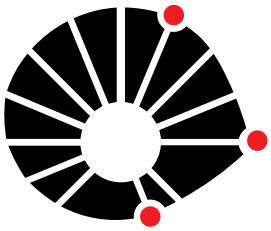


UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

RAFAEL DAIGO HIRAMA

Álgebras Nil e Nilpotentes

Campinas

2018

Rafael Daigo Hirama

Álgebras Nil e Nilpotentes

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática.

Orientador: Plamen Emilov Kochloukov

Este exemplar corresponde à versão final da Dissertação defendida pelo aluno Rafael Daigo Hirama e orientada pelo Prof. Dr. Plamen Emilov Kochloukov.

Campinas

2018

Agência(s) de fomento e nº(s) de processo(s): Não se aplica.

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

H613a

Hirama, Rafael Daigo, 1986-
Álgebras nil e nilpotentes / Rafael Daigo Hirama. – Campinas, SP : [s.n.], 2018.

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

1. Álgebra não-comutativa. 2. Identidade polinomial. 3. PI-álgebras. 4. Representações de grupos. I. Kochloukov, Plamen Emilov, 1958-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Nil and nilpotent algebras
Palavras-chave em inglês:
Noncommutative algebra
Polynomial identity
PI-algebras
Representations of groups
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Plamen Emilov Kochloukov [Orientador]
Ivan Chestakov
Eduardo Tengan
Data de defesa: 26-02-2018
Programa de Pós-Graduação: Matemática

Dissertação de Mestrado defendida em 26 de fevereiro de 2018 e aprovada pela banca examinadora composta pelos Profs. Drs.

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

Prof(a). Dr(a). IVAN CHESTAKOV

Prof(a). Dr(a). EDUARDO TENGAN

As respectivas assinaturas dos membros encontram-se na Ata de defesa

Agradecimentos

Agradeço aos meus pais, Morio e Marlene, pela insistência e pelo apoio para eu concluir o mestrado, e por todo o resto. Ao meu irmão Danilo, pelo companheirismo.

Agradeço ao meu orientador Plamen Koshlukov, pelo convite para fazer o mestrado, sem o qual nada disto teria acontecido, pela atenção, pelo suporte e pela paciência durante este longo período.

Agradeço aos professores Ivan Chestakov e Eduardo Tengan, por aceitarem compor a banca, por dedicarem tempo para avaliar a minha dissertação, pelas correções e pelas valiosas sugestões.

Agradeço a todos os amigos e professores que conheci durante as várias Olimpíadas de Matemática, que fizeram com que eu, mesmo me formando em Engenharia, jamais perdesse o interesse e a admiração pela Matemática.

Por fim, agradeço a todos que de alguma forma me ajudaram e permitiram este momento.

"A Matemática pura é, à sua maneira,
a poesia das ideias lógicas."
(Albert Einstein)

Resumo

Em 1952, Nagata demonstrou que uma álgebra associativa, sobre um corpo de característica 0 e nil de índice limitado é nilpotente. Neste trabalho apresentaremos este e outros resultados relacionados sobre álgebras associativas. Primeiramente, vamos demonstrar o teorema da altura de Shirshov e obter que uma álgebra finitamente gerada, nil e que satisfaz uma identidade polinomial é nilpotente. Em seguida apresentaremos o teorema de Golod e Shafarevich, que mostra que existem álgebras finitamente geradas nil mas não nilpotentes. Este teorema produz também um exemplo de um grupo finitamente gerado, periódico mas infinito.

Então vamos explorar resultados sobre o índice de nilpotência de álgebras nil de índice limitado em característica 0. Vamos começar mostrando as cotas obtidas por Higman, alguns anos após Nagata. Depois vamos provar a cota inferior $n(n+1)/2$ obtida por Kuzmin. Por fim, usando a teoria de representações do grupo simétrico, apresentaremos a demonstração de Nagata, e usando identidades polinomiais com traço, provaremos a cota superior n^2 obtida por Razmyslov.

Palavras-chave: Álgebra não-comutativa; Identidade polinomial; PI-álgebras; Representações de grupos

Abstract

In 1952, Nagata proved that an associative algebra over a field of characteristic 0 that is nil of bounded index is nilpotent. In this work we will present this and other related results on associative algebras. First, we will prove the Shirshov height theorem and deduce that a finitely generated nil algebra that satisfies a polynomial identity is nilpotent. Next, we will present the Golod and Shafarevich theorem which shows that there are finitely generated nil algebras that are not nilpotent. This theorem also provides an example of a finitely generated periodic group which is not finite.
Then we will explore results on the nilpotency index of nil algebras of bounded index, over fields of characteristic 0. We will start by showing the bounds proved by Higman, a couple of years after Nagata. After that, we will prove the lower bound $n(n+1)/2$ due to Kuzmin. Finally, using representation theory of the symmetric group, we will show Nagata's proof, and then, using trace identities, we will prove the upper bound n^2 due to Razmyslov.

Keywords: Noncommutative algebra; Polynomial identity; PI-algebras; Group representations

Sumário

Introdução

Em 1941, Kurosh formulou o seguinte problema sobre álgebras:

> **(Problema de Kurosh)** Seja A uma álgebra associativa finitamente gerada em que todo elemento de A é algébrico. A álgebra A tem dimensão finita? Em particular, se A for nil, ela será nilpotente?

O problema de Kurosh é o análogo para álgebras do famoso problema de Burnside sobre grupos, que foi proposto em 1902. O problema foi posteriormente provado falso por Golod e Shafarevich, em 1964, que encontraram um exemplo de álgebra nil, finitamente gerada mas não nilpotente. A partir desse exemplo eles também construíram um contraexemplo para o problema de Burnside. Porém, se assumirmos que os elementos da álgebra satisfazem algum polinômio, a resposta é afirmativa, como foi demonstrado nos trabalhos de Jacobson, Kaplansky e Levitzki entre 1945 e 1948. Esse foi um dos marcos iniciais da chamada teoria das álgebras com identidades polinomiais.

As álgebras com identidades polinomiais ou PI-álgebras são definidas como as álgebras para as quais existe um polinômio não nulo, em variáveis não necessariamente comutativas, que se anula sobre tal álgebra. Alguns exemplos de PI-álgebras são as álgebras comutativas e também as álgebras de dimensão finita, das quais se destacam as álgebras das matrizes de qualquer ordem. A teoria das álgebras com identidades polinomiais é uma área relativamente recente, apesar de podermos encontrar resultados de forma implícita em artigos de Wagner em 1922, Dehn em 1936 e Hall em 1943. Também é possível encontrar conceitos parecidos com a ideia de identidades polinomiais nas pesquisas de Sylvester, por volta de 1852.

Em 1950, Amitsur e Levitzki mostraram, utilizando métodos combinatórios, que a álgebra das matrizes de ordem n com entradas em um corpo satisfazem um certo polinômio de grau 2n, denominado de polinômio standard (que é o somatório alternado de todos os produtos de 2n matrizes), e que ele é a identidade de menor grau para esta álgebra. Este resultado marcou o começo de uma nova abordagem à PI-teoria, que busca a descrição das identidades polinomiais satisfeitas por uma álgebra dada. É interessante notar que argumentos combinatórios foram usados para obter ou apresentar novas demonstrações para vários resultados importantes sobre PI-álgebras. Alguns exemplos são o já citado teorema de Amitsur–Levitzki, o teorema de Regev sobre o produto tensorial, que diz que o produto tensorial de PI-álgebras também é uma PI-álgebra, e o teorema da altura de Shirshov, que, além da sua importância na álgebra, pode ser usado para deduzir de maneira imediata os teoremas de Levitzki e de Kaplansky (até versões bem mais gerais desses

importantes resultados). Cabe também lembrar que o teorema de Shirshov foi demonstrado também, com as devidas adaptações, para classes de álgebras não associativas.

Considerando novamente o problema de Kurosh sobre álgebras nil, em 1953, Nagata demonstrou que uma álgebra nil de grau limitado n sobre um corpo de característica zero é nilpotente e que o grau de nilpotência $d(n)$ depende apenas de n. O valor exato de $d(n)$ ainda é desconhecido exceto para $n \leqslant 4$, mas são conhecidas cotas que limitam esse valor, mais precisamente $n(n+1)/2 \leqslant d(n) \leqslant n^2$. Esses resultados serão o foco do capítulo 3 desta dissertação. O interesse em saber cotas mais precisas do grau de nilpotência $d(n)$ justifica-se pela importância desse grau na teoria de invariantes bem como na PI teoria e na combinatória algébrica.

Aqui também é interessante comentar que a demonstração original de Nagata usa métodos de outra área que frequentemente fornece ferramentas para a teoria de PI-álgebras: a teoria de representações do grupo simétrico. Aqui os exemplos são fartos, como por exemplo o teorema de Amitsur que toda PI-álgebra satisfaz alguma potência do polinômio standard e a obtenção de bases de identidades para várias álgebras, mas vamos trabalhar apenas com duas demonstrações relacionadas ao Teorema de Nagata-Higman: a prova original devida a Nagata e a cota superior $d(n) \leqslant n^2$ obtida por Razmyslov em 1974. Sobre a demonstração de Razmyslov ainda cabe o comentário que ela faz parte de uma teoria muito mais ampla sobre as identidades polinomiais com traço, cujo principal resultado é que todas as identidades polinomiais da álgebra das matrizes são consequência do teorema de Cayley–Hamilton (conhecido da Álgebra Linear).

O foco desta dissertação será o problema de decidir quando uma álgebra nil é nilpotente, principalmente sobre corpos de característica zero. Para tanto, este trabalho está organizado da seguinte forma:

No primeiro capítulo começamos com as definições e algumas propriedades básicas das estruturas algébricas que usaremos nesta dissertação (grupos, anéis, álgebras, módulos). Então introduzimos o conceito de PI-álgebras e algumas ferramentas usadas ao estudá-las. Nas seções 1.7 e 1.8 citamos os resultados da teoria de representações do grupo simétrico que serão usados em algumas das demonstrações do último capítulo. Na seção seguinte apresentamos uma interessante aplicação de ideias combinatórias no estudo de PI-álgebras na forma da demonstração do teorema de Regev sobre o produto tensorial. Para a demonstração do teorema de Regev precisamos também um outro resultado de grande importância na teoria de PI algebras. Mais precisamente, mostramos mais um teorema de Regev: se A é uma álgebra que satisfaz uma identidade polinomial de grau d então as suas codimensões têm crescimento limitado superiormente por $(d-1)^{2n}$. Para destacar a importância deste último resultado, ressaltamos que, grosseiramente, ele diz que os ideais de identidades são "muito grandes". Por fim, na última seção definimos os polinômios com traço e as álgebras com traço, tecemos um breve comentário sobre a

teoria desenvolvida por Razmyslov (e paralelamente por Procesi) e apresentamos uma demonstração para o teorema de Amitsur–Levitzki.

No capítulo 2, iniciamos com comentários sobre o problema principal desta dissertação, que é decidir quando uma álgebra nil é nilpotente. Então apresentamos o teorema de Shirshov sobre a altura, com o qual obtemos que uma PI-álgebra nil e finitamente gerada é nilpotente, além de obter que uma PI-álgebra algébrica de grau limitado e finitamente gerada é de dimensão finita. Na seção 2.3 mostramos, através do contraexemplo obtido por Golod e Shafarevich, que mesmo uma álgebra nil e finitamente gerada pode não ser nilpotente. Este teorema também produz um exemplo de um grupo finitamente gerado, periódico mas infinito, sendo um contraexemplo para o problema de Burnside. Cabe aqui comentar que este é o primeiro (e mais geral) dos problemas de Burnside. O segundo foi se um grupo é finitamente gerado e periódico com as ordens dos elementos limitadas, sempre é finito. Este segundo problema também teve resposta negativa. Já o terceiro problema pergunta o seguinte. Seja G um grupo gerado por n elementos, tal que as ordens de todos os elementos de G são menores ou iguais a algum k. Existe então um número $N = N(n, k)$ tal que todo grupo finito G com a propriedade de cima tem ordem $|G| \leqslant N$? Este último problema foi resolvido em afirmativo por E. I. Zelmanov, resultado que lhe rendeu a Medalha Fields em 1994.

No capítulo 3 estudamos o resultado mais conhecido como teorema de Nagata–Higman (ver os comentários históricos no início do Capítulo 3), apresentando várias demonstrações relacionadas às cotas inferiores e superiores. Começamos com os resultados de Higman, que provou que $n^2/e^2 < d(n) \leqslant 2^n - 1$ e que $d(3) = 6$. Então passamos para a cota inferior $d(n) \geqslant n(n+1)/2$ obtida por Kuzmin. Por fim, apresentamos a demonstração original de Nagata como uma forma de mostrar a aplicação da teoria de representações do grupo simétrico e terminamos com a demonstração de Razmyslov da cota superior $d(n) \leqslant n^2$, que também utiliza fortemente as representações do grupo simétrico, além das álgebras com traço e suas identidades.

1 Preliminares

Neste capítulo introduziremos os conceitos e alguns resultados básicos necessários no decorrer da presente dissertação e também aproveitaremos esta oportunidade para definir a notação a ser usada.

Primeiramente definiremos as estruturas algébricas citadas na dissertação. Ao final de cada uma dessas seções vamos explorar algumas das estruturas concretas que iremos utilizar (grupo simétrico, anel de polinômios em várias variáveis, álgebras associativas livres, álgebras do grupo simétrico). Então definiremos as álgebras com identidades polinomiais e algumas ferramentas básicas que temos para trabalhar com elas. O próximo passo é explorar as representações do grupo simétrico, cujos resultados serão usados em algumas das demonstrações. Na seção 1.9, apresentaremos uma demonstração do teorema de Regev como um exemplo do uso de ideias combinatórias para obter resultados em PI-álgebras. Por fim, expandiremos as álgebras de polinômios em várias variáveis para definirmos as álgebras com traço e as usaremos para obter uma demonstração do Teorema de Amitsur-Levitzki.

1.1 Grupos

Definição 1.1.1. *Sejam G conjunto não vazio e $\cdot : G \times G \to G$ uma operação binária. O par $(G, \cdot)$ é um* ***grupo*** *se valem as seguintes propriedades:*

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, *para todo* $a, b, c \in G$, *isto é, a operação* $\cdot$ *é associativa.*

(ii) Existe um elemento $e \in G$, *chamado de elemento neutro, tal que* $a \cdot e = e \cdot a = a$, *para todo* $a \in G$.

(iii) Para todo $a \in G$, *existe* $b \in G$, *chamado de inverso de* a, *tal que* $a \cdot b = b \cdot a = e$. *Denotaremos tal elemento por* a^{-1}.

Vamos definir duas estruturas mais gerais.

Definição 1.1.2. *Sejam G conjunto não vazio e $\cdot : G \times G \to G$ uma operação binária. O par $(G, \cdot)$ é um* ***semigrupo*** *se satisfaz a propriedade (i) acima.*

Definição 1.1.3. *Sejam G conjunto não vazio e $\cdot : G \times G \to G$ uma operação binária. O par $(G, \cdot)$ é um* ***monóide*** *se satisfaz as propriedades (i) e (ii) acima.*

Notação 1.1.1. *Por simplicidade, diremos que G é um grupo (semigrupo, monóide) sob $\cdot$ ou com relação a $\cdot$ quando $(G, \cdot)$ o for, ou apenas que G é um grupo (semigrupo, monóide)*

quando a operação estiver clara pelo contexto. Em geral, utilizaremos $\cdot$ como a operação e iremos denotar a operação pela justaposição dos elementos, isto é, usaremos ab no lugar de $a \cdot b$.

Definição 1.1.4. *Um grupo é **finito** se tem uma quantidade finita de elementos. O número de elementos de G é chamado de **ordem** de G e será denotado por $|G|$.*

Definição 1.1.5. *Um grupo é **comutativo** ou **abeliano** se satisfaz $ab = ba$ para todo $a, b \in G$.*

Definição 1.1.6. *Seja G um grupo e $S \subset G$ um subconjunto não vazio. S é um **subgrupo** de G se S for um grupo, com a mesma operação de G.*

Definição 1.1.7. *Sejam $(G, \cdot)$, $(H, \circ)$ grupos e $f\colon G \to H$ uma função. Então f é **homomorfismo de grupos** se, para todo g, $h \in G$, a seguinte condição é satisfeita:*

$$f(g \cdot h) = f(g) \circ f(h).$$

Definição 1.1.8. *Sejam G, H grupos e $f\colon G \to H$ um homomorfismo de grupos. Então f é um **isomorfismo** se f for uma função biunívoca. Ainda, dizemos que G e H são isomorfos e denotamos por $G \simeq H$.*

Definição 1.1.9. *Seja G um grupo e $a \in G$ um elemento. Então a **ordem** de a é o menor inteiro positivo m tal que $a^m = e$ (em que definimos por indução $a^n = a^{n-1}a$ e $a^1 = a$). Caso m exista dizemos que a tem **ordem finita**.*

Definição 1.1.10. *Seja G um grupo. Dados $x, y \in G$, dizemos que x e y são **conjugados** se existe $g \in G$ tal que $y = g^{-1}xg$. Definimos então a **classe de conjugação** de $x \in G$ como o conjunto $\{g^{-1}xg : g \in G\}$. Note que "ser conjugado a" é uma relação de equivalência.*

Definição 1.1.11. *Sejam G um grupo e X um conjunto. A função $\varphi : G \times X \to X$ é uma **ação (à esquerda) de grupo** se para todo $x \in X$ valem as seguintes propriedades:*

(i) $\varphi(e, x) = x$, *em que e é o elemento neutro de G*

(ii) $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$, *para todo $g, h \in G$*

*Analogamente definimos **ação à direita de grupo** como a função $\psi : X \times G \to X$ que obedece:*

(i) $\psi(x, e) = x$, *em que e é o elemento neutro de G*

(ii) $\psi(\psi(x, g), h) = \psi(x, gh)$, *para todo $g, h \in G$*

É comum omitir a função e usar a notação $\varphi(g, x) = gx$ ou $g(x)$ e $\psi(x, g) = xg$.

Definição 1.1.12. *Seja X um conjunto sob a ação de um grupo G. A* ***órbita*** *de um elemento $x \in X$ é o conjunto*

$$G(x) = \{gx \mid g \in G\}$$

Note que pelas propriedades de um grupo, o conjunto das órbitas dos elementos de X forma uma partição de X.

Agora vamos definir um grupo que será bastante utilizado nesta dissertação.

Definição 1.1.13. *Seja X um conjunto e considere o conjunto de todas as permutações de X, isto é, de todas as funções biunívocas $f\colon X \to X$. Temos que tal conjunto é um grupo sob a operação usual de composição de funções e vamos denominá-lo de* ***grupo simétrico****. No caso em que X é finito e possui n elementos denotaremos por S_n o grupo simétrico de n elementos.*

Observação 1.1.1. *Nesta dissertação, a não ser que dito o contrário, iremos considerar a aplicação das permutações da esquerda para a direita.*

Seja $\sigma \in S_n$, uma permutação do grupo simétrico de n elementos $\{1, 2, \ldots, n\}$. Uma das notações mais comuns usadas para representar σ é

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Outra notação, que será a mais usada nesta dissertação, é a notação cíclica:

$$\sigma = (a_{11}a_{12}\ldots a_{1n_1})(a_{21}a_{22}\ldots a_{2n_2})\cdots(a_{m1}a_{m2}\ldots a_{mn_m})$$

em que não há repetições de números, e $\sigma(a_{ji}) = a_{j,i+1}, j = 1, \ldots, m, i = 1, \ldots, n_j - 1$ e $\sigma(a_{jn_j}) = a_{j1}$. Dizemos que cada $(a_{i1}a_{i2}\ldots a_{in_i})$ é um ciclo de tamanho n_i. Note que os ciclos $(a_{i1}a_{i2}\ldots a_{in_i})$ e $(a_{i2}\ldots a_{in_i}a_{i1})$ são equivalentes e então um ciclo não se altera ao permutarmos ciclicamente os seus elementos. No caso em que $n_i = 1$, é comum omitir o ciclo (a_{i1}) da notação.

Definição 1.1.14. *Também chamamos de* ***ciclo*** *uma permutação composta por apenas um ciclo de tamanho diferente de 1. Um ciclo de tamanho 2, isto é, uma permutação que troca apenas dois elementos e preserva os outros, é denominado* ***transposição****.*

Definição 1.1.15. *Dois ciclos são* ***disjuntos*** *se cada elemento é movido por no máximo um desses ciclos, isto é, σ e τ em S_n são disjuntos se $\sigma(m) = m$ ou $\tau(m) = m$, para cada $m = 1, \ldots, n$. Note que se dois ciclos σ e τ em S_n são disjuntos, então eles comutam, isto é, $\sigma\tau = \tau\sigma$.*

A partir da própria definição da notação em ciclos conseguimos ver que toda permutação pode ser escrita como um produto de ciclos disjuntos e que essa decomposição é única a menos da ordem dos ciclos. Além disso, podemos verificar diretamente que

$$(a_1a_2 \dots a_i \dots a_m)(a_1a_i) = (a_1a_2 \dots a_{i-1})(a_i \dots a_m) \tag{1.1}$$

$$(a_1a_2 \dots a_i \dots a_m) = (a_1a_2 \dots a_{i-1})(a_i \dots a_m)(a_1a_i) \tag{1.2}$$

em particular, tomando $i = m$ em (1.2)

$$(a_1a_2 \dots a_m) = (a_1a_2 \dots a_{m-1})(a_1a_m)$$

Então conseguimos decompor um ciclo de tamanho m em $m-1$ transposições:

$$(a_1a_2 \dots a_m) = (a_1a_2)(a_1a_3) \cdots (a_1a_m)$$

Com isso demonstramos que todo elemento de S_n pode ser escrito como produto de transposições. Diremos que uma permutação é par quando puder ser escrita como produto de uma quantidade par de transposições e analogamente definimos uma permutação ímpar. Note que nesta definição não estamos excluindo a possibilidade de uma permutação ser par e ímpar ao mesmo tempo, porém podemos demonstrar que tal situação nunca ocorre (uma outra demonstração pode ser encontrada em (5)).

Demonstração. Como vimos anteriormente, uma permutação pode ser escrita de forma única como produto de ciclos disjuntos e cada ciclo de tamanho m pode ser decomposto em $m-1$ transposições. Então diremos que uma permutação será par (ímpar) se tiver uma quantidade par (ímpar) de ciclos de tamanho par e vamos mostrar que ao multiplicar uma permutação por uma transposição (a_ia_j) obtemos uma permutação do outro tipo. Temos dois casos:

(i) Se a_i e a_j estiverem no mesmo ciclo, vamos considerar a representação desse ciclo que tem a_i como o primeiro elemento. Usando (1.1) temos que esse ciclo será quebrado em dois ciclos menores disjuntos. Se esse ciclo for de tamanho par, os ciclos menores terão tamanho ambos pares ou ambos ímpares, caso contrário, um ciclo menor terá tamanho par e o outro ímpar. Em ambos os casos o número de ciclos de tamanho par é alterado em $+1$ ou -1.

(ii) Se a_i e a_j estiverem em ciclos distintos, vamos considerar as representações desses ciclos que têm a_i e a_j como os primeiros elementos. Usando (1.2) temos que esses dois ciclos serão unidos em um único ciclo. Se o tamanho dos ciclos menores for de mesma paridade, o ciclo maior terá tamanho par, caso contrário o ciclo maior terá tamanho ímpar. Em ambos os casos o número de ciclos de tamanho par é alterado em $+1$ ou -1.

Portanto, ao multiplicarmos uma permutação par por uma transposição conseguimos uma permutação ímpar e vice-versa. □

Com isso podemos definir o seguinte:

Definição 1.1.16. *O **sinal** de uma permutação σ, denotada por* $\operatorname{sgn}(\sigma)$ *é igual a* 1 *se a permutação for par e* -1 *se a permutação for ímpar*

Agora vamos caracterizar as classes de conjugação de S_n. Primeiramente vamos fazer a seguinte definição:

Definição 1.1.17. *Seja $\sigma \in S_n$ e $(a_{11} \dots a_{1n_1}) \cdots (a_{m1} \dots a_{mn_m})$ a representação de σ como produto de ciclos disjuntos, sem omitir os ciclos de tamanho* 1*, tal que $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_m$. Diremos que o **tipo** de σ é $(n_1, n_2, \dots, n_m)$.*

Note que para cada tipo de permutação $(n_1, n_2, \dots, n_m)$, temos $n_1 + n_2 + \cdots + n_m = n$, e reciprocamente, para cada conjunto de números inteiros $n_1, \dots, n_m$ tais que $n_1 \geqslant n_2 \geqslant \dots \geqslant n_m \geqslant 1$, com $n_1 + \cdots + n_m = n$, existe pelo menos uma permutação $\sigma \in S_n$ de tipo $(n_1, \dots, n_m)$.

Definição 1.1.18. *Uma **partição** de n (com n inteiro positivo) é um conjunto de números inteiros $(n_1, n_2, \dots, n_m)$ tais que $n_1 \geqslant \cdots \geqslant n_m \geqslant 1$ e $n_1 + \cdots + n_m = n$. Denotaremos por $(n_1, n_2, \cdots, n_m) \vdash n$.*

Por fim, provaremos que existe uma correspondência biunívoca entre as classes de conjugação de S_n e as partições de n.

Proposição 1.1.1. *Sejam σ, $\tau \in S_n$ tais que $\sigma = (a_{11} \dots a_{1n_1}) \cdots (a_{m1} \dots a_{mn_m})$ é um produto de ciclos disjuntos. Então $\tau^{-1}\sigma\tau = (\tau(a_{11}) \dots \tau(a_{1n_1})) \cdots (\tau(a_{m1}) \dots \tau(a_{mn_m}))$.*

Demonstração. Suponha que $\sigma(i) = j$. Vamos denotar por $s = \tau(i)$ e $t = \tau(j)$. Com isso temos que $(\tau^{-1}\sigma\tau)(s) = \tau(\sigma(\tau^{-1}(s))) = \tau(\sigma(i)) = \tau(j) = t$, isto é, $\tau^{-1}\sigma\tau$ leva $\tau(i)$ a $\tau(j)$ e então temos o resultado. □

Corolário 1.1.1. *Duas permutações são conjugadas se e somente se têm o mesmo tipo, isto é, existe uma correspondência natural entre as classes de conjugação de S_n e as partições de n.*

1.2 Anéis

Definição 1.2.1. *Seja R um conjunto não vazio e $+ : R \times R \mapsto R$ e $\cdot : R \times R \mapsto R$ duas operações binárias denominadas soma (ou adição) e produto (ou multiplicação). A terna $(R, +, \cdot)$ é um **anel** se valem as seguintes propriedades:*

(i) $(R, +)$ *é um grupo abeliano*

(ii) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$, $c \cdot (a + b) = (c \cdot a) + (c \cdot b)$, *para todo* $a, b, c \in R$.

Notação 1.2.1. *Por simplicidade e quando não houver ambiguidades com relação às operações, diremos que* R *é um anel ao invés de* $(R, +, \cdot)$. *Em geral também omitiremos o produto* $\cdot$ *e o denotaremos por justaposição, isto é, usaremos* ab *no lugar de* $a \cdot b$.

