_1 \cdots c_{i-1}[c_i, x]c_{i+1} \cdots c_m \in N_m$ e, assim, $[g, x] \in N'_m$, uma vez que $[g, x] \in N_m \subset N'_m$.

ii) Se $x \in Z$, então

$$c_1 \cdots c_{i-1}[c_i, x]c_{i+i} \cdots c_m =$$

$$= c_1 \cdots c_{i-1}c_i x c_{i+1} \cdots c_m - c_1 \cdots c_{i-1}x c_i c_{i+1} \cdots c_m \in N_{m+1} \subseteq N'_m.$$

Assim, $[g, x] \in N'_m$.

Afirmação 2: Sejam $x_{i_1}, x_{i_2}, \cdots, x_{i_n} \in X$. Se $g = [x_{i_1}, x_{i_2}, \cdots, x_{i_s}]$, em que $s \geq 2$, então $g \in N'_1$.

Faremos indução em s. Para $s = 2$, temos:

- se $x_{i_1}, x_{i_2} \in Y$, pelo Caso 2 da Definição 3.1.5, temos o resultado;
- se $x_{i_1} \in Z$ e $x_{i_2} \in Y$, pelo Caso 1 da Definição 3.1.5, temos o resultado;
- se $x_{i_2} \in Z$ e $x_{i_1} \in Y$, então $[x_{i_1}, x_{i_2}] = -[x_{i_2}, x_{i_1}]$ e, pelo Caso 1 da Definição 3.1.5, temos o resultado;
- se $x_{i_2}, x_{i_1} \in Z$, então os dois são normais. Logo, $[x_{i_1}, x_{i_2}] \in N_2$.

Agora, por hipótese de indução, tomemos

$$g_1 = [x_{i_1}, \ldots, x_{s-1}] \in N_1' = \sum_{t=1}^{\infty} N_t.$$

Assim, $g_1 = \sum_j g_t$, com $g_j \in N_{t_j}$. Pela Afirmação 1,

$$[g_j, x_{i_s}] \in N_{t_j}' \subset N_1' \Longrightarrow g = \sum_j [g_j, x_{i_s}] \in N_1'.$$

Afirmação 3: Sejam $i_1 \leq \cdots \leq i_s$ e $s \geq 0$. Então o polinômio $(y^q - y)y_{i_1} \cdots y_{i_s}$ é uma combinação linear de polinômios

$$y_{j_1} \cdots y_{j_t}[y^q - y, y_{j_{t+1}}, \cdots, y_{j_s}],$$

em que $0 \leq t \leq s, j_1 \leq \cdots \leq j_t$ e $j_{t+1} \leq \cdots \leq j_s$.

A demonstração será por indução em s. Para $s = 0$, o resultado é trivial.

Por hipótese de indução, $(y^q - y)y_{i_1} \cdots y_{i_{s-1}}$ é uma combinação linear de polinômios

$$y_{j_1} \cdots y_{j_t}[y^q - y, y_{j_{t+1}}, \cdots, y_{j_{s-1}}],$$

em que $0 \leq t \leq s-1, j_1 \leq \cdots \leq j_t$ e $j_{t+1} \leq \cdots \leq j_{s-1}$. Em particular, $(y^q - y)y_{i_1} \cdots y_{i_{s-1}}y_{i_s}$ é uma combinação linear de polinômios

$$y_{j_1} \cdots y_{j_t}[y^q - y, y_{j_{t+1}}, \cdots, y_{j_{s-1}}]y_{i_s}.$$

Como

$$y_{j_1} \cdots y_{j_t}[y^q - y, y_{j_{t+1}}, \cdots, y_{j_{s-1}}]y_{i_s} =$$

$$y_{j_1} \cdots y_{j_t}y_{i_s}[y^q - y, y_{j_{t+1}}, \cdots, y_{j_{s-1}}] + y_{j_1} \cdots y_{j_t}[y^q - y, y_{j_{t+1}}, \cdots, y_{j_{s-1}}, y_{i_s}],$$

a afirmação está provada.

Agora, vamos provar o lema por meio das afirmações anteriores.

Pelo Lema 3.1.4, $\mathbb{K}\langle X\rangle$ é gerado, como espaço vetorial, por todos os polinômios

$$y_1^{a_1} \cdots y_s^{a_s} z_1^{b_1} \cdots z_s^{b_s} c_1 \cdots c_m,$$

em que $a_1, \cdots, a_s, b_1, \cdots, b_s \geq 0, s \geq 0, c_i \in D_1$, para todo i, $m \geq 0$.

Pela Afirmação 2,

$$c_1 \cdots c_m \in N_m'.$$

Todo z_i é um polinômio normal. Assim, $\mathbb{K}\langle X\rangle$ é gerado, como espaço vetorial, pelo conjunto de todos os polinômios

$$y_1^{a_1}\cdots y_s^{a_s}f_m,$$

em que $0 \leq a_1, \cdots, a_s, s \geq 0, f_m \in N_m, m \geq 0$.

Se $a_i \geq q$ para algum i, então

$$y_1^{a_1}\cdots y_i^{a_i}\cdots y_s^{a_s}f_m = y_1^{a_1}\cdots y_i^{a_i-q}(y_i^q - y_i + y_i)\cdots y_s^{a_s}f_m =$$
$$= \underbrace{y_1^{a_1}\cdots y_i^{a_i-q}(y_i^q - y_i)\cdots y_s^{a_s}f_m}_{u} + \underbrace{y_1^{a_1}\cdots y_i^{a_i-q+1}\cdots y_s^{a_s}f_m}_{v}.$$

Agora, aplicamos a Afirmação 3 no polinômio u e, se necessário, usamos um argumento análogo em v também. Após alguns passos, teremos o desejado. ■

Denote por $\mathrm{Sym}(s)$ o grupo de permutações de $\{1, \ldots, s\}$.

Lema 3.1.8 *Seja $z \in Z$ e $y, \bar{y} \in Y$. Se $\sigma \in Sym(s)$, então:*

a) $[z, y_{\sigma(1)}, \ldots, y_{\sigma(s)}] = [z, y_1, \ldots, y_s] + g$, *para algum* $g \in N_2'$.

b) $[y, \bar{y}, y_{\sigma(1)}, \ldots, y_{\sigma(s)}] = [y, \bar{y}, y_1, \ldots, y_s] + g$, *para algum* $g \in N_2'$.

c) $[y^q - y, y_{\sigma(1)}, \ldots, y_{\sigma(s)}] = [y^q - y, y_1, \ldots, y_s] + g$, *para algum* $g \in N_2'$.

Demonstração: Uma vez que toda permutação é um produto de transposições consecutivas, é suficiente considerar a transposição $\sigma = (t,\ t+1)$. Escreva

$$c = [\underbrace{u, y_1, \ldots, y_{t-1}}_{c'}, y_{t+1}, y_t, y_{t+2}, \ldots, y_s],$$

em que $u = z,\ u = [y, \bar{y}]$ ou $u = y^q - y$. Denote $c' = [u, y_1, \ldots, y_{t-1}]$. Note que

$$c = [c', y_{t+1}, y_t, y_{t+2}, \ldots, y_s].$$

Considere a Identidade de Jacobi

$$[x, y, z] = [x, [y, z]] + [x, z, y].$$

Façamos

$$c = [\underbrace{c'}_{x}, \underbrace{y_{t+1}}_{y}, \underbrace{y_t}_{z}, y_{t+2}, \ldots, y_s]$$

e, então,

$$\begin{aligned}
c &= [[c', y_{t+1}, y_t], y_{t+2}, \ldots, y_s] \\
&= [[c', [y_{t+1}, y_t]] + [c', y_t, y_{t+1}], y_{t+2}, \ldots, y_s] \\
&= [[c', [y_{t+1}, y_t]], y_{t+2}, \ldots, y_s] + [[c', y_t, y_{t+1}], y_{t+2}, \ldots, y_s] \\
&= -[[c', [y_t, y_{t+1}]], y_{t+2}, \ldots, y_s] + [[c', y_t, y_{t+1}], y_{t+2}, \ldots, y_s] \\
&= [[[y_t, y_{t+1}], c'], y_{t+2}, \ldots, y_s] + [[c', y_t, y_{t+1}], y_{t+2}, \ldots, y_s] \\
&= [y_t, y_{t+1}, c', y_{t+2}, \ldots, y_s] + [c', y_t, y_{t+1}, y_{t+2}, \ldots, y_s] \\
&= [c', y_t, y_{t+1}, y_{t+2}, \ldots, y_s] + \underbrace{[y_t, y_{t+1}, c', y_{t+2}, \ldots, y_s]}_{g}.
\end{aligned}$$

Afirmação: Se $x \in N_2'$ e $w_1, \ldots, w_n \in X$, então $[x, w_1, \ldots, w_n] \in N_2'$.

Para provar isso, faremos indução no número de variáveis n.

Primeiramente, vejamos o caso base $n = 1$, ou seja, se $x \in N_2'$ e $w \in X$, então $[x, w] \in N_2'$.

Se $x \in N_2'$, então x é combinação linear de

$$c_1 c_2 \cdots c_m,\ m \geq 2,$$

com c_i normal, para todo $1 \leq i \leq m$.

Façamos $v = c_1 \cdots c_m$. Já vimos, na afirmação 1 do Lema 3.1.7, que, a partir da igualdade

$$[ab, d] = a[b, d] + [a, d]b,$$

temos

$$[v, w] = \sum_{i=1}^{m} c_1 \cdots c_{i-1}[c_i, w]c_{i+1} \cdots c_m.$$

Note que, se $w \in Y$, como c_i é normal, então $[c_i, w]$ é normal. Logo, como também $c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_m$ são normais, segue que $[v, w] \in N_2'$.

Agora, se $w \in Z$, então, novamente pela afirmação 1 do Lema 3.1.7,

$$c_1 \cdots c_{i-1}[c_i, w]c_{i+1} \cdots c_m \in N_{m+1} \subset N_m' \subseteq N_2',\ m \geq 2.$$

Assim, $[v, w] \in N_2'$.

Dessa forma, como x é combinação linear de elementos do tipo $v = c_1 \cdots c_m$, temos $[x, w] \in N_2'$.

Agora, suponha, por hipótese de indução, que o resultado vale para $n-1$. Assim, estamos supondo que, se $x \in N_2'$ e $w_1, \ldots, w_{n-1} \in X$, então $[x, w_1, \ldots, w_{n-1}] \in N_2'$.

Seja $y = [x, w_1, \ldots, w_{n-1}]$. Desse modo, $[x, w_1, \ldots, w_{n-1}, w_n] = [y, w_n]$. Pela hipótese de indução, $y \in N_2'$. Dessa forma, pelo caso base, $[y, w_n] \in N_2'$.

Portanto, $[x, w_1, \ldots, w_n] \in N_2'$ e, consequentemente, concluímos a afirmação.

Agora, como

$$g = [y_t, y_{t+1}, c', y_{t+2}, \ldots, y_s] = [[y_t, y_{t+1}]c' - c'[y_t, y_{t+1}], y_{t+2}, \ldots, y_s]$$

e $[y_t, y_{t+1}]$ e c' são normais, então $[y_t, y_{t+1}]c',\ c'[y_t, y_{t+1}] \in N_2 \subset N_2'$. Dessa forma, utilizando a afirmação provada, $g = [y_t, y_{t+1}, c', y_{t+2}, \ldots, y_s] \in N_2'$ e, portanto, concluímos a demonstração. ■

Definição 3.1.9 *Um polinômio normal f é chamado de polinômio E-normal se ele for de uma das três formas abaixo:*

a) $f = [z_i, y_{i_1}, y_{i_2}, \ldots, y_{i_s}]$, *com* $i_1 \leq i_2 \leq \ldots \leq i_s$;

b) $f = [y_j, y_{i_1}, y_{i_2}, \ldots, y_{i_s}]$, *com* $j > i_1 \leq i_2 \leq \ldots \leq i_s$;

c) $f = [y_i^q - y_i, y_{i_1}, y_{i_2}, \ldots, y_{i_s}]$, *com* $i_1 \leq i_2 \leq \ldots \leq i_s$.

Definição 3.1.10 *Dado $m \geq 1$, seja E_m o subespaço vetorial de $\mathbb{K}\langle X\rangle$ gerado pelo conjunto de todos os polinômios*

$$c_1 c_2 \cdots c_m,$$

em que $c_i \in \mathbb{K}\langle X\rangle$ é um polinômio E-normal de grau ≥ 1, para todo i. Denote

$$E_m' = \sum_{t=m}^{\infty} E_t$$

e $E_0 = \mathbb{K}$.

Lema 3.1.11 $N_m \subseteq E_m + N_{m+1}'$.