Definição 1.2.2. *Um anel* R *é* ***associativo*** *se* $(ab)c = a(bc)$, *para todo* $a, b, c \in R$.

Definição 1.2.3. *Um anel* R *é* ***com unidade*** *ou* ***unitário*** *se existir* $1 \in R$ *tal que* $1a = a1 = a$, *para todo* $a \in R$. *O elemento* 1 *é chamado de* ***unidade*** *de* R.

Definição 1.2.4. *Um anel* R *é* ***comutativo*** *se* $ab = ba$, *para todo* $a, b \in R$.

Definição 1.2.5. *Diremos que* R *é um* ***domínio*** *ou* ***domínio de integridade*** *se* R *for um anel e* $ab = 0$ *implicar que* $a = 0$ *ou* $b = 0$, *para todo* $a, b \in R$.

Definição 1.2.6. *Um anel* R *é* ***de divisão*** *ou* ***com divisão*** *se* A *for anel com unidade* 1 *e se para todo* $a \in A$, $a \neq 0$, *existir* $b \in A$ *tal que* $ab = ba = 1$. *Denotaremos tal elemento por* a^{-1}.

Definição 1.2.7. *Diremos que* K *é* ***corpo*** *se* K *for um anel de divisão comutativo.*

Seguindo o foco deste trabalho, quando dissermos **anel**, estaremos nos referindo a um **anel associativo, não necessariamente comutativo e não necessariamente com unidade**.

Vamos definir algumas terminologias para elementos e subestruturas de um anel. Considere que R é um anel.

Definição 1.2.8. *Um elemento* $a \in R$ *é dito ser* ***nilpotente*** *se existe* $n \in \mathbb{N}$ *tal que* $a^n = 0$.

Definição 1.2.9. *Um elemento* $a \in R$ *é dito ser* ***idempotente*** *se* $a^2 = a$.

Definição 1.2.10. *Um subconjunto não vazio* $S \subset R$ *é um* ***subanel*** *se* S *for um anel sob as operações induzidas de* R.

Definição 1.2.11. *Definimos o* ***centro*** *de um anel, denotado por* $Z(R)$, *como o conjunto dos elementos que comutam com todos os elementos desse anel, isto é*

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

Note que o centro de um anel é um subanel de R *e se* R *for um anel de divisão então* $Z(R)$ *é um corpo.*

Definição 1.2.12. *Seja I um subgrupo aditivo de R, então I é um* ***ideal à esquerda****, denotado por $I \lhd_l R$, se $ai \in I$, para todo $a \in R$ e $i \in I$. Analogamente, I é um* ***ideal à direita****, denotado por $I \lhd_r R$, se $ia \in I$, para todo $a \in R$ e $i \in I$. Por fim, I é um* ***ideal bilateral****, ou simplesmente* ***ideal****, denotado por $I \lhd R$, se $ia, ai \in I$, para todo $a \in R$ e $i \in I$.*

Definição 1.2.13. *Seja $(S, \oplus, \odot)$ um anel. Uma função $f : R \to S$ é denominada* ***homomorfismo de anéis*** *se $f(a+b) = f(a) \oplus f(b)$ e $f(a \cdot b) = f(a) \odot f(b)$, para todo $a, b \in R$. Se R e S admitem unidades 1_R e 1_S, respectivamente, exigiremos também que $f(1_R) = 1_S$.*

Definição 1.2.14. *Seja S um anel e $f : R \to S$ um homomorfismo de anéis. Então f é um* ***isomorfismo de anéis*** *se for biunívoca. Ainda, dizemos que R e S são isomorfos e denotamos por $R \simeq S$.*

Agora vamos introduzir mais uma definição sobre corpos.

Definição 1.2.15. *Seja K um corpo. A* ***característica*** *de K é o menor inteiro positivo n tal que $n \cdot 1 = 0$. Se não existir tal inteiro positivo, dizemos que a característica do corpo é 0.*

Observação 1.2.1. *A característica de um corpo é sempre zero ou um número primo.*

Por fim, como um exemplo de anel e de corpo que iremos utilizar neste trabalho temos o anel de polinômios e seu corpo de frações. Maiores detalhes podem ser vistos no livro de Herstein (5).

Definição 1.2.16. *Seja K um corpo. O* ***anel de polinômios*** *em uma variável x sobre o corpo K, denotado por $K[x]$, é o anel formado pelos polinômios na variável x com coeficientes em K e com as propriedades usuais de igualdade, soma e produto de polinômios. Também consideraremos polinômios em várias variáveis comutativas $X = \{x_1, \ldots, x_t\}$ e denotaremos o anel de tais polinômios por $K[X]$ ou $K[x_1, \ldots, x_t]$.*

Como o anel de polinômios $K[x]$ é um domínio, podemos construir o seu corpo de frações.

Notação 1.2.2. *Seja K um corpo e x uma variável. Denotaremos por $K(x)$ o corpo de frações de $K[x]$, que é o menor corpo que contém $K[x]$. Ele também é chamado de corpo das funções racionais.*

Definição 1.2.17. *Um corpo K é* ***algebricamente fechado*** *se todo o polinômio não nulo de $K[x]$ tiver uma raiz em K.*

1.3 Álgebras

Começaremos com a definição de álgebra:

Definição 1.3.1. *Sejam A um espaço vetorial sobre um corpo K e uma operação binária $\cdot$ em A que denominaremos de produto. Dizemos que A é uma* ***álgebra*** *sobre o corpo K, ou simplesmente uma K-álgebra, se $\cdot$ é bilinear sobre K, isto é, satisfaz:*

(i) $(a_1 + \alpha a_2) \cdot b = a_1 \cdot b + \alpha(a_2 \cdot b)$, *para todo* $a_1, a_2, b \in A$, *e* $\alpha \in K$

(ii) $a \cdot (b_1 + \alpha b_2) = a \cdot b_1 + \alpha(a \cdot b_2)$, *para todo* $a, b_1, b_2 \in A$, *e* $\alpha \in K$

Notação 1.3.1. *Quando não houver ambiguidades com relação ao produto vamos omiti-lo, representando o produto pela simples justaposição dos elementos.*

Definição 1.3.2. *Uma álgebra A é* ***associativa*** *se $(ab)c = a(bc)$, para todo $a, b, c \in A$.*

Definição 1.3.3. *Uma álgebra A é* ***com unidade*** *ou* ***unitária*** *se existir $1 \in A$ tal que $1a = a1 = a$, para todo $a \in A$. O elemento 1 é chamado de* ***unidade*** *de A.*

Definição 1.3.4. *Uma álgebra A é* ***comutativa*** *se $ab = ba$, para todo $a, b \in A$.*

Seguindo o foco deste trabalho, quando dissermos **álgebra**, estaremos nos referindo a uma **álgebra associativa, não necessariamente comutativa e não necessariamente com unidade**.

Exemplo 1.3.1. *As matrizes $n \times n$ sobre um corpo K (ou anel de divisão) formam uma álgebra sobre K (sobre o centro $Z(K)$ de K), que denotaremos por $M_n(K)$, com a soma e o produto usual de matrizes. Esta álgebra é associativa e com unidade. Ela é comutativa apenas quando K é corpo e $n = 1$. Se $n > 1$ ou K é um anel de divisão não comutativo, $M_n(K)$ não é comutativa.*

Note que toda álgebra (associativa) é um anel. Todas as estruturas envolvendo álgebras (subálgebras, ideais, homomorfismos ...) são definidas de forma análoga ao caso de anéis, com a exigência adicional de que a estrutura seja compatível com a ação dos elementos do corpo (isto é, que trabalhemos sobre espaços vetoriais). Nas definições a seguir considere que A é uma álgebra sobre K.

Definição 1.3.5. *Um subespaço vetorial $S \subset A$ é uma* ***subálgebra*** *se $s_1 s_2 \in S$, para todo $s_1, s_2 \in S$.*

Definição 1.3.6. *Seja $I \subset A$ um subespaço vetorial, então I é um* ***ideal à esquerda****, denotado por $I \lhd_l A$, se $ai \in I$, para todo $a \in A$ e $i \in I$. Analogamente, I é um* ***ideal à direita****, denotado por $I \lhd_r A$, se $ia \in I$, para todo $a \in A$ e $i \in I$. Por fim, I é um* ***ideal***

***bilateral**, ou simplesmente **ideal**, denotado por $I \lhd A$, se $ia, ai \in I$, para todo $a \in A$ e $i \in I$.*

Definição 1.3.7. *Dizemos que A é **simples** se $A^2 \neq 0$, isto é, o produto é não nulo (existem $a, b \in A$ tais que $ab \neq 0$), e os únicos ideais bilaterais de A são 0 e A.*

Definição 1.3.8. *Definimos o **centro** de uma álgebra, denotado por $Z(A)$, como o conjunto dos elementos que comutam com todos os elementos da álgebra, isto é*

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

Exemplo 1.3.2. *Se K é um corpo, então a álgebra das matrizes $M_n(K)$ é uma álgebra simples e o centro de $M_n(K)$ são as matrizes escalares. Se K é um anel de divisão, $M_n(K)$ de novo é simples e seu centro consiste das matrizes escalares cujas entradas na diagonal estão no centro $Z(K)$ de K.*

Definição 1.3.9. *Seja B uma álgebra sobre o mesmo corpo K. Uma função $f : A \to B$ é denominada **homomorfismo de álgebras** se f é uma transformação K-linear e $f(ab) = f(a)f(b)$, com o primeiro produto em A e o segundo em B, para todo $a, b \in A$. Se A e B admitem unidades 1_A e 1_B, respectivamente, exigiremos também que $f(1_A) = 1_B$.*

Definição 1.3.10. *Seja B uma álgebra sobre o mesmo corpo K e $f : A \to B$ um homomorfismo de álgebras. Então f é um **isomorfismo de álgebras** se for biunívoco. Ainda, dizemos que A e B são isomorfas e denotamos por $A \simeq B$.*

Vamos definir a álgebra quociente. Este conceito também está presente em grupos e em anéis, mas como nesta dissertação o usaremos apenas para álgebras optamos por deixá-lo nesta seção.

Sejam A uma álgebra sobre o corpo K e $I \lhd A$ um ideal bilateral. Então, podemos construir a álgebra quociente A/I da seguinte maneira. Para cada $a \in A$, definimos o conjunto $a + I = \{a + i : i \in I\} \subset A$, que denominamos de classe de equivalência de a. O elemento a é denominado representante da classe. Por fim, denotamos o conjunto de todas as classes de equivalência por $A/I = \{a + I : a \in A\}$.

Para dar uma estrutura de álgebra para A/I, vamos definir a soma e produto por $(a + I) + (b + I) = (a + b) + I$, $(a + I)(b + I) = ab + I$, para todo $a, b \in A$ e o produto por escalar por $\alpha(a + I) = \alpha a + I$, para todo $\alpha \in K$ e $a \in A$. A/I é de fato uma álgebra pois podemos provar que:

(i) $a + I = b + I$ ou $(a + I) \cap (b + I) = \varnothing$, para todo $a, b \in A$,

(ii) $a + I = b + I$ se e só se $a - b \in I$,

(iii) a soma, o produto e o produto por escalar definidos acima estão bem definidos, isto é, não dependem da escolha do representante, em outras palavras, se $a + I = a' + I$, $b + I = b' + I$ e $\alpha \in K$, então

- $(a + I) + (b + I) = (a' + I) + (b' + I)$,
- $(a + I)(b + I) = (a' + I)(b' + I)$.
- $\alpha(a + I) = \alpha(a' + I)$.

Definição 1.3.11. *Sejam A e B duas álgebras sobre um mesmo corpo K com a operação produto definida por $\circ_A$ e $\circ_B$ respectivamente. Sabemos que o produto tensorial $A \otimes B$ tem a estrutura de espaço vetorial. Podemos então definir o* ***produto tensorial como álgebras*** *definindo uma multiplicação $\circ$ em $A \otimes B$, bilinear, da seguinte forma*

$$(a_1 \otimes b_1) \circ (a_2 \otimes b_2) = (a_1 \circ_A a_2) \otimes (b_1 \circ_B b_2).$$

Segue da propriedade universal do produto tensorial de espaços vetoriais que $A \otimes B$ com a operação $\circ$ é uma K-álgebra.

Agora vamos definir os objetos de estudo desta dissertação:

Definição 1.3.12. *Uma álgebra A sobre um corpo K é* ***nil*** *se todo elemento $a \in A$ é nilpotente, isto é, para cada $a \in A$ existe um número natural n (que pode depender de a) tal que $a^n = 0$. O menor número com tal propriedade é chamado de grau ou índice de nilpotência do elemento a. Uma álgebra é nil de grau limitado se existe um número natural n fixo tal que $a^n = 0$ para todo $a \in A$.*

Definição 1.3.13. *Uma álgebra A sobre um corpo K é* ***nilpotente*** *se existe um número natural n fixo tal que o produto de quaisquer n elementos de A é igual a zero, isto é $A^n = 0$. O menor número n com esta propriedade é chamado grau ou índice de nilpotência da álgebra A.*

Definição 1.3.14. *Uma álgebra A sobre um corpo K é* ***algébrica*** *se todo elemento $a \in A$ é algébrico, isto é, é raiz de algum polinômio não nulo com coeficientes em K.*

Definiremos uma álgebra muito importante nesta dissertação:

Definição 1.3.15. *Seja $\mathscr{B}$ uma classe de álgebras (não necessariamente associativas) e seja F uma álgebra gerada por um conjunto X. Dizemos que F é uma* ***álgebra livre em*** *$\mathscr{B}$ se, para cada $A \in \mathscr{B}$ e cada função $f : X \to A$, existe um único homomorfismo de álgebras $F \to A$ que estende f. Define-se o* ***posto*** *de F como sendo a cardinalidade do conjunto X.*

Em particular, a álgebra de polinômios não comutativos é uma álgebra livre:

Teorema 1.3.1. *Para cada conjunto X, a álgebra $K\langle X\rangle$, espaço vetorial que tem como base todos os monômios*

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

em que $n\in\mathbb{N}$ e $x_{i_1},\ldots,x_{i_n}\in X$ e a multiplicação é definida por justaposição:

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

é uma álgebra livre na classe de todas as álgebras associativas unitárias sobre o corpo K. Se considerarmos o subespaço de $K\langle X\rangle$ gerado por todas os monômios de tamanho maior ou igual a 1, que denotaremos por $K^+\langle X\rangle$, então obteremos a álgebra associativa não comutativa livre, que será livre na classe de todas as álgebras associativas. Denotaremos por $K\langle X_n\rangle$ ou $K\langle x_1,\ldots,x_n\rangle$ a álgebra livre não-comutativa associativa unitária de posto $n\in\mathbb{N}$.

A seguir definiremos alguns termos que usaremos relacionadas a polinômios.

Definição 1.3.16. *Dado um monômio $g = x_{i_1}\cdots x_{i_n}\in K\langle X\rangle$ nas variáveis $x_{i_1},\ldots,x_{i_n}\in X$, dizemos que o **grau** de g é n, denotado por $\deg g$. Também definimos o grau de um monômio em relação à variável x_i, que denotaremos por $\deg_{x_i} g$, como o número de vezes que ela aparece na representação do monômio. Se $X=\{x_1,\ldots x_m\}$, definimos o **multigrau** de g pela sequência $(\deg_{x_1} g,\ldots,\deg_{x_m} g)$.*

Definição 1.3.17. *Dado um polinômio $f\in K\langle X\rangle$, diremos que o **grau** do polinômio, denotado por $\deg f$, é igual ao maior entre os graus de seus monômios. Analogamente definimos o grau de um polinômio em relação à variável x_i, que denotaremos por $\deg_{x_i} f$, como o maior entre os graus em relação à x_i de seus monômios. Se todos os monômios de f tem o mesmo multigrau, então dizemos que f é **multi-homogêneo** de multigrau $(\deg_{x_1} f,\cdots,\deg_{x_m} f)$.*

Definição 1.3.18. *Ao trabalharmos com monômios não comutativos é comum usarmos os termos **alfabeto** para o conjunto X de variáveis, **letra** no lugar de variável e **palavra** no lugar de monômios. Também usamos o termo **comprimento** para o grau do monômio e chamamos de **palavra vazia** a palavra de comprimento zero. Dizemos que v é uma **subpalavra** de uma palavra w se existem palavras w_1 e w_2, possivelmente vazias, tais que $w = w_1vw_2$.*

Uma construção semelhante à álgebra $K\langle X\rangle$ é a obtida a partir de um grupo e um corpo de escalares.

Definição 1.3.19. *Seja G um grupo (ou um semigrupo) e K um corpo. A **álgebra de grupo de** G **sobre** K, denotada por KG, é o espaço vetorial formal sobre K com base $\{e_g\}_{g\in G}$, com o produto definido na base por $e_ge_h = e_{gh}, g,h\in G$. Muitas vezes denotaremos os elementos da base pelos elementos do grupo, ou seja, usamos $g := e_g\in KG$.*

1.4 Módulos

Nesta seção apenas apresentaremos definições e terminologia básica sobre módulos, além de alguns resultados usados no decorrer da dissertação. Uma exposição bem mais detalhada pode ser encontrada no livro de Lambek (7).

Definição 1.4.1. *Sejam R um anel, $(M,+)$ um grupo abeliano e uma operação $\cdot : R\times M \to M$ denominada produto ou multiplicação por escalar. Dizemos que M é um R-**módulo** (à esquerda) se para todo $m,n \in M$ e $r,s \in R$ temos:*

(i) $r\cdot(m+n) = r\cdot m + r\cdot n$,

(ii) $r\cdot(s\cdot m) = (rs)\cdot m$,

(iii) $(r+s)\cdot m = r\cdot m + s\cdot m$,

Se R admitir unidade 1, dizemos que M é um R-módulo unitário (à esquerda) e exigimos também que:

(iv) $1\cdot m = m$.

De forma análoga, definimos R-módulo à direita, em que a ação é dada pela direita, isto é, consideramos a operação $\cdot : M\times R \to M$.

Notação 1.4.1. *Quando não houver ambiguidades omitiremos o produto $\cdot$ e o denotaremos por justaposição, isto é, usaremos mr no lugar de $m\cdot r$.*

Definição 1.4.2. *Sejam M um R-módulo e $N \subset M$ um subconjunto não vazio. Dizemos que N é um R-**submódulo** se N for um subgrupo aditivo de M e $rn \in N$ para todo $n \in N$ e $r \in R$.*

Observação 1.4.1. *Sejam R um anel e $I \lhd_l R$ um ideal à esquerda. Então I admite naturalmente uma estrutura de R-módulo à esquerda. Em particular, o próprio anel R é um R-módulo à esquerda. Além disso, os ideais à esquerda de R são todos os R-submódulos do R-módulo à esquerda R.*

Definição 1.4.3. *Sejam M e N R-módulos e $f : M \to N$ função. Dizemos que f é **homomorfismo de R-módulos** se, para todo $m,n \in M$ e $r \in R$,*

(i) $f(m+n) = f(m) + f(n)$,

(ii) $f(rm) = rf(m)$.

Definição 1.4.4. *Sejam M e N R-módulos e $f : M \to N$ um homomorfismo de R-módulos. O* ***núcleo*** *de f é o conjunto* $\ker f := \{m \in M : f(m) = 0\}$ *e a* ***imagem*** *de f é o conjunto $f(M) := \{f(m) : m \in M\}$. Note que* $\ker f$ *e $f(M)$ são R-submódulos de M e N respectivamente.*

Definição 1.4.5. *Um homomorfismo de R-módulos $f : M \to N$ é um* ***isomorfismo*** *se for f for biunívoco. Ainda, dizemos que M e N são isomorfos e denotamos por $M \simeq N$.*

Enunciaremos um dos teoremas de isomorfismo de módulos:

Teorema 1.4.1. *Seja $f : M \to N$ um homomorfismo sobrejetor de R-módulos. Então $M/Ker\, f \simeq N$.*

Também podemos definir módulos sobre álgebras. As definições de submódulo e de homomorfismo neste caso são análogas às do caso de módulos sobre anéis, com a exigência adicional de ser compatível com a ação dos elementos do corpo.

Definição 1.4.6. *Seja A uma álgebra sobre um corpo K, M um espaço vetorial também sobre K e considere uma operação $(a, m) \in A \times M \mapsto am \in M$. Dizemos que M é um* ***A-módulo*** *(à esquerda) se essa operação satisfaz, para todo $\alpha \in K$, $m, n \in M$ e $a, b \in A$,*

(i) $(ab)m = a(bm)$,

(ii) $(a + b)m = am + bm$,

(iii) $a(m + n) = am + an$,

(iv) $\alpha(am) = (\alpha a)m = a(\alpha m)$.

De forma análoga podemos definir A-módulo à direita.

Definição 1.4.7. *Seja M um R-módulo. M é* ***irredutível*** *se $RM \neq 0$ e os únicos submódulos de M são 0 e M.*

Definição 1.4.8. *Um R-módulo M é* ***completamente redutível*** *(ou semissimples) se M for soma direta de alguns de seus submódulos irredutíveis.*

Definição 1.4.9. *Um anel R é* ***completamente redutível*** *se for completamente redutível como um R-módulo à esquerda.*

Aqui iremos citar o importante teorema de Wedderburn-Artin que classifica os anéis completamente redutíveis. Uma demonstração pode ser encontrada no livro de Lambek (7).

Teorema 1.4.2 (Wedderburn-Artin)**.** *Seja R um anel com unidade 1. Então*

(i) R *é completamente redutível se e só se* $R = \bigoplus_{i=1}^{m} R_i$*, com cada* R_i *anel completamente redutível e simples,*

(ii) R *é completamente redutível e simples se e só se* $R \simeq M_n(D)$*, para algum* $n \in \mathbb{N}$ *e algum anel de divisão* D*.*

1.5 Álgebras com Identidades Polinomiais

Nesta seção definiremos o contexto principal no qual estaremos trabalhando nesta dissertação: as álgebras com identidade polinomial, ou simplesmente, PI-álgebras.

Definição 1.5.1. *Seja* A *uma álgebra associativa. Dizemos que* A *é uma* ***álgebra com identidade polinomial****, ou simplesmente* ***PI-álgebra****, se existe um polinômio não trivial* $f(x_1, \ldots, x_m) \in K\langle X\rangle$ *tal que* $f(a_1, \ldots, a_m) = 0$*, para todo* $a_1, \ldots, a_m \in A$*. Neste caso, dizemos que* A *satisfaz a* ***identidade polinomial*** $f(x_1, \ldots, x_m)$*, ou simplesmente* f *(ou ainda* $f = 0$*) é uma identidade de* A*.*

Observação 1.5.1. *Um polinômio* $f \in K\langle X\rangle$ *é uma identidade de uma álgebra* A *se e somente se para todo homomorfismo de álgebras* $\psi : K\langle X\rangle \to A$*, temos* $\psi(f) = 0$*.*

Vamos dar alguns exemplos de PI-álgebras.

Exemplo 1.5.1. *Uma álgebra* A *é comutativa se e somente se satisfaz a identidade* $[x_1, x_2] = x_1x_2 - x_2x_1 = 0$*. Denominamos* $[a, b]$ *de* ***comutador*** *de dois elementos* a *e* b*.*

Definição 1.5.2. *O* ***polinômio standard*** *é*

$$s_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) x_{\sigma(1)} \cdots x_{\sigma(n)}.$$

Definição 1.5.3. *O* ***polinômio de Capelli*** *é*

$$d_n(x_1, \ldots, x_n, y_1, \ldots, y_{n-1}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) x_{\sigma(1)} y_1 x_{\sigma(2)} \cdots y_{n-1} x_{\sigma(n)}.$$

Exemplo 1.5.2. *Uma álgebra* A *de dimensão finita* m *satisfaz a identidade standard* s_n *e a identidade de Capelli* d_n *para todo* $n > m$*. Para provar essa afirmação, note que esses polinômios são multilineares logo é necessário apenas verificar a propriedade para os elementos de uma base. Como* $n > m$*, algum elemento da base se repete e então, como os polinômios são antissimétricos em* $x_1, \ldots, x_n$*, temos que eles são identidades para elementos dessa base. Portanto* A *satisfaz as duas identidades. O leitor pode fazer a analogia com a bem conhecida propriedade do determinante da álgebra linear básica: se a matriz tem duas linhas (ou colunas) iguais, então seu determinante é igual a 0. Este fato é usado para deduzir que o determinante é uma função alternada nas suas linhas ou colunas.*

Estes dois últimos exemplos mostram que as PI-álgebras são uma generalização tanto de álgebras comutativas quanto de álgebras de dimensão finita.

Vamos definir mais um polinômio, e fazer uma observação sobre ele.

Definição 1.5.4. *A **identidade de algebricidade** é*

$$\begin{aligned} a_n(x, y_1, \ldots, y_n) &= d_{n+1}(1, x, \ldots, x^n, y_1, \ldots, y_{n+1}) \\ &= \sum_{\sigma \in S_{n+1}} \operatorname{sgn}(\sigma) x^{\sigma(0)} y_1 x^{\sigma(1)} \cdots y_n x^{\sigma(n)} \end{aligned}$$

em que $\sigma \in S_{n+1}$ age sobre $\{0, 1, \ldots, n\}$.

Observação 1.5.2. *Seja A uma álgebra sobre o corpo K. Se $a \in A$ é algébrico, isto é, se existe um polinômio de grau n e coeficientes em K tal que a é solução desse polinômio, então $1, a, \ldots, a^n$ são linearmente dependentes e portanto $a_n(a, y_1, \ldots, y_n) = 0$. Assim, se A é uma álgebra algébrica de grau limitado n então ela satisfaz a identidade de algebricidade a_n.*

A seguir, iremos discutir as principais ideias para se estudar as identidades de uma álgebra:

Definição 1.5.5. *Seja R uma álgebra. O conjunto de todas as identidades polinomiais de R, que denotaremos por $T(R)$, formam um ideal bilateral da álgebra livre $K\langle X\rangle$ e é chamado de **T-ideal** de R.*

É comum na literatura encontrar a denominação *ideal verbal* para os T-ideais; tal terminologia vem da teoria de grupos.

Primeiramente, veja que T é um ideal bilateral porque multiplicar uma identidade polinomial à direita ou à esquerda por algum outro polinômio continua resultando em uma identidade polinomial. Além disso, note que se $f(x_1, \ldots, x_m)$ é uma identidade polinomial de R, então para quaisquer polinômios $w_1, \ldots, w_m \in K\langle X\rangle$ temos que $f(w_1, \ldots, w_m) = 0$, ou seja, um T-ideal é invariante sob substituições por elementos de $K\langle X\rangle$. Como todo endomorfismo φ de $K\langle X\rangle$ é completamente definido pelos valores que os elementos de X assumem, $\varphi(x_i) = w_i \in K\langle X\rangle$, podemos dizer que um T-ideal é invariante por endomorfismos de $K\langle X\rangle$. Por outro lado, se temos um ideal bilateral T de $K\langle X\rangle$ invariante por endomorfismos, então a álgebra quociente $K\langle X\rangle/T$ é uma álgebra cujo T-ideal é T.

Definição 1.5.6. *Diremos que uma identidade polinomial $g(x_1, \ldots, x_m)$ é uma **consequência** das identidades polinomiais $f_i(x_1, \ldots, x_{m_i})$, $i \in I$, se toda álgebra que satisfaz as identidades f_i também satisfaz g. Dado um conjunto de identidades polinomiais $F \subset K\langle X\rangle$, definimos o T-ideal T de $K\langle X\rangle$ **gerado** por F como sendo o menor T-ideal*

contendo F que denotaremos por $\langle F\rangle^T$. Se $F = \{f_1, \ldots, f_n\}$, denotaremos o T-ideal também por $\langle f_1, \ldots, f_n\rangle^T$. O conjunto F é chamado de ***base*** *das identidades polinomiais de T, mesmo que não seja um conjunto gerador minimal. Dizemos que dois conjuntos de identidades polinomiais F e G são* ***equivalentes*** *se elas geram o mesmo ideal, o que ocorre se e somente se F é consequência de G e G é consequência de F.*

Na prática, um polinômio g será consequência de $f_i(x_1, \ldots, x_{m_i})$, $i \in I$ se for possível obter g na seguinte forma

$$\sum u_{iw} f_i(w_1, \ldots, w_{m_i}) v_{iw}$$

em que $w_i, u_{iw}, v_{iw} \in K\langle X\rangle$.

Observação 1.5.3. *Ao trabalharmos com álgebras não unitárias, devemos considerar a álgebra associativa não unitária livre $K^+\langle X\rangle$ ao invés de $K\langle X\rangle$. A diferença mais importante em relação às considerações anteriores é que em $K^+\langle X\rangle$ um polinômio g será consequência de $f_i(x_1, \ldots, x_{m_i})$, $i \in I$ se for possível obter g na seguinte forma*

$$\sum u_{iw} f_i(w_1, \ldots, w_{m_i}) v_{iw}$$

em que $w_i \in K^+\langle X\rangle$ e $u_{iw}, v_{iw} \in K + K^+\langle X\rangle = K\langle X\rangle$.

Agora vamos reformular as duas definições sobre álgebras que serão o objeto principal desta dissertação em termos de PI-álgebras:

Definição 1.5.7. *Uma álgebra A é nil de grau (ou índice) limitado menor ou igual a n se e somente se A satisfaz a identidade polinomial $x^n = 0$.*

Definição 1.5.8. *Uma álgebra A é nilpotente de grau (ou índice) menor ou igual a n se e somente se A satisfaz a identidade polinomial $x_1 \cdots x_n = 0$.*

Isso nos permite reformular a principal questão do Capítulo 3 "uma álgebra nil de grau limitado é nilpotente? Se sim, qual é o grau de nilpotência?" para "a identidade $x_1 \cdots x_m = 0$ é consequência de $x^n = 0$ para algum m? Qual é o menor m tal que a identidade é válida?".

Na grande maioria das demonstrações desse capítulo faremos uso da álgebra associativa livre, do T-ideal T gerado por $x^n = 0$ e da álgebra quociente $K^+\langle X\rangle/T$. O que nos permite afirmar que é suficiente analisar tal situação são as observações a seguir:

Definição 1.5.9. *Seja $F = \{f_i(x_1, \ldots, x_{m_i}), i \in I\} \subset K\langle X\rangle$. A classe $\mathscr{U}$ de todas as álgebras associativas que satisfazem todas as identidades polinomiais $f_i = 0$, $i \in I$ é chamada de* ***variedade de álgebras associativas gerada*** *pelo sistema de identidades polinomiais $\{f_i = 0 \mid i \in I\}$. Denotaremos por $T(\mathscr{U})$ o T-ideal de todas as identidades polinomiais satisfeitas por $\mathscr{U}$.*

Existe uma correspondência biunívoca π entre os T-ideais de $K\langle X\rangle$ e as variedades de álgebras associativas: Para todo T-ideal T nós definimos $\mathscr{U} = \pi(T)$ como a variedade definida pelas identidades polinomiais de T. Esta é uma "correspondência de Galois", isto é, para dois T-ideais $T_1 \subset T_2$ temos que $\pi(T_1) \supset \pi(T_2)$.

Definição 1.5.10. *Seja $\mathscr{U}$ uma variedade. Uma álgebra F é dita ser* ***relativamente livre em*** *$\mathscr{U}$ se F for livre na classe $\mathscr{U}$.*

Observação 1.5.4. *A álgebra quociente $F(\mathscr{U}) = K^+\langle X\rangle/T(\mathscr{U})$ é a álgebra associativa não unitária relativamente livre de posto enumerável na variedade $\mathscr{U}$.*

1.6 Ferramentas para Identidades Polinomiais

Nesta seção veremos alguns fatos e ferramentas básicas para trabalharmos com identidades polinomiais. Os resultados aqui mostrados estão baseados no livro de Drensky (3). Começaremos com um conceito que será muito explorado neste trabalho.

Denotaremos por T_n o espaço dos polinômios multilineares de grau n nas variáveis $x_1, \ldots, x_n$. Note que T_n é um espaço vetorial e $\{x_{\sigma(1)} \cdots x_{\sigma(n)} : \sigma \in S_n\}$ é uma base de T_n.

Teorema 1.6.1. *Seja $f(x_1, \ldots, x_m) \in K\langle X\rangle$ e escreva $f = \sum_{i=0}^{n} f_i$, com f_i homogêneo de grau i em relação à x_1. Então:*

(i) Se K contém mais que n elementos (por exemplo, quando K é infinito), então $f_i = 0$ é consequência de $f = 0$, para cada $i = 0, 1, \ldots, n$.

(ii) Se a característica de K for 0 (ou maior que $\deg f$), então $f = 0$ é equivalente a um conjunto finito de polinômios multilineares, os quais podem ser sobre uma quantidade maior de variáveis do que f.

Demonstração. (i) Sejam $\alpha_0, \alpha_1, \ldots, \alpha_n \in K$ distintos e seja $T = \langle f\rangle^T$ o T-ideal gerado por f. Então, como T é fechado por endomorfismos, segue que

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

para $j = 0, 1, \cdots, n$. Então, escrevendo em forma matricial, temos

$$\begin{pmatrix} f(\alpha_0 x_1, x_2, \ldots, x_m) \\ f(\alpha_1 x_1, x_2, \ldots, x_m) \\ \vdots \\ f(\alpha_n x_1, x_2, \ldots, x_m) \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \ldots & \alpha_0^n \\ 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^n \end{pmatrix}}_{M} \begin{pmatrix} f_0(x_1, \ldots, x_m) \\ f_1(x_1, \ldots, x_m) \\ \vdots \\ f_n(x_1, \ldots, x_m) \end{pmatrix}$$

A matriz M é uma matriz de Vandermonde, cujo determinante é $\prod_{i<j}(\alpha_i - \alpha_j) \neq 0$, e portanto é invertível. Assim f_i é combinação linear de $f(\alpha_j x_1, x_2, \ldots, x_m) \in T$ e portanto $f_i = 0$ é consequência de $f = 0$, para todo $i = 0, 1, \ldots, n$.

(ii) Iremos usar o processo de linearização. De (i), podemos assumir f homogêneo em cada variável, ou seja, multi-homogêneo. Seja $d = \deg_{x_1} f$, podemos escrever

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

em que cada f_i é a componente homogênea de grau i em relação à y_1. De (i), $f_i \in T$. Como $\deg_{y_1} f_i < d$ e $\deg_{y_2} f_i < d$ para $i = 1, \ldots, d-1$, podemos continuar esse processo e obter um conjunto de polinômios multilineares. Para verificarmos que f é equivalente a essas identidades, basta notar que

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

e o coeficiente binomial é diferente de zero pois a característica do corpo é 0 ou maior que d.

□

Definição 1.6.1. *Denominamos de **linearização parcial** o passo usado na demonstração anterior de considerar $f(y_1+y_2, x_2, \ldots, x_m)$ e tomar a componente de grau $d-1$ em relação à y_1 e linear em y_2. A **linearização total** é obtida ao repetir esse processo até obter um polinômio multilinear.*

Um polinômio extremamente importante nesta dissertação pode ser definido da seguinte maneira

Definição 1.6.2. *Denotaremos por e_n o resultado da linearização total da identidade $x^n = 0$.*

$$e_n(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} x_{\sigma(1)} \cdots x_{\sigma(n)}. \tag{1.3}$$

Esta identidade polinomial é consequência de x^n, e caso o corpo tenha característica 0 ou maior que n, ela é equivalente a x^n.

Por fim, vamos provar que qualquer PI-álgebra satisfaz alguma identidade multilinear, independentemente do corpo base.

Proposição 1.6.1. *Seja A uma PI-álgebra. Então A satisfaz uma identidade multilinear.*

Demonstração. Seja $f(x_1, \ldots, x_m)$ uma identidade de A. Se $d = \deg_{x_1} f > 1$, então

$$\begin{aligned} g(y_1, y_2, x_2, \ldots, x_m) =& f(y_1 + y_2, x_2, \ldots, x_m) \\ & - f(y_1, x_2, \ldots, x_m) - f(y_2, x_2, \ldots, x_m) \end{aligned}$$

tem uma componente homogênea de grau $d-1$ em relação à y_1 e linear em y_2 e nenhuma componente homogênea de grau d em relação à y_1 ou y_2. Continuando com esse processo de aumentar o número de variáveis e de diminuir os seus graus, conseguimos linearizar em relação à variável x_1. Repetindo para as outras variáveis obtemos uma identidade multilinear. □

1.7 Representações de Grupo

Nesta seção apresentaremos as definições básicas de representações de grupos e alguns resultados que serão necessários na seção seguinte. Fixaremos G um grupo finito. Dado V um espaço vetorial, denotaremos por $GL(V)$ o grupo de todos os automorfismos de V.

Definição 1.7.1. *Uma* ***representação*** *de G em V é um homomorfismo de grupos $\rho\colon G \to GL(V)$. O grau da representação é definido como a dimensão do espaço vetorial V e diremos que a representação é finita se o grau for finito.*

Notação 1.7.1. *Por simplicidade, diremos representação V para nos referirmos à representação $\rho\colon G \to GL(V)$. Além disso, também utilizaremos a notação $\rho_s := \rho(s)$, para cada $s \in G$.*

Definição 1.7.2. *Sejam G grupo e $\rho_1 : G \to GL(V_1)$ e $\rho_2 : G \to GL(V_2)$ duas representações. Dizemos que ρ_1 e ρ_2 são* ***equivalentes*** *ou* ***isomorfas*** *se existe um isomorfismo $T : V_1 \to V_2$ tal que $T \circ \rho_1(s) = \rho_2(s) \circ T, \forall s \in G$.*

Definição 1.7.3. *Seja $\rho : G \to GL(V)$ uma representação e $W \subset V$ um subespaço tal que $\rho_s(W) \subset W$, para todo $s \in G$. Então a representação $\psi : G \to GL(W)$ definida por $\psi_s(w) = \rho_s(w)$ é uma* ***subrepresentação*** *de ρ.*

Definição 1.7.4. *Dada uma representação $\rho : G \to GL(V)$, dizemos que V é* ***irredutível*** *se não admite subrepresentações diferentes de 0 e V.*

Definição 1.7.5. *Sejam $\rho_1 : G \to GL(V_1)$ e $\rho_2 : G \to GL(V_2)$ duas representações. A* ***soma direta*** *dessas representações é a representação $\rho = \rho_1 \oplus \rho_2 : G \to GL(V_1 \oplus V_2)$ definida por*

$$(\rho(s))(v_1, v_2) = ((\rho_1(s))(v_1), (\rho_2(s))(v_2))$$

em que $s \in G$, $v_1 \in V_1$, e $v_2 \in V_2$.

Um teorema muito importante sobre a decomposição de representações em somas diretas é o Teorema de Maschke.

Teorema 1.7.1. *Sejam G um grupo finito e K um corpo de característica zero ou $p > 0$ tal que p não divide $|G|$. Sejam $\rho : G \to GL(V)$ uma representação finita e $W \subset V$ uma subrepresentação. Então existe uma subrepresentação $W_0 \subset V$ tal que $V = W \oplus W_0$.*

Demonstração. Seja W' um subespaço qualquer de V tal que $V = W \oplus W'$, e considere a projeção $\pi : W \oplus W' \to W$. Definimos

$$\pi_0 = \frac{1}{|G|} \sum_{s \in G} \rho_s^{-1} \pi \rho_s.$$

Temos que π_0 é uma projeção, pois $\pi_0(V) \subset W$ e se $w \in W$, então $\rho_s(w) \in W$, para todo $s \in G$, e

$$\pi_0(w) = \frac{1}{g} \sum_{s \in G} \rho_s^{-1}(\underbrace{\pi(\rho_s(w))}_{\rho_s(w)}) = \frac{1}{g} \sum_{s \in G} w = w$$

e portanto $\pi_0^2 = \pi_0$ e $\pi_0(V) = W$. Segue que $V = W \oplus \ker \pi_0$, e mostraremos que $\ker \pi_0$ é uma subrepresentação de V.

Note que para todo $s \in G$, $\rho_s^{-1} \pi_0 \rho_s = \pi_0$, e assim $\pi_0 \rho_s = \rho_s \pi_0$. Então dado $x \in \ker \pi_0$, temos $\pi_0(\rho_s(x)) = \rho_s(\pi_0(x)) = 0$, e daí, $\rho_s(x) \in \ker \pi_0$. Portanto, $\rho_s(\ker \pi_0) \subset \ker \pi_0$ e segue que $\ker \pi_0$ é subrepresentação de V, o que conclui a demonstração. □

Observação 1.7.1. *A representação $\rho : G \to GL(V)$ é totalmente determinada pelas subrepresentações $\rho_W : G \to GL(W)$ e $\rho_{W_0} : G \to GL(W_0)$, isto é, V tem uma base $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_m\}$ em que $\{v_1, \ldots, v_k\}$ e $\{v_{k+1}, \ldots, v_m\}$ são bases de W e W_0, respectivamente, de forma que, para todo $s \in G$, temos, escrevendo os automorfismos na forma matricial:*

$$[\rho_s] = \begin{pmatrix} [\rho_W(s)] & 0 \\ 0 & [\rho_{W_0}(s)] \end{pmatrix}.$$

O teorema de Maschke mostra que toda representação não irredutível pode ser escrita como soma direta de duas subrepresentações. Podemos repetir o processo para cada subrepresentação (o processo terminará pois, por hipótese, a dimensão de V é finita) e concluir que V é soma direta de representações irredutíveis, isto é, temos o seguinte corolário. Muitas vezes ele é chamado de Teorema de Maschke.

Corolário 1.7.1. *Se G é um grupo finito e o corpo base tem característica p tal que $p = 0$ ou p não divide $|G|$ então toda representação de G de grau finito é soma direta de representações irredutíveis.*

Agora, vamos estudar a álgebra de grupo KG e relacioná-la com as representações de G:

Observação 1.7.2. *Como toda representação $\rho : G \to GL(V)$ de um grupo G em V define uma ação linear de G em V, podemos considerar V como um KG-módulo à esquerda. Neste*

caso os conceitos de subrepresentações e irredutibilidade de ρ correspondem a conceitos similares no KG-módulo V.

Em particular, temos a ***representação regular****, que é a representação de G em KG definida por*

$$\rho_g : \sum_{h\in G} \alpha_h h \mapsto \sum_{h\in G} \alpha_h gh$$

em que $g \in G$ e $\alpha_h \in K$. Considerando KG como um KG-módulo à esquerda, podemos assumir que G age sobre KG à esquerda permutando os elementos da base G. As subrepresentações de ρ correspondem aos ideais à esquerda da álgebra KG e as subrepresentações irredutíveis correspondem aos ideais à esquerda minimais de KG.

Notação 1.7.2. *Em alguns lugares diremos que V é um G-módulo ao invés de KG-módulo.*

Definição 1.7.6. *Considere $\rho : G \to GL(V)$, com V um espaço vetorial não nulo qualquer, dado por $\rho(s) = I$ para todo $s \in G$, em que I é a identidade. Essa representação é denominada* ***representação trivial****.*

Exemplo 1.7.1. *Seja G um grupo e considere a representação regular $\rho : G \to GL(KG)$. Considere W o subespaço gerado por $e = \sum_{g\in G} e_g$. Temos que W é uma subrepresentação de KG e que ela se comporta como a representação trivial, pois $\rho_s(e) = e$, para todo $s \in G$.*

Pelo teorema de Maschke (Corolário 1.7.1), se G é um grupo finito e K é um corpo de característica 0, então KG é completamente redutível. Pelo Teorema de Wedderburn–Artin (Teorema 1.4.2), como KG é de dimensão finita sobre K e se K for algebricamente fechado, temos que

$$KG \simeq M_{d_1}(K) \oplus \cdots \oplus M_{d_m}(K). \tag{1.4}$$

Observamos que este último fato pode ser deduzido sem utilizar o teorema de Wedderburn–Artin. Mas para os nossos objetivos esta foi a maneira mais rápida e fácil para deduzir as propriedades das quais precisaremos.

Vamos explorar um pouco as propriedades de KG e das representações de G

Proposição 1.7.1. *Sejam G um grupo finito, K um corpo de característica p tal que $p = 0$ ou p não divide $|G|$ e M um G-módulo irredutível. Então M é isomorfo a um ideal minimal à esquerda de KG.*

Demonstração. Tome m um elemento não nulo de M e considere a aplicação $\psi : KG \to M$ tal que $\psi(r) = rm$. Tal aplicação é um homomorfismo de G-módulos e é sobrejetora pois $\psi(KG)$ é um submódulo de M, M é irredutível e $\psi(KG) \neq 0$, logo $\psi(KG) = M$. Além disso, $\ker(\psi)$ é um submódulo de KG, isto é, um ideal à esquerda de KG, portanto, pelo Teorema 1.7.1, existe W um G-submódulo de KG tal que $KG = \ker\psi \oplus W$ e portanto $M \simeq KG/\ker\psi \simeq W$. Como M é irredutível então W é minimal. □

Proposição 1.7.2. *Sejam G um grupo finito e K um corpo algebricamente fechado de característica p tal que $p = 0$ ou p não divide $|G|$ e seja I um ideal minimal à esquerda de KG. Então existe $e \in I$ idempotente tal que $I = (KG)e$.*

Demonstração. Pela Equação 1.4, um ideal minimal à esquerda de KG deve ser um ideal minimal à esquerda de alguma das subálgebras de matrizes. Seja J um ideal minimal à esquerda de $M_d(K)$, temos que $J_0 = J \cdot M_d(K)$ é um ideal bilateral e como $M_d(K)$ é uma álgebra simples, então $J_0 = M_d(K)$. Suponha por absurdo que $J^2 = 0$. Neste caso,

$$J_0^2 = (J \cdot M_d(K) \cdot J) \cdot M_d(K) = J^2 \cdot M_d(K) = 0,$$

impossível, logo $J^2 \neq 0$.

Então, como $J^2 \subset J$ é um ideal à esquerda e J é minimal, temos que $J^2 = J$ logo existe $a \in J$ tal que $Ja \neq 0$, mas como $Ja \subset J$ é um ideal à esquerda não nulo, $Ja = J$. Em particular $a \in J$, logo existe $e \in J$ tal que $ea = a$. Daí, $e^2a = ea$ e assim $(e^2 - e)a = 0$. Considere $A = \{r \in J : ra = 0\}$. Temos que A é ideal à esquerda, e $A \subset J$, e como J é minimal temos $A = 0$ ou $A = J$ (o que não ocorre, pois $e \notin A$), portanto, $A = 0$. Como $e^2 - e \in A$, temos $e^2 - e = 0$, ou seja, $e^2 = e$, logo e é idempotente. Como $e \in J$, $Je \subset J$ é um ideal à esquerda, e como J é minimal e $Je \neq 0$ (pois $e = e^2 \in Je$) então $Je = J$. □

Ainda, lembrando que os ideais à esquerda de $M_n(K)$ correspondem aos subespaços de K^n (um ideal à esquerda de $M_n(K)$ é composto pelas matrizes cujas linhas estão em um subespaço de K^n), temos que um ideal minimal à esquerda $(KG)e$ de KG é tal que $\dim_K (KG)e = n_i$, $(KG)e$ aparece n_i vezes na composição de KG e $(KG)e$ está contido num ideal bilateral minimal de dimensão n_i^2.

Novamente usando a Equação 1.4, temos

$$Z(KG) \simeq Z(M_{d_1}(K)) \oplus \cdots \oplus Z(M_{d_m}(K))$$

e como o centro de $M_d(K)$ são as matrizes de escalares, temos $\dim_K Z(M_{n_i}(K)) = 1$. Segue que $\dim_K Z(KG) = m$.

Sejam $C_1, \ldots, C_s$ as classes de conjugação de G e defina o elemento $c_i = \sum_{x \in C_i} x \in KG$, $i = 1, \ldots, s$ em cada uma delas. Note que, para todo $g \in G$, $gc_ig^{-1} = c_i$ já que para cada $x \in C_i$, temos $gxg^{-1} \in C_i$, e a conjugação é um isomorfismo de grupos. Essas duas observações permitem provar o seguinte resultado:

Proposição 1.7.3. *O número de componentes simples na decomposição de KG é igual à quantidade de classes de conjugação de G.*

Demonstração. Pelo discutido anteriormente, temos que $m = \dim_K Z(KG)$, logo é suficiente provarmos que $\dim_K Z(KG) = s$, em que s é a quantidade de classes de conjugação de G. Seja $x = \sum_{g\in G} \alpha_g g \in Z(KG)$. Como x está no centro de KG temos, para todo $h \in G$,

$$x = hxh^{-1} = \sum_{g\in G} \alpha_g hgh^{-1} = \sum_{g\in G} \alpha_{h^{-1}gh} g$$

e comparando os coeficientes temos $\alpha_g = \alpha_{h^{-1}gh}$, ou seja, os coeficientes de x são constantes nos elementos de uma mesma classe de conjugação e portanto x é combinação linear de $c_1, \ldots, c_s$. Por outro lado, como os elementos que compõem cada c_i são distintos, eles devem ser linearmente independentes. Logo $\{c_1, \cdots, c_s\}$ é uma base de $Z(KG)$ e $\dim_K KG = s$. □

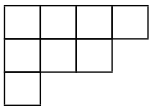
1.8 Representações de S_n e PI-álgebras

Agora vamos explorar especificamente as representações do grupo simétrico S_n. Nesta seção, consideraremos $n \in \mathbb{N}$, o grupo simétrico $G = S_n$, um corpo de característica zero K e $A = KS_n$. Como vimos anteriormente, KS_n é completamente redutível logo pode ser escrito como soma de KS_n-módulos à esquerda irredutíveis. Agora o nosso objetivo é apresentar uma ferramenta que permite caracterizar todos os KS_n-módulos irredutíveis: as tabelas de Young.

Isso vai nos permitir concluir que as representações irredutíveis de S_n sobre o corpo dos racionais $\mathbb{Q}$ são absolutamente irredutíveis. Isto quer dizer que elas permanecem irredutíveis sob qualquer extensão de corpos; em outras palavras, continuam irredutíveis sobre qualquer corpo de característica 0.

Nesta seção, o produto de duas permutações $\sigma, \tau \in S_n$ será da direita para a esquerda. Assim, uma ação de S_n no conjunto $I_n = \{1, 2, \cdots, n\}$ é tal que $\sigma(\tau m) = (\sigma\tau)m$, para cada $m \in I_n$.

Definição 1.8.1. *Seja $\lambda = (n_1, \cdots, n_k) \vdash n$ uma partição de n. Um **diagrama de Young** D_λ é uma malha (tabela) com n_1 espaços na primeira linha, n_2 espaços na segunda linha, etc. Por exemplo, se $\lambda = (4, 3, 1)$, o diagrama D_λ será*



Definição 1.8.2. *Seja $\lambda = (n_1, \cdots, n_k) \vdash n$ uma partição de n e D_λ um diagrama de Young. Uma **$\lambda-$tabela de Young** T_λ de conteúdo $\alpha = (\alpha_1, \ldots, \alpha_m)$ em que $\alpha_1 + \cdots + \alpha_m = n$ é obtida ao preencher a tabela com α_1 números 1, α_2 números 2, ..., α_m números m. Uma tabela é semistandard se suas entradas crescem (não necessariamente estritamente)*

da esquerda para direira nas linhas e aumentam (estritamente) de cima para baixo nas colunas. Uma tabela é standard se ela é semistandard e de conteúdo $(1, \ldots, 1)$*. Por exemplo, para a partição* $\lambda = (4, 3, 1)$*, uma tabela semistandard de conteúdo* $(2, 3, 1, 1)$ *seria:*

1	1	2	4
2	2		
3			

.

A tabela a seguir é standard:

1	3	6	7
2	4		
5			

,

e esta última é de conteúdo $(1, \ldots, 1)$ *e não é standard:*

1	2	3	4
6	5		
7			

.

Definição 1.8.3. *Para uma partição* λ *de* n*, o grupo simétrico* S_n *age sobre as* λ*-tabelas de conteúdo* $(1, \ldots, 1)$ *da seguinte forma. Se uma caixa de* T_λ *contém o número* k*, a mesma caixa de* σT_λ *conterá o número* $\sigma(k)$*, em que* $\sigma \in S_n$*. Dada uma tabela* T_λ*, denotamos por* $R(T_\lambda)$ *e* $C(T_\lambda)$ *os subgrupos de* S_n *que mantêm os elementos de* T_λ *nas mesmas linhas e colunas, respectivamente. Por exemplo, na última tabela apresentada temos*

$$R(T_\lambda) = S_4(1, 2, 3, 4) \oplus S_2(6, 5) \oplus S_1(7)$$
$$C(T_\lambda) = S_3(1, 6, 7) \oplus S_2(2, 5) \oplus S_1(3) \oplus S_1(4)$$

Observação 1.8.1. *Temos que* $R(T_\lambda) \cap C(T_\lambda) = 1$*. De fato, se* $\sigma \in R(D_\lambda) \cap C(D_\lambda)$*, então* σ *não move nenhum elemento para outra linha e nem para outra coluna, logo deve fixar cada elemento e então* $\sigma = 1$*.*

O teorema a seguir descreve as representações irredutíveis do grupo simétrico em termos de tabelas de Young. Uma demonstração para esses resultados pode ser vista no livro de Curtis e Reiner (1).

Teorema 1.8.1. *Seja* K *um corpo de característica* 0*,* λ *uma partição de* n*,* T_λ *uma* λ*-tabela de conteúdo* $(1, \ldots, 1)$*, e* $R(T_\lambda)$ *e* $C(T_\lambda)$ *os subgrupos que permutam as linhas e as colunas, respectivamente, de* T_λ*. Definimos o elemento* $e(T_\lambda)$ *da álgebra* KS_n *associado à tabela de Young* T_λ*:*

$$e(T_\lambda) = \sum_{\sigma \in R(T_\lambda),\ \tau \in C(T_\lambda)} \operatorname{sgn}(\tau)\sigma\tau.$$

Então temos:

(i) A menos de uma constante multiplicativa, $e(T_\lambda)$ *é igual a um idempotente da álgebra* KS_n *e gera um ideal à esquerda minimal de* KS_n *(tal ideal é da forma* $KS_n \cdot e(T_\lambda)$ *e é um* S_n*-módulo à esquerda)*

(ii) *Se T_μ é uma tabela associada a uma partição μ, então $KS_n \cdot e(T_\mu) \simeq KS_n \cdot e(T_\lambda)$ se e somente se $\lambda = \mu$;*

(iii) *todo S_n-módulo irredutível à esquerda é isomorfo a algum $KS_n \cdot e(T_\lambda)$ para alguma partição $\lambda \vdash n$.*

(iv) *Se T_λ e T'_λ são duas λ-tabelas e seja $\rho \in S_n$ tal que $T'_\lambda = \rho T_\lambda$, então a função $\psi : KS_n \cdot e(T_\lambda) \mapsto KS_n \cdot e(T'_\lambda)$ tal que $\psi(x) = x\rho^{-1}$ é bem definida e é um isomorfismo entre S_n-módulos.*

Juntamente com o teorema anterior, o fato de KS_n ser completamente redutível implica o corolário:

Corolário 1.8.1. *Seja K um corpo de característica 0, n um número natural e $e(T_\lambda)$ definido no Teorema 1.8.1. Temos que*

$$KS_n = \sum KS_n \cdot e(T_\lambda)$$

em que a soma percorre todas as tabelas de conteúdo $(1, \ldots, 1)$ geradas sobre todas as partições de n.