Demonstração: Seja $f = [y_{i_1}, \ldots, y_{i_s}] \in N_1$. Pelo Lema 3.1.8,

$$f = [y_{j_1}, y_{j_2}, y_{j_3}, \ldots, y_{j_s}] \ \ (mod\ N_2'),$$

em que $i_1 = j_1,\ i_2 = j_2,\ j_3 \leq j_4 \leq \ldots \leq j_s$.

i) Se $j_2 = \min\{j_1, j_2, \ldots, j_s\}$, então $[y_{j_1}, y_{j_2}, y_{j_3}, \ldots, y_{j_s}] \in E_1$.

ii) Se $j_1 = \min\{j_1, j_2, \ldots, j_s\}$, então

$$[y_{j_1}, y_{j_2}, y_{j_3}, \ldots, y_{j_s}] = -[y_{j_2}, y_{j_1}, y_{j_3}, \ldots, y_{j_s}] \in E_1.$$

iii) Se $j_3 = \min\{j_1, j_2, \ldots, j_s\}$, pela Identidade de Jacobi, temos

$$[y_{j_1}, y_{j_2}, y_{j_3}, \ldots, y_{j_s}] = -[y_{j_2}, y_{j_3}, y_{j_1}, \ldots, y_{j_s}] + [y_{j_1}, y_{j_3}, y_{j_2}, \ldots, y_{j_s}].$$

Agora, aplicamos o Lema 3.1.8 em cada parcela do lado direito outra vez:

$$\begin{aligned}[y_{j_1}, y_{j_2}, y_{j_3}, \ldots, y_{j_s}] &= -[y_{j_2}, y_{j_3}, y_{j_1}, \ldots, y_{j_s}] + [y_{j_1}, y_{j_3}, y_{j_2}, \ldots, y_{j_s}] \\ &= \underbrace{-[y_{j_2}, y_{j_3}, y_{i_1}, y_{i_2}, \ldots, y_{i_{s-2}}]}_{\in E_1} + \underbrace{g_1}_{\in N_2'} + \underbrace{[y_{j_1}, y_{j_3}, y_{k_1}, y_{k_2}, \ldots, y_{k_{s-2}}]}_{\in E_1} + \underbrace{g_2}_{\in N_2'},\end{aligned}$$

com $i_1 \leq i_2 \leq \cdots \leq i_{s-2}$, $k_1 \leq k_2 \leq \cdots \leq k_{s-2}$ e $i_1, \ldots, i_{s-2}, k_1, , \ldots, k_{s-2} \in \{j_1, j_2, \ldots, j_s\}$.

Pelos três itens anteriores, provamos que $f \in E_1 + N_2'$, ou seja, $N_1 \subseteq E_1 + N_2'$. Logo,

$$N_m = \underbrace{N_1 \cdots N_1}_{m-vezes} \subseteq \underbrace{(E_1 + N_2') \cdots (E_1 + N_2')}_{m-vezes} \subseteq E_m + N_{m+1}'.$$

Para provarmos a última inclusão, faremos indução sobre m.

Para $m = 1$, temos $E_1 + N_2' \subseteq E_1 + N_2'$.

Agora, suponha que $(E_1 + N_2')^m \subset E_m + N_{m+1}'$. Dessa forma,

$$\begin{aligned}(E_1 + N_2')^{m+1} &= (E_1 + N_2')(E_1 + N_2')^m \subset (E_1 + N_2')(E_m + N_{m+1}') \\ &= E_1E_m + E_1N_{m+1}' + N_2'E_m + N_2'N_{m+1}'. \ \blacksquare\end{aligned}$$

Notação 3.1.12 *Se $f \in \mathbb{K}\langle X\rangle, y \in Y$ e $d \geq 1$, denotamos*

$$[f, y^{(d)}] = [f, \underbrace{y, y, \ldots, y}_{d\ fatores}].$$

Além disso, denotamos $[f, y^{(0)}] = f$.

Definição 3.1.13 *Um polinômio E-normal é chamado H-normal se ele for de uma das três formas abaixo:*

a) $f = [z_i, y_1^{(d_1)}, \ldots, y_s^{(d_s)}]$, *com* $0 \leq d_1, \ldots, d_s < q$.

b) $f = [y_j, y_1^{(d_1)}, \ldots, y_s^{(d_s)}]$, *com* $0 \leq d_1, \ldots, d_s < q$.

c) $f = [y_i^q - y_i, y_1^{(d_1)}, \ldots, y_s^{(d_s)}]$, *com* $0 \leq d_1, \ldots, d_s < q$.

Definição 3.1.14 *Dado $m \geq 1$, seja H_m o subespaço vetorial de $\mathbb{K}\langle X\rangle$ gerado pelo conjunto de todos os polinômios*

$$c_1 c_2 \cdots c_m,$$

em que $c_i \in \mathbb{K}\langle X\rangle$ é um polinômio H-normal de grau ≥ 1, para todo i. Denote

$$H'_m = \sum_{t=m}^{\infty} H_t$$

e $H_0 = \mathbb{K}$.

Lema 3.1.15 *Se $f \in \mathbb{K}\langle X\rangle$ e $y \in Y$, então*

$$[f, y^{(q)}] = [f, y^q].$$

Em particular,

$$[f, y^{(q)}] = [f, y^q - y] + [f, y].$$

Demonstração: Primeiramente, provaremos, por indução em m, que

$$[f, y^{(m)}] = \sum_{i=0}^{m} (-1)^i \binom{m}{i} y^i f y^{m-i}.$$

Para $m = 1$, temos

$$\begin{aligned}\sum_{i=0}^{1} (-1)^i \binom{1}{i} y^i f y^{1-i} &= (-1)^0 \binom{1}{0} y^0 f y^{1-0} + (-1)^1 \binom{1}{1} y^1 f y^{1-1} \\ &= fy - yf = [f, y] = [f, y^{(1)}].\end{aligned}$$

Suponha $m \geq 2$. Assim,

$$\begin{aligned}[f, y^{(m)}] = [f, y^{(m-1)}, y] &= [f, y^{(m-1)}]y - y[f, y^{(m-1)}] \\ &= \left(\sum_{i=0}^{m-1} \binom{m-1}{i} y^i f y^{m-1-i}\right) y + y\left(\sum_{i=0}^{m-1} (-1)^i \binom{m-1}{i} y^i f y^{m-1-i}\right. \\ &= \sum_{i=0}^{m-1} (-1)^i \binom{m-1}{i} y^i f y^{m-i} - \sum_{i=0}^{m-1} (-1)^i \binom{m-1}{i} y^{i+1} f y^{m-1-i} \\ &= f y^m + \sum_{i=1}^{m-1} (-1)^i \binom{m-1}{i} y^i f y^{m-i} - \underbrace{\sum_{i=0}^{m-1} (-1)^i \binom{m-1}{i} y^{i+1} f y^{m-1-i}}_{(\star)}.\end{aligned}$$

Em $(\star)$, façamos $j = i + 1$. Logo,

- quando $i = 0,\ j = 1$;

- quando $i = m-1,\ j = m$.

Então,

$$\sum_{i=0}^{m-1}(-1)^i\binom{m-1}{i}y^{i+1}fy^{m-1-i} = \sum_{j=1}^{m}(-1)^i\binom{m-1}{j-1}y^jfy^{m-j}.$$

Substituindo na expressão anterior, temos

$$\begin{aligned}
[f, y^{(m)}] =& fy^m + \sum_{i=1}^{m-1}(-1)^i y^i f y^{m-1} - \left(\sum_{i=1}^{m}(-1)^{i-1}\binom{m-1}{i-1}y^i f y^{m-i}\right)\\
=& fy^m + \sum_{i=1}^{m-1}(-1)^i y^i f y^{m-1} - \left(\sum_{i=1}^{m-1}(-1)^{i-1}\binom{m-1}{i-1}y^i f y^{m-i} + \right.\\
& \left.(-1)^{m-1}\binom{m-1}{m-1}y^m f y^{m-m}\right)\\
=& fy^m + \sum_{i=1}^{m-1}(-1)^i\binom{m-1}{i}y^i f y^{m-i} + \sum_{i=1}^{m-1}(-1)^i\binom{m-1}{i-1}y^i f y^{m-i} +\\
& (-1)^m y^m f\\
=& \sum_{i=0}^{m}(-1)^i\binom{m}{i}y^i f y^{m-i}.
\end{aligned}$$

Denote por p a característica do corpo $\mathbb{K}$. Daí, $q = |\mathbb{K}| = p^t$, para algum $t \geq 1$. Temos, pelo Lema 1.1.20,

$$\binom{q}{i} = 0, \text{ para todo } 1 \leq i \leq q-1.$$

Logo,

$$[f, y^{(q)}] = \sum_{i=0}^{q}(-1)^i\binom{q}{i}y^i f y^{q-i} = fy^q + (-1)^q y^q f = [f, y^q],$$

como queríamos demonstrar. ■

Lema 3.1.16 $E_m \subseteq H_m + N'_{m+1}$.

Demonstração: Primeiramente, provaremos que $E_1 \subseteq H_1 + N'_2$.
Seja $c = [z, y_1^{(d_1)}, \ldots, y_s^{(d_s)}] \in E_1$, em que $d_i \geq 0$, para todo i. Vamos provar, por indução em s, que $c \in H_1 + N'_2$.

O caso $s = 0$ é trivial.

Suponha $s \geq 1$. Por hipótese de indução, existem $f \in H_1$ e $g \in N'_2$ tais que

$$[z, y_1^{(d_1)}, \ldots, y_{s-1}^{(d_{s-1})}] = f + g,$$

ou seja,

$$c = [[z, y_1^{(d_1)}, \ldots, y_{s-1}^{(d_{s-1})}], y_s^{(d_s)}] = [f, y_s^{(d_s)}] + [g, y_s^{(d_s)}].$$

i) Se $d_s < q$, então $[f, y_s^{(d_s)}] \in H_1$ e $[g, y_s^{(d_s)}] \in N_2'$, pois, como

$$g \in N_2' = \sum_{t=2}^{\infty} N_t,$$

escrevemos $g = \sum_j g_j$, com $g_j \in N_{t_j},\ t_j \geq 2$. Pela afirmação 1 do Lema 3.1.7, temos

$$[g_j, y_s^{(d_s)}] \in N_{t_j}' \subseteq N_2'.$$

Assim,

$$[g, y_s^{(d_s)}] = \sum_j [g_j, y_s^{(d_s)}] \in N_2'.$$

Dessa forma, $c \in H_1 + N_2'$.

ii) Se $d_s \geq q$, pelo Lema 3.1.15, temos

$$\begin{aligned}
c =& [f, y_s^{(q)}, y_s^{(d_s-q)}] + [g, y_s^{(d_s)}] \\
=& [[f, y_s] + [f, y_s^q - y_s], y_s^{(d_s-q)}] + [g, y_s^{(s_s)}] \\
=& [f, y_s, y_s^{(d_s-q)}] + [f, y_s^q - y_s, y_s^{(d_s-q)}] + [g, y_s^{(d_s)}] \\
=& [f, y_s^{(d_s-q+1)}] + [f(y_s^q - y_s) - (y_s^q - y_s)f, y_s^{(d_s-q)}] + [g, y_s^{(d_s)}] \\
=& [f, y_s^{(d_s-q+1)}] + [f(y_s^q - y_s), y_s^{(d_s-q)}] - [(y_s^q - y_s)f, y_s^{(d_s-q)}] + [g, y_s^{(d_s)}] \\
=& [f, y_s^{(d_s-q+1)}] + [f, y_s^{(d_s-q)}](y_s^q - y_s) + f[y_s^q - y_s, y_s^{(d_s-q)}] + \\
& - [y_s^q - y_s, y_s^{(d_s-q)}]f - (y_s^q - y_s)[f, y_s^{(d_s-q)}] + [g, y_s^{(d_s)}].
\end{aligned}$$

Logo,

$$c = [f, y_s^{(d_s-q+1)}] + h,$$

em que

$$h = [f, y_s^{(d_s-q)}](y_s^q - y_s) + f[y_s^q - y_s, y_s^{(d_s-q)}]$$

$$-[y_s^q - y_s, y_s^{(d_s-q)}]f - (y_s^q - y_s)[f, y_s^{(d_s-q)}] + [g, y_s^{(d_s)}] \in N_2'.$$

Se $d_s - q + 1 \geq q$, repetimos o argumento na parcela $[f, y_s^{(d_s-q+1)}]$. Após alguns passos, vamos obter $c \in H_1 + N_2'$.

Se $c = [y_i^q - y_i, y_1^{(d_1)}, \ldots, y_s^{(d_s)}] \in E_1$, com $d_j \geq 0$, para todo j, com um argumento análogo ao outro caso vemos que $c \in H_1 + N_2'$.