Observação 1.8.2. *No corolário é suficiente tomar a soma apenas nas tabelas standard, mas não precisaremos usar esse fato.*

Além disso, pelo teorema também obtemos que o ideal bilateral $KS_n \cdot e(T_\lambda) \cdot KS_n$, que é gerado pelo elemento $e(T_\lambda)$, é igual à soma de todos os ideais à esquerda minimais isomorfos a $KS_n \cdot e(T_\lambda)$. Portanto obtemos outro corolário:

Corolário 1.8.2. *Seja K um corpo de característica 0, n um número natural e $e(T_\lambda)$ definido no Teorema 1.8.1, temos que*

$$KS_n = \sum KS_n \cdot e(T_\lambda) \cdot KS_n$$

em que na soma tomamos qualquer uma das tabelas de conteúdo $(1, \ldots, 1)$ geradas sobre cada uma das partições de n.

Por fim, iremos comentar como podemos aplicar a teoria desenvolvida para obter resultados sobre PI-álgebras. Seja P_n o conjunto de todos os polinômios multilineares de grau n na álgebra associativa livre $K\langle X\rangle$. Temos que P_n admite uma estrutura natural de S_n-módulo, dada pela seguinte ação:

$$\sigma\left(\sum \alpha_i x_{i_1} \ldots x_{i_n}\right) = \sum \alpha_i x_{\sigma(i_1)} \ldots x_{\sigma(i_n)}$$

para cada $\sigma \in S_n$, $\alpha_i \in K$ e $x_{i_1} \ldots x_{i_n} \in P_n$.

Dada uma PI-álgebra A e T o seu T-ideal, temos que $P_n \cap T$ é um S_n-submódulo de P_n. De fato, T é invariante sob todas as substituições, então se $f(x_1, \ldots, x_n) \in P_n \cap T$ temos que

$$\sigma(f(x_1, \ldots, x_n)) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in P_n \cap T$$

para todo $\sigma \in S_n$. Assim, dados $f, g \in P_n$, f é consequência de g se e somente se $f \in KS_n g$.

Como já comentamos, para estudar as identidades polinomiais de uma álgebra A sobre um corpo de característica 0, é suficiente considerar apenas as identidades multilineares satisfeitas por A. Assim podemos estudar $P_n \cap T(A)$ como um S_n-módulo usando a teoria das representações do grupo S_n. Por bem da verdade, na maioria das vezes estuda-se o quociente $P_n/P_n \cap T(A)$. Os principais motivos para isso veremos na próxima seção.

1.9 Codimensões e o Teorema de Regev

Nesta seção apresentaremos o Teorema de Regev sobre o produto tensorial de PI-álgebras. A exposição é baseada na prova de Latyshev que se encontra no livro de Drensky (2), mas usamos uma demonstração para o lema combinatório um pouco diferente da presente no livro.

Definição 1.9.1. *Se T é um T-ideal de $K\langle X\rangle$, definimos $T_n = P_n \cap T$ e a n-ésima* ***codimensão*** *$c_n(T)$ de T como a dimensão do espaço vetorial P_n/T_n, isto é, $c_n(T) = \dim_K(P_n/T_n)$.*

Definição 1.9.2. *Uma permutação $\pi \in S_n$ é d-boa se não possui subsequências decrescentes de tamanho d, isto é, se os inteiros $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$ são tais que $\pi(i_1) > \pi(i_2) > \cdots > \pi(i_k)$, então $k < d$.*

Exemplo 1.9.1. *Para $n = 6$ e*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 4 & 1 & 6 \end{pmatrix}$$

a maior subsequência decrescente tem tamanho 4 ($= 5-3-2-1$), e portanto π é 5-boa e 6-boa.

Teorema 1.9.1. *O número de permutações d-boas de S_n é menor ou igual a $(d-1)^{2n}$.*

Demonstração. Seja $\sigma \in S_n$ uma permutação. Para cada $i = 1, 2, \ldots, n$ defina $D(i)$ como o tamanho da maior subsequência decrescente que começa no i-ésimo elemento. Por exemplo, para $n = 6$ e

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 1 & 6 & 2 \end{pmatrix}$$

temos que

$$D = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 3 & 2 & 1 & 2 & 1 \end{pmatrix}.$$

Note que σ é d-boa se e somente se $D(i) < d$ para todo i. A quantidade de funções D tais que $D(i) < d$ para todo i é igual a $(d-1)^n$, porém é possível que mais de uma permutação corresponda à mesma função D, por exemplo,

$$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 1 & 5 & 2 \end{pmatrix}$$

corresponde à mesma D citada anteriormente. Porém, dada uma função D, o número de maneiras de reconstruir σ é limitado pelo seguinte: Se $i < j$ e $D(i) = D(j)$ então $\sigma(i) < \sigma(j)$. De fato, se $i < j$ e $\sigma(i) > \sigma(j)$, então é possível construir uma sequência de tamanho $D(j) + 1$ adicionando o i-ésimo elemento à maior subsequência decrescente que começa no j-ésimo elemento e assim $D(i) > D(j)$. Logo, para cada $k = 1, 2, \ldots, d-1$, a subsequência formada pelos elementos com $D(i) = k$ é crescente. Isso significa que a reconstrução da permutação é completamente definida pela partição do conjunto $\{1, 2, \ldots, n\}$ nas $d-1$ sequências. O número de partições é limitado por $(d-1)^n$ (pois para cada $\{1, 2, \ldots, n\}$, basta escolher uma das $d-1$ sequências). Nem todos os pares compostos por uma função D e uma partição de $\{1, 2, \ldots, n\}$ são válidos (podendo até gerar uma permutação, mas cujo D não corresponde aos valores esperados), porém cada permutação d-boa gera um par diferente. Logo o número de permutações d-boas de S_n é menor ou igual a $(d-1)^{2n}$. □

Teorema 1.9.2. *Se R é uma PI-álgebra e o T-ideal T de R contém uma identidade polinomial de grau d, então o espaço vetorial dos polinômios multilineares de grau n em $K\langle X\rangle$ é gerado, módulo T, pelos monômios $x_{\pi(1)} \cdots x_{\pi(n)}$ em que $\pi \in S_n$ é d-boa.*

Demonstração. Como T contém uma identidade polinomial de grau d, ele contém uma identidade multilinear de grau d. Sem perda de generalidade, podemos assumir que R satisfaz uma identidade da forma

$$x_d x_{d-1} \cdots x_1 = \sum_{\sigma \in S_d} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(d)},$$

em que $\alpha_\sigma \in K$ e a soma percorre todas as permutações diferentes da permutação $\delta \in S_d$ definida como

$$\delta = \begin{pmatrix} 1 & 2 & \ldots & d-1 & d \\ d & d-1 & \ldots & 2 & 1 \end{pmatrix}.$$

Iremos trabalhar em $P_n(R) = P_n/T_n$, isto é, o espaço vetorial dos polinômios multilineares de grau n módulo as identidades polinomiais de R. Defina G_d como o conjunto de todos os monômios $x_{\sigma(1)} \cdots x_{\sigma(n)} \in P_n(R)$ tais que a permutação $\sigma \in S_n$ é d-boa. Vamos mostrar que G_d gera $P_n(R)$. Considerando a ordem lexicográfica dos monômios (isto é, $x_{i_1} x_{i_2} \cdots x_{i_p} < x_{j_1} x_{j_2} \cdots x_{j_q}$ se e somente se $i_1 = j_1$, $i_2 = j_2$, …, $i_k = j_k$ e $i_{k+1} < j_{k+1}$ para

algum k), defina $h = x_{\pi(1)} \cdots x_{\pi(n)}$ como o menor monômio que não está no espaço vetorial gerado por G_d. Então, por definição, π tem uma sequência decrescente de tamanho d, isto é, existem $i_1 < \cdots < i_d$ tais que $\pi(i_1) > \cdots \pi(i_d)$ e portanto podemos escrever h na forma

$$h = h_0 x_{\pi(i_1)} h_1 x_{\pi(i_2)} h_2 \cdots h_{d-1} x_{\pi(i_d)} h_d.$$

Aplicando a identidade polinomial de grau d usando $\overline{x}_d = x_{\pi(i_1)} h_1$, $\overline{x}_{d-1} = x_{\pi(i_2)} h_2$, ..., $\overline{x}_2 = x_{\pi(i_{d-1})} h_{d-1}$, $\overline{x}_1 = x_{\pi(i_d)} h_d$ obtemos

$$\begin{aligned} h = h_0 \cdot (\overline{x}_d \cdots \overline{x}_1) &= \sum_{\sigma \in S_d} \alpha_\sigma h_0 \overline{x}_{\sigma(1)} \cdots \overline{x}_{\sigma(d)} \\ &= \sum_{\sigma' \in S_d} \alpha_{\sigma'} h_0 x_{\pi(i_{\sigma'(d)})} h_{\sigma'(d)} x_{\pi(i_{\sigma'(d-1)})} h_{\sigma'(d-1)} \cdots x_{\pi(i_{\sigma'(1)})} h_{\sigma'(1)} \end{aligned}$$

em que $\sigma'(i) = d + 1 - \sigma(d + 1 - i)$. Como $\pi(i_1) > \cdots > \pi(i_d)$ e a soma percorre as permutações diferentes de δ, temos que todos os monômios da última soma são lexicograficamente menores que h, e portanto devem estar no espaço gerado por G_d. Portanto h também está no espaço gerado por G_d, absurdo. Concluímos que G_d gera $P_n(R)$. □

Dos dois teoremas anteriores temos que:

Corolário 1.9.1. *Seja R uma PI-álgebra com uma identidade polinomial de grau d. Então a codimensão de R satisfaz $c_n(R) \leqslant (d-1)^{2n}$, $n = 0, 1, 2, \ldots$*

Observamos aqui que $\dim P_n = n!$. O teorema de Regev nos diz que se R é uma PI-álgebra então $\dim(P_n/P_n \cap T(R)) < c^n$ para todo n, onde c é alguma constante. Assim, as codimensões de uma PI-álgebra têm crescimento exponencial mas não fatorial. Por outro lado, se R é uma PI-álgebra então as dimensões de $P_n \cap T(R)$ crescem muito rápido, mais que qualquer função exponencial. Portanto, ao invés de estudar as identidades multilineares de uma álgebra, é "mais fácil" estudar as "não-identidades", isto é, os elementos de $P_n/P_n \cap T(R)$.

Agora vamos demonstrar o teorema de Regev sobre o produto tensorial de PI-álgebras.

Teorema 1.9.3 (Regev)**.** *O produto tensorial $R = R_1 \otimes_K R_2$ de duas PI-álgebras R_1 e R_2 sobre um corpo K é também uma PI-álgebra.*

Demonstração. Suponha que R_1 e R_2 satisfazem identidades polinomiais de grau d_1 e d_2, respectivamente. Então, pelo Corolário 1.9.1,

$$c_n(R_1) \leqslant (d_1 - 1)^{2n}, \; c_n(R_2) \leqslant (d_2 - 1)^{2n}.$$

Escolhemos n tal que $c_n(R_1)c_n(R_2) < n!$. Isso sempre é possível pois $a^n < n!$ para n suficientemente grande. Sejam

$$\{g_i(x_1, \ldots, x_n) \mid i = 1, 2, \ldots, c' = c_n(R_1)\},$$
$$\{h_j(x_1, \ldots, x_n) \mid j = 1, 2, \ldots, c'' = c_n(R_2)\}$$

bases de $P_n(R_1)$ e $P_n(R_2)$, respectivamente. Para toda permutação $\pi \in S_n$ consideramos $x_{\pi(1)} \cdots x_{\pi(n)}$ como um elemento de $P_n(R_1)$ e o escrevemos como uma combinação linear

$$x_{\pi(1)} \cdots x_{\pi(n)} = \sum_{i=1}^{c'} \beta_{\pi i} g_i(x_1, \ldots, x_n)$$

em que $\beta_{\pi i} \in K$. Da mesma forma, para $P_n(R_2)$

$$x_{\pi(1)} \cdots x_{\pi(n)} = \sum_{i=1}^{c''} \gamma_{\pi j} h_j(x_1, \ldots, x_n)$$

em que $\gamma_{\pi j} \in K$.

Note que as duas equações acima são identidades polinomiais de R_1 e R_2, isto é, elas são automaticamente satisfeitas para quaisquer $u_1, \ldots, u_n \in R_1$ e $v_1, \ldots, v_n \in R_2$, respectivamente. Agora nós procuramos por uma identidade polinomial de grau n para o produto tensorial $R = R_1 \otimes R_2$ de K-álgebras. Seja

$$f(x_1, \ldots, x_n) = \sum_{\pi \in S_n} \xi_\pi x_{\pi(1)} \cdots x_{\pi(n)} = 0$$

a identidade polinomial de R que procuramos. Como $f = 0$ é multilinear, é suficiente mostrar que ela é válida para $u_1 \otimes v_1, \ldots, u_n \otimes v_n$ arbitrários, em que $u_1, \ldots, u_n \in R_1$ e $v_1, \ldots, v_n \in R_2$. Calculando $f(u_1 \otimes v_1, \ldots, u_n \otimes v_n)$ obtemos

$$\begin{aligned}
f(u_1 \otimes v_1, \ldots, u_n \otimes v_n) &= \sum_{\pi \in S_n} \xi_\pi (u_{\pi(1)} \otimes v_{\pi(1)}) \cdots (u_{\pi(n)} \otimes v_{\pi(n)}) \\
&= \sum_{\pi \in S_n} \xi_\pi (u_{\pi(1)} \cdots u_{\pi(n)}) \otimes (v_{\pi(1)} \ldots u_{\pi(n)}) \\
&= \sum_{\pi \in S_n} \sum_{i=1}^{c'} \sum_{i=1}^{c''} \xi_\pi \beta_{\pi i} \gamma_{\pi j} g_i(u_1, \ldots, u_n) h_j(u_1, \ldots, u_n) \\
&= \sum_{i=1}^{c'} \sum_{i=1}^{c''} (\sum_{\pi \in S_n} \xi_\pi \beta_{\pi i} \gamma_{\pi j}) g_i(u_1, \ldots, u_n) h_j(u_1, \ldots, u_n) = 0.
\end{aligned}$$

Assim, consideramos o sistema linear homogêneo

$$\sum_{\pi \in S_n} \xi_\pi \beta_{\pi i} \gamma_{\pi j} = 0$$

em que $i = 1, \ldots, c'$ e $j = 1, \ldots, c''$. A quantidade de variáveis ξ_π é $n!$ e a de equações é $c'c'' = c_n(R_1)c_n(R_2) < n!$, portanto o sistema tem uma solução não nula. Tal solução corresponde a uma identidade polinomial para $R = R_1 \otimes R_2$. □

Faremos um comentário sobre a importância do teorema de Regev. Ele providencia uma maneira bastante natural (mas não trivial) de construção de PI-álgebras a partir de álgebras dadas que são também PI-álgebras. Além disso tal maneira não é evidente como por exemplo o caso de somas diretas finitas ou subálgebras. Ainda mais, a demonstração acima mostra a importância dos métodos provenientes da combinatória algébrica para o estudo das PI-álgebras. Ressaltamos aqui que as identidades da álgebra de Grassmann E são bastante imediatas para descrever, enquanto ainda as de $E \otimes E$ são altamente não triviais. Mais um exemplo: as identidades de $M_2(K)$ em característica 0 são bem conhecidas, mas as de $M_2(K) \otimes E \cong M_2(E)$ ainda não são conhecidas apesar dos esforços de diversos pesquisadores. Por outro lado o teorema de Regev nos diz que essas álgebras satisfazem identidades polinomiais.

1.10 Álgebras com traço e identidades com traço

Uma das álgebras mais importantes é a álgebra das matrizes $M_n(K)$, então é natural se perguntar quais são as identidades polinomiais que ela satisfaz. Como vimos no Exemplo 1.5.2, uma álgebra de dimensão finita é uma PI-álgebra. Então, em particular, a álgebra das matrizes $M_n(K)$ é uma PI-álgebra que satisfaz a identidade standard s_{n^2+1}. Porém, esse não é o menor m tal que $M_n(K)$ satisfaz s_m. Em 1950, Amitsur e Levitzki (13) demonstraram que $M_n(K)$ satisfaz s_{2n} e também que não satisfaz s_{2n-1}, nem qualquer outra identidade de grau menor que $2n$. Eles ainda provaram que exceto o caso em que $n = 2$ e K é o corpo de 2 elementos, s_{2n} é a única, a menos de múltiplo por escalar, identidade de $M_n(K)$. Nesta seção iremos explorar algumas definições, citar alguns resultados relacionados com as identidades da álgebra de matrizes $M_n(K)$ e apresentar uma demonstração do teorema de Amitsur–Levitzki.

Vamos começar definindo o polinômio de Cayley–Hamilton. Pelo teorema de Cayley–Hamilton da Álgebra Linear elementar, uma matriz $y \in M_n(K)$ satisfaz o seu polinômio característico $p(\lambda) = \det(\lambda I_n - y)$. Podemos reescrever tal polinômio da seguinte forma

$$\det(\lambda I_n - y) = \sum_{i=0}^{n} (-1)^i \sigma_i(\lambda_1, \ldots, \lambda_n) \lambda^{n-i}$$

em que $\lambda_1, \ldots, \lambda_n$ são os autovalores de y (no fecho algébrico de K, contados com sua multiplicidade), e σ_i são os polinômios (comutativos) simétricos elementares. Note que tal polinômio não é uma identidade polinomial de $M_n(K)$ pois os coeficientes dependem da matriz y. Porém, em característica 0, podemos usar as identidades de Newton para obter os polinômios simétricos elementares a partir das somas de potências $\lambda_1^k + \cdots + \lambda_n^k = \mathrm{tr}(a^k)$, $k = 1, \ldots, n$ e assim existem g_i tais que

$$\sigma_i(\lambda_1, \ldots, \lambda_n) = g_i(tr(y), \ldots, tr(y^n))$$

e portanto podemos escrever o polinômio característico na forma

$$\sum_{i=0}^{n}(-1)^i g_i(\mathrm{tr}(y),\ldots,\mathrm{tr}(y^n))y^{n-i} \tag{1.5}$$

Este último polinômio pode ser considerado como um polinômio em uma variável y, com coeficientes constantes, se permitirmos o traço na definição do polinômio. Analisando o grau do polinômio característico e das identidades de Newton, podemos observar que ele é homogêneo de grau n em y. Denotaremos tal polinômio por $f_n(y)$. Com isso $f_n(y)$ é, de certa forma, uma identidade polinomial da álgebra de matrizes $M_n(K)$. Um resultado importantíssimo obtido independentemente por Razmyslov (9) e Procesi (18), é que toda identidade polinomial com traço de $M_n(K)$ é consequência de $f_n(y)$. Iremos detalhar um pouco mais este argumento.

Primeiramente, vamos definir a álgebra das matrizes genéricas, que é a álgebra relativamente livre da variedade das álgebras que satisfazem as identidades polinomiais de $M_n(K)$ em que K é um corpo infinito.

Fixamos $n \geqslant 2$ e denotamos por $\Omega = \Omega_n$ a K-álgebra dos polinômios em infinitas variáveis comutativas

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

Aqui denotaremos por $e_{ij}, 1 \leqslant i,j \leqslant n$, as matrizes que possuem 1 na entrada da i-ésima linha e j-ésima coluna, e 0 nas demais.

Definição 1.10.1. *As matrizes $n \times n$ com entradas em Ω_n*

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

em que $i = 1,2,\ldots$ são chamadas de ***matrizes genéricas*** *$n \times n$. A álgebra R_n gerada pelas matrizes genéricas $n \times n$ é a* ***álgebra das matrizes genéricas*** *$n \times n$.*

A demonstração para o fato que R_n é relativamente livre pode ser encontrada no livro de Drensky (3) (Proposição 1.3.2). Agora vamos definir mais dois objetos relacionados:

Definição 1.10.2. *A* ***álgebra com traço pura*** *C_n é a subálgebra unitária de Ω_n gerada por todos os traços dos produtos de matrizes genéricas*

$$\mathrm{tr}(y_{i_1}\cdots y_{i_m})$$

em que $i_j = 1,2,\ldots$ e $m = 1,2,\ldots$. Identificando a matriz identidade com 1, podemos assumir $\Omega_n \subset M_n(\Omega_n)$ e definir a ***álgebra com traço*** *T_n como a álgebra gerada pelas matrizes genéricas $y_1, y_2, \ldots$ e os elementos de C_n.*

Denominamos os elementos da álgebra com traço T_n de **polinômios com traço**. De forma similar aos polinômios ordinários podemos definir o grau de um monômio em relação à variável y_i como o número de vezes que ele aparece na sua representação e usar as definições similares de multigrau e de polinômio multilinear. Aqui podemos notar que o grau está bem definido pois podemos considerar os polinômios com traço como o produto tensorial $K\langle X\rangle \otimes C_n$. Se $f(y_1, y_2, \ldots, y_l)$ é um polinômio com traço, dizemos que $f = 0$, ou simplesmente f, é uma identidade com traço para a álgebra de matrizes $n \times n$ se $f(a_1, \ldots, a_m) = 0$ para todo $a_1, \ldots, a_m \in M_n(K)$.

Agora vamos enunciar o resultado obtido por Razmyslov e Procesi.

Teorema 1.10.1. *Seja K um corpo de característica 0. Então toda identidade polinomial com traço da álgebra das matrizes $M_n(K)$ é consequência do polinômio de Cayley-Hamilton.*

Este resultado é obtido a partir do seguinte teorema, conhecido como Segundo Teorema Fundamental sobre Invariantes de Matrizes.

Teorema 1.10.2 (Segundo Teorema Fundamental sobre Invariantes de Matrizes)**.** *Seja K um corpo de característica 0. A cada permutação $\sigma \in S_m$ escrita como produto de ciclos disjuntos sem omitir ciclos*

$$\sigma = (i_1 \ldots i_p) \cdots (j_1 \ldots j_q),$$

associamos uma função traço

$$\mathrm{tr}_\sigma(x_1, \ldots, x_n) = \mathrm{tr}(x_{i_1} \cdots x_{i_p}) \cdots \mathrm{tr}(x_{j_1} \cdots x_{j_q}).$$

Então

(i) Seja f um polinômio com traço multilinear de grau m

$$f(x_1, \ldots, x_m) = \sum_{\sigma \in S_m} \alpha_\sigma \, \mathrm{tr}_\sigma(x_1, \ldots, x_m)$$

em que $\alpha_\sigma \in K$. Então $f = 0$ é uma identidade com traço para a álgebra de matrizes $n \times n$ se e somente se

$$\sum_{\sigma \in S_m} \alpha_\sigma \sigma$$

está no ideal bilateral $J(n, m)$ da álgebra de grupo KS_m gerada pelo elemento

$$\sum_{\sigma \in S_{n+1}} \mathrm{sgn}(\sigma)\sigma$$

em que $n < m$ e identificamos o grupo S_{n+1} agindo sobre $1, \ldots, n+1$ com o subgrupo de S_m que age sobre $1, \ldots, m$ e fixa os elementos $n+2, \ldots, m$

(ii) O ideal bilateral $J(n,m)$ de KS_m é uma soma direta de ideais bilaterais minimais de KS_m que correspondem às partições $\lambda = (\lambda_1, \ldots, \lambda_m)$ com pelo menos $n+1$ partes, isto é, tais que $\lambda_{n+1} \neq 0$.

Podemos verificar diretamente que a identidade com traço fundamental

$$\sum_{\sigma \in S_{n+1}} \operatorname{sgn}(\sigma) \operatorname{tr}_\sigma(x_1, \ldots, x_{n+1}) = 0$$

é obtida a partir da linearização total da identidade $\operatorname{tr}(f_n(y)z) = 0$. Além disso, como $\operatorname{tr}(xz)$ é uma forma bilinear não degenerada, a identidade com traço fundamental e $f_n(y)$ são equivalentes. Vamos ilustrar esses fatos para o caso das matrizes de ordem 2. Neste caso, o polinômio de Cayley–Hamilton é

$$f_2(y) = y^2 - \operatorname{tr}(y)y + \det(y) = 0.$$

Temos que, para matrizes de ordem 2, $\det(y) = (\operatorname{tr}^2(y) - \operatorname{tr}(y^2))/2$, assim

$$f_2(y) = y^2 - \operatorname{tr}(y)y + \frac{1}{2}(\operatorname{tr}^2(y) - \operatorname{tr}(y^2)) = 0.$$

Linearizando esta última expressão obtemos

$$\psi(x_1, x_2) = x_1x_2 + x_2x_1 - \operatorname{tr}(x_1)x_2 - \operatorname{tr}(x_2)x_1 + \operatorname{tr}(x_1)\operatorname{tr}(x_2) - \operatorname{tr}(x_1x_2) = 0.$$

Então obtemos a identidade com traço fundamental considerando $\operatorname{tr}(\psi(x_1, x_2)x_3)$:

$$\begin{aligned}\operatorname{tr}(\psi(x_1, x_2)x_3) =& \operatorname{tr}(x_1x_2x_3) + \operatorname{tr}(x_2x_1x_3) - \operatorname{tr}(x_1)\operatorname{tr}(x_2x_3) - \operatorname{tr}(x_2)\operatorname{tr}(x_1x_3) \\ &+ \operatorname{tr}(x_1)\operatorname{tr}(x_2)\operatorname{tr}(x_3) - \operatorname{tr}(x_1x_2)\operatorname{tr}(x_3) \\ =& \sum_{\sigma \in S_3} \operatorname{sgn}(\sigma) \operatorname{tr}_\sigma(x_1, x_2, x_3) = 0.\end{aligned}$$

Por fim vamos demonstrar o Teorema de Amitsur–Levitzki, em característica 0, usando identidades com traço. A demonstração que apresentaremos foi obtida por Razmyslov (9) e consiste em provar que o polinômio standard s_{2n} é consequência do polinômio de Cayley–Hamilton, e portanto a álgebra das matrizes $M_n(K)$ satisfaz s_{2n}.

Teorema 1.10.3. *Seja K um corpo de característica 0. Então, a álgebra de matrizes $n \times n$, $M_n(K)$, satisfaz a identidade multilinear s_{2n}.*

Demonstração. Primeiramente vamos verificar que s_{2n} é consequência de y^n. A linearização total de y^n resulta no $e_n(y_1, \ldots, y_n)$ da Definição 1.6.2. Substituindo as variáveis por comutadores $y_i = [x_{2i-1}, x_{2i}] = x_{2i-1}x_{2i} - x_{2i}x_{2i-1}$ e tomando a soma antissimétrica obtemos:

$$\sum_{\sigma \in S_{2n}} \operatorname{sgn}(\sigma)\sigma(e_n([x_1, x_2], \ldots, [x_{2n-1}, x_{2n}]) = \beta s_{2n}$$

em que σ age permutando as variáveis. Podemos verificar que $\beta = n!2^n \neq 0$, e portanto s_{2n} é consequência de y^n.

O mesmo argumento pode ser usado para o polinômio de Cayley–Hamilton f_n, notando que

$$f_n(y) = y^n + \sum_{r_0+\cdots+r_t=n} \alpha_{r_0,r_1,\ldots,r_t} y^{r_0} \operatorname{tr}(y^{r_1}) \cdots \operatorname{tr}(y^{r_t}) \tag{1.6}$$

em que $t \geqslant 1$, os r_0 são inteiros não negativos, $r_1, \ldots, r_t$ são inteiros positivos e $\alpha_{r_0,r_1,\ldots,r_t}$ são coeficientes racionais; e que as somas antissimétricas de cada um dos termos de $f_n(y)$ diferentes de y^n é 0, ou seja,

$$\sum_{\sigma \in S_{2n}} \operatorname{sgn}(\sigma)\sigma(a_0 \operatorname{tr}(a_1) \cdots \operatorname{tr}(a_t)) = 0$$

em que $a_0, \ldots, a_t$ são palavras nas variáveis $y_i = [x_{2i-1}, x_{2i}]$ e que $a_0 \cdots a_t$ tem grau 1 em relação a cada y_i. Esse último fato ocorre pois, definindo r_i como a quantidade de termos $y_1, \ldots, y_n$ em cada a_i, podemos dividir os termos do somatório em somas do tipo

$$s_{2r_0} \operatorname{tr}(s_{2r_1}) \cdots \operatorname{tr}(s_{2r_t}).$$

Como $\operatorname{tr}(ab) = \operatorname{tr}(ba)$ para quaisquer matrizes $a, b \in M_n(K)$ então $\operatorname{tr}(s_{2m}) = 0$ para todo m inteiro positivo.

Por exemplo, tome $n = 3$ e o termo $x_1x_2 \operatorname{tr}(x_3x_4x_5x_6)$. Considerando as permutações de S_6 que levam as variáveis x_5 e x_6 em x_1 e x_2, o somatório dos termos relacionados é igual a $s_2(x_5, x_6) \operatorname{tr}(s_4(x_1, x_2, x_3, x_4))$ e

$$\begin{aligned}
\operatorname{tr}(s_4(x_1, x_2, x_3, x_4)) = {} & (\operatorname{tr}(x_1x_2x_3x_4) - \operatorname{tr}(x_4x_1x_2x_3)) + (\operatorname{tr}(x_3x_4x_1x_2) - \operatorname{tr}(x_2x_3x_4x_1)) \\
& - (\operatorname{tr}(x_1x_2x_4x_3) - \operatorname{tr}(x_3x_1x_2x_4)) - (\operatorname{tr}(x_4x_3x_1x_2) - \operatorname{tr}(x_2x_4x_3x_1)) \\
& - (\operatorname{tr}(x_1x_3x_2x_4) - \operatorname{tr}(x_4x_1x_3x_2)) - (\operatorname{tr}(x_2x_4x_1x_3) - \operatorname{tr}(x_3x_2x_4x_1)) \\
& + (\operatorname{tr}(x_1x_3x_4x_2) - \operatorname{tr}(x_2x_1x_3x_4)) + (\operatorname{tr}(x_4x_2x_1x_3) - \operatorname{tr}(x_3x_4x_2x_1)) \\
& + (\operatorname{tr}(x_1x_4x_2x_3) - \operatorname{tr}(x_3x_1x_4x_2)) + (\operatorname{tr}(x_2x_3x_1x_4) - \operatorname{tr}(x_4x_2x_3x_1)) \\
& - (\operatorname{tr}(x_1x_4x_3x_2) - \operatorname{tr}(x_2x_1x_4x_3)) - (\operatorname{tr}(x_3x_2x_1x_4) - \operatorname{tr}(x_4x_3x_2x_1)) \\
& = 0
\end{aligned}$$

Portanto os termos não nulos da soma antissimétrica de f_n são obtidos apenas de y^n e portanto s_{2n} é consequência de f_n. □

Para concluir o teorema, vamos verificar que $m = 2n$ é o menor valor tal que $M_n(K)$ satisfaz s_m.

Teorema 1.10.4. *Seja K um corpo. Então, a álgebra de matrizes $n \times n$, $M_n(K)$, não satisfaz identidades multilineares de grau menor que $2n$.*

Demonstração. Note que as matrizes e_{ij} satisfazem $e_{ij}e_{kl} = \delta_{jk}e_{il}$, em que δ_{kl} é o delta de Kronecker ($\delta_{kl} = 1$ se $k = l$ e $\delta_{kl} = 0$ caso contrário).

Se uma álgebra satisfaz uma identidade de grau d, então ela satisfaz uma identidade multilinear de grau no máximo d. Mostraremos que $M_n(K)$ não satisfaz identidades multilineares de grau $2n-1$. Seja f um polinômio multilinear não nulo de grau $2n-1$ escrito da seguinte forma

$$f(x_1, \ldots, x_{2n-1}) = \alpha x_1 \ldots x_{2n-1} + \sum_{\sigma \in S_{2n-1}} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(2n-1)}$$

em que S_{2n-1} age sobre $\{1, 2, \ldots, 2n-1\}$, $\alpha_\sigma \in K$, $\alpha \in K$ e σ percorre todas as permutações exceto a identidade. Podemos assumir sem perda de generalidade que $\alpha \neq 0$ pois $f \neq 0$, caso contrário podemos aplicar um homomorfismo que permuta as variáveis de f. Então tomando $x_{2i-1} = e_{ii}$, para $i = 1, \ldots, n$ e $x_{2i} = e_{i(i+1)}$, para $i = 1, \ldots, n-1$:

$$f(e_{11}, e_{12}, e_{22}, e_{23}, \ldots, e_{n-1,n-1}, e_{n-1,n}, e_{nn}) = \alpha e_{1n} + \sum_{\sigma \in S_{2n-1}} \alpha_\sigma 0 = \alpha e_{1n} \neq 0$$

e portanto f não é uma identidade de $M_n(K)$. □

Este último teorema tem o nome "Lema sobre a escada". Tal nome pode ser justificado facilmente, desenhando numa matriz as posições dos elementos e_{11}, e_{12}, e_{22}, e_{23}, ... e observando que ligando-as obteremos uma "escada".

2 Álgebras Nil e Nilpotentes

2.1 Comentários

O objetivo desta dissertação é explorar resultados sobre as condições sob as quais uma álgebra nil é nilpotente. Na sua versão mais geral a implicação é claramente falsa, basta, por exemplo, tomar a álgebra comutativa (sem unidade) dos polinômios nas variáveis x_1, x_2, ..., e considerar o quociente pelo ideal gerado por x_1^2, x_2^2, ... Essa álgebra é nil: o quadrado de todo monômio é igual a 0 e se um polinômio a tem m termos, então a^{m+1} é composto por termos em que pelo menos um dos monômios repete, logo $a^{m+1} = 0$. Ela não é nilpotente, pois os produtos $x_1 x_2 \cdots x_n$ são não nulos para todo n.

Logo precisamos de restrições adicionais. Uma direção é considerar um limite na quantidade de geradores. Em 1941, Kurosh formulou o seguinte problema sobre álgebras:

> **(Problema de Kurosh)** Seja A uma álgebra associativa finitamente gerada em que todo elemento de A é algébrico. A álgebra A tem dimensão finita? Em particular, se A for nil, ela será nilpotente?

O problema de Kurosh é o análogo para anéis do problema de Burnside sobre grupos proposto em 1902. Porém, em 1964, Golod e Shafarevich deram um contra-exemplo para ambos os problemas, o qual apresentaremos na seção 2.3.

Então podemos considerar álgebras em que todo elemento é algébrico com um grau limitado n. Neste caso, temos que para todo elemento $a \in A$, os elementos 1, a, a^2, ..., a^n são linearmente dependentes, e portanto a álgebra A deve satisfazer a identidade de algebricidade (veja a Observação 1.5.2). No caso de álgebras nil de índice limitado, temos que ela é uma PI-álgebra que satisfaz a identidade $x^n = 0$. Logo faz sentido considerarmos o problema de Kurosh para PI-álgebras:

> **(Problema de Kurosh para PI-álgebras)** Seja A uma PI-álgebra associativa finitamente gerada em que todo elemento de A é algébrico. A álgebra A tem dimensão finita? Em particular, se A for nil, ela será nilpotente?

Para este problema a resposta é positiva e foi provada por Levitzki (17) para álgebras nil e por Kaplansky (15) no caso geral. As demonstrações originais utilizam a teoria estrutural de anéis e podem ser encontradas no livro de Herstein (4). Porém iremos apresentar na seção 2.2 uma demonstração para ambos os teoremas como consequência do Teorema de Shirshov.

2.2 Teorema de Shirshov sobre a altura

Nesta seção iremos explorar o teorema de Shirshov sobre a altura, e como ele pode ser usado para provar os teoremas de Levitzki e de Kaplansky, dando uma resposta positiva para o problema de Kurosh no caso de álgebras com identidades polinomiais. É uma demostração bastante interessante pois usa argumentos combinatórios para produzir um resultado profundo sobre a estrutura das álgebras. Vamos usar como referência principal o livro de Drensky e Formanek (3), apresentando uma forma simplificada de uma demonstração dada por Belov.

Vamos fixar o número m de geradores de uma álgebra associativa livre. Seja $W = \langle x_1, x_2, \ldots, x_m \rangle$ o conjunto de todos os monômios (palavras) em $K\langle X_m \rangle$. W é o monóide livre gerado por m geradores. Para $w = x_{i_1} x_{i_2} \cdots x_{i_n} \in W$ denotamos por $|w|$ o comprimento (ou grau) de w. Denotaremos a palavra vazia por 1.

Definição 2.2.1. *Definimos uma ordem parcial em W, assumido que as letras do alfabeto têm uma ordem $x_1 < x_2 < \cdots < x_m$, que estendemos para W da seguinte maneira:*

$$x_{i_1} x_{i_2} \cdots x_{i_p} > x_{j_1} x_{j_2} \cdots x_{j_q}$$

se e somente se $i_1 = j_1$, $i_2 = j_2$, $\ldots$, $i_k = j_k$ e $i_{k+1} > j_{k+1}$ para algum $k \geqslant 0$. Note que duas palavras u e v são incomparáveis se uma é o início da outra, isto é, $u = vw$ para algum $w \in W$, $w \neq 1$. Um subconjunto finito de W é dito incomparável se contém duas palavras incomparáveis.

Definição 2.2.2. *Uma palavra $w \in W$ é dita d-decomponível se pode ser escrita da forma*

$$w = w_0 w_1 \cdots w_d w_{d+1}$$

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

$$w_0 w_1 \cdots w_d w_{d+1} > w_0 w_{\sigma(1)} \cdots w_{\sigma(d)} w_{d+1}$$

para toda permutação não trivial $\sigma \in S_d$.

Por exemplo,

$$w = x_2 x_1 x_3 x_2 x_1 x_2 x_3 x_1 x_2 x_4 x_1 = (x_2 x_1)(x_3 x_2 x_1 x_2)(x_3 x_1 x_2)(x_4 x_1)$$

é uma 2-decomposição, com $w_0 = x_2 x_1$ e $w_3 = x_4 x_1$. A palavra w também possui uma 4-decomposição:

$$w = (x_2 x_1)(x_3 x_2 x_1 x_2)(x_3 x_1)(x_2 x_4)(x_1), w_0 = x_2 x_1, w_5 = 1.$$

Lema 2.2.1. *Se $w \in W$ pode ser escrita como $w = pq = rp$, para r, p, q palavras não vazias, então w é da forma a^n ou $abab \cdots aba = (ab)^{n-1}a$, para a, $b \neq 1$ e $n > 1$.*

Demonstração. (i) Se $|p| < |r|$, então $r = pb$ e assim $w = pbp$, logo tome $a = p$ e temos $w = aba$.

(ii) Caso contrário, se $|p| \geqslant |r|$, então $p = rp_1$. Logo $w = rp_1q = rrp_1$ e $p_1q = rp_1$. Se $|r| \leqslant |p_1|$, então $p_1 = rp_2$ e da mesma forma $p_2q = rp_2$. Continuando esse processo obteremos $p_k = rp_{k+1}$ e $p_{k+1}q = rp_{k+1}$, em que $|p_{k+1}| < |r|$. Temos dois casos para considerar:

(a) $p_{k+1} = 1$, então $p = r^{k+1}$ e $w = r^{k+2} = a^{k+2}$ se tomarmos $a = r$;

(b) $p_{k+1} \neq 1$, então $p_{k+1}q = rp_{k+1}$ e $|p_{k+1}| < |r|$, que cai no caso (i), logo $a = p_{k+1}$, $r = ab$ e $p = r^{k+1}p_{k+1}$ e portanto

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

Todos os casos foram considerados e o lema foi demonstrado. □

Lema 2.2.2. *Seja*

$$v = w_0ww_1ww_2 \cdots ww_{d-1}ww_d$$

uma palavra tal que a subpalavra w tem d subpalavras comparáveis distintas. Então v é d-decomponível.

Demonstração. Seja $w = a_iv_ib_i$, $i = 1, \ldots, d$, e $v_1 > v_2 > \cdots > v_d$. Então v tem a d-decomposição:

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

Isso mostra que v é d-decomponível. □

Lema 2.2.3. *Sejam p e q duas palavras comparáveis. Então a palavra $w = p^{d-1}q$ contém d subpalavras comparáveis.*

Demonstração. Se $p > q$, temos que $p^{d-1}q > p^{d-2}q > \cdots > pq > q$. Caso contrário, $p < q$ e $p^{d-1}q < p^{d-2}q < \cdots < pq < q$. □

Definição 2.2.3. *Seja $w \in W$ tal que $|w| \geqslant d$. Podemos escrever*

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

em que e_i é um início de w e $|e_i| = i - 1$. Logo $|w_i| = |w| - i + 1$ e chamamos as palavras $w_1, w_2, \ldots, w_d$ de d-fins de w.

Lema 2.2.4. *Seja $|w| \geqslant d$ e suponha que os d-fins de w são incomparáveis. Então $w = ab^tc$, em que $|a| + |b| < d$, $t \geqslant 1$ e ou $c = 1$ ou c é um início de b. Se $|w| \geqslant dk$, então $t \geqslant k$ e, em particular, w contém uma subpalavra b^k tal que $|b| < d$.*

Demonstração. Sejam w_i e w_j dois d-fins de w incomparáveis, $i < j$. Então $w = aw_i$ e $w = abw_j$, e portanto $w_i = bw_j$. Como w_i e w_j são incomparáveis, $w_i = w_j u$ e pelo Lema 2.2.1 (pois $w_i = bw_j = w_j u$) temos que $w_i = b^t c$, em que $c = 1$ ou c é um início de b, e portanto $w = aw_i = ab^t c$. Como $w = abw_j$, $|a| + |b| = j - 1 < d$. Agora, se $dk \leqslant |w|$, então

$$dk \leqslant |w| = |a| + |b| + (t-1)|b| + |c| < d + (t-1)|b| + |c| < d + t|b| < (t+1)d,$$

o que implica $k \leqslant t$. □

Lema 2.2.5. *Seja $w \in W$ tal que $|w| = kd$. Se w não contém uma subpalavra b^k, $|b| < d$, então $w = vu$, os d-fins de v são comparáveis e v pertence a um conjunto finito S cuja cardinalidade $|S|$ é limitada por*

$$|S| \leqslant s(d,k) = \binom{d}{2}(k-1)m^d.$$

Demonstração. Se os d-fins de w são incomparáveis, então pelo Lema 2.2.4 a palavra w contém uma subpalavra b^k, $|b| < d$. Portanto os d-fins de w são comparáveis. Seja v um início de w de comprimento mínimo tal que os d-fins de v são comparáveis. Pela Definição 2.2.3, $|v| \geqslant d$. Seja $v = qx$, em que x é uma letra. Então ou $|q| < d$ ou $|q| \geqslant d$ e os d-fins de q são incomparáveis. No segundo caso, pelo Lema 2.2.4, temos $q = a(cb)^t c$, em que $c, b \neq 1$, $|a| + |b| + |c| < d$ e $t \geqslant 1$ ou $q = ab^t$, em que $b \neq 1$ e $|a| + |b| < d$. O caso $t \geqslant k$ é impossível pois w contém v, logo contém $(bc)^t$ e $|bc| = |b| + |c| < d$. Então $t < k$. Podemos considerar o primeiro caso ($|q| < d$) incluído na contagem do caso $q = ab^t$ em que $t = 1$ (Note que no segundo caso deveríamos ter $t > 1$, senão $|q| = |a| + |b| < d$).

Denotaremos por S o conjunto das palavras que podem ser escritas da forma $v = a(cb)^t cx$ em que $b \neq 1$, $1 \leqslant t \leqslant k-1$, $|a| + |b| + |c| \leqslant d - 1$ e a letra x é diferente da primeira letra de b.

Vamos encontrar um limite superior para a quantidade de palavras. Seja $l = |a| + |b| + |c|$. Para um número l fixado, a quantidade de ternas de inteiros não negativos $(|a|, |b|, |c|)$ tais que $|a| + |b| + |c| = l$ e $|b| \geqslant 1$ é $\binom{l+1}{2}$ (Substituindo $|b| = B + 1$, temos $|a| + B + |c| = l - 1$ com $|a|, B, |c|$ inteiros não negativos, cujo número de soluções é dado por $\binom{l-1+2}{2}$).

Temos então m possibilidades para cada uma das l letras de abc, $k-1$ possibilidades para o expoente t e $m-1$ possibilidades para a letra x, totalizando $\binom{l+1}{2}m^l(k-1)(m-1)$ para cada l. Somando para todo l obtemos:

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

Com isso terminamos a demonstração. □

Agora vamos fazer alguns comentários sobre a estratégia geral da demonstração. O queremos é, de alguma forma, limitar o comprimento uma palavra que seja não d-decomponível. Para tanto, a ideia é verificar que se uma palavra for grande o suficiente, ela conterá uma subpalavra w que contém d subpalavras comparáveis e que aparece d vezes (disjuntas mas não necessariamente consecutivas). Podemos tomar uma dessas subpalavras comparáveis em cada uma das ocorrências da palavra w de forma a obter d subpalavras disjuntas em ordem decrescente. Então, pelo Lema 2.2.2, a palavra original seria d-decomponível.

Para obter a palavra w temos que tratar dois casos de forma paralela: se w contém uma subpalavra b^k podemos usar o Lema 2.2.3 e obter d subpalavras comparáveis. Por outro lado, se w não contém uma subpalavra b^k, em que $|b| < d$, pelo Lema 2.2.5 então w terá d subpalavras comparáveis (os d-fins de w). Em ambos os casos, a palavra w não pode aparacer d vezes na palavra original, o que limita o comprimento da palavra original. Vamos detalhar esse argumento a seguir:

Teorema 2.2.1. *(Belov) Seja w uma palavra no semigrupo livre $\langle x_1, \ldots, x_m \rangle$, $m > 1$ e sejam k e d inteiros fixados tais que $k \geqslant d > 1$. Se a palavra w não é d-decomponível, então w pode ser escrita na forma*

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

em que

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

as palavras v_i e c_i não tem início comum e, se $c_i = 1$, então v_i e v_{i+1} não têm início comum. Aqui $s(d,k)$ é o mesmo do Lema 2.2.5.

Demonstração. Se $|w| \leqslant d^2 ks(d,k)$, então podemos assumir $c_0 = w$ e o teorema é válido. Caso $|w| > d^2 ks(d,k)$, então podemos escrever w como

$$w = u_1 w_1 u_2 w_2 \cdots u_t w_t u_{t+1},$$

em que $t = ds(d,k)$, $|w_i| = kd$ e os u_i são arbitrários. Se nenhuma palavra w_i contém uma subpalavra b^k, $|b| < d$, então, pelo Lema 2.2.5, $w_i = v_i x_i$, em que v_i pertence ao conjunto S definido no mesmo lema e v_i contém d subpalavras comparáveis. Como $t = ds(d,k) \geqslant d|S|$, existe algum v_i que aparece pelo menos d vezes em w, e pelo Lema 2.2.2, a palavra w é d-decomponível, absurdo.

Portanto alguma subpalavra w_i (e portanto w) contém uma subpalavra b^k, $|b| < d$. Seja c_0 o início de w de comprimento mínimo dentre os inícios tais que $w = c_0 v_1^{k_1} w_1$, em que $|v_1| < d$, $k_1 \geqslant k$ e as palavras v_1 e w_1 não têm início comum. De fato, sempre

podemos ter v_1 e w_1 sem início comum pois tome uma apresentação $w = c_0 v_1^{k_1} w_1$ qualquer. Denotando $v_1 = pq$ e $w_1 = pr$, em que q e r não têm início comum, basta tomar $w = c_0 p(qp)^{k_1} r$, e então qp e r não terão início comum. Prosseguindo, se w_1 tiver uma subpalavra b^k, $|b| < d$, podemos fazer o mesmo procedimento, obtendo $w_1 = c_1 v_2^{k_2} w_2$, em que v_2 e k_2 não têm início comum. Continuando enquanto for possível teremos, no final:

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

em que $|v_i| < d$, $k_i \geqslant k$, c_i não têm subpalavras da forma b^k, $|b| < d$, e ou v_i e c_i não possuem início comum ou $c_1 = 1$ então v_i e v_{i+1} não têm início comum. Então w contém $r-1$ subpalavras $v_i^{d-1} x_i$ disjuntas, $i = 1, \ldots, r-1$, em que x_i é uma letra diferente da primeira letra de v_i. O número de palavras distintas da forma $v^{d-1}x$, em que $|v| < d$ e x é uma letra diferente da primeira letra de v é

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

Suponha por contradição que $r \geqslant dm^d$. Então alguma palavra da forma $v^{d-1}x$, $|v| < d$ em que x é diferente da primeira letra de v aparece pelo menos d vezes em w:

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

Pelo Lema 2.2.3, a palavra $v^{d-1}x$ tem d subpalavras comparáveis, então pelo Lema 2.2.2 temos que w é d-decomponível, absurdo. Logo $r < dm^d$.

Agora para provar a desigualdade para $\sum_{i=0}^{r} |c_i|$, vamos dividir cada uma das palavras c_i em várias subpalavras consecutivas de comprimento dk e mais uma subpalavra de comprimento menor que dk. Conseguimos então

$$p = \sum_{i=0}^{r} \left\lfloor \frac{|c_i|}{dk} \right\rfloor > \frac{1}{dk} \sum_{i=0}^{r} c_i - (r+1) \tag{2.1}$$

intervalos de comprimento dk. Como c_i não contém subpalavras da forma b^k, $|b| < d$, pelo Lema 2.2.5 cada um desses intervalos tem um início no conjunto S e portanto contém d subpalavras comparáveis. Suponha por contradição que $p \geqslant ds(d,k)$, então pelo menos algum elemento de S aparece pelo menos d vezes como uma subpalavra de w. Então novamente pelo Lema 2.2.2, w seria d-decomponível, absurdo. Logo $p < ds(d,k)$. Da Equação 2.1 temos:

$$\sum_{i=0}^{r} c_i < dk(p + (r+1)),$$

e portanto, usando a desigualdade do Lema 2.2.5

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

Assim concluímos a demonstração. □

Definição 2.2.4. *Seja R uma álgebra gerada por $r_1, \ldots, r_m$. Seja H um conjunto finito de palavras formadas por $r_1, \ldots, r_m$. Dizemos que R tem altura h relativa ao conjunto de palavras H se h é o menor inteiro tal que R é gerado como espaço vetorial pelos produtos*

$$u_{i_1}^{k_1} \cdots u_{i_t}^{k_t}$$

tais que $u_{i_1}, \ldots, u_{i_t} \in H$ e $t \leqslant h$.

Agora demonstraremos o teorema de Shirshov

Teorema 2.2.2. *(Shirshov) Seja R uma PI-álgebra gerada por m elementos $r_1, \ldots, r_m$ e satisfazendo uma identidade polinomial de grau $d > 1$. Então R tem altura finita com relação ao conjunto de todas as palavras $r_{i_1} \cdots r_{i_s}$ de comprimento $s < d$.*

Demonstração. Sabemos que se R é uma PI-álgebra, então ela satisfaz uma identidade polinomial multilinear. Vamos assumir que R satisfaz uma identidade polinomial multilinear da forma

$$x_1 \cdots x_d = \sum_{\sigma \in S_d, \sigma \neq 1} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(d)}, \quad \alpha_\sigma \in K,$$

em que a soma é sobre todas as permutações não triviais $\sigma \in S_d$. Considere um produto $w = r_{i_1} \cdots r_{i_p} \in R$. Se a palavra w é d-decomponível, então podemos escrevê-la como um produto de $d+2$ subpalavras e

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

para qualquer permutação não trivial $\sigma \in S_d$. Então aplicamos a identidade polinomial:

$$w_0(w_1 \cdots w_d)w_{d+1} = \sum_{\sigma \in S_d} \alpha_\sigma w_0(w_{\sigma(1)} \cdots w_{\sigma(d)})w_{d+1}.$$

Obtemos assim que w é uma combinação linear de palavras que são lexicograficamente menores que w (na ordem dada em Definição 2.2.1). Continuando esse processo obtemos que todos os elementos de R são combinações lineares de palavras que são não d-decomponíveis. Agora vamos tomar $k = d$ no Teorema 2.2.1. Então se uma palavra é não d-decomponível ela pode ser escrita na forma

$$w = c_0 v_1^{k_1} c_1 v_2^{k_2} \cdots v_t^{k_t} c_t,$$

em que

$$|v_i| < d, k_i \geqslant k = d, t < dm^d, \sum_{i=0}^{t} |c_i| \leqslant \frac{d^4 k^2 m^d}{2} = \frac{d^6 m^d}{2}.$$

Considerando a palavra c_i de comprimento $q_i = |c_i|$ como um produto de q_i palavras de comprimento 1, escreveremos $c_i = u_{j_1} \cdots u_{j_{q_i}}$ em que cada u_{j_k}, $k = 1, \ldots, q_i$ é igual a

algum $r_1, \ldots, r_m$, e assim concluímos que R é gerado como espaço vetorial por palavras do tipo

$$w = u_1 \cdots u_{p_0} v_1^{k_1} u_{p_0+1} \cdots u_{p_1} v_2^{k_2} \cdots v_t^{k_t} u_{p_{t-1}+1} \cdots u_{p_t}$$

em que $p_0 = q_0$, $p_1 = q_0 + q_1$, $\ldots$, $p_t = q_0 + \ldots + q_t$ e todas as palavras u_i e v_j tem comprimento $< d$. Portanto a altura de R está limitada pela soma de t e $\sum_{i=0}^{t} |c_i| = p_t$ e ambos estão limitados em termos de d e m

$$h \leqslant t + p_t < dm^d + \frac{d^6 m^d}{2}.$$

A altura h está limitada, e temos a demonstração do teorema. □

Agora vamos aplicar o teorema de Shirshov para obter os resultados de Levitzki e de Kaplansky sobre o problema de Kurosh. Intuitivamente, o teorema de Shirshov limita a altura mas não os expoentes dos elementos da base (como espaço vetorial) da PI-álgebra. Para o número de elementos da base ser limitado, falta apenas controlar o expoente, o que será possível através das condições da álgebra ser nil ou algébrica. Note que não precisamos da propriedade nil ou da algebricidade de todos os elementos como nos resultados originais, apenas para os produtos de geradores de comprimento $< d$.