Seja $c = [y_j, y_1^{(d_1)}, \ldots, y_s^{(d_s)}] \in E_1$, com $d_i \geq 0$, para todo i. Relembramos que $\deg(c) \geq 2$. Vamos provar, por indução em $s \geq 1$, que $c \in H_1 + N_2'$.

Se $s = 1$, ou seja, $c = [y_j, y_1^{(d_1)}]$, temos três casos a considerar:

i) Se $d_1 < q$, então $[y_j, y_1^{(d_1)}] \in H_1$.

ii) Se $d_1 = q$, pelo Lema 3.1.15, obtemos

$$c = [y_j, y_1^{(q)}] = [y_j, y_1] + [y_j, y_1^q - y_1] = [y_j, y_1] - [y_1^q - y_1, y_j].$$

Logo, $c \in H_1$.

iii) Se $d_1 > q$, pelo Lema 3.1.15 e pelo Lema 3.1.8 (c), temos

$$\begin{aligned}
c &= [y_j, y_1^{(d_1)}] = [y_j, y_1^{(q)}, y_1^{(d_1-q)}] = [[y_j, y_1^{(q)}], y_1^{(d_1-q)}] \\
&= [[y_j, y_1^q - y_1] + [y_j, y_1], y_1^{(d_1-q)}] \\
&= [[y_j, y_1^q - y_1], y_1^{(d_1-q)}] + [[y_j, y_1], y_1^{(d_1-q)}] \\
&= [y_j, y_1^{(d_1-q+1)}] - [y_1^q - y_1, y_j, y_1^{(d_1-q)}] \\
&= [y_j, y_1^{(d_1-q+1)}] - [y_1^q - y_1, y_1^{(d_1-q)}, y_j] + h_1 \\
&= [y_j, y_1^{(d_1-q+1)}] + h,
\end{aligned}$$

para alguns $h_1, h \in N_2'$. Se $d_1 - q + 1 \geq q$, repetimos o argumento ao somando $[y_j, y_1^{(d_1-q+1)}]$. Após alguns passos, vamos obter $c \in H_1 + N_2'$.

Logo, o caso $s = 1$ está provado. Os demais passos da indução são feitos de maneira análoga ao anterior.

Pelos casos vistos, provamos que $E_1 \subset H_1 + N_2'$. Dessa forma,

$$E_m = E_1 \cdots E_1 \subseteq (H_1 + N_2') \cdots (H_1 + N_2') \subseteq H_m + N_{m+1}'. \quad \blacksquare$$

Definição 3.1.17 *Um polinômio $H-$normal f é chamado $L-$normal se ele for de uma das três formas abaixo:*

a) $f = [z_i, y_1^{(d_1)}, \ldots, y_s^{(d_s)}]$, *com* $0 \leq d_1, \ldots, d_s < q$;

b) $f = [y_j, y_1^{(d_1)}, \ldots, y_j^{(d_j-1)}, \ldots, y_s^{(d_s)}]$, *com* $0 \leq d_1, \ldots, d_s < q$;

c) $f = [y_i^q - y_i, y_1^{(d_1)}, \ldots, y_{i-1}^{(d_i-1)}, y_{i+1}^{(d_i+1)}, \ldots, y_s^{(d_s)}]$, *com* $0 \leq d_1, \ldots, d_s < q$.

Com respeito à Definição 3.1.17, relembramos que:

- em a): $s \geq 0$;

- em b): $d_t \neq 0$, para algum $t \neq j$. Além disso, se $d_1 = d_2 = \cdots = d_{t-1} = 0$, então $j > t$, ou seja, o índice da variável que ocupa a primeira posição no comutador é maior do que o índice da variável que ocupa a segunda posição no comutador;

- em c): $s \geq 0$.

Definição 3.1.18 *Dado $m \geq 1$, seja L_m o subespaço vetorial de $\mathbb{K}\langle X\rangle$ gerado pelo conjunto de todos os polinômios*

$$c_1 c_2 \cdots c_m,$$

em que $c_i \in \mathbb{K}\langle X\rangle$ é um polinômio $L-$normal de grau ≥ 1, para todo i. Denote

$$L'_m = \sum_{t=m}^{\infty} L_t$$

e $L_0 = \mathbb{K}$.

Lema 3.1.19 *Seja A uma álgebra. Para quaisquer $a, b, y_1, y_2, \ldots, y_k \in A$, $[ab, y_1, y_2, \ldots\ y_k]$ é uma combinação linear de produtos*

$$[a, y_{i_1}, \ldots, y_{i_r}][b, y_{j_1}, \ldots, y_{j_s}],$$

com $i_1, \ldots, i_r, j_1, \ldots, j_s \in \{1, \ldots, k\}$. Quando $r = 0$ (respectivamente, $s = 0$), convencionamos que $[a] = a$ (respectivamente, $[b] = b$).

Demonstração: Faremos indução sobre k.

Para $k = 1$,

$$[ab, y_1] = a[b, y_1] + [a, y_1]b.$$

Seja, agora, $c = [ab, y_1, \ldots, y_k]$. Suponha, por hipótese de indução, que

$$c = \sum \alpha [a, y_{i_1}, \ldots, y_{i_r}][b, y_{j_1}, \ldots, y_{j_s}],$$

com $i_1, \ldots, i_r, j_1, \ldots, j_s \in \{1, \ldots, k\}$.

Note que

$$[ab, y_1, \ldots, y_{k+1}] = [c, y_{k+1}].$$

Assim,

$$\begin{aligned}\Big[\sum \alpha [a, y_{i_1}, \ldots, y_{i_r}][b, y_{j_1}, \ldots, y_{j_s}, y_{k+1}]\Big] &= \sum \alpha [[a, y_{i_1}, \ldots, y_{i_r}][b, y_{j_1}, \ldots, y_{j_s}], y_{k+1}] \\ &= \sum \alpha \Big([a, y_{i_1}, \ldots, y_{i_r}][b, y_{j_1}, \ldots, y_{j_s}, y_{k+1}] + \\ &\quad + [a, y_{i_1}, \ldots, y_{i_r}, y_{k+1}][b, y_{j_1}, \ldots, y_{j_s}] \Big).\end{aligned}$$

Portanto, temos o resultado. ■

Lema 3.1.20 $H_m \subseteq L_m + N'_{m+1}$.

Demonstração: Denote por

$$[x_{j_1}, \ldots, x_{j_{k-1}}, \widehat{x_{j_k}}, x_{j_{k+1}}, \ldots, x_{j_n}] = [x_{j_1}, \ldots, x_{j_{k-1}}, x_{j_{k+1}}, \ldots, x_n].$$

Seja $c = [y_j, y_1^{(d_1)}, \ldots, y_j^{(d_j)}, \ldots, y_s^{(d_s)}] \in H_1$, em que $0 \leq d_i < q$, para todo i. Provaremos que $c \in L_1 + N'_2$.

i) Se $d_j < q-1$, então $c \in L_1$.

ii) Suponha que $d_j = q-1$. Nesse caso, temos $c = [y_j, y_1^{(d_1)}, \ldots, y_j^{(q-1)}, \ldots, y_s^{(d_s)}]$. Sem perda de generalidade, podemos supor $d_1 \neq 0$. Pelos Lemas 3.1.8 e 3.1.15, existe $g \in N'_2$ tal que:

$$\begin{aligned}
c &= + [y_j, y_1, y_j^{(q-1)}, y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, \widehat{y_j^{(q-1)}}, \ldots, y_s^{(d_s)}] + g \\
&= - [y_1, y_j^{(q)}, y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, \widehat{y_j^{(q-1)}}, \ldots, y_s^{(d_s)}] + g \\
&= - [y_1, y_j, y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, \widehat{y_j^{(q-1)}}, \ldots, y_s^{(d_s)}] + \\
&\quad - [y_1, y_j^q - y_j, y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, \widehat{y_j^{(q-1)}}, \ldots, y_s^{(d_s)}] + g \\
&= + [y_j, y_1^{(d_1)}, y_2^{(d_2)}, \ldots, \widehat{y_j^{(q-1)}}, \ldots, y_s^{(d_s)}] + \\
&\quad + [y_j^q - y_j, y_1^{(d_1)}, y_2^{(d_2)}, \ldots, \widehat{y_j^{(q-1)}}, \ldots, y_s^{(d_s)}] + g.
\end{aligned}$$

Logo, $c \in L_1 + N'_2$.

Agora, seja $c = [y_i^q - y_i, y_1^{(d_1)}, \ldots, y_i^{(d_i)}, \ldots, y_s^{d_s)}]$, em que $0 \leq d_i < q$, para todo i. Provaremos que $c \in L_1 + N'_2$.

i) Se $d_i = 0$, então $c \in L_1$.

ii) Suponha $d_i \neq 0$. Sem perda de generalidade, podemos supor $d_1 \neq 0$. Pelo Lema 3.1.8 e pela Identidade de Jacobi, existe $g \in N'_2$ tal que

$$\begin{aligned}
c &= + [y_i^q - y_i, y_1, y_i, y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, y_i^{(d_i-1)}, \ldots, y_s^{(d_s)}] + g \\
&= + [y_i, y_1, y_i^q - y_i, y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, y_i^{(d_i-1)}, \ldots, y_s^{(d_s)}] + g \\
&= + [[y_i, y_1](y_i^q - y_i), y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, y_i^{(d_i-1)}, \ldots, y_s^{(d_s)}] \\
&\quad - [(y_i^q - y_i)[y_i, y_1], y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, y_i^{(d_i-1)}, \ldots, y_s^{(d_s)}] + g.
\end{aligned}$$

Pelo Lema 3.1.19, $[ab, y_{l_1}, y_{l_2}, \ldots, y_{l_r}]$ é igual a uma combinação linear de produtos $[a,\ldots][b,\ldots]$. Assim,

$$+ [[y_i, y_1](y_i^q - y_i), y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, y_i^{(d_i-1)}, \ldots, y_s^{(d_s)}]$$
$$- [(y_i^q - y_i)[y_i, y_1], y_1^{(d_1-1)}, y_2^{(d_2)}, \ldots, y_i^{(d_i-1)}, \ldots, y_s^{(d_s)}] \in N_2'.$$

Logo, $c \in N_2'$.

Agora, seja $c = [z_i, y_1^{(d_1)}, \ldots, y_s^{(d_s)}] \in H_1$. Nesse caso, $c \in L_1$.
Provamos que $H_1 \subseteq L_1 + N_2'$. Portanto,

$$H_m = H_1 \cdots H_1 \subseteq (L_1 + N_2') \cdots (L_1 + N_2') \subseteq L_m + N_{m+1}'. \ \blacksquare$$

3.2 O Teorema Principal

Nosso objetivo, agora, é descrever explicitamente uma base para o T_G-ideal das identidades polinomiais graduadas de UT_n, para qualquer graduação elementar fixada.

Lema 3.2.1 *Seja*

$$\Omega = \{y_{(i,j)}^l; l \geq 1 \ e \ 1 \leq i \leq j \leq n\} \cup \{z_{(i,j)}^l; \ l \geq 1 \ e \ 1 \leq i \leq j \leq n\}$$

um conjunto infinito de variáveis, e denote por $\mathbb{K}[\Omega]$ a álgebra comutativa livre, livremente gerada por Ω sobre $\mathbb{K}$. Se

$$Y_l = \sum_{i=1}^{n} y_{(i,i)}^l e_{(i,i)} + \sum_{i=1}^{n-1} y_{(i,i+1)}^l e_{(i,i+1)} \quad e \quad Z_l = \sum_{i=1}^{n-1} z_{(i,i+1)}^l e_{(i,i+1)}$$

são elementos de $UT_n(\mathbb{K}[\Omega])$, então

a) $[Z_l, Y_1, \ldots, Y_s] = \sum_{i=1}^{n-1} \left(z_{(i,i+1)}^l \prod_{t=1}^{s} \left(y_{(i+1,i+1)}^t - y_{(i,i)}^t \right) \right) e_{(i,i+1)} + u;$

b) $[Y_l, Y_1, \ldots, Y_s] = \sum_{i=1}^{n-1} \Big((y_{(i,i+1)}^l y_{(i+1,i+1)}^1 + y_{(i,i)}^l y_{(i,i+1)}^1 - y_{(i,i+1)}^1 y_{(i+1,i+1)}^l - y_{(i,i)}^1 y_{(i,i+1)}^l) \times$
$\prod_{t=2}^{s} (y_{(i+1,i+1)}^t - y_{(i,i)}^t) \Big) e_{(i,i+1)} + v;$

c) $[Y_l^q - Y_l, Y_1, \ldots, Y_s] = \sum_{i=1}^{n-1} \Big(\Big(y_{(i,i+1)}^l \big(\sum_{t=0}^{q-1} (y_{(i,i)}^l)^t (y_{(i+1,i+1)}^l)^{q-1-t} - 1 \big) \Big) \times$
$\times \prod_{t=1}^{s} (y_{(i+1,i+1)}^t - y_{(i,i)}^t) \Big) e_{(i,i+1)} + w,$

em que u, v e w são combinações lineares de matrizes $e_{(i,j)}$, com coeficientes em $\mathbb{K}[\Omega]$, tais que $j - i \geq 2$.