Teorema 2.2.3. *Seja R uma PI-álgebra que satisfaz uma identidade polinomial de grau d e que é gerada por uma quantidade finita de elementos $r_1, \ldots, r_m$. Seja P o conjunto de todos os produtos $r_{i_1} \cdots r_{i_k}$, $k < d$. Então*

(i) (Levitzki (17)) Se todo elemento do conjunto P é nilpotente, então a álgebra R é nilpotente.

(ii) (Kaplansky (15)) Se todo elemento do conjunto P é algébrico, então a álgebra R é de dimensão finita.

Demonstração. Pelo Teorema 2.2.2, R é gerado como espaço vetorial pelos produtos

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

em que t é limitado pela altura h e u_{i_j} são palavras de comprimento $< d$ em relação aos geradores $r_1, \ldots, r_m$. Como a quantidade de palavras u_{i_j} possíveis é finita, existe um limite superior n para o grau de nilpotência ou para o grau de algebricidade dessas palavras. Então, se todos os u_{i_j} são nilpotentes e a soma $k_1 + \cdots + k_t$ é suficientemente grande ($> h(n-1)$), então algum u_{i_j} aparece com grau maior que $n-1$ e portanto a palavra vale 0. Se os elementos u_{i_j} são algébricos de grau $\leqslant n$, então os expoentes $\geqslant n$ podem ser expressos como combinação linear de $1, u_{i_j}, \ldots, u_{i_j}^{n-1}$. Logo R é gerado como espaço vetorial por todas as palavras com $k_i < n$, cuja quantidade é finita. □

2.3 Teorema de Golod e Shafarevich

Nesta seção apresentaremos o contraexemplo obtido por Golod e Shafarevich demonstrando a existência de álgebras finitamente geradas nil que não são nilpotentes. Como consequência obteremos a existência de um grupo finitamente gerado, periódico e infinito, resolvendo negativamente o problema de Burnside. A construção que utilizaremos aqui foi desenvolvida por Regev e Regev em (10). Ela é interessante pois é bastante elementar e substitui por uma indução as técnicas sobre séries de Hilbert usadas na demonstração presente no livro de Herstein (4) e na demonstração original.

Cabe notar que as demonstrações são essencialmente iguais (Começando com um ideal homogêneo, primeiro obtém-se a mesma desigualdade sobre as dimensões das componentes homogêneas do ideal. Depois prova-se que, sob certas condições, ela implica dimensão infinita. Por fim, constrói-se um ideal homogêneo que obedece essas condições tal que o quociente de $K\langle X_d\rangle$ por esse ideal seja nil) mas a prova apresentada aqui utiliza passos que são um pouco mais acessíveis.

Vamos fixar um corpo K e tomar um número inteiro $d \geqslant 2$ e $T = K\langle X_d\rangle$ a álgebra associativa não-comutativa de polinômios em d variáveis. Denotaremos por $T_{\geqslant 1} = K^+\langle X_d\rangle$ os polinômios sem termo constante. Se $I \subseteq T_{\geqslant 1}$ é um ideal bilateral, então a álgebra quociente $T_{\geqslant 1}/I$ é finitamente gerada.

O teorema principal que iremos demonstrar é

Teorema 2.3.1. *Existe um ideal bilateral homogêneo $I \subset T_{\geqslant 1}$ tal que a álgebra finitamente gerada $T_{\geqslant 1}/I$ é nil e de dimensão infinita.*

Note que isto é suficiente para demonstrar que $T_{\geqslant 1}/I$ não é nilpotente pois uma álgebra finitamente gerada e nilpotente necessariamente tem dimensão finita. Para tanto faremos a seguinte definição:

Definição 2.3.1. *Seja $H = \{f_1, f_2, \dots\}$ uma sequência de polinômios homogêneos. Assumimos que $\deg f_j \geqslant 2$ para todo $j = 1, 2, \dots$. Seja r_l o número de elementos de H de grau l. Seja $I = I_H$ o ideal bilateral gerado em $T_{\geqslant 1}$ por H. A sequência H é uma sequência G.S. (de Golod e Shafarevich) se o ideal I_H e os números r_l satisfazem:*

(i) Para todo polinômio $g \in T_{\geqslant 1}$ existe um n tal que $g^n \in I$

(ii) Para algum $\varepsilon > 0$ satisfazendo $d - 2\varepsilon > 1$, $r_l \leqslant \varepsilon^2(d - 2\varepsilon)^{l-2}$ para todo $l \geqslant 2$.

E o Teorema 2.3.1 será consequência dos dois teoremas a seguir

Teorema 2.3.2. *Seja $H \subset T_{\geqslant 1}$ uma sequência G.S., então a álgebra quociente $T_{\geqslant 1}/I$ é nil e de dimensão infinita.*

Teorema 2.3.3. *Existem sequências G.S.*

Denotaremos por $T_n \subset T$ os espaços vetoriais dos polinômios homogêneos de grau n, então $\dim T_n = d^n$ e

$$T = \bigoplus_{n=0}^{\infty} T_n.$$

Também denotaremos por

$$T_{\geqslant k} = \bigoplus_{n=k}^{\infty} T_n.$$

Em particular, $T_{\geqslant 1} \subset T$ são os polinômios sem termo constante.

Seja $H = \{f_1, f_2, \dots\}$ uma sequência de polinômios homogêneos. Assumimos que $\deg f_j \geqslant 2$, ou seja, $H \subset T_{\geqslant 2}$. Seja r_n o número de elementos de H com grau n. Então

$$H = \bigcup_{n=2}^{\infty} H_n,$$

em que $H_n = \{f_j \mid \deg f_j = n\}$ e $|H_n| = r_n$.

Seja R o espaço vetorial gerado por H, então

$$R = \bigoplus_{n=0}^{\infty} R_n = \bigoplus_{n=2}^{\infty} R_n,$$

em que R_n é o espaço vetorial gerado por H_n. Note que $\dim R_n \leqslant r_n$. Como $\deg f_j \geqslant 2$, temos que $r_0 = r_1 = 0$ e $R \subseteq T_{\geqslant 2} \subseteq T_{\geqslant 1}$. Como $T_{\geqslant 1} = TT_1$, temos que $R \subseteq TT_1$. Seja $I = \langle f_1, f_2, \dots \rangle$ o ideal bilateral de T gerado pela sequência H, temos que

$$I = TRT \subseteq T_{\geqslant 2} \subseteq T_{\geqslant 1}.$$

Seja $A = T_{\geqslant 1}/I$ a álgebra quociente. Como I é gerado por polinômios homogêneos de grau $\geqslant 2$,

$$I = \bigoplus_{n=0}^{\infty} I_n = \bigoplus_{n=2}^{\infty} I_n$$

em que $I_n = I \cap T_n$. Seja $B_n \subseteq T_n$ um complemento do espaço vetorial I_n

$$T_n = I_n \oplus B_n \tag{2.2}$$

e denote $b_n = \dim B_n$. Como $I_0 = I_1 = 0$, então $B_0 = T_0 = K$ e $B_1 = T_1$, portanto $b_0 = \dim_K K = 1$ e $b_1 = \dim_K T_1 = d$. Denotando $B = \bigoplus_{n \geqslant 0} B_n$, temos que $T = I \oplus B$.

Teorema 2.3.4. *Seja $d \geqslant 2$, $T = K\langle X_d \rangle = \bigoplus_n T_n$, $I \subseteq T$ um ideal bilateral homogêneo, $I = \bigoplus_n I_n$. Seja $T_n = I_n \oplus B_n$ e seja $b_n = \dim B_n$. Relembre que $I = \langle f_1, f_2, \dots \rangle$ em que f_j são homogêneos de grau $\geqslant 2$, e seja r_l o número de f_j de grau l (e portanto $r_0 = r_1 = 0$). Então para todo $n \geqslant 2$*

$$b_n \geqslant db_{n-1} - \sum_{j=0}^{n-2} r_{n-j} b_j \tag{2.3}$$

Demonstração. Lembrando que R é o espaço vetorial gerado por H e que $T = I \oplus B$, vamos mostrar primeiramente que

$$I = IT_1 + BR. \tag{2.4}$$

Note que $T = T_{\geqslant 1} \oplus K = TT_1 \oplus K$, logo

$$I = TRT = TR(TT_1 \oplus K) = (TRT)T_1 + TR = IT_1 + TR. \tag{2.5}$$

Agora, como $T = I \oplus B$, $R \subseteq TT_1$ e $IT = I$, temos

$$TR = (I \oplus B)R = IR + BR \subseteq ITT_1 + BR = IT_1 + BR. \tag{2.6}$$

Como $IT_1 + IT_1 = IT_1$, de (2.5) e (2.6)

$$I = IT_1 + TR \subseteq IT_1 + (IT_1 + BR) = IT_1 + BR. \tag{2.7}$$

Como $I \supseteq IT_1$ e $I \supseteq BR$, temos que $I = IT_1 + BR$, logo demonstramos (2.4).

Tomando a n-ésima componente homogênea de (2.4) temos

$$I_n = I_{n-1}T_1 + \sum_{k=0}^{n} B_{n-k}R_k = I_{n-1}T_1 + \sum_{k=2}^{n} B_{n-k}R_k. \tag{2.8}$$

Note que $\dim(I_{n-1}T_1) \leqslant (\dim I_{n-1})(\dim T_1) = (\dim I_{n-1})d$ e $\dim(B_{n-k}R_k) \leqslant b_{n-k}r_k$. Então, calculando as dimensões de (2.8)

$$\dim I_n \leqslant (\dim I_{n-1})d + \sum_{k=2}^{n} b_{n-k}r_k. \tag{2.9}$$

Substituindo $j = n - k$, obtemos

$$\dim I_n \leqslant (\dim I_{n-1})d + \sum_{j=0}^{n-2} b_j r_{n-j}. \tag{2.10}$$

De (2.2), $d^n = \dim T_n = \dim I_n + \dim B_n = \dim I_n + b_n$, então $\dim I_n = d^n - b_n$. Da mesma forma, $\dim I_{n-1} = d^{n-1} - b_{n-1}$. Substituindo em (2.10) temos a desigualdade (2.3). □

Agora vamos provar uma proposição com uma estimativa para o crescimento de b_n.

Proposição 2.3.1. *Sejam b_n e r_l as sequências do Teorema 2.3.4, que então obedecem à desigualdade (2.3). Seja $v > 0$ um número real que satisfaz a condição a seguir:*

Existem números reais $c, u > 0$ satisfazendo

(a) Para todo $n \geqslant 0$, $r_{n+2} \leqslant cu^n$;

(b) $\dfrac{vd-c}{v+u} \geqslant v$ *(e em particular* $vd > c$*).*

Então, para todo $n \geqslant 0$*,*

$$b_n \geqslant (d-v)^n. \tag{2.11}$$

Demonstração. Primeiramente, vamos provar que

$$vb_{n+1} \geqslant \sum_{j=0}^{n} cu^{n-j}b_j \tag{2.12}$$

por indução em n.

Para $n = 0$ temos $vb_1 \geqslant cb_0 = c$, que é verdade pela propriedade (b). Supondo que (2.12) é válida para n, vamos provar que é verdade para $n+1$, isto é,

$$vb_{n+2} \geqslant \sum_{j=0}^{n+1} cu^{n+1-j}b_j.$$

Pela hipótese da indução e pela propriedade (b) temos que

$$\frac{vd-c}{v+u}b_{n+1} \geqslant vb_{n+1} \geqslant \sum_{j=0}^{n} cu^{n-j}b_j.$$

Pela propriedade (a), para todo j temos $cu^{n-j} \geqslant r_{n+2-j}$ portanto

$$(vd-c)b_{n+1} \geqslant \sum_{j=0}^{n}(vcu^{n-j} + ucu^{n-j})b_j \geqslant \sum_{j=0}^{n}(vr_{n+2-j} + ucu^{n-j})b_j.$$

Logo

$$vdb_{n+1} \geqslant v\sum_{j=0}^{n} r_{n+2-j}b_j + u\sum_{j=0}^{n} cu^{n-j}b_j + cb_{n+1},$$

portanto

$$vdb_{n+1} - v\sum_{j=0}^{n} r_{n+2-j}b_j \geqslant u\sum_{j=0}^{n} cu^{n-j}b_j + cb_{n+1},$$

Combinando com (2.3)

$$vb_{n+2} \geqslant vdb_{n+1} - v\sum_{j=0}^{n} r_{n+2-j}b_j \geqslant u\sum_{j=0}^{n} cu^{n-j}b_j + cb_{n+1} = \sum_{j=0}^{n+1} cu^{n+1-j}b_j$$

isto é,

$$vb_{n+2} \geqslant \sum_{j=0}^{n+1} cu^{n+1-j}b_j,$$

que é o queríamos demonstrar.

Note que, por (2.12) e pela propriedade (a),

$$vb_{n+1} \geqslant \sum_{j=0}^{n} cu^{n-j}b_j \geqslant \sum_{j=0}^{n} r_{n+2-j}b_j$$

e portanto

$$vb_{n+1} \geqslant \sum_{j=0}^{n} r_{n+2-j} b_j. \tag{2.13}$$

Vamos mostrar que (2.3) e (2.13) implicam que para todo n

$$b_{n+2} \geqslant (d-v) b_{n+1} \tag{2.14}$$

o que implica (2.11). Por (2.13):

$$db_{n+1} - (d-v)b_{n+1} = vb_{n+1} \geqslant \sum_{j=0}^{n} r_{n+2-j} b_j,$$

logo

$$db_{n+1} - \sum_{j=0}^{n} r_{n+2-j} b_j \geqslant (d-v)b_{n+1}.$$

Por (2.3) temos

$$b_{n+2} \geqslant db_{n+1} - \sum_{j=0}^{n} r_{n+2-j} b_j \geqslant (d-v)b_{n+1},$$

o que prova (2.14), e portanto a demonstração está concluída. □

Com essa proposição conseguimos provar o seguinte:

Proposição 2.3.2. *Sejam b_n e r_l as sequências do Teorema 2.3.4, que então obedecem à desigualdade (2.3). Seja $\varepsilon > 0$ tal que $d - 2\varepsilon > 1$. Se $r_l \leqslant \varepsilon^2 (d-2\varepsilon)^{l-2}$ para todo $l \geqslant 2$, então para todo n, $b_n \geqslant 1$ (de fato, b_n cresce exponencialmente), e portanto a álgebra $A = T_{\geqslant 1}/I$ é de dimensão infinita.*

Demonstração. Na Proposição 2.3.1, tome $v = \varepsilon$, $c = \varepsilon^2$ e $u = d - 2\varepsilon$. Então $r_{n+2} \leqslant \varepsilon^2 (d-2\varepsilon)^n = cu^n$ para todo $n \geqslant 0$ e

$$\frac{vd - c}{v + u} = \frac{\varepsilon(d-\varepsilon)}{d-\varepsilon} = \varepsilon = v.$$

Então as hipóteses da Proposição 2.3.1 são satisfeitas e portanto $b_n \geqslant (d-v)^n \geqslant 1$ pois $d - v = d - \varepsilon > d - 2\varepsilon = u > 1$. □

Então, vamos fixar $\varepsilon > 0$ tal que $d - 2\varepsilon > 1$. Seguindo a Definição 2.3.1, vamos construir uma sequência de polinômios homogêneos, de grau $\geqslant 2$, $f_1, f_2, \ldots \in T_{\geqslant 2} \subset T_{\geqslant 1} \subset T = K\langle X_d \rangle$ com as seguintes propriedades:

(i) Para todo polinômio $g \in T_{\geqslant 1}$ existe um n tal que $g^n \in I$, em que $I = \langle f_1, f_2, \ldots \rangle$ é o ideal bilateral gerado pelos f_i;

(ii) Seja r_l o número de f_i de grau l, então $r_{l+2} \leqslant \varepsilon^2 (d-2\varepsilon)^l$.

Seja $A = T_{\geqslant 1}/I$, então A é gerada pelos d elementos $x_1 + I, \ldots, x_d + I$, logo é finitamente gerada. Por (i), A é nil, e por (ii) e pela Proposição 2.3.2, A é de dimensão infinita. Para demonstrar que existem sequências G.S. vamos precisar de mais alguns lemas e definições:

Definição 2.3.2. *Sejam q e n inteiros positivos. Definimos os seguintes conjuntos de n-uplas:*

(i) $I(q,n) = \{(i_1, \ldots, i_n) \mid 1 \leqslant i_1, \ldots, i_n \leqslant q\}$

(ii) $J(q,n) = \{(i_1, \ldots, i_n) \mid 1 \leqslant i_1 \leqslant \cdots \leqslant i_n \leqslant q\} \subseteq I(q,n)$

Observação 2.3.1. *Note que $|I(q,n)| = q^n$. Também temos que $|J(q,n)| = \binom{n+q-1}{q-1}$. Uma forma de provar essa última afirmação é ver que $i_1 - 1$, $i_2 - i_1$, $i_3 - i_2$, $\ldots$, $i_n - i_{n-1}$, $q - i_n$ são $n+1$ inteiros não negativos que são solução da equação $(i_1 - 1) + (i_2 - i_1) + (i_3 - i_2) + \cdots + (i_n - i_{n-1}) + (q - i_n) = q - 1$ e portanto a afirmação segue. Por outro lado,*

$$|J(q,n)| = \binom{n+q-1}{q-1} \leqslant (n+q-1)^{q-1} \tag{2.15}$$

e o lado direito é um polinômio em n de grau $q-1$.

Dados $\pi \in S_n$ e $\bar{i} = (i_1, \ldots, i_n) \in I(q,n)$, defina a ação à esquerda de S_n $\pi(\bar{i}) = (i_{\pi^{-1}(1)}, \ldots, i_{\pi^{-1}(n)})$. Então $\sigma(\pi(\bar{i})) = (\sigma\pi)(\bar{i})$, logo $I(q,n)$ é a união disjunta das órbitas correspondentes. Dado $\bar{i} \in I(q,n)$, seja $O_{\bar{i}} = \{\pi(\bar{i}) | \pi \in S_n\}$ a órbita de $\bar{i}$ sob a ação de S_n. Então

$$I(q,n) = \bigcup_{\bar{j} \in J(q,n)} O_{\bar{j}}$$

é uma união de órbitas disjuntas.

Seja $\bar{j} = (j_1, \ldots, j_n) \in J(q,n)$ então $\bar{j} = (1, \ldots, 1, 2, \ldots, 2, \ldots)$, que denotaremos por $\bar{j} = (1^{\mu_1}, \ldots, q^{\mu_q})$, em que k aparece μ_k vezes em $\bar{j}$. Então $S_{\mu_1} \times \cdots \times S_{\mu_q}$ fixa $\bar{j}$ e portanto

$$|O_{\bar{j}}| = \frac{n!}{\mu_1! \cdots \mu_q!}.$$

Definição 2.3.3. *Seja $\bar{j} \in J(q,n)$, $\bar{j} = (j_1, \ldots, j_n) = (1^{\mu_1}, \ldots, q^{\mu_q})$ definimos o polinômio multi-homogêneo completo de multigrau $(\mu_1, \ldots, \mu_q)$*

$$s_{\bar{j}}(y_1, \ldots, y_n) = \sum_{\bar{i} \in O_{\bar{j}}} y_{i_1} \cdots y_{i_n}.$$

Note que, em característica 0, também podemos escrever

$$s_{\bar{j}}(y_1, \ldots, y_n) = \frac{1}{\mu_1! \cdots \mu_q!} \sum_{\pi \in S_n} y_{j_{\pi^{-1}(1)}} \cdots y_{j_{\pi^{-1}(n)}}.$$

Lembre-se que $d \geqslant 2$. Seja $c > 0$ um inteiro, denotaremos por $q = d+d^2+\cdots+d^c$. Então q é o número de monômios de grau entre 1 e c nas variáveis não comutativas $x_1, \ldots, x_d$. Seja $\{M_1, \ldots, M_q\}$ o conjunto desses monômios. Dado um inteiro $n > 0$, e $\overline{j} \in J(q,n)$, denote por

$$h_{\overline{j}}(x) = h_{\overline{j}}(x_1, \ldots, x_d) = s_{\overline{j}}(M_1, \ldots, M_q). \tag{2.16}$$

Com estas notações provaremos

Lema 2.3.1. *Sejam um inteiro $c > 0$, $q = d + d^2 + \cdots + d^c$, e $\{M_1, \ldots, M_q\}$ os monômios de grau entre 1 e c. Seja um inteiro $n > 0$ e seja $I \subseteq K\langle X_d\rangle$ um ideal bilateral contendo $h_{\overline{j}}$ para todo $\overline{j} \in J(q,n)$, em que $h_{\overline{j}}(x)$ é dado por (2.16). Seja $g = g(x_1, \ldots, x_d) \in T_{\geqslant 1}$ um polinômio de grau $\leqslant c$. Então $g^n \in I$.*

Demonstração. Como $M_1, \ldots, M_q$ são todos monômios não constantes em $x_1, \ldots, x_d$ de grau $\leqslant c$, então podemos escrever

$$g = \sum_{i=1}^{q} \alpha_i M_i$$

com $\alpha_i \in K$. Então

$$g^n = \sum_{1 \leqslant i_1, \ldots, i_n \leqslant q} (\alpha_{i_1} M_{i_1}) \cdots (\alpha_{i_n} M_{i_n}) = \sum_{1 \leqslant i_1, \ldots, i_n \leqslant q} (\alpha_{i_1} \cdots \alpha_{i_n})(M_{i_1} \cdots M_{i_n}).$$

Juntando os termos em cada órbita e usando a notação (2.16) temos:

$$\begin{aligned} g^n &= \sum_{\overline{j} \in J(q,n)} (\alpha_{j_1} \cdots \alpha_{j_n}) \sum_{\overline{i} \in O_{\overline{j}}} (M_{i_1} \cdots M_{i_n}) = \sum_{\overline{j} \in J(q,n)} (\alpha_{j_1} \cdots \alpha_{j_n}) s_{\overline{j}}(M_1, \ldots, M_q) \\ &= \sum_{\overline{j} \in J(q,n)} (\alpha_{j_1} \cdots \alpha_{j_n}) h_{\overline{j}}(x_1, \ldots, x_d) \end{aligned}$$

e portanto g^n é combinação linear dos polinômios $\{h_{\overline{j}}(x_1, \ldots, x_d) | \overline{j} \in J(q,n)\}$, e como eles estão em I, temos que $g^n \in I$. □

Observação 2.3.2. *Vimos no Observação 2.3.1 que $|J(q,n)| \leqslant (n+q-1)^{q-1}$. O lado direito é um polinômio em n de grau $q-1$, então cresce mais lentamente que qualquer função exponencial em n, em particular, que $\varepsilon^2\alpha^n$, desde que $\varepsilon > 0$ e $\alpha > 1$. Isso implica que, sendo $d \geqslant 2$, $\varepsilon > 0$ tal que $d - 2\varepsilon > 1$, então para um n suficientemente grande temos*

$$|J(q,n)| \leqslant \varepsilon^2 (d - 2\varepsilon)^{n-2}. \tag{2.17}$$

Agora vamos provar o teorema

Teorema 2.3.5. *Existem sequências G.S. Mais precisamente, se $d \geqslant 2$, $\varepsilon > 0$ tal que $d - 2\varepsilon > 1$, então existe uma sequência $f_1, f_2, \ldots \in T$ de polinômios homogêneos de grau $\geqslant 2$ satisfazendo as condições da Definição 2.3.1.*

Demonstração. A construção é indutiva, começando pela sequência vazia. Na hipótese da indução assumimos que no k-ésimo passo nós escolhemos inteiros $c_k \leqslant c'_k$ e uma sequência de polinômios homogêneos $f_1, \ldots, f_{m_k}$ de graus entre 2 e c'_k. Assumimos que $f_1, \ldots, f_{m_k}$ satisfazem a seguinte condição:

(1) Para todo $l \leqslant c'_k$, o número r_l de elementos f_i de grau l satisfaz $r_{l+2} \leqslant \varepsilon^2(d-2\varepsilon)^l$;

(2) Para qualquer $g \in T_{\geqslant 1}$ de grau $\leqslant c_k$ existe algum expoente n tal que $g^n \in I_k$, em que $I_k = \langle f_1, \ldots, f_{m_k}\rangle$.

Então para o próximo passo escolhemos inteiros $c_{k+1} \leqslant c'_{k+1}$ tais que $c'_k < c_{k+1}$ e construímos outro bloco de polinômios $f_{m_k+1}, \ldots, f_{m_{k+1}}$ com graus $c'_k < \deg f_j < c'_{k+1}$, obtendo a sequência $f_1, \ldots, f_{m_k}, f_{m_k+1}, \ldots, f_{m_{k+1}}$.

A construção começa escolhendo um $c_{k+1} > c'_k$ qualquer. Seja $q = q_{k+1} = d + d^2 + \cdots + d^{c_{k+1}}$ e tome n grande o suficiente tal que $c'_k < n$ e

$$|J(q,n)| < \varepsilon^2(d-2\varepsilon)^{n-2}. \tag{2.18}$$

Pela Observação 2.3.2, tal n existe. Tomamos $c'_{k+1} = nc_{k+1}$, $m_{k+1} = |J(q,n)| + m_k$ e f_{m_k+1}, $\ldots$, $f_{m_{k+1}}$ como todos os $|J(q,n)|$ polinômios

$$h_{\overline{j}}(x_1, \ldots, x_d) = s_{\overline{j}}(M_1, \ldots, M_q), \overline{j} \in J(q,n)$$

dados por (2.16). Note que, para $\overline{j} \in J(q,n)$, temos $\deg s_{\overline{j}}(y_1, \ldots, y_q) = n$ e $1 \leqslant \deg M_i \leqslant c_{k+1}$, logo

$$c'_k < n \leqslant \deg s_{\overline{j}}(M_1, \ldots, M_q) \leqslant nc_{k+1} = c'_{k+1}. \tag{2.19}$$

Agora vamos demonstrar que a nova sequência $f_1, \ldots, f_{m_k}, f_{m_k+1}, \ldots, f_{m_{k+1}}$ obedece às condições da indução.

Note que $\langle f_{m_k+1}, \ldots, f_{m_{k+1}}\rangle \subseteq \langle f_{m_1}, \ldots, f_{m_k}, f_{m_k+1}, \ldots, f_{m_{k+1}}\rangle = I_{k+1}$. Pelo Lema 2.3.1, para todo polinômio $g \in T_{\geqslant 1}$ de grau $\leqslant c_{k+1}$, temos $g^n \in \langle f_{m_k+1}, \ldots, f_{m_{k+1}}\rangle$ e portanto $g^n \in I_{k+1}$, que é a parte (2) da condição para $k+1$.

Pela hipótese da indução, os graus de $f_1, \ldots, f_{m_k}$ são todos $\leqslant c'_k$. Pela escolha de n, temos que $c'_k < n$ e por (2.19) os graus de $f_{m_k+1}, \ldots, f_{m_{k+1}}$ estão entre n e $c'_{k+1} = c_{k+1}n$. Portanto para $l \leqslant c'_k$, os r_l anteriores não mudam. Note também que para $l > c'_k$ apenas $f_{m_k+1}, \ldots, f_{m_{k+1}}$ contribuem em r_l.

Para $l > c'_k$, podemos assumir $l \geqslant n$ pois os graus de $f_{m_k+1}, \ldots, f_{m_{k+1}}$ são pelo menos n. De (2.18) temos

$$r_l \leqslant |J(q,n)| < \varepsilon^2(d-2\varepsilon)^{n-2} \leqslant \varepsilon^2(d-2\varepsilon)^{l-2}$$

o que termina a demonstração. □

Por fim, vamos construir o contraexemplo para o problema de Burnside.

Teorema 2.3.6. *Seja p um número primo qualquer. Então existe um grupo G infinito finitamente gerado tal que todo elemento tem ordem finita e igual a uma potência de p.*

Demonstração. Tome $K = \mathbb{Z}_p$ o corpo primo de p elementos e $A = T/I$ com T e I definidos nesta seção. Vamos definir $a_1 = x_1 + I$, $a_2 = x_2 + I$, $\ldots$, $a_d = x_d + I$ elementos de A e G o semigrupo multiplicativo em A gerado por $1 + a_1$, $1 + a_2$, $\ldots$, $1 + a_d$. Note que todo elemento de G é do tipo $1 + a$ em que $a \in T_{\geqslant 1}/I$. Como a é nilpotente, existe um n suficientemente grande tal que $a^{p^n} = 0$, logo $(1 + a)^{p^n} = 1 + a^{p^n} = 1$ pois estamos em característica p. Logo G é um grupo e todo elemento de G tem ordem finita. Afirmamos que G é infinito. De fato, se G fosse finito então as combinações lineares dos seus elementos formariam uma álgebra B de dimensão finita sobre K. Como 1 e $1 + a_i$ estão em G então $(1 + a_i) - 1 = a_i \in B$. Como 1, a_1, $\ldots$, a_d geram A então $A = B$, contradizendo o fato que A é de dimensão infinita. Portanto G é infinito e o teorema está provado. □

3 Teorema de Nagata-Higman

3.1 Comentários Históricos

Neste capítulo nós nos dedicaremos a explorar os resultados relacionados ao Teorema de Nagata–Higman sobre a nilpotência de álgebras nil de grau limitado. Primeiro vamos enunciar o teorema:

Teorema 3.1.1. *Seja R uma álgebra associativa não unitária sobre um corpo K de característica 0. Se R satisfaz a identidade polinomial $x^n = 0$, então existe um inteiro $d = d(n)$ que depende apenas de n tal que R é nilpotente de grau d, isto é, R satisfaz a identidade polinomial $x_1x_2\cdots x_d = 0$.*

Primeiro observaremos que a demonstração do teorema vale não apenas em característica 0 mas ainda se a característica de K é $p > n$.

O teorema acima foi provado inicialmente em 1953 por Nagata (8), que obteve uma cota superior bem grande, utilizando representações do grupo simétrico. Em 1956, Higman (6) obteve a cota superior $d(n) \leqslant 2^n - 1$ e a cota inferior $d(n) \geqslant n^2/e^2$ através de métodos mais elementares. Muito mais tarde foi descoberto que Dubnov e Ivanov já haviam obtido esse resultado em 1943 (14), mas ficou desconhecido pelos pesquisadores, até a década de 90. Então é mais justo nos referirmos a esse teorema como o teorema de Dubnov–Ivanov–Nagata–Higman.

Em 1974, Razmyslov (9), estudando as identidades polinomiais com traço da álgebra $M_n(K)$ obteve a cota superior $d(n) \leqslant n^2$. Por outro lado, em 1975, Kuzmin (16) mostrou que existe uma álgebra nil de grau n que não satisfaz a identidade $x_1x_2\cdots x_m = 0$ para $m = \frac{1}{2}n(n+1)-1$, isto é, $d(n) \geqslant \frac{n(n+1)}{2}$ e conjecturou que de fato $d(n) = \frac{n(n+1)}{2}$.

Pouco se sabe em relação aos valores concretos da conjectura. Para $n \leqslant 3$ temos que a conjectura é válida, pois $d(1) = 1$, $d(2) = 3$ e $d(3) = 6$ (também obtido por Higman em (6)). Para $n = 4$, em 1993, Vaughan-Lee (11), utilizou representações do grupo simétrico para reduzir o problema e conseguiu usar métodos computacionais para confirmar que $d(4) = 10$. Para $n = 5$, Shestakov e Zhukavets (19) confirmaram a conjectura para n = 5, no caso de álgebras e superálgebras de 2 geradores.

Nesta seção, a não ser quando dito o contrário, iremos considerar as álgebras sobre corpos de característica 0.

3.2 A cota $d(n) \leqslant 2^n - 1$

Nesta seção apresentaremos uma demonstração para a cota superior $2^n - 1$ obtida por Higman (6). Seguiremos o livro de Drensky e Formanek (2) ou (3) que utiliza uma prova devida a Higgins. Vamos começar pelo caso $n = 2$.

Proposição 3.2.1. *Seja R uma álgebra associativa não unitária sobre um corpo K de característica 0. Então a identidade $x^2 = 0$ implica $x_1x_2x_3 = 0$.*

Demonstração. Linearizando $x^2 = 0$ obtemos:

$$e_2(x, y) = (x + y)^2 - x^2 - y^2 = xy + yx = 0.$$

Então, utilizando as substituições adequadas obtemos:

$$\begin{aligned} e_2(x_1x_2, x_3) &= x_1x_2x_3 + x_3x_1x_2 = 0; \\ e_2(x_2x_3, x_1) &= x_2x_3x_1 + x_1x_2x_3 = 0; \\ e_2(x_3x_1, x_2) &= x_3x_1x_2 + x_2x_3x_1 = 0. \end{aligned}$$

Resolvendo o sistema concluímos que

$$x_1x_2x_3 = x_2x_3x_1 = x_3x_1x_2 = 0.$$

□

Agora vamos demonstrar o resultado geral:

Teorema 3.2.1 (Higman)**.** *Nas condições do Teorema 3.1.1, temos que $d(n) \leqslant 2^n - 1$. Mais precisamente, se $n > 1$ e $d(n-1)$ existe, então $d(n) \leqslant 2d(n-1) + 1$.*

Higgins. Aplicando a linearização parcial na identidade $x^n = 0$:

$$f(x, y) = x^{n-1}y + x^{n-2}yx + \cdots + xyx^{n-2} + yx^{n-1} = 0.$$

Com algumas manipulações algébricas obtemos:

$$f(x, yz^j)z^{n-j-1} = x^{n-1}yz^{n-1} + x^{n-2}yz^jxz^{n-j-1} + \cdots + xyz^jx^{n-2}z^{n-j-1} + yz^jx^{n-1}z^{n-j-1} = 0.$$

E somando para $j = 0, 1, \ldots, n-1$:

$$\sum_{j=0}^{n-1} f(x, yz^j)z^{n-j-1} = nx^{n-1}yz^{n-1} + \sum_{i=0}^{n-2} x^iyf(z, x^{n-i-1}) = 0.$$

Como $f = 0$ e a característica do corpo é 0, obtemos para x, y, $z \in R$:

$$x^{n-1}yz^{n-1} = 0. \tag{3.1}$$

Assumindo que $d(n-1)$ existe temos que $x_1x_2\cdots x_{d(n-1)}$ é consequência x^{n-1}, logo pode ser escrito como $x_1x_2\cdots x_{d(n-1)} = \sum_i a_i b_i^{n-1} c_i$ em que b_i são polinômios e a_i, c_i são polinômios ou são constantes em K. Analogamente, $x_{d(n-1)+2}\cdots x_{2d(n-1)+1} = \sum_j u_j v_j^{n-1} w_j$ em que v_j são polinômios e u_j, w_j são polinômios ou são constantes em K. Portanto:

$$x_1\cdots x_{d(n-1)}x_{d(n-1)+1}x_{d(n-1)+2}\cdots x_{2d(n-1)+1} = \sum_{i,j} a_i(b_i^{n-1}(c_i x_{d(n-1)+1}u_j)v_j^{n-1})w_j = 0,$$

pois basta tomar $x = b_i$, $y = c_i x_{d(n-1)+1}u_j$, $z = v_j$ em (3.1). Logo $d(n) \leqslant 2d(n-1)+1$.

Temos claramente que $d(1) = 1 = 2^1 - 1$. Por indução, se $d(n-1) \leqslant 2^{n-1} - 1$ então $d(n) \leqslant 2d(n-1)+1 \leqslant 2(2^{n-1}-1)+1 = 2^n - 1$. □

Observação 3.2.1. *Considerando a demonstração anterior e que $d(4) = 10$, podemos obter uma cota superior um pouco melhor: $d(n) = 11\cdot 2^{n-4} - 1$ para $n \geqslant 4$. Isso significa que para $n = 5$ a melhor cota superior é $d(5) \leqslant 21$.*

3.3 Alguns comentários e a cota $d(n) > n^2/e^2$

Observando a demonstração da proposição Proposição 3.2.1, conseguimos obter as seguintes relações:

$$x_1x_2x_3 = \frac{1}{2}(e_2(x_1x_2, x_3) + e_2(x_2x_3, x_1) - e_2(x_3x_1, x_2)) \tag{3.2}$$

$$\begin{aligned} x_1x_2x_3 =& \frac{1}{2}((x_1x_2 + x_3)^2 + (x_2x_3 + x_1)^2 - (x_3x_1 + x_2)^2 \\ &- (x_1x_2)^2 - (x_2x_3)^2 + (x_3x_1)^2 - x_1^2 + x_2^2 - x_3^2) \end{aligned} \tag{3.3}$$

Isto é, $x_1x_2x_3$ pode ser escrito tanto como combinação linear de elementos do tipo $e(x, y)$ como também como combinação linear de quadrados.

Naturalmente, como $x_1x_2x_3$ está no T-ideal gerado por x^2, esperamos que $x_1x_2x_3 = \sum_i a_i b_i^2 c_i$ para b_i polinômios e a_i, c_i polinômios ou constantes em K. Porém, as equações (3.2) e (3.3) sugerem que é possível obter somas em que a_i, c_i são constantes. Vamos mostrar que isso é verdade. Aqui apresentamos a demonstração encontrada no livro de Zhevlakov, Slin'ko, Shestakov e Shirshov (12):

Teorema 3.3.1. *Seja K um corpo de característica 0. O T-ideal gerado por x^n na álgebra livre não-unitária $K^+\langle X\rangle$ coincide com o espaço vetorial gerado por todas as n-ésimas potências. Em particular, para $m \geqslant d(n)$ o monômio $x_1\cdots x_m$ pode ser escrito na forma:*

$$x_1\cdots x_m = \sum \alpha_u u^n$$

para alguns $\alpha_u \in K$ e $u \in K^+\langle X\rangle$

Demonstração. Todo elemento do T-ideal gerado por x^n é uma combinação linear de elementos do tipo b^n, ab^n, b^nc, ab^nc para alguns polinômios a, b, c (sem termos constantes) na álgebra livre. Então é suficiente mostrar que ab^n, b^nc, ab^nc são combinações lineares de alguns $u_1^n, \ldots, u_k^n$.

A linearização total de qualquer identidade polinomial $f(x_1, \ldots, x_m)$ é obtida através de argumentos baseados em sistemas lineares e do determinante de Vandermonde, e portanto são combinações lineares de $f(u_1, \ldots, u_m)$, $u_i \in K^+\langle X\rangle$. Em particular, $e_n(x_1, \ldots, x_n)$ pode ser escrita como combinação linear de termos do tipo w^n em que w é um polinômio.

Temos a seguinte igualdade:

$$e_n(ab, a, \ldots, a) = ae_n(b, a, \ldots, a)$$

logo $ae_n(b, a, \ldots, a)$ é uma combinação linear de potências n-ésimas. Tomando a linearização total dessa última expressão temos que

$$\sum_{i=1}^{n} a_i e_n(b, a_1, \ldots, \hat{a_i}, \ldots, a_n)$$

em que $\hat{a_i}$ indica que omitimos o termo a_i, também é uma combinação linear de potências n-ésimas.

Tomando $a_1 = a$ e $a_2 = \cdots = a_n = b$ temos

$$ae_n(b, \ldots, b) + (n-1)be_n(a, b, \ldots, b).$$

Como já demonstramos que $be_n(a, b, \ldots, b)$ é combinação linear de potências n-ésimas, concluímos que $ae_n(b, \ldots, b) = n!ab^n$ e portanto ab^n também são. Para b^nc o procedimento é análogo.

Agora para ab^nc observe que:

$$ab^nc = (ab^n)c = \sum \alpha_i u_i^n c = \sum \alpha_i \sum \beta_{ij} v_{ij}^n.$$

Logo o resultado está provado. □

Corolário 3.3.1. *O T-ideal gerado por x^n na álgebra livre não-unitária $K^+\langle X\rangle$ é gerado como espaço vetorial por*

$$e_n(u_1, \ldots, u_n) = \sum_{\sigma \in S_n} u_{\sigma(1)} \cdots u_{\sigma(n)}, \tag{3.4}$$

em que $u_1, \ldots, u_n$ são monômios em $K^+\langle X\rangle$.

Demonstração. A identidade $x^n = 0$ é equivalente à sua linearização total

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

e $e_n(x,\dots,x) = n!x^n$. Pelo Teorema 3.3.1, o T-ideal $\langle x^n\rangle^T$ gerado por x^n é gerado como espaço vetorial por $u^n, u \in K^+\langle X\rangle$. Como K tem característica 0, então $x^n = e_n(x,\dots,x)/n!$ e assim $\langle x^n\rangle^T$ é gerado como espaço vetorial por $e_n(u_1,\dots,u_n)$, em que u_1, $\dots$, $u_n \in K^+\langle X\rangle$. Como $e_n(x_1,\dots,x_n)$ é multilinear, podemos assumir que u_1, $\dots$, u_n são monômios. □

A partir desse corolário conseguimos obter a cota inferior obtida por Higman:

Teorema 3.3.2. *Nas condições do Teorema 3.1.1 e para n suficientemente grande temos que* $d(n) > n^2/e^2$

Demonstração. Pelo corolário anterior, se $D \geqslant d(n)$ então $x_1\cdots x_D$ pode ser escrito como combinação linear de termos $e_n(u_1,\dots,u_n)$. Como $e_n(u_1,\dots,u_n)$ é homogêneo, então u_1, $\dots$, u_n devem ter grau total 1 para cada x_i. Vamos contar o número de polinômios $e_n(u_1,\dots,u_n)$ que existem.
Note que $u_1\cdots u_n$ obtido através da concatenação dos u_i é uma permutação de x_1, $\dots$, x_D, e que podemos tomar qualquer permutação de x_1, $\dots$, x_D e escolher $n-1$ dentre as $D-1$ posições entre dois termos consecutivos para separar a permutação e obter os monômios u_1, $\dots$, u_n. Como a ordem dos monômios u_1, $\dots$, u_n não importa, contamos cada $e_n(u_1,\dots,u_n)$ um total de $n!$ vezes. Logo o número de $e_n(u_1,\dots,u_n)$ é

$$\frac{D!\binom{D-1}{n-1}}{n!} = \frac{D!(D-1)!}{n!(n-1)!(D-n)!}.$$

Esta quantidade deve ser no mínimo igual ao número de permutações de x_1, $\dots$, x_D, logo:

$$\frac{D!(D-1)!}{n!(n-1)!(D-n)!} \geqslant D! \Rightarrow \frac{(D-1)!}{n!(n-1)!(D-n)!} \geqslant 1.$$

Utilizando a aproximação de Stirling e considerando um n suficientemente grande, temos:

$$D^{n-1} > \frac{(D-1)!}{(D-n)!} \geqslant n!(n-1)! = \frac{(n!)^2}{n} > \frac{1}{n}\left(\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\right)^2 > \left(\frac{n}{e}\right)^{2n-2}.$$

Portanto $d(n) > n^2/e^2$. □

3.4 A igualdade $d(3) = 6$

Vamos fazer um pequeno desvio para demonstrar o caso $n = 3$, cujo valor é $d(3) = 6$. A demonstração a seguir é baseada na de Higman (6).

Linearizando parcialmente $x^3 = 0$ obtemos

$$f(x,y) = x^2y + xyx + yx^2 = 0,$$

e linearizando totalmente temos

$$e_3(x,y,z) = xyz + xzy + yxz + yzx + zxy + zyx = 0.$$

Logo as seguintes expressões se anulam:

$$\begin{aligned}
0 = e_3(a, x^2b, c) &= ax^2bc + acx^2b + x^2bac + x^2bca + cax^2b + cx^2ba,\\
0 = e_3(ax, xb, c) &= ax^2bc + axcxb + xbaxc + xbcax + cax^2b + cxbax,\\
0 = e_3(ax^2, b, c) &= ax^2bc + ax^2cb + bax^2c + bcax^2 + cax^2b + cbax^2.
\end{aligned}$$

Observe que

$$\begin{aligned}
acx^2b + axcxb + ax^2cb &= a(cx^2 + xcx + x^2c)b = af(x,c)b = 0,\\
x^2bac + xbaxc + bax^2c &= (x^2ba + xbax + bax^2)c = f(x,ba)c = 0,\\
x^2bca + xbcax + bcax^2 &= f(x,bca) = 0,\\
cx^2ba + cxbax + cbax^2 &= c(x^2ba + xbax + bax^2) = cf(x,ba) = 0.
\end{aligned}$$

E portanto, somando as três expressões obtemos

$$ax^2bc + cax^2b = e_2(ax^2b, c) = 0. \tag{3.5}$$

Como sabemos que $d(2) = 3$, de uma forma semelhante à dedução de Proposição 3.2.1, porém partindo da igualdade acima podemos obter

$$abcdef + fabcde = 0. \tag{3.6}$$

Por outro lado, substituindo ax^2d no lugar de a na identidade

$$2aef = e_2(ae, f) + e_2(a, ef) - e_2(fa, e),$$

temos que cada termo pode ser obtido de (3.5), logo $ax^2def = 0$, que linearizado gera

$$abcdef + acbdef = 0. \tag{3.7}$$

Agora note que (3.6) e (3.7) equivalem a uma permutação cíclica e uma transposição de termos consecutivos, logo podem ser usados para gerar todo o grupo simétrico e então $abcdef$ é uma função alternada dos seus fatores. Considerando $e_3(ab, cd, ef) = 0$, veja que todos os termos são permutações pares e portanto $0 = e_3(ab, cd, ef) = 6abcdef$ e assim concluímos que $abcdef = 0$ e portanto $d(3) \leqslant 6$. Na seção a seguir veremos que $d(3) \geqslant 6$, portanto $d(3) = 6$.

3.5 A cota inferior $d(n) \geqslant n(n+1)/2$

Nesta seção apresentaremos a prova de Kuzmin (16) para a cota inferior do índice de nilpotência. Para tanto, seguiremos o livro de Drensky (3). (O artigo de Kuzmin, até agora, não foi traduzido em inglês, e mesmo em russo, não está disponível facilmente.) A ideia é mostrar que o monômio em duas variáveis x, y:

$$u = yxyx^2y\cdots x^{n-2}yx^{n-1} \tag{3.8}$$

não está contido no T-ideal gerado por x^n.

Nós iremos trabalhar na álgebra livre não-unitária gerada por dois elementos $K^+\langle x, y\rangle$. Vamos denotar por $J = \langle x^n\rangle^T$ o T-ideal de $K^+\langle x, y\rangle$ gerado por x^n. Vamos introduzir uma série de notações:

$A^{(k)}$ é o espaço vetorial gerado por todos os monômios do tipo

$$u_a = x^{a_1}yx^{a_2}y\cdots x^{a_{k-1}}yx^{a_k} \tag{3.9}$$

de grau $k-1$ em relação à y, $1 \leqslant k \leqslant n$;

$B^{(k)}$ é o subespaço de $A^{(k)}$ gerado por todos os polinômios dos três tipos a seguir:

(1) u_a da forma (3.9) tal que $a_i = a_j$ para algum par de índices distintos i, j;

(2) u_a da forma (3.9) tal que $a_i \geqslant n$ para algum índice i;

(3) as somas da forma $x^{a_1}y\cdots x^{a_i}\cdots x^{a_j}\cdots yx^{a_k} + x^{a_1}y\cdots x^{a_j}\cdots x^{a_i}\cdots yx^{a_k}$ para algum par de índices distintos i, j.

Denote $A = A^{(n)}$ e $B = B^{(n)}$ e por fim, denote por C o subespaço de A gerado por todos os monômios do tipo

$$x^{\sigma(0)}yx^{\sigma(1)}y\cdots x^{\sigma(n-2)}yx^{\sigma(n-1)},$$

em que $\sigma \in S_n$ e S_n age sobre o conjunto $\{0, 1, \ldots, n-1\}$.

Vamos provar que $C \cap J \subset B$. Como o monômio (3.8) é de grau

$$(0 + 1 + 2 + \cdots + (n-1)) + (n-1) = \frac{n(n+1)}{2} - 1$$

e não pertence a B, poderemos concluir que $d(n) \geqslant n(n+1)/2$.

Para simplificar a notação, vamos considerar a bijeção φ_k entre os polinômios nas variáveis comutativas $t_1, \ldots, t_k$ e os elementos de $A^{(k)}$ definida da seguinte maneira:

$$\varphi_k : t_1^{a_1}t_2^{a_2}\cdots t_{k-1}^{a_{k-1}}t_k^{a_k} \mapsto x^{a_1}yx^{a_2}y\cdots x^{a_{k-1}}yx^{a_k}$$

Para podermos trabalhar em $K[t_1, \ldots, t_k]$ vamos definir as seguintes notações: $A_0^{(k)} = K[t_1, \ldots, t_k]$, $J_0^{(k)} = \varphi_k^{-1}(J \cap A^{(k)})$, $B_0^{(k)} = \varphi_k^{-1}(B^{(k)})$, $A_0 = A_0^{(n)}$, $\varphi = \varphi_n$, $J_0 = J_0^{(n)}$, $B_0 = B_0^{(n)}$, $C_0 = \varphi^{-1}(C)$.

Note que para qualquer polinômio $f(t_1, \ldots, t_{k-1}) \in B_0^{(k-1)}$ e qualquer c_1, o polinômio $t_1^{c_1} f(t_2, \ldots, t_k) \in B_0^{(k)}$. Finalmente, para quaisquer inteiros $k \leqslant n$ e $p \geqslant 1$, defina

$$h_{k,p}(t_1, \ldots, t_k) = \sum_{c_1 + \cdots + c_k = p} t_1^{c_1} \cdots t_k^{c_k}. \tag{3.10}$$

A seguir vamos provar dois lemas que vão nos permitir caracterizar alguns dos polinômios do espaço vetorial $B_0^{(k)}$.

Lema 3.5.1. *Seja*

$$u = u(t_1, \ldots, t_k) = t_1^{a_1} t_2^{a_2} \cdots t_k^{a_k}$$

um monômio tal que $0 \leqslant a_1 < a_2 < \cdots < a_k \leqslant n-1$ *e* $a_1 + k + p > n$.

Então

$$h_{k,p}(t_1, \ldots, t_k) u(t_1, \ldots, t_k) \in B_0^{(k)}.$$

Demonstração. A prova é por indução em k. Se $k = 1$, então $u = t_1^{a_1}$, $0 \leqslant a_1 \leqslant n-1$, $h_{1,p} = t_1^p$, $h_{1,p} u = t_1^{a_1 + p}$ e como $a_1 + k + p = a_1 + 1 + p > n$ temos $a_1 + p \geqslant n$ e assim

$$h_{1,p}(t_1) u(t_1) = t_1^{n+q}$$

para algum $q \geqslant 0$. Portanto, $h_{1,p}(t_1) u(t_1) \in B_0^{(1)}$ pela condição (2) da definição de $B^{(k)}$.

Suponha agora que $k > 1$. Então

$$h_{k,p} u = \sum_{\sum c_i = p} t_1^{a_1 + c_1} t_2^{a_2 + c_2} \cdots t_k^{a_k + c_k}. \tag{3.11}$$

Tome um termo arbitrário de $h_{k,p} u$

$$t_1^{a_1 + d_1} t_2^{a_2 + d_2} \cdots t_k^{a_k + d_k}. \tag{3.12}$$

Se $0 \leqslant d_1 < a_2 - a_1$, então a soma de todos os monômios em (3.11) tais que $c_1 = d_1$ é

$$\sum_{\sum c_i = p - d_1} t_1^{a_1 + d_1} t_2^{a_2 + c_2} \cdots t_k^{a_k + c_k} = t_1^{a_1 + d_1} h_{k-1, p-d_1}(t_2, \ldots, t_k) t_2^{a_2} \cdots t_k^{a_k}.$$

Como $d_1 < a_2 - a_1$, temos que $a_1 + d_1 < a_2$ e portanto $a_1 + d_1 + 1 \leqslant a_2$,

$$\begin{aligned} n &< a_1 + k + p = a_1 + k + (d_1 + c_2 + \cdots + c_k) \\ &= (a_1 + d_1 + 1) + (k-1) + (c_2 + \cdots + c_k) \leqslant a_2 + (k-1) + p' \end{aligned}$$

em que $p' = c_2 + \cdots + c_k$.

Como $a_2+(k-1)+p' > n$, temos por indução que $h_{k-1,p-d_1}(t_2,\ldots,t_k)t_2^{a_2}\cdots t_k^{a_k} \in B_0^{(k-1)}$ e portanto

$$h_{k,p}u = t_1^{a_1+d_1}h_{k-1,p-d_1}(t_2,\ldots,t_k)t_2^{a_2}\cdots t_k^{a_k} \in B_0^{(k-1)}.$$

Porém, se o termo (3.12) é tal que $d_1 \geqslant a_2 - a_1$, temos que $d_1 = a_2 - a_1 + i$ e $d_2 = j$ para alguns $i, j \geqslant 0$. Considere então o termo

$$t_1^{a_1+e_1}t_2^{a_2+e_2}t_3^{a_3+d_3}\cdots t_k^{a_k+d_k} \tag{3.13}$$

em que $e_1 = a_2 - a_1 + j$ e $e_2 = i$. Agora temos duas possibilidades:

1. Caso $i = j$ então os termos (3.12) e (3.13) são ambos iguais a

   $$t_1^{a_1+(a_2-a_1+i)}t_2^{a_2+i}t_3^{a_3+d_3}\cdots t_k^{a_k+d_k} = t_1^{a_2+i}t_2^{a_2+i}t_3^{a_3+d_3}\cdots t_k^{a_k+d_k}$$

   e portanto pertencem a $B_0^{(k)}$ pela condição (1) da definição de $B^{(k)}$;

2. Caso $i \neq j$ então os termos (3.12) e (3.13) são distintos e sua soma é igual a

   $$(t_1^{a_2+i}t_2^{a_2+j} + t_1^{a_2+j}t_2^{a_2+i})t_3^{a_3+d_3}\cdots t_k^{a_k+d_k}$$

   e portanto pertencem a $B_0^{(k)}$ pela condição (3) da definição de $B^{(k)}$.