Demonstração: Provaremos o item a) por indução em s.

Se $s = 1$, então

$$
\begin{aligned}
[Z_l, Y_1] &= \left[\sum_{i=1}^{n-1} z^l_{(i,i+1)}e_{(i,i+1)}, \sum_{i=1}^{n} y^1_{(i,i)}e_{(i,i)} + \sum_{i=1}^{n-1} y^1_{(i,i+1)}e_{(i,i+1)}\right] \\
&= \left[\sum_{i=1}^{n-1} z^l_{(i,i+1)}e_{(i,i+1)}, \sum_{i=1}^{n} y^1_{(i,i)}e_{(i,i)}\right] + \underbrace{\left[\sum_{i=1}^{n-1} z^l_{(i,i+1)}e_{(i,i+1)}, \sum_{i=1}^{n-1} y^1_{(i,i+1)}e_{(i,i+1)}\right]}_{u'} \\
&= \left[\sum_{i=1}^{n-1} z^l_{(i,i+1)}e_{(i,i+1)}, \sum_{i=1}^{n} y^1_{(i,i)}e_{(i,i)}\right] + u' \\
&= [z^l_{(1,2)}e_{(1,2)} + z^l_{(2,3)}e_{(2,3)} + \cdots + z_{(n-1,n)}e_{(n-1,n)}, \sum_{i=1}^{n} y^1_{(i,i)}e_{(i,i)}] \\
&= [z^l_{(1,2)}, \sum_{i=1}^{n} y^1_{(i,i)}e_{(i,i)}] + \cdots + [z^l_{(n-1,n)}e_{(n-1,n)}, \sum_{i=1}^{n} y^1_{(i,i)}e_{(i,i)}] + u' \\
&= [z^l_{(1,2)}e_{(1,2)}, y^1_{(1,1)}e_{(1,1)} + y^1_{(2,2)}e_{(2,2)} + \cdots + y^1_{(n,n)}e_{(n,n)}] + \cdots + \\
&\quad [z^l_{(n-1,n)}e_{(n-1,n)}, y^1_{(1,1)}e_{(1,1)} + \cdots + y^1(n-1,n-1)e_{(n-1,n-1} + y^1_{(n,n)}e_{(n,n)}] + u' \\
&= (z^l_{(1,2)}e_{(1,2)})(y^1_{(1,1)}e_{(1,1)} + y^1_{(2,2)}e_{(2,2)} + \cdots + y^1_{(n,n)}e_{(n,n)}) - \\
&\quad (y^1_{(1,1)}e_{(1,1)} + y^1_{(2,2)}e_{(2,2)} + \cdots + y^1_{(n,n)}e_{(n,n)})(z^l_{(1,2)}e_{(1,2)}) + \cdots + \\
&\quad (z^l_{(n-1,n)}e_{(n-1,n)})(y^1_{(1,1)}e_{(1,1)} + \cdots + y^1_{(n-1,n-1)}e_{(n-1,n-1)} + y^1_{(n,n)}e_{(n,n)}) - \\
&\quad (y^1_{(1,1)}e_{(1,1)} + \cdots + y^1_{(n-1,n-1)}e_{(n-1,n-1)} + y^1_{(n,n)}e_{(n,n)})(z^l_{(n-1,n)}e_{(n-1,n)}) \\
&= z^l_{(1,2)}e_{(1,2)}y^1_{(2,2)}e_{(2,2)} - y^1_{(1,1)}e_{(1,1)}z^l_{(1,2)}e_{(1,2)} + \cdots + z^l_{(n-1,n)}e_{(n-1,n)}y^1_{(n,n)}e_{(n,n)} - \\
&\quad y^1_{(n-1,n-1)}e_{(n-1,n-1)}z^l_{(n-1,n)}e_{(n-1,n)} + u' \\
&= z^l_{(1,2)}y^1_{(2,2)}e_{(1,2)}e_{(2,2)} - y^1_{(1,1)}z^l_{(1,2)}e_{(1,1)}e_{(1,2)} + \cdots + z^l_{(n-1,n)}y^1_{(n,n)}e_{(n-1,n)}e_{(n,n)} - \\
&\quad y^1_{(n-1,n-1)}z^l_{(n-1,n)}e_{(n-1,n-1)}e_{(n-1,n)} + u' \\
&= z^l_{(1,2)}y^1_{(2,2)}e_{(1,2)} - y^1_{(1,1)}z^l_{(1,2)}e_{(1,2)} + \cdots + z^l_{(n-1,n)}y^1_{(n,n)}e_{(n-1,n)} - \\
&\quad y^1_{(n-1,n-1)}z^l_{(n-1,n)}e_{(n-1,n)} + u' \\
&= z^l_{(1,2)}y^1_{(2,2)}e_{(1,2)} - z^l_{(1,2)}y^1_{(1,1)}e_{(1,2)} + \cdots + z^l_{(n-1,n)}y^1_{(n,n)}e_{(n-1,n)} - \\
&\quad z^l_{(n-1,n)}y^1_{(n-1,n-1)}e_{(n-1,n)} + u' \\
&= z^l_{(1,2)}(y^1_{(2,2)} - y^1_{(1,1)})e_{(1,2)} + \cdots + z^l_{(n-1,n)}(y^1_{(n,n)} - y^1_{(n-1,n-1)})e_{(n-1,n)} + u' \\
&= \sum_{i=1}^{n-1}(z^l_{(i,i+1)}(y^1_{(i+1,i+1)} - y^1_{(i,i)}))e_{(i,i+1)} + u'.
\end{aligned}
$$

em que u' é combinação linear de matrizes $e_{(i,j)}$, com coeficientes em $\mathbb{K}[\Omega]$, tais que $j - i \geq 2$.

Suponha, por hipótese de indução, que

$$[Z_l, Y_1, \ldots, Y_{s-1}] = \sum_{i=1}^{n-1} \big(z^l_{(i,i+1)} \prod_{t=1}^{s-1} (y^t_{(i+1,i+1)} - y^t_{(i,i)}\big) e_{(i,i+1)} + u'',$$

em que u'' é combinação linear de matrizes $e_{(i,j)}$, com coeficientes em $\mathbb{K}[\Omega]$, tais que $j - i \geq 2$. Escreva $g^t_i = y^t_{(i+1,i+1)} - y^t_{(i,i)}$. Então,

$$\begin{aligned}
[[Z_l, Y_1, \ldots, Y_{s-1}], Y_s] &= \left[\sum_{i=1}^{n-1} \left(z^l_{(i,i+1)} \prod_{t=1}^{s-1} g^t_i \right) e_{(i,i+1)} + u'', \sum_{i=1}^{n} y^s_{(i,i)} e_{(i,i)} + \sum_{i=1}^{n-1} y^s_{(i,i+1)} e_{(i,i+1)} \right] \\
&= \left[\sum_{i=1}^{n-1} \left(z^l_{(i,i+1)} \prod_{t=1}^{s-1} g^t_i \right) e_{(i,i+1)}, \sum_{i=1}^{n} y^s_{(i,i)} e_{(i,i)} \right] + \\
&+ \left[\sum_{i=1}^{n-1} \left(z^l_{(i,i+1)} \prod_{t=1}^{s-1} g^t_i \right) e_{(i,i+1)}, \sum_{i=1}^{n-1} y^s_{(i,i+1)} e_{(i,i+1)} \right] + \\
&+ \left[u'', \sum_{i=1}^{n} y^s_{(i,i)} e_{(i,i)} + \sum_{i=1}^{n-1} y^s_{(i,i+1)} e_{(i,i+1)} \right] \\
&= \left[\sum_{i=1}^{n-1} \left(z^l_{(i,i+1)} \prod_{t=1}^{s-1} g^t_i \right) e_{(i,i+1)}, \sum_{i=1}^{n} y^s_{(i,i)} e_{(i,i)} \right] + u \\
&= \sum_{i=1}^{n-1} \left[\left(z^l_{(i,i+1)} \prod_{t=1}^{s-1} g^t_i \right) e_{(i,i+1)}, \sum_{i=1}^{n} y^s_{(i,i)} e_{(i,i)} \right] + u \\
&= \sum_{i=1}^{n-1} \left(z^l_{(i,i+1)} \prod_{t=1}^{s} g^t_i \right) e_{(i,i+1)} + u,
\end{aligned}$$

em que u é combinação linear de matrizes $e_{(i,j)}$, com coeficientes em $\mathbb{K}[\Omega]$, tais que $j-i \geq 2$.

Também provaremos o item b) por indução em s. Se $s = 1$, então,

$$\begin{aligned}
[Y_l, Y_1] &= \left[\sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)} + \sum_{i=1}^{n-1} y^l_{(i,i+1)} e_{(i,i+1)}, \sum_{i=1}^{n} y^1_{(i,i)} e_{(i,i)} + \sum_{i=1}^{n-1} y^1_{(i,i+1)} e_{(i,i+1)} \right] \\
&= \left[\sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)}, \sum_{i=1}^{n-1} y^1_{(i,i+1)} e_{(i,i+1)} \right] + \left[\sum_{i=1}^{n-1} y^l_{(i,i+1)} e_{(i,i+1)}, \sum_{i=1}^{n} y^1_{(i,i)} e_{(i,i)} \right] + \\
&+ \underbrace{\left[\sum_{i=1}^{n-1} y^l_{(i,i+1)} e_{(i,i+1)}, \sum_{i=1}^{n-1} y^1_{(i,i+1)} e_{(i,i+1)} \right]}_{v'} \\
&= \sum_{i=1}^{n-1} (y^l_{(i,i)} y^1_{(i,i+1)} - y^l_{(i,i+1)} y^1_{(i+1,i+1)}) e_{(i,i+1)} + \\
&+ \sum_{i=1}^{n-1} (y^l_{(i,i+1)} y^1_{(i+1,i+1)} - y^l_{(i,i)} y^1_{(i,i+1)}) e_{(i,i+1)} + v' \\
&= \sum_{i=1}^{n-1} (y^l_{(i,i)} y^1_{(i,i+1)} - y^l_{(i,i+1)} y^1_{(i+1,i+1)} + y^l_{(i,i+1)} y^1_{(i+1,i+1)} - y^l_{(i,i)} y^1_{(i,i+1)}) e_{(i,i+1)} + v',
\end{aligned}$$

em que v' é combinação linear de matrizes $e_{(i,j)}$, com coeficientes em $\mathbb{K}[\Omega]$, tais que $j-i \geq 2$. Provamos que o caso $s=1$ é verdadeiro. Agora, utilizando a hipótese de indução e um argumento análogo ao item a), é possível provar a veracidade do item b) de maneira análoga.

O item c) também possui uma verificação análoga às dos outros itens. ■

Corolário 3.2.2 *Seja*

$$\Omega = \{y^l_{(i,j)}; l \geq 1 \text{ e } 1 \leq i \leq j \leq n\} \cup \{z^l_{(i,j)};\ l \geq 1 \text{ e } 1 \leq i \leq j \leq n\}$$

um conjunto infinito de variáveis, e denote por $\mathbb{K}[\Omega]$ a álgebra comutativa livre, livremente gerada por Ω sobre $\mathbb{K}$. Se

$$Y_l = \sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)} + \sum_{i=1}^{n-1} y^l_{(i,i+1)} e_{(i,i+1)} \quad e \quad Z_l = \sum_{i=1}^{n-1} z^l_{(i,i+1)} e_{(i,i+1)}$$

são elementos de $UT_n(\mathbb{K}[\Omega])$, então

a) $[Z_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}] = \sum_{i=1}^{n-1} \left(z^l_{(i,i+1)} \prod_{t=1}^{s} (y^t_{(i+1,i+1)} - y^t_{(i,i)})^{d_t} \right) e_{(i,i+1)} + u;$

b) $[Y_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}] = \sum_{i=1}^{n-1} \big((y^l_{(i,i+1)} y^1_{(i+1,i+1)} + y^l_{(i,i)} y^1_{(i,i+1)} - y^1_{(i,i+1)} y^l_{(i+1,i+1)} - y^1_{(i,i)} y^l_{(i,i+1)})$
$(y^1_{(i+1,i+1)} - y^1_{(i,i)})^{d_1 - 1} \times \prod_{t=2}^{s} (y^t_{(i+1,i+1)} - y^t_{(i,i)})^{d_t} \big) e_{(i,i+1)} + v;$

c) $[Y_l^q - Y_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}] = \sum_{i=1}^{n-1} \Big(y^l_{(i,i+1)} (\sum_{t=0}^{q-1} (y^l_{(i,i)})^t (y^l_{(i+1,i+1)})^{q-1-t} - 1) \times$
$\times \prod_{t=1}^{s} (y^t_{(i+1,i+1)} - y^t_{(i,i)})^{d_t} \Big) e_{(i,i+1)} + w,$

em que u, v e w são combinações lineares de matrizes $e_{(i,j)}$, com coeficientes em $\mathbb{K}[\Omega]$, tais que $j-i \geq 2$.

Tendo estabelecido as ferramentas e os lemas necessários nas seções anteriores, estamos, agora, em posição de apresentar o resultado central deste trabalho. O teorema a seguir representa o objetivo para o qual convergiram todos os nossos esforços teóricos até aqui.

Teorema 3.2.3 *Seja G um grupo e seja $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n) \in G^n$. Se $\mathbb{K}$ é um corpo finito de q elementos, então:*

a) $T_G(UT_n, \varepsilon)$ é gerado, como um T_G-ideal, pelo conjunto de todos os $\eta-$polinômios, em que $\eta = (\eta_1, \ldots, \eta_m)$ é $\varepsilon-$ruim e $m \leq n$.

b) A álgebra quociente $\frac{\mathbb{K}\langle X\rangle}{T_G(UT_n,\varepsilon)}$ tem uma base, como espaço vetorial, formada pelo conjunto de todos os polinômios $u + T_G(UT_n, \varepsilon)$, em que

$$u = y_1^{a_1} \cdots y_s^{a_s} c_1 c_2 \cdots c_m,$$

$0 \leq a_1, \ldots, a_s < q$, $s \geq 0$, $c_1, \ldots, c_m$ são polinômios $L-$normais de grau ≥ 1, $0 \leq m \leq n-1$ e $(\deg_G(c_1), \ldots, \deg_G(c_m))$ é $\varepsilon-$boa.

Demonstração: Seja $I(\varepsilon)$ o T_G-ideal de $\mathbb{K}\langle X\rangle$ gerado pelo conjunto de todos os $\eta-$polinômios, em que $\eta=(\eta_1,\ldots,\eta_m)$ é $\varepsilon-$ruim e $m\leq n$.

Pelo Lema 2.0.10, temos $I(\varepsilon)\subseteq T_G(UT_n,\varepsilon)$. Vamos mostrar a outra inclusão.

Afirmação 1: Se $c_1,\ldots,c_m$ são polinômios normais e $\eta=(\deg_G(c_1),\ldots,\deg_G(c_m))$ é $\varepsilon-$ruim, então $c=c_1\cdots c_m\in I(\varepsilon)$.

Para cada $j=1,\ldots,m$, denote $\eta_j=\deg_G(c_j)$. Defina c_j' como segue:

a) Se $\eta_j\neq 1$, então $c_j'=x_j^{\eta_j}$.

b) Seja $\eta_j=1$. Se $c_j=y_j^q-y_j$, para cada j, então $c_j'=y_{2j}^q-y_{2j}$. Caso contrário, $c_j=[y_{2j},y_{2j+1}]$.

Então, $c=c_1\cdots c_m$ é consequência de $c'=c_1'\cdots c_m'$. Se $m\leq n$, então c' é um $\eta-$polinômio e $(\deg_G(c_1'),\ldots,\deg_G(c_m'))=\eta$ é $\varepsilon-$ruim. Assim, $c'\in I(\varepsilon)$ e, consequentemente, $c\in I(\varepsilon)$. Se $m\geq n+1$, então c' é consequência de $c''=c_1'\cdots c_n'$ e $(\deg_G(c_1'),\ldots,\deg_G(c_n'))$ é $\varepsilon-$ruim. Assim, $c''\in I(\varepsilon)$ e, consequentemente, $c\in I(\varepsilon)$.

Afirmação 2: $N_n'\subseteq I(\varepsilon)$.

Seja $c=c_1\cdots c_m$, em que $c_1,\ldots,c_m$ são polinômios normais e $m\geq n$. Como o índice de nilpotência do radical de Jacobson de UT_n é n, $\eta=(\deg_G(c_1),\ldots,\deg_G(c_m))$ é $\varepsilon-$ruim e, pela Afirmação 1, obtemos $c\in I(\varepsilon)$.

Pelos Lemas 3.1.11, 3.1.16 e 3.1.20, temos

$$\begin{aligned}N_m&\subseteq E_m+N_{m+1}'\\&\subseteq H_m+N_{m+1}'\\&\subseteq L_m+N_{m+1}'.\end{aligned}$$

Assim, pela Afirmação 2, obtemos

$$\begin{aligned}N_0+N_1+\cdots+N_{n-1}+N_n'&\subseteq (L_0+\underbrace{N_1'}_{N_1'})+N_1+\cdots+N_{n-1}+N_n'\\&=L_0+N_1+\cdots+N_{n-1}+N_n'\\&\subseteq L_0+(L_1+\underbrace{N_2'}_{N_2'})+N_2+\cdots+N_{n-1}+N_n'\\&=L_0+L_1+N_2+\cdots+N_{n-1}+N_n'\\&\vdots\\&\subseteq L_0+L_1+\cdots+L_{n-1}+N_n'\\&\subseteq L_0+L_1+\cdots+L_{n-1}+I(\varepsilon).\end{aligned}$$

Logo, pelo Lema 3.1.7, segue que $\dfrac{\mathbb{K}\langle X\rangle}{I(\varepsilon)}$ é gerado, como espaço vetorial, pelo conjunto de todos os polinômios $u + I(\varepsilon)$, em que

$$u = y_1^{a_1} \cdots y_s^{a_s} c_1 c_2 \cdots c_m, \tag{3.2}$$

$0 \leq a_1, \cdots, a_s < q,\ s \geq 0,\ c_1, \ldots, c_m$ são polinômios $L-$normais de grau $\geq 1,\ 0 \leq m \leq n-1$ e, pela contrapositiva da Afirmação 1, $(\deg_G(c_1), \ldots, \deg_G(c_m))$ é $\varepsilon-$boa.

Afirmação 3: O conjunto de todos os elementos $u + T_G(UT_n, \varepsilon)$, em que u é dado por (3.2), é um subconjunto linearmente independente de $\dfrac{\mathbb{K}\langle X\rangle}{T_G(UT_n, \varepsilon)}$.

Seja

$$f = \sum_a \alpha_a y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} + \sum_{(a,c)} \alpha_{(a,c)} y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} c \in T_G(UT_n, \varepsilon),$$

em que $c = c_1 \cdots c_m,\ a = (a_1, \ldots, a_s),\ 0 \leq a_1, \ldots, a_s < q,\ s \geq 0,\ c_1, \ldots, c_m$ são polinômios $L-$normais de grau $\geq 1,\ 1 \leq m \leq n-1,\ \alpha_a \in \mathbb{K},\ \alpha_{(a,c)} \in \mathbb{K}$ e $(\deg_G(c_1), \ldots, \deg_G(c_m))$ é $\varepsilon-$boa. Devemos provar que cada coeficiente é zero. Nossa prova será por indução em n.

Para $n = 1$,

$$f = \sum_a \alpha_a y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} \in T_G(UT_n, \varepsilon).$$

Como $UT_1 \simeq \mathbb{K}$, então $T_G(UT_1, \varepsilon) = T_G(\mathbb{K}) = T(\mathbb{K})$. Dessa forma, como $0 \leq a_1, \ldots, a_s < q$, pelo Lema 3.1.2, obteremos $\alpha_a = 0$, para cada a.

Para $n \geq 2$, seja $R_l = \text{span}\{e_{i,j}; 1 \leq i \leq j \leq n, i \neq l \text{ e } j \neq l\}$. Já vimos no Exemplo 1.4.15 que R_l é isomorfa como álgebra graduada à UT_{n-1} com respeito à graduação elementar

$$\overline{\varepsilon}_l = (\varepsilon_1, \ldots, \varepsilon_{l-1}, \varepsilon_{l+1}, \ldots, \varepsilon_n).$$

Assim, para cada $l = 1, \ldots n$, obtemos

$$f \in T_G(UT_n, \varepsilon) \subseteq T_G(UT_{n-1}, \overline{\varepsilon_l}).$$

Seja $g = \alpha_{(a,c)} y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} c_1 c_2 \ldots c_m$ uma parcela de f e assuma $m \leq n-2$. Como a sequência associada $\overline{\eta}_g = (\deg_G(c_1), \ldots, \deg_G(c_m))$ é $\varepsilon-$boa, existe uma sequência de m matrizes elementares

$$\left(e_{(r_1,r_2)}, e_{(r_2,r_3)}, \ldots, e_{(r_{m-1},r_m)}, e_{(r_m,r_{m+1})}\right)$$

no radical de Jacobson de UT_n tal que

$$\deg_G\left(e_{(r_i,r_{i+1})}\right) = \deg_G(c_i).$$

Como $m+1 \leq n-1$, existe $1 \leq l \leq n$ tal que todas essas matrizes estão em R_l. Assim, $\overline{\eta}_g$ é uma sequência $\overline{\varepsilon}_l-$boa com respeito à $G-$graduação de UT_{n-1} induzida por $\overline{\varepsilon}_l$. Para cada $1 \leq l \leq n$, seja

$$f_l = \sum \alpha_{(a,c)} y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} c$$

a componente de f dada pelas parcelas $g = \alpha_{(a,c)} y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} c$ tais que a sequência correspondente $\overline{\eta}_g$ é $\overline{\varepsilon}_l-$boa. Assim, podemos decompor f da seguinte maneira

$$f = \Big(\sum_a \alpha_a y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} + f_l\Big) + f',$$

em que f' é a soma de todos os $g = \alpha_{(a,c)} y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} c$ tais que a sequência correspondente $\overline{\eta}_g$ é $\overline{\varepsilon}_l-$ruim. Como $f' \in T_G(UT_{n-1}, \overline{\varepsilon}_l)$, obtemos

$$\Big(\sum_a \alpha_a y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} + f_l\Big) \in T_G(UT_{n-1}, \overline{\varepsilon}_l),$$

para todo $1 \leq l \leq n$. Por hipótese de indução, temos $\alpha_a = 0$, para todo a, e $\alpha_{(a,c)} = 0$, para todo (a,c) aparecendo em f_l. Como l é arbitrário, obtemos que $\alpha_{(a,c)} = 0$, para todo (a,c) tal que $c = c_1 \cdots c_m$ e $m \leq n-2$, $\alpha_a = 0$, para todo a. Assim,

$$f = \sum_{(a,c)} \alpha_{(a,c)} y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} c_1 c_2 \cdots c_{n-1}, \tag{3.3}$$

em que $f \in T_G(UT_n, \varepsilon)$, $0 \leq a_1, \ldots, a_s < q$ são polinômios $L-$normais de grau ≥ 1 e $(\deg_G(c_1), \ldots, \deg_G(c_{n-1}))$ é $\varepsilon-$boa.

Como existe uma única sequência $\varepsilon-$boa $\overline{\eta} = (\eta_1, \ldots, \eta_{n-1})$, temos

$$\eta_i = \deg_G(e_{(i,i+1)}) = \deg_G(c_i),$$

para todo i e $c = c_1 c_2 \ldots c_{n-1}$ que aparece em (3.3).

Seja $\Omega = \{y^l_{(i,j)}; l \geq 1 \text{ e } 1 \leq i \leq j \leq n\} \cup \{z^l_{(i,j)};\ l \geq 1 \text{ e } 1 \leq i \leq j \leq n\}$ um conjunto de variáveis comutativas independentes.

Denote

$$Y_l = \sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)} + \sum_{i=1}^{n-1} y^l_{(i,i+1)} e_{(i,i+1)} \quad \text{e} \quad Z_l = \sum_{i=1}^{n-1} z^l_{(i,i+1)} e_{(i,i+1)}$$

como no Lema 3.2.1.