Desta maneira nós dividimos a expressão $h_{k,p}u$ em três partes, cada uma delas contidas em $B_0^{(k)}$: os termos com $d_1 < a_2 - a_1$, os termos com $d_1 = a_2 - a_1 + i$ e $d_2 = i$ e os pares de monômios com $d_1 = a_2 - a_1 + i$ e $d_2 = j$ e $e_1 = a_2 - a_1 + j$ e $e_2 = i$ com $i \neq j$. Concluímos que $h_{k,p}u \in B_0^{(k)}$. □

Lema 3.5.2. *Seja*

$$u = u(t_1,\ldots,t_k) = t_1^{a_1}t_2^{a_2}\cdots t_k^{a_k}$$

um monômio tal que $k + p > n$. Então

$$h_{k,p}(t_1,\ldots,t_k)u(t_1,\ldots,t_k) \in B_0^{(k)}.$$

Demonstração. Inicialmente, suponha que

$$u(t_1,\ldots,t_k) = t_1^{a_1}t_2^{a_2}\cdots t_k^{a_k} \in B_0^{(k)}.$$

Neste caso, $a_i \geqslant n$ para algum i ou $a_i = a_j$ para alguns i, j distintos. Se $a_i \geqslant n$, então $a_i + c_i \geqslant n$ para tal i em cada termo de $h_{k,p}u$ e portanto

$$h_{k,p}u = \sum_{\sum c_i = p} t_1^{a_1+c_1}t_2^{a_2+c_2}\cdots t_k^{a_k+c_k} \in B_0^{(k)}.$$

Se $a_i = a_j$ para $i < j$, vamos dividir os termos de $h_{k,p}u$ em duas partes:

1. Caso $c_i = c_j$ então os termos são da forma

$$t_1^{a_1+c_1} \cdots t_i^{a_i+c_i} \cdots t_i^{a_i+c_i} \cdots t_i^{a_k+c_k}$$

e portanto pertencem a $B_0^{(k)}$ pela condição (1) da definição de $B^{(k)}$;

2. Os outros termos serão divididos nos pares

$$t_1^{a_1+c_1} \cdots t_i^{a_i+c_i} \cdots t_i^{a_i+c_j} \cdots t_i^{a_k+c_k} + t_1^{a_1+c_1} \cdots t_i^{a_i+c_j} \cdots t_i^{a_i+c_i} \cdots t_i^{a_k+c_k}$$

em que $c_i < c_j$ e que portanto pertencem a $B_0^{(k)}$ pela condição (3) da definição de $B^{(k)}$.

Agora, caso

$$u(t_1, \ldots, t_k) = t_1^{a_1} t_2^{a_2} \cdots t_k^{a_k} \notin B_0^{(k)}$$

então os a_i são dois a dois distintos e $a_i < n$. Como $a_1, \ldots, a_k$ se comportam de forma simétrica, podemos assumir que $0 \leqslant a_1 < a_2 < \cdots < a_k \leqslant n-1$. A condição $a_1 + k + p > n$ vem automaticamente de $k + p > n$ e portanto pelo Lema 3.5.1 a prova está completa. □

Agora vamos mostrar que os polinômios $e_n(u_1, \ldots, u_n)$ com grau $n-1$ em relação à y estão no espaço vetorial B.

Lema 3.5.3. *Seja $e_n(x_1, \ldots, x_n)$ a linearização total do polinômio x^n (Definição 1.6.2) e sejam $w_1, \ldots, w_{k-1}$, $k \leqslant n$, monômios em x, y que dependem essencialmente de y, isto é, cujo grau em relação a y é pelo menos 1. Seja $\deg_y w_1 + \cdots + \deg_y w_{k-1} = n-1$. Então a soma*

$$e_n(w_1, \ldots, w_{k-1}, \underbrace{x, \ldots, x}_{n-k+1 \text{ vezes}})$$

pertence ao espaço vetorial B.

Demonstração. Vamos definir $p = n - k + 1$. Temos a seguinte igualdade:

$$e_n(w_1, \ldots, w_{k-1}, \underbrace{x, \ldots, x}_{p \text{ vezes}}) = p! \sum_j \sum_{\sum c_i = p} x^{c_1} w_{j_1} x^{c_2} w_{j_2} \cdots w_{j_{k-1}} x^{c_k}$$

na qual o somatório externo é sobre todas as permutações $j_1, \ldots, j_k$ de $1, 2, \ldots, k-1$ e o somatório interno é sobre todas as k-uplas $(c_1, \ldots, c_k)$ com soma igual a p. Vamos demonstrar que toda soma interna v_j pertence a B. Denotando cada w_j na forma $w_j = x^{b'_j} y \cdots y x^{b''_j}$, o somatório interno se torna:

$$\begin{aligned} v_j &= \sum_{\sum c_i = p} x^{c_1} w_{j_1} x^{c_2} w_{j_2} \cdots w_{j_{k-1}} x^{c_k} \\ &= \sum_{\sum c_i = p} x^{a_1+c_1} y \cdots y x^{a_2+c_2} y \cdots y x^{a_3+c_3} \cdots x^{a_{k-1}+c_{k-1}} y \cdots y x^{a_k+c_k} \end{aligned}$$

em que $a_1 = b'_{j_1}$, $a_2 = b''_{j_1} + b'_{j_2}$, $\ldots$, $a_{k-1} = b''_{j_{k-2}} + b'_{j_{k-1}}$, $a_k = b''_{j_{k-1}}$.

Se o grau de y em alguns w_j for maior que 1 então $w_j = x^{b'_j} y \cdots y x^{b''_j}$ pode conter mais alguns x e y entre os y mostrados. Note que esses termos entre os dois ys apresentados estão fixados dentro do somatório. Usando a bijeção $\varphi : K[t_1, \ldots, t_n] = A_0 \to A$ que definimos no começo da seção:

$$\varphi^{-1}(v_j) = v' \sum_{\sum c_i = p} t_1^{a_1+c_1} t_{m_2}^{a_2+c_2} \cdots t_{m_{k-1}}^{a_{k-1}+c_{k-1}} t_n^{a_k+c_k}$$

em que $v' = t_{q_1}^{b_1} \cdots t_{q_{n-k}}^{b_{n-k}}$, $b_i \geqslant 0$ e os índices $\{q_1, \ldots, q_{n-k}\}$ completam o conjunto $\{m_1 = 1, m_2, \ldots, m_{k-1}, m_k = n\}$ para formar $\{1, \ldots, n\}$. Assim

$$\varphi^{-1}(v_j) = v'(t_{q_1}, \ldots, t_{q_k}) h_{k,p}(t_{m_1}, \ldots, t_{m_k}) u(t_{m_1}, \ldots, t_{m_k}).$$

Como $k + p = n + 1 > n$, pelo Lema 3.5.2, $h_{k,p}(t_1, \ldots, t_k) u(t_1, \ldots, t_k) \in B_0^{(k)}$. Como os conjuntos $\{q_1, \ldots, q_{n-k}\}$ e $\{m_1 = 1, m_2, \ldots, m_{k-1}, m_k = n\}$ são disjuntos então

$$\varphi^{-1}(v_j) = v' h_{k,p} u \in B_0$$

e assim $v_j \in B$ e o lema está provado. □

Note que para provarmos o teorema falta apenas permitir expoentes > 1 para os termos x dentro do e_n no lema anterior. Para tanto, vamos recordar que o operador linear δ é uma derivação se satisfaz $\delta(uv) = \delta(u)v + u\delta(v)$ para quaisquer $u, v \in R$.

Além disso, se $\delta_0 : X \to K^+\langle X \rangle$ é uma aplicação qualquer, existe uma única derivação δ de $K^+\langle X \rangle$ que estende δ_0.

Proposição 3.5.1. *Seja C o espaço vetorial gerado por todos os monômios da forma*

$$x^{\sigma(0)} y x^{\sigma(1)} y \cdots x^{\sigma(n-2)} y x^{\sigma(n-1)}$$

em que $\sigma \in S_n$ e S_n age sobre o conjunto $\{0, 1, \ldots, n-1\}$, e seja $J = \langle x^n \rangle^T$. Então $C \cap J \subset B$.

Demonstração. Pelo Corolário 3.3.1, J é gerado como espaço vetorial por todos os polinômios do tipo $e_n(u_1, \ldots, u_n)$ de (3.4). Como estamos interessados apenas na intersecção $C \cap J$, podemos considerar apenas os $e_n(u_1, \ldots, u_n)$ que pertencem ao espaço vetorial A, isto é, tais que u_1, $\ldots$, u_n são monômios em x e y com grau total $n-1$ em relação à y. Para cada inteiro positivo a definimos uma derivação δ_a de $K^+\langle x, y \rangle$ da seguinte forma:

$$\delta_a(x) = x^a, \delta_a(y) = 0.$$

Note que $\delta_a(A) \subseteq A$ pois δ_a não altera o grau de y quando aplicado em um polinômio. Como $\delta_a(x^c) = c x^{c+a-1}$ e $a \geqslant 1$ podemos verificar que δ_a envia os polinômios dos tipos (1),

(2) e (3) da definição de B em combinações lineares de polinômios dos mesmos tipos e portanto $\delta_a(B) \subseteq B$. Por fim,

$$\delta_a(e_n(u_1, \ldots, u_n)) = \sum_{j=1}^{n} e_n(u_1, \ldots, \delta_a(u_j), \ldots, u_n)$$

e então $\delta_a(J) \subseteq J$. Os elementos $e_n(u_1, \ldots, u_n)$ que devemos considerar são os da forma

$$e_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_p})$$

em que $w_1, \ldots, w_k$ são monômios que dependem essencialmente de y, $p = n-k+1$ e $k \leqslant n$. O elemento $\delta_a(w_j)$ é uma combinação linear de monômios todos dependendo essencialmente de y e $\delta_a(x^c) = cx^{c+a-1}$. Como $c \geqslant 1$ e $a \geqslant 1$, então $\delta_a(e_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_p}))$ é uma combinação linear de elementos da mesma forma.

Pelo Lema 3.5.3

$$e_n(w_1, \ldots, w_{k-1}, \underbrace{x, \ldots, x}_{n-k+1 \text{ vezes}}) \in B.$$

Portanto

$$\begin{aligned}\delta_a(e_n(w_1, \ldots, w_{k-1}, x, \ldots, x)) = &\sum_{j=1}^{k-1} e_n(w_1, \ldots, \delta_a(w_j), \ldots, w_{k-1}, x, \ldots, x) \\ &+ pe_n(w_1, \ldots, w_{k-1}, x^a, \ldots, x) \in B.\end{aligned}$$

Todo $e_n(w_1, \ldots, \delta_a(w_j), \ldots, w_{k-1}, x, \ldots, x)$ pertence a B, logo

$$e_n(w_1, \ldots, w_{k-1}, x^a, x, \ldots, x) \in B$$

para todo a inteiro positivo. Aplicando δ_b no último polinômio

$$\begin{aligned}\delta_b(e_n(w_1, \ldots, w_{k-1}, x^a, \ldots, x)) = &\sum_{j=1}^{k-1} e_n(w_1, \ldots, \delta_b(w_j), \ldots, w_{k-1}, x^a, x, \ldots, x) \\ &+ e_n(w_1, \ldots, w_{k-1}, x^{a+b-1}, x, \ldots, x) \\ &+ (p-1)e_n(w_1, \ldots, w_{k-1}, x^a, x^b, x, \ldots, x) \in B.\end{aligned}$$

Novamente observando que todos elementos $e_n(w_1, \ldots, \delta_b(w_j), \ldots, w_{k-1}, x^a, x, \ldots, x)$ e $e_n(w_1, \ldots, w_{k-1}, x^{a+b-1}, x, \ldots, x)$ pertencem a B, temos que

$$e_n(w_1, \ldots, w_{k-1}, x^a, x^b, x, \ldots, x) \in B.$$

Continuando esse processo obteremos no final

$$e_n(w_1, \ldots, w_{k-1}, x^{a_1}, x^{a_2}, \ldots, x^{a_p}) \in B$$

para quaisquer a_1, a_2, …, a_p positivos. Concluímos então que $A \cap J \subseteq B$ e em particular que $C \cap J \subseteq B$. □

Teorema 3.5.1. *O grau de nilpotência no teorema de Dubnov–Ivanov–Nagata–Higman satisfaz a desigualdade*

$$d(n) \geqslant \frac{n(n+1)}{2}.$$

Demonstração. O monômio $u = yxyx^2 \cdots x^{n-2}yx^{n-1}$ em (3.8) tem grau total

$$d = \frac{n(n+1)}{2} - 1.$$

É suficiente mostrar que u não pertence ao T-ideal de $K^+\langle x, y\rangle$ gerado por x^n. Claramente, $u \in C \subset A$ e $u \notin B$, então pela Proposição 3.5.1 temos que $u \notin J = \langle x^n \rangle^T$. □

3.6 Demostração de Nagata

Apesar de a demostração de Nagata obter uma cota superior muito pior que a obtida por Higman, ela é extremamente instrutiva ao mostrar uma abordagem do problema utilizando a teoria de representações do grupo simétrico. Ao contrário das demonstrações anteriores que tentam obter o monômio multilinear $x_1x_2 \cdots x_d$ diretamente da identidade $x^n = 0$, Nagata usou o fato da álgebra de grupo KS_t ser completamente redutível para K com característica 0, isto é, que é igual à soma dos ideais à esquerda irredutíveis, para verificar que é suficiente obter os polinômios do tipo $\sum_{\sigma,\tau} \operatorname{sgn}(\tau) x_{\sigma\tau(1)}x_{\sigma\tau(2)} \cdots x_{\sigma\tau(d)}$ em que σ e τ percorrem todas as permutações que preservam respectivamente as linhas e as colunas de um certo diagrama de Young.

Vamos começar a demonstração pela parte da teoria das representações do grupo simétrico. Para simplificar um pouco a notação, denotaremos KS_t por D_t. Seja α uma tabela de Young para as letras $1, \ldots, t$, em que t é um número natural e denote por R_α e C_α os subgrupos de S_t que preservam respectivamente as linhas e as colunas de α. Defina também os elementos $R_\alpha^* = \sum_{\sigma \in R_\alpha} \sigma$ e $C_\alpha^* = \sum_{\tau \in C_\alpha} \operatorname{sgn}(\tau)\tau$ de D_t. Sabemos pelo Corolário 1.8.1 que

$$D_t = \sum_\alpha D_t \sum_{\substack{\sigma \in R_\alpha \\ \tau \in C_\alpha}} (\operatorname{sgn}(\tau)\sigma\tau) = \sum_\alpha D_t R_\alpha^* C_\alpha^*. \tag{3.14}$$

Seja g um número inteiro positivo. Definimos os dois ideais a seguir:

(1) Para um subconjunto de g letras $i_1, i_2, \ldots, i_g$ de $1, \ldots, t$ tal que $i_1 < i_2 < \cdots < i_g$, seja $S(i_1, i_2, \ldots, i_g)$ o subgrupo simétrico nas letras $i_1, \ldots, i_g$ (ou seja, o subgrupo das permutações que preservam as outras letras) e denote $S^*(i_1, i_2, \ldots, i_g) = \sum_{\sigma \in S(i_1,\ldots,i_g)} \sigma$. Definimos o ideal à esquerda $M_1 = \sum_{(i_1,\ldots,i_g)} D_t S^*(i_1, i_2, \ldots, i_g)$.

(2) Para um subconjunto de g letras $j_1, j_2, \ldots, j_g$ de $1, \ldots, t$ tal que $j_1 < j_1+1 < j_2 < j_2+1 < \cdots < j_g < j_g+1 \leqslant t$, seja $A(j_1, j_2, \ldots, j_g)$ o subgrupo das permutações $\sigma \in S_t$ tais que:

a) σ permuta apenas $j_1, j_1+1, j_2, j_2+1, \ldots, j_g, j_g+1$; e

b) σ permuta $\{j_1, j_2, \cdots, j_g\}$ entre si e $\sigma(j_k+1) = \sigma(j_k)+1$ para todo $k = 1, \ldots, g$.

Ou seja, σ permuta g blocos disjuntos de 2 letras consecutivas, preservando as outras letras. Denote $A^*(j_1, j_2, \ldots, j_g) = \sum_{\sigma \in A(j_1 \ldots, j_g)} \sigma$. Por fim, definimos o ideal à esquerda $M_2 = \sum_{(j_1, \ldots, j_g)} D_t A^*(j_1, j_2, \ldots, j_g)$.

Lema 3.6.1. *Se $t \geqslant g^3 - 2g^2 + 2g$, então $M_1 + M_2 = D_t$.*

Demonstração. De (3.14), basta mostrarmos que para cada tabela de Young α, o ideal à esquerda $D_t R^*_\alpha C^*_\alpha$ está contido em M_1 ou em M_2.

Como $\sigma^{-1} R^*(i_1, \ldots, i_g)\sigma = R^*(\sigma(i_1), \ldots, \sigma(i_g))$ para todo $\sigma \in S_t$, temos que M_1 é um ideal bilateral. Se α for uma tabela de Young com pelo menos uma linha com pelo menos g elementos temos que $R^*_\alpha \in M_1$ e portanto $D_t R^*_\alpha C^*_\alpha \in M_1$.

Caso contrário α tem menos que g colunas. Seja B o conjunto de letras que estão na primeira coluna de α, e defina os conjuntos $B' = \{s; s \in B, s+1 \in B\}$ e $B'' = \{s; s \in B, s \neq t, s+1 \notin B\}$. Como α tem no máximo $g-1$ colunas e como $(g-1)(g^2-g+1) = g^3 - 2g^2 + 2g - 1$, a primeira coluna terá pelo menos $g^2 - g + 2$ elementos. Temos as seguintes possibilidades:

1. Se B' tem pelo menos $2g-1$ elementos, podemos escolher $j_1, j_2, \ldots, j_g \in B'$ tais que $j_1 < j_1+1 < j_2 < j_2+1 < \cdots < j_g < j_g+1 \leqslant t$. Como $A(j_1, j_2, \ldots, j_g) \subset C_\alpha$, temos que $C^*_\alpha \in M_2$ e portanto $D_t R^*_\alpha C^*_\alpha \in M_2$.

2. Caso contrário, o número de elementos de B'' será no mínimo $(g^2-g+2)-(2g-2)-1 = g^2 - 3g + 3 = (g-1)(g-2)+1$. Para cada $s \in B''$ considere as letras $s+1$. Pela definição de B'' elas estão em uma das $g-2$ outras colunas. Logo existe pelo menos uma coluna que contém pelo menos g desses elementos, ou seja, conseguimos escolher $j_1, j_2, \ldots, j_g \in B''$ tais que $j_1+1, j_2+1, \ldots, j_g+1$ estão na mesma coluna. Logo $A(j_1, j_2, \ldots, j_g) \subset C_\alpha$, e portanto $C^*_\alpha \in M_2$ e $D_t R^*_\alpha C^*_\alpha \in M_2$.

□

Agora vamos deduzir polinômios a partir de $x^n = 0$. Seja R uma álgebra associativa sobre o corpo K tal que $x^n = 0$ para todo $x \in R$. Para $y_1, \ldots, y_t \in R$ e

$X \in D_t$ tal que $X = \sum_i a_i\sigma_i$, $a_i \in K$ e $\sigma_i \in S_t$, denotaremos por $X(y_1 \cdots y_t)$ a soma $\sum_i a_i y_{\sigma_i(1)} \cdots y_{\sigma_i(t)}$. Ainda, denote por (K, R) a álgebra obtida adicionando uma unidade à álgebra R.

Primeiramente, aplicando a linearização parcial na identidade $x^n = 0$ obtemos:

$$f(x, y) = x^{n-1}y + x^{n-2}yx + \cdots + xyx^{n-2} + yx^{n-1} = 0.$$

Logo

$$f(x, y)x^{n-1} = x^{n-1}yx^{n-1} + x^{n-2}yx^n + \cdots + xyx^{2n-3} + yx^{2n-2} = 0.$$

Portanto

$$x^{n-1}yx^{n-1} = 0. \tag{3.15}$$

Nos dois lemas a seguir denotaremos por $\langle a \rangle$ o ideal bilateral de (K, R) gerado por a.

Lema 3.6.2. *Seja m o menor inteiro tal que $m > n/2$ e tome um $u \in R$. Então, para qualquer $z \in (K, R)$, $\overline{z} = uz + \langle u^2 \rangle \in (K, R)/\langle u^2 \rangle$ é tal que $\overline{z}^m = 0$.*

Demonstração. É suficiente mostrar que para qualquer $z \in R$, $(uz)^{m-1}u \equiv 0 \pmod{u^2}$.

A partir da linearização total de $x^n = 0$ obtemos $e_n(y_1, \ldots, y_n) = 0$. Tome $y_1 = \cdots = y_{n+1-m} = u$ e $y_{n+2-m} = \cdots = y_n = z$, e considere $e_n(y_1, \ldots, y_n) = 0$ para n ímpar e $e_n(y_1, \ldots, y_n)u = 0$ para n par. O único termo de cada soma que não terá dois u consecutivos será $(uz)^{m-1}u$.

Portanto, para n ímpar temos $(uz)^{m-1}u \equiv e_n(y_1, \ldots, y_n) = 0 \pmod{u^2}$ e para n par temos $(uz)^{m-1}u \equiv e_n(y_1, \ldots, y_n)u = 0 \pmod{u^2}$. □

Lema 3.6.3. *Seja m o menor inteiro tal que $m > n/2$. Defina r como o menor inteiro tal que $n - 1 \leqslant 2^r$ e suponha que exista $d(m)$. Então para qualquer $u \in R$, $\langle u \rangle^{g(n)} = 0$, em que $g(n) = 2d(m)^r$ se $n - 1 = 2^r$ ou $g(n) = d(m)^r$ se $n - 1 < 2^r$.*

Demonstração. Pelo Lema 3.6.2 e por $d(m)$ existir temos $\prod_{i=1}^{d(m)} \overline{z_i} = 0$, isto é, $\prod_{i=1}^{d(m)} uz_i \subset \langle u^2 \rangle$. Portanto $\langle u \rangle^{d(m)} \subset \langle u^2 \rangle$. Logo $\langle u \rangle^{d(m)^r} \subset \langle u^2 \rangle^{d(m)^{r-1}} \subset \cdots \subset \langle u^{2^r} \rangle$. Se $n - 1 < 2^r$, o resultado segue diretamente. Caso $n - 1 = 2^r$, usando (3.15) obtemos $\langle u \rangle^{2d(m)^r} \subset \langle u^{n-1} \rangle^2 = 0$. □

Lema 3.6.4. *Com o mesmo $g(n)$ do lema anterior e assumindo a existência de $d(m)$, tome $t \geqslant g(n)$ $y_1, \ldots, y_t \in R$ e $1 \leqslant i_1 < i_2 < \cdots < i_{g(n)} \leqslant t$ inteiros. Então*

$$S^*(i_1, \ldots, i_{g(n)})(y_1 \cdots y_t) = 0.$$

Demonstração. Pelo Lema 3.6.3 temos que $w_0uw_1uw_2\cdots uw_{g(n)} = 0$ em que $w_i \in (K, R)$ e portanto usando as substituições $w_0 = y_1\cdots y_{i_1-1}$, $w_1 = y_{i_1+1}\cdots y_{i_2-1}$, $\ldots$, $w_{g(n)} = y_{i_{g(n)}+1}\cdots y_t$ podemos obter $z_1z_2\cdots z_t = 0$ em que $z_i = u$ se $i \in \{i_1, \ldots, i_{g(n)}\}$ e $z_i = y_i$ caso contrário.

Aplicando a linearização total em u obtemos a identidade desejada. □

Corolário 3.6.1. *Com o mesmo $g(n)$ do lema anterior e assumindo a existência de $d(m)$, tome $t \geqslant 2g(n)$ $y_1, \ldots, y_t \in R$ e $j_1, \ldots, j_{g(n)}$ de forma que $A(j_1, \ldots, j_{g(n)})$ pode ser definida. Então*

$$A^*(j_1, \ldots, j_{g(n)})(y_1\cdots y_t) = 0.$$

Demonstração. No Lema 3.6.4, usando $t - g(n)$ ao invés de t, substituindo y_{i_k} por $y_{i_k}y'_{i_k}$ e renomeando os y_k obtemos a identidade desejada. □

Agora vamos demonstrar o teorema.

Teorema 3.6.1. *Seja R uma álgebra sobre o corpo K de característica 0. Se $u^n = 0$ para todo $u \in R$, então existe um inteiro positivo $f(n)$ dependendo apenas de n tal que $R^{f(n)} = 0$.*

Demonstração. Vamos provar por indução. Como podemos verificar na Proposição 3.2.1 $f(2) = 3$. Agora tome m como o menor inteiro tal que $m > n/2$ e suponha que $f(m)$ exista (note que se $n \geqslant 3$ então $m < n$).

Seja $g = g(n)$ obtido no Lema 3.6.4 e faça $t = f(n) = g^3 - 2g^2 + 2g$. Provaremos que $R^t = 0$. Para tanto, podemos supor sem perda de generalidade que $R = F/P$, em que F é a álgebra sobre K livremente gerada por uma quantidade suficiente de geradores x_λ e P o ideal bilateral de F gerado pelas n-ésimas potências de elementos de F. Sejam $x_1, \ldots, x_t$ elementos de $\{x_\lambda\}$, dois a dois distintos. Então P é invariante à esquerda pela ação de D_t e então $M = \{X | X \in D_t, X(x_1\cdots x_t) \in P\}$ é um ideal à esquerda de D_t. Pelo Lema 3.6.4 e pelo Corolário 3.6.1, todos os $S^*(i_1, \ldots, i_g)$ e $A^*(j_1, \ldots, j_g)$ estão em M. Então pelo Lema 3.6.2 temos $M = D_t$ e em particular $1 \in M$, o que implica $x_1\cdots x_t \in P$ e o portanto $R^t = 0$. □

3.7 A cota superior $d(n) \leqslant n^2$

Nesta seção iremos apresentar a demonstração da cota superior $d(n) \leqslant n^2$. Vamos nos basear no artigo de Razmyzlov (9) em que foi provado que todas as identidades polinomiais com traço da álgebra de matrizes sobre um corpo de característica 0 são consequências do polinômio de Cayley-Hamilton, mas vamos nos ater apenas aos elementos necessários ao nosso resultado.

De uma forma similar à demonstração de Nagata, vamos utilizar a teoria de representações e o fato que KS_n é completamente redutível para obter o monômio multilinear $x_1 \cdots x_d$ como combinação de outros polinômios e vamos verificar que eles são consequência de x^n. Porém, na demostração de Nagata, a permutação $\sigma \in S_n$ é associada ao monômio multilinear $x_{\sigma(1)} \cdots x_{\sigma(n)}$, e a ação de S_n à direita equivale a uma permutação dos termos de cada monômio. Esta construção faz com que um T-ideal seja apenas invariante sob a ação de S_n à esquerda (o que equivale a uma renomeação das variáveis), e então os polinômios usados são os geradores dos ideais à esquerda minimais de KS_n. Após isso, encontramos uma