Já vimos, no Corolário 3.2.2, que

$$\left[Z_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}\right] = \sum_{i=1}^{n-1} \left(z^l_{(i,i+1)} \prod_{t=1}^{s} (y^t_{(i+1,i+1)} - y^t_{(i,i)})^{d_t} \right) e_{(i,i+1)} + u; \tag{3.4}$$

$$\begin{aligned}[Y_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}] = \sum_{i=1}^{n-1} \big(& (y^l_{(i,i+1)} y^1_{(i+1,i+1)} + y^l_{(i,i)} y^1_{(i,i+1)} - y^1_{(i,i+1)} y^l_{(i+1,i+1)} - y^1_{(i,i)} y^l_{(i,i+1)}) \\ & (y^1_{(i+1,i+1)} - y^1_{(i,i)})^{d_1 - 1} \times \prod_{t=2}^{s} (y^t_{(i+1,i+1)} - y^t_{(i,i)})^{d_t} \big) e_{(i,i+1)} + v; \end{aligned} \tag{3.5}$$

$$\begin{aligned}\left[Y_l^q - Y_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}\right] = \sum_{i=1}^{n-1} \Big(& y^l_{(i,i+1)} \Big(\sum_{t=0}^{q-1} (y^l_{(i,i)})^t (y^l_{(i+1,i+1)})^{q-1-t} - 1 \Big) \times \\ & \prod_{t=1}^{s} (y^t_{(i+1,i+1)} - y^t_{(i,i)})^{d_t} \Big) e_{(i,i+1)} + w, \end{aligned} \tag{3.6}$$

em que u, v e w são combinações lineares de matrizes $e_{(i,j)}$, com $j - i \geq 2$.

Suponha que exista $\alpha_{(a,c)}$ em (3.3) tal que $\alpha_{(a,c)} \neq 0$. Seja

$$g = \alpha_{(a,c)} y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} c_1 c_2 \cdots c_{n-1}$$

uma parcela não nula de f e considere o monômio

$$m_g = x_{j_1} x_{j_2} \cdots x_{j_{n-1}} \in \mathbb{K}\langle X \rangle,$$

em que x_{j_k} é a variável na primeira posição do comutador c_k, caso c_k seja da forma a) ou b) da definição de $L-$normal, e y_i, caso seja da forma c). Note que $\deg_G(x_{j_k}) = \deg_G(c_k)$. Considere a ordem lexicográfica à esquerda no conjunto

$$M_f = \{m_g;\ g \text{ é uma parcela não nula de } f\},$$

em que $y_1 < y_2 < \cdots < z_1 < z_2 < \cdots$. Denote por $m = x_{i_1} x_{i_2} \cdots x_{i_{n-1}}$ o elemento maximal de M_f. Dizemos que $k, r \in \{1, 2, \ldots, n-1\}$ são equivalentes se $x_{i_k} = x_{i_r}$ e vamos denotar por Γ_k a classe de equivalência de k.

Defina $\overline{Y_l}$ e $\overline{Z_l}$ como segue:

a) Se $y_l = x_{i_k}$, para algum $1 \leq k \leq n-1$, então

$$\overline{Y_l} = \sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)} + \sum_{i \in \Gamma_k} y^l_{(i,i+1)} e_{(i,i+1)}.$$

b) Se $y_l \neq x_{i_k}$ para todo $1 \leq k \leq n-1$, então

$$\overline{Y_l} = \sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)}.$$

c) Se $z_l = x_{i_k}$ para algum $1 \leq k \leq n-1$, então

$$\overline{Z_l} = \sum_{i \in \Gamma_k} z^l_{(i,i+1)} e_{(i,i+1)}.$$

d) Se $z_l \neq x_{i_k}$, então

$$\overline{Z_l} = 0.$$

Dado um homomorfismo $\psi : \mathbb{K}[\Omega] \longrightarrow \mathbb{K}[\Omega]$, já vimos, na Proposição 1.4.16, que existe $F : UT_n(\mathbb{K}[\Omega]) \longrightarrow UT_n(\mathbb{K}[\Omega])$ homomorfismo tal que $F(\sum_{i \leq j} \rho_{i,j} e_{i,j}) = \sum_{i \leq j} \psi(\rho_{i,j}) e_{i,j}$. Defina

$$(a)\ \ \psi(y^l_{(i,i+1)}) = \begin{cases} y^l_{(i,i+1)}, \text{ se } y_l = x_{i_k} \text{ e } i \in \Gamma_k \\ 0, \text{ caso contrário} \end{cases};$$

$$(b)\ \ \psi(y^l_{(i,i)}) = y^l_{(i,i)};$$

$$(c)\ \ \psi(z^l_{(i,i+1)}) = \begin{cases} z^l_{(i,i+1)}, \text{ se } z_l = x_{i_k} \text{ e } i \in \Gamma_k \\ 0, \text{ caso contrário} \end{cases}.$$

Note que o valor que ψ assume em $y^l_{(i,j)}$, com $j \neq i$ ou $j \neq i+1$, não influenciará nos cálculos. Analogamente, para $z^l_{(i,j)}$, com $j \neq i+1$.

Agora, observe que

$$\begin{aligned} F(Y_l) &= F\Big(\sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)} + \sum_{i=1}^{n-1} y^l_{(i,i+1)} e_{(i,i+1)}\Big) \\ &= \sum_{i=1}^{n} \psi(y^l_{(i,i)}) e_{(i,i)} + \sum_{i=1}^{n-1} \psi(y^l_{(i,i+1)}) e_{(i,i+1)} \\ &= \sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)} + \sum_{i=1}^{n-1} \psi(y^l_{(i,i+1)}) e_{(i,i+1)}. \end{aligned}$$

Sabemos que $\psi(y^l_{(i,i+1)}) = \begin{cases} y^l_{(i,i+1)}, \text{ se } y_l = x_{i_k} \text{ e } i \in \Gamma_k \\ 0, \text{ caso contrário} \end{cases}$. Assim, se $y_l = x_{i_k}$ e $i \in \Gamma_k$,

$$F(Y_l) = \sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)} + \sum_{i=1}^{n-1} y^l_{(i,i+1)} e_{(i,i+1)} = \overline{Y_l}$$

e, caso contrário,

$$F(Y_l) = \sum_{i=1}^{n} y^l_{(i,i)} e_{(i,i)} + 0 = \overline{Y_l}.$$

De modo análogo,

$$\begin{aligned} F(Z_l) &= F\Big(\sum_{i=1}^{n-1} z^l_{(i,i+1)} e_{(i,i+1)}\Big) \\ &= \sum_{i=1}^{n-1} \psi(z^l_{(i,i+1)}) e_{(i,i+1)}. \end{aligned}$$

Sabemos que $\psi(z^l_{(i,i+1)}) = \begin{cases} z^l_{(i,i+1)}, \text{ se } z_l = x_{i_k} \text{ e } i \in \Gamma_k \\ 0, \text{ caso contrário} \end{cases}$. Assim, se $z_l = x_{i_k}$ e $i \in \Gamma_k$,

$$F(Z_l) = \sum_{i=1}^{n-1} z^l_{(i,i+1)} e_{(i,i+1)} = \overline{Z_l}$$

e, caso contrário,

$$F(Z_l) = 0 = \overline{Z_l}.$$

Desse modo, em todo caso, temos $F(Y_l) = \overline{Y_l}$ e $F(Z_l) = \overline{Z_l}$.

Além disso, dado um polinômio $L-$normal $c_k = c_k(y_1, \ldots, y_s, z_1, \ldots, z_s)$, denote por $\mu(c_k)$ o coeficiente de $e_{(k,k+1)}$ em $c_k(\overline{Y_1}, \ldots, \overline{Y_s}, \overline{Z_1}, \ldots, \overline{Z_s})$. Temos:

a) Seja $c_k = [z_l, y_1^{(d_1)}, \ldots, y_s^{(d_s)}]$. Assim, por (3.4), se $z_l = x_{i_k}$, então

$$\begin{aligned} \Big[Z_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}\Big] &= \sum_{k=1}^{n-1} \Big(z^l_{(k,k+1)} \prod_{t=1}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t}\Big) e_{(k,k+1)} + u \\ \Longrightarrow F\Big(\Big[Z_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}\Big]\Big) &= F\Big(\sum_{k=1}^{n-1} \Big(z^l_{(k,k+1)} \prod_{t=1}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t}\Big) e_{(k,k+1)} + u\Big) \\ \Longrightarrow \Big[\overline{Z_l}, \overline{Y_1}^{(d_1)}, \ldots, \overline{Y_s}^{(d_s)}\Big] &= \sum_{k=1}^{n-1} \psi(z^l_{(k,k+1)} \prod_{t=1}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t}) e_{(k,k+1)} + u \\ \Longrightarrow \Big[\overline{Z_l}, \overline{Y_1}^{(d_1)}, \ldots, \overline{Y_s}^{(d_s)}\Big] &= \sum_{k=1}^{n-1} \psi(z^l_{(k,k+1)}) \prod_{t=1}^{s} (\psi(y^t_{(k+1,k+1)}) - \psi(y^t_{(k,k)}))^{d_t} e_{(k,k+1)} + u \\ \Longrightarrow \Big[\overline{Z_l}, \overline{Y_1}^{(d_1)}, \ldots, \overline{Y_s}^{(d_s)}\Big] &= \sum_{k=1}^{n-1} \underbrace{z^l_{(k,k+1)} \prod_{t=1}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t}}_{\mu(c_k)} e_{(k,k+1)} + u. \end{aligned}$$

Logo,

$$\mu(c_k) = z^l_{(k,k+1)} \prod_{t=1}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t}. \tag{3.7}$$

b) Seja $c_k = [y_l, y_1^{(d_1)}, \ldots, y_l^{(d_l)}, \ldots, y_s^{(d_s)}]$. Assim, por (3.5), se $y_l = x_{i_k}$, então

$$\begin{aligned}
[Y_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}] &= \sum_{i=1}^{n-1} \big((y^l_{(k,k+1)} y^1_{(k+1,k+1)} + y^l_{(k,k)} y^1_{(k,k+1)} - y^1_{(k,k+1)} y^l_{(k+1,k+1)} \\
&- y^1_{(k,k)} y^l_{(k,k+1)})(y^1_{(k+1,k+1)} - y^1_{(k,k)})^{d_1 - 1} \times \prod_{t=2}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t} \big) e_{(k,k+1)} + v \\
\Longrightarrow F\Big([Y_l, Y_1^{(d_1)}, \ldots, Y_s^{(d_s)}]\Big) &= F\Big(\sum_{i=1}^{n-1} \big((y^l_{(k,k+1)} y^1_{(k+1,k+1)} + y^l_{(k,k)} y^1_{(k,k+1)} - y^1_{(k,k+1)} y^l_{(k+1,k+1)} \\
&- y^1_{(k,k)} y^l_{(k,k+1)})(y^1_{(k+1,k+1)} - y^1_{(k,k)})^{d_1 - 1} \times \prod_{t=2}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t} \big) e_{(k,k+1)} + v \Big) \\
\Longrightarrow [\overline{Y_l}, \overline{Y_1}^{(d_1)}, \ldots, \overline{Y_s}^{(d_s)}] &= \sum_{i=1}^{n-1} \psi\big((y^l_{(k,k+1)} y^1_{(k+1,k+1)} + y^l_{(k,k)} y^1_{(k,k+1)} - y^1_{(k,k+1)} y^l_{(k+1,k+1)} \\
&- y^1_{(k,k)} y^l_{(k,k+1)})(y^1_{(k+1,k+1)} - y^1_{(k,k)})^{d_1 - 1} \times \prod_{t=2}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t} \big) e_{(k,k+1)} + v \\
\Longrightarrow [\overline{Y_l}, \overline{Y_1}^{(d_1)}, \ldots, \overline{Y_s}^{(d_s)}] &= \sum_{i=1}^{n-1} (\psi(y^l_{(k,k+1)}) \psi(y^1_{(k+1,k+1)}) + \psi(y^l_{(k,k)}) \psi(y^1_{(k,k+1)}) \\
&- \psi(y^1_{(k,k+1)}) \psi(y^l_{(k+1,k+1)}) - \psi(y^1_{(k,k)}) \psi(y^l_{(k,k+1)}))(\psi(y^1_{(k+1,k+1)}) - \psi(y^1_{(k,k)}))^{d_1 - 1} \times \\
&\prod_{t=2}^{s} (\psi(y^t_{(k+1,k+1)}) - \psi(y^t_{(k,k)}))^{d_t} e_{(k,k+1)} + v \\
\Longrightarrow [\overline{Y_l}, \overline{Y_1}^{(d_1)}, \ldots, \overline{Y_s}^{(d_s)}] &= \sum_{i=1}^{n-1} (y^l_{(k,k+1)} y^1_{(k+1,k+1)} + y^l_{(k,k)} y^1_{(k,k+1)} - y^1_{(k,k+1)} y^l_{(k+1,k+1)} \\
&- y^1_{(k,k)} y^l_{(k,k+1)})(y^1_{(k+1,k+1)} - y^1_{(k,k)})^{d_1 - 1} \times \prod_{t=2}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t} e_{(k,k+1)} + v.
\end{aligned}$$

Dessarte,

$$\begin{aligned}
\mu(c_k) = (y^l_{(k,k+1)} y^1_{(k+1,k+1)} + y^l_{(k,k)} y^1_{(k,k+1)} - y^1_{(k,k+1)} y^l_{(k+1,k+1)} - y^1_{(k,k)} y^l_{(k,k+1)}) \times \\
\times (y^1_{(k+1,k+1)} - y^1_{(k,k)})^{d_1 - 1} \times \prod_{t=2}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t}.
\end{aligned} \tag{3.8}$$

c) Seja $c_k = [y_l^q - y_l, y_1^{(d_1)}, \ldots, y_{l-1}^{(d_l-1)}, y_{l+1}^{(d_l-1)} \ldots, y_s^{(d_s)}]$. Assim, por (3.6), se $y_l = x_{i_k}$, então

$$\begin{aligned}
&\Big[Y_l^q - Y_l, Y_1^{(d_1)}, \ldots, Y_{l-1}^{(d_{l-1})}, Y_{l+1}^{(d_{l+1})}, \ldots, Y_s^{(d_s)}\Big] = \\
&= \sum_{k=1}^{n-1} \Big(y^l_{(k,k+1)} (\sum_{t=0}^{q-1} (y^l_{(k,k)})^t (y^l_{(k+1,k+1)})^{q-1-t} - 1) \times \\
&\quad \times \prod_{t=1,\, d_l=0}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t} \Big) e_{(k,k+1)} + w \\
\Longrightarrow &F\Big(\Big[Y_l^q - Y_l, Y_1^{(d_1)}, \ldots, Y_{l-1}^{(d_{l-1})}, Y_{l+1}^{(d_{l+1})}, \ldots, Y_s^{(d_s)}\Big] \Big) = \\
&= F\Big(\sum_{k=1}^{n-1} \Big(y^l_{(k,k+1)} (\sum_{t=0}^{q-1} (y^l_{(k,k)})^t (y^l_{(k+1,k+1)})^{q-1-t} - 1) \times \\
&\quad \times \prod_{t=1,\, d_l=0}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t} \Big) e_{(k,k+1)} + w \Big) \\
\Longrightarrow &\Big[\overline{Y_l^q} - \overline{Y_l}, \overline{Y_1}^{(d_1)}, \ldots, \overline{Y_{l-1}}^{(d_{l-1})}, \overline{Y_{l+1}}^{(d_{l+1})}, \ldots, \overline{Y_s}^{(d_s)}\Big] = \\
&= \sum_{k=1}^{n-1} \psi(y^l_{(k,k+1)}) (\sum_{t=0}^{q-1} (y^l_{(k,k)})^t (y^l_{(k+1,k+1)})^{q-1-t} - 1) \times \\
&\quad \times \prod_{t=1,\, d_l=0}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t} e_{(k,k+1)} + w \\
\Longrightarrow &\Big[\overline{Y_l^q} - \overline{Y_l}, \overline{Y_1}^{(d_1)}, \ldots, \overline{Y_{l-1}}^{(d_{l-1})}, \overline{Y_{l+1}}^{(d_{l+1})}, \ldots, \overline{Y_s}^{(d_s)}\Big] = \\
&= \sum_{k=1}^{n-1} \psi(y^l_{(k,k+1)}) (\sum_{t=0}^{q-1} \psi(y^l_{(k,k)})^t \psi(y^l_{(k+1,k+1)})^{q-1-t} - \psi(1)) \times \\
&\quad \times \prod_{t=1,\, d_l=0}^{s} (\psi(y^t_{(k+1,k+1)}) - \psi(y^t_{(k,k)}))^{d_t}) e_{(k,k+1)} + w \\
\Longrightarrow &\Big[\overline{Y_l^q} - \overline{Y_l}, \overline{Y_1}^{(d_1)}, \ldots, \overline{Y_{l-1}}^{(d_{l-1})}, \overline{Y_{l+1}}^{(d_{l+1})}, \ldots, \overline{Y_s}^{(d_s)}\Big] = \\
&= \sum_{k=1}^{n-1} y^l_{(k,k+1)} (\sum_{t=0}^{q-1} (y^l_{(k,k)})^t (y^l_{(k+1,k+1)})^{q-1-t} - 1) \times \\
&\quad \times \prod_{t=1,\, d_l=0}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t} e_{(k,k+1)} + w.
\end{aligned}$$

Dessa forma,

$$\mu(c_k) = y^l_{(k,k+1)} \Big(\sum_{t=0}^{q-1} (y^l_{(k,k)})^t (y^l_{(k+1,k+1)})^{q-1-t} - 1 \Big) \times \prod_{t=1,\, d_l=0}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t}. \quad (3.9)$$

Afirmação 4: Seja $g(y_1, \ldots, y_s, z_1, \ldots, z_s) = \alpha_{(a,c)} y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} c_1 c_2 \cdots c_{n-1}$ uma parcela não nula de f. Se $g(\overline{Y_1}, \ldots, \overline{Y_s}, \overline{Z_1}, \ldots, \overline{Z_s}) \neq 0$, então $m_g = m$.

Suponha $m_g = x_{j_1}x_{j_2}\cdots x_{j_{n-1}} \neq x_{i_1}x_{i_2}\cdots x_{i_{n-1}}$. Então existe $1 \leq k \leq n-1$ tal que

$$x_{j_1} = x_{i_1},\ x_{j_2} = x_{i_2}, \ldots, x_{j_{k-1}} = x_{i_{k-1}},\ x_{j_k} \neq x_{i_k}. \tag{3.10}$$

Temos os seguintes casos:

a) Seja $c_k = [z_l, y_1^{(d_1)}, \ldots, y_s^{(d_s)}]$, em que $z_l = x_{j_k}$. Como $x_{j_k} \neq x_{i_k}$, então $z_l \neq x_{i_k}$. Assim, pela construção de ψ no item (c), temos $z^l_{(k,k+1)} = 0$. Dessa forma, como

$$\mu(c_k) = z^l_{(k,k+1)} \prod_{t=1}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t},$$

então $\mu(c_k) = 0$. Assim, $g(\overline{Y_1}, \ldots, \overline{Y_s}, \overline{Z_1}, \ldots, \overline{Z_s}) = 0$. Absurdo.

b) Seja $c_k = [y_l, y_{p_1}, y_{p_2}, \ldots, y_{p_s}]$, com $l > p_1 \leq p_2 \leq \cdots \leq p_s$ e $y_l = x_{j_k}$. Por (3.5), se $y_l \neq x_{i_k}$, então $y_{p_1} = x_{i_k}$. Assim, $x_{j_k} > x_{i_k}$ e, por (3.10), obtemos que m não é maximal em M_f. Absurdo.

c) Seja $c_k = [y_l^q - y_l, y_1^{(d_1)}, \ldots, y_{l-1}^{(d_{l-1})}, y_{l+1}^{(d_{l+1})}, \ldots, y_s^{(d_s)}]$, em que $y_l = x_{j_k}$. Como $x_{j_k} \neq x_{i_k}$, então $y_l \neq x_{i_k}$. Assim, novamente pela construção de ψ no item (a), $y^l_{(k,k+1)} = 0$ e, sendo

$$\mu(c_k) = y^l_{(k,k+1)} \Big(\sum_{t=0}^{q-1} (y^l_{(k,k)})^t (y^l_{(k+1,k+1)})^{q-1-t} - 1 \Big) \times \prod_{t=1,\ d_l=0}^{s} (y^t_{(k+1,k+1)} - y^t_{(k,k)})^{d_t},$$

segue que $\mu(c_k) = 0$. Assim, $g(\overline{Y_1}, \ldots, \overline{Y_s}, \overline{Z_1}, \ldots, \overline{Z_s}) = 0$. Absurdo.

Assim, a Afirmação 4 está finalizada.

Defina uma ordem parcial em Ω tal que

$$y^t_{(k,k)} < y^t_{(k+1,k+1)}, \quad y^t_{(k,k)} < y^{t+1}_{(k,k)},$$

$$y^t_{(k,k)} < z^l_{(k,k+1)} < y^t_{(k+1,k+1)},\ y^t_{(k,k)} < y^l_{(k,k+1)} < y^t_{(k+1,k+1)}, \quad y^l_{(k,k+1)} < z^l_{(k,k+1)},$$

para todo $k, t, l \geq 1$. Agora, considere a ordem lexicográfica à direita nos monômios em $\mathbb{K}[\Omega]$. Denote por $\overline{\mu}(c_k)$ o monômio máximo de $\mu(c_k)$. Por (3.4), (3.5) e (3.6), obtemos, respectivamente,

$$\overline{\mu}(c_k) = z^l_{(k,k+1)} \prod_{t=1}^{s} (y^t_{(k+1,k+1)})^{d_t}$$

no caso a);

$$\overline{\mu}(c_k) = y^l_{(k,k+1)} \prod_{t=1}^{s} (y^t_{(k+1,k+1)})^{d_t}$$

no caso b);

$$\overline{\mu}(c_k) = y^l_{(k,k+1)} \prod_{t=1,\ d_l=q-1}^{s} (y^t_{(k+1,k+1)})^{d_t}$$

no caso c).

Relembre que c_k é $L-$normal.

Seja

$$g = g(y_1, \ldots, y_s, z_1, \ldots, z_s) = \alpha_{(a,c)} y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} c_1 c_2 \cdots c_{n-1}$$

um somando não nulo de f tal que $m_g = x_{i_1} x_{i_2} \cdots x_{i_{n-1}}$. Então $g(\overline{Y_1}, \ldots, \overline{Y_s}, \overline{Z_1}, \ldots, \overline{Z_s}) = \omega_g e_{(1,n)}$, em que $\omega_g \in \mathbb{K}[\Omega]$. Note que

$$\hat{g} = \alpha_{(a,c)} \prod_{r=1}^{s} (y^r_{(1,1)})^{a_r} \prod_{k=1}^{n-1} \overline{\mu}(c_k)$$

é o monômio maximal que aparece em ω_g. Além disso, $g \longrightarrow \hat{g}$ é uma função bijetiva e $\deg_u \hat{g} < q$, para todo $u \in \Omega$. Escreva $f(\overline{Y_1}, \ldots, \overline{Y_s}, \overline{Z_1}, \ldots, \overline{Z_s}) = \omega_f e_{(1,n)}$, em que $\omega_f \in \mathbb{K}[\Omega]$. Note que

$$f(\overline{Y_1}, \ldots, \overline{Y_s}, \overline{Z_1}, \ldots, \overline{Z_s}) = \sum g(\overline{Y_1}, \ldots, \overline{Y_s}, \overline{Z_1}, \ldots, \overline{Z_s}),$$

em que $m_g = x_{i_1} x_{i_2} \cdots x_{i_{n-1}}$. Logo, $\omega_f = \sum \omega_g$, em que $m_g = x_{i_1} x_{i_2} \cdots x_{i_{n-1}}$. O monômio máximo $\hat{f}$ que aparece em ω_f é o elemento maximal do conjunto $A = \{\hat{g};\ m_g = x_{i_1} x_{i_2} \cdots x_{i_{n-1}}\}$. Pela bijeção $g \longrightarrow \hat{g}$, obtemos

$$\hat{f} = \hat{g} = \alpha_{(a,c)} \prod_{r=1}^{s} (y^r_{(1,1)})^{a_r} \prod_{k=1}^{n-1} \overline{\mu}(c_k), \tag{3.11}$$

em que $\hat{g}$ é o elemento maximal de A. Agora, $f \in T_G(UT_n, \varepsilon)$, ou seja, $\omega_f \in T(\mathbb{K})$. Pelo Lema 3.1.2, obtemos o coeficiente em (3.11), $\alpha_{(a,c)} = 0$. Usando esse argumento várias vezes, obtemos $\alpha_{(a,c)} = 0$, para todo (a, c) desejado. Desse modo, a Afirmação 3 está finalizada.

O espaço vetorial $\dfrac{\mathbb{K}\langle X\rangle}{I(\varepsilon)}$ é gerado pelos polinômios em (3.2), e esses polinômios são linearmente independentes em $\dfrac{\mathbb{K}\langle X\rangle}{T_G(UT_n, \varepsilon)}$. Portanto, como $I(\varepsilon) \subseteq T_G(UT_n, \varepsilon)$, segue que $I(\varepsilon) = T_G(UT_n, \varepsilon)$. ■

A partir dos Teoremas 2.0.7 e 3.2.3, obtemos a descrição das identidades polinomiais $G-$graduadas de UT_n, para toda $G-$graduação em UT_n, grupo G e corpo finito $\mathbb{K}$.

Corolário 3.2.4 *Se $\mathbb{K}$ é um corpo finito, então*

$$T(UT_n(\mathbb{K})) = (T(\mathbb{K}))^n,$$

para todo $n \geq 1$.

Demonstração: Seja $G = \{1\}$ um grupo com apenas um elemento. Denote por ε a $n-$upla $(1, \ldots, 1)$. Então, $T_G(UT_n, \varepsilon) = T(UT_n)$. Note que ε é a única sequência $\varepsilon-$ruim de comprimento $\leq n$.

Assim, pelo Teorema 3.2.3, temos $T(UT_1) = T(\mathbb{K})$ é o T_G-ideal gerado por

$$[y_1, y_2] \text{ e } y_1^q - y_1,$$

e $T(UT_n)$ é o $T-$ideal gerado pelos polinômios

$$c_1 c_2 \cdots c_n,$$

em que $c_j \in \{[y_{2j}, y_{2j+1}], y_{2j}^q - y_{2j}\}$. Logo,

$$T(UT_n) \subseteq (T(\mathbb{K}))^n.$$

Agora, seja $f_i(y_1, \ldots, y_s) \in T(\mathbb{K})$, com $1 \leq i \leq n$, e sejam $Y_1, \ldots, Y_s \in UT_n$. Como $f_i(Y_1, \ldots, Y_s) \in J(UT_n)$, temos que $f = f_1 \cdots f_n \in T(UT_n)$, ou seja,

$$(T(\mathbb{K}))^n \subseteq T(UT_n). \quad \blacksquare$$

Corolário 3.2.5 *Seja G um grupo finito e $\mathbb{K}$ um corpo finito. O conjunto de todas as identidades polinomiais $G-$graduadas de UT_n é finitamente gerado, como T_G-ideal, para toda $G-$graduação de $UT_n(\mathbb{K})$.*

Demonstração: Fixada uma $n-$upla $\varepsilon \in G^n$, seja Λ o conjunto de todos os $\eta-$polinômios, em que $\eta \in G^m$ e $1 \leq m \leq n$.

Note, agora, que, sendo $\eta = (\eta_1, \ldots, \eta_m)$, temos $|G|$ possibilidades para cada η_j. Assim, existem $|G|^m$ escolhas possíveis para η.

Além disso, para cada $j = 1, \ldots, m$, existem, no máximo, duas possíveis escolhas para c_j :

- se $\eta_j = 1$, existem duas escolhas;
- se $\eta_j \neq 1$, existe apenas uma escolha.

Desse modo, existem, no máximo, 2^m produtos distintos do tipo

$$c_1 \cdot c_2 \cdots c_m.$$

Logo, conjunto Λ tem cardinalidade

$$|\Lambda| \leq \sum_{m=1}^{n} 2^m |G|^m.$$

Pelo Teorema 3.2.3, existe um conjunto gerador de $T_G(UT_n, \varepsilon)$, como um T_G-ideal, contido em Λ. Assim, como Λ é finito, segue, portanto, que $T_G(UT_n, \varepsilon)$ é finitamente gerado. ■

Note que o Corolário 3.2.5 também é válido quando $\mathbb{K}$ é um corpo infinito. Para mais detalhes, o leitor pode verificar [12].

Referências Bibliográficas

[1] ALJADEFF, E.; KANEL-BELOV, A. Representability and Specht problem for G-graded algebras. *Advances in Mathematics,* 225, n. 5, p. 2391-2428, 2010. 3

[2] AMITSUR, S. A.; LEVITZKI, J. Minimal identities for algebras. *Proceedings of the American Mathematical Society,* v. 1, n. 1, p. 449-463, 1950. 2

[3] AXLER, S. *Finite fields.* 4. ed. Cham: Springer, 2024.

[4] AZEVEDO, S. S.; FIDELIS, M.; KOSHLUKOV, P. Tensor product theorems in positive characteristic, *Journal of Algebra*, n. 276, p. 836-845, 2004.

[5] BELOV, A. Y. On non-Spechtian varieties. *Fundamentalnaya i Prikladnaya Matematika*, v. 5, n. 1, p. 47-66, 1999. Em alemão. 2

[6] BRANDÃO JUNIOR, A. P. [s.d.]. *Grupos.* Universidade Federal de Campina Grande, Campina Grande. Notas de aula.

[7] BRANDÃO JUNIOR, A. P. [s.d.]. *Introdução às PI-Álgebras.* Universidade Federal de Campina Grande, Campina Grande. Notas de aula.

[8] BREUILLARD, E.; GREEN, B.; GURALNICK, R.; TAO, T.Strongly dense free subgroups of semisimple algebraic groups. *Israel Journal of Mathematics*, v. 192, n. 1, p. 347-379, 2012. 2

[9] COX, D. *Galois Theory.* 2. ed. Wiley, 2012. 12

[10] DEHN, M. Über die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme. *Mathematische Annalen*, v. 85, n. 1, p. 184-194, 1922. 1

[11] DI VINCENZO, O. M.; NARDOZZA, V. Graded polynomial identities of verbally prime algebra. *Journal of Algebra and Its Applications*, v. 6, n. 3, p. 385-401, 2007. 3

[12] DI VINCENZO, O. M.; KOSHLUKOV, P.; VALENTI, A. Gradings on the algebra of upper triangular matrices and their graded identities. *Journal of Algebra*, v. 275, p. 550-566, 2003. 4, 80

[13] DI VINCENZO, O. M. On the graded identities of $M_{1,1}(E)$. *Israel Journal of Mathematics*, v. 80, n. 3, p. 323-335, 1992. 3

[14] DOMINGUES, H. H.; IEZZI, G. *Álgebra Moderna*. 4. ed. São Paulo: Atual, 2003.

[15] DRENSKY, V. A minimal basis of identities for a second-order matrix algebra over a field of characteristic 0. *Algebra i Logika*, v. 20, n. 3, p. 282-290, 1980. 2

[16] DRENSKY, V. *Free Algebras and PI-Algebras. Graduate Course in Algebra*. Singapore: Springer-Verlag Singapore, 2000. 3

[17] DRENSKY, V.; FORMANEK, E. *Polynomial Identity Rings*. Boston: Springer Basel AG (eBook), 2004.

[18] FONSÊCA, E. P. DA. *Graduações e identidades na álgebra das matrizes triangulares superiores como álgebra associativa, de Lie e de Jordan.* Orientador: Prof. Dr. Diogo Diniz Pereira da Silva e Silva. Dissertação (Mestrado em Matemática) – Universidade Federal de Campina Grande, Campina Grande, 2022.

[19] GENOV, G. K. A basis of identities of the algebra of third-order matrices over a finite field. *Algebra and Logic*, v. 20, p. 241-257, 1981. 2

[20] GENOV, G. K.; SIDEROV, P. N. A basis for identities of the algebra of fourth-order matrices over a finite field I, II. *Serdica Mathematical Journal*, v. 8, p. 351-366, 1982. 2

[21] GONÇALVES, D. J.; RIVA, E. Graded polynomial identities for the upper triangular matrix algebra over a finite field. *Journal of Algebra*, v. 559, p. 625-645, 2020. 4, 50

[22] GONÇALVES, A. *Introdução à Álgebra*. 6. ed. Rio de Janeiro: IMPA, 2017.

[23] GRISHIN, A. V. Examples of T-spaces and T-ideals over a field of characteristic 2 without the finite basis property. *Fundamentalnaya i Prikladnaya Matematika,* v. 5, n. 1, p. 101-118, 1999. 2

[24] JACOBSON, N. Structure theory of algebraic algebras of bounded degree. *Annals of Mathematics*, v. 46, p. 695-707, 1945.

[25] KAPLANSKY, I. Rings with a polynomial identity. *Bulletin of the American Mathematical Society*, v. 54, p. 575-580, 1948. 2

[26] KEMER, A. R. Finite basability of identities of associative algebras. *Algebra i Logika*, v. 26, p. 597-641, 1987. Em russo. 2

[27] KEMER, A. R. *Ideals of identities of associative algebras.* Translated from the Russian by C. W. Kohls. Providence: American Mathematical Society, 1991. 3

[28] KOSHLUKOV, P.; AZEVEDO, S. S. Graded identities for T-prime algebras over field of positive characteristic. *Israel Journal of Mathematics*, v. 128, p. 157-176, 2002

[29] LATYSHEV, V. N. Generalization of Hilbert's theorem on the finiteness of bases. *Sibirskii Matematicheskii Zhurnal*, v. 7, p. 1422-1424, 1966. Em russo. 3

[30] LEVITZKI, J. On a problem of A. Kurosch. *Bulletin of the American Mathematical Society*, v. 52, p. 1033-1035, 1946. 2

[31] LIDL, R.; NIEDERREITER, H. *Finite fields.* 2. ed. Cambridge: Cambridge University Press, 1997.

[32] MAL'TSEV, Y. N.; KUZ'MIN, E. N. A basis for identities of the algebra of second-order matrices over a finite field. *Algebra i Logika*, v. 17, p. 28-32, 1978. 2

[33] MAL'TSEV, Y. N. Basis for identities of upper triangular matrices. *Algebra and Logic*, v. 10, p. 242-247, 1971. 3

[34] MARTÍNEZ, F. E. B.; OLIVEIRA, D. A. DE; JESUS, L. G. C. S. DE. *Polinômios Irredutíveis sobre Corpos Finitos.* Rio de Janeiro: Instituto de Matemática Pura e Aplicada (35º Colóquio Brasileiro de Matemática), 2025.

[35] MORANDI, P. *Field and Galois Theory*, New York: Springer, 1996. 12

[36] RAZMYSLOV, Y. P. Finite basing of the identities of a matrix algebra of second order over a field of characteristic zero. *Algebra Logika*, v. 12, n. 1, p. 83-113, 1973. 2

[37] RIVA, E. *Identidades polinomiais graduadas para a álgebra das matrizes triangulares superiores sobre um corpo finito.* Orientador: Prof. Dr. Dimas José Gonçalves. Tese (Doutorado em Matemática) – Universidade Federal de São Carlos, São Carlos, 2021.

[38] SANTOS, J. DOS. *Congruências modulares, corpos finitos e aplicações.* Orientador: Prof. Dr. Zaqueu Alves Ramos. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal de Sergipe, São Cristóvão, 2015. 7

[39] SANTOS, R. B. DOS; VIEIRA, A. C. *PI-álgebras: uma introdução à PI-teoria*, Rio de Janeiro: Instituto de Matemática Pura e Aplicada (33º Colóquio Brasileiro de Matemática), 2021.

[40] SHCHIGOLEV, V. V. Examples of infinitely based T-ideals. *Fundamentalnaya i Prikladnaya Matematika*, v. 5, p. 307-312, 1999. 2

[41] SIDEROV, P. N. A basis for identities of an algebra of triangular matrices over an arbitrary field. *Pliska Studia Mathematica*, v. 2, p. 143-152, 1981. Em russo. 3

[42] SPECHT, W. Gesetze in ringen. *Mathematische Zeitschrift*, v. 52, p. 557-589, 1950. Em alemão. 2

[43] SILVA, D. D. P. DA S. *Introdução às Álgebras com Identidades Polinomiais.* Campina Grande, 2024. Notas de aula.

[44] SILVA, J. L. G. DA. *Identidade de Cayley-Hamilton para álgebras de matrizes.* Orientador: Claudemir Fidelis Bezerra Junior. Dissertação (Mestrado em Matemática) – Universidade Federal de Campina Grande, Campina Grande, 2020.

[45] SILVA, I. T. DE A. E. *Graduações na Álgebra das Matrizes Triangulares superiores e suas Identidades Graduadas.* Orientador: Prof. Dr. Diogo Diniz Pereira da

Silva e Silva. Dissertação (Mestrado em Matemática) – Universidade Federal de Campina Grande, Campina Grande, 2022.

[46] SVIRIDOVA, I. Identities of PI-algebras graded by a finite abelian group. *Communications in Algebra*, v. 39, n. 9, p. 3462-3490, 2011. 3

[47] VALENTI, A.; ZAICEV, M. V. Group gradings on upper triangular matrices. *Archiv der Mathematik*, v. 89, n. 1, p. 33–40, 2007. 3, 4, 40

[48] VASILOVSKY, S. Yu. $\mathbb{Z}_n-$graded polynomial identities of the full matrix algebra of order n. *Proceedings of the American Mathematical Society*, v. 127, n. 12, p. 3517-3524, 1999. 3

[49] WAGNER, W. Über die Grundlagen der projektiven Geometrie und allgemeine Zahlensysteme. *Annals of Mathematics*, v. 113, p. 528–567, 1936. 1

[50] ZAICEV, M. V. Finite gradings on simple Artinian rings. *Vestnik Moskovskogo Universiteta. Seriya 1. Matematika. Mekhanika*, v. 3, p. 21-24, 2001. 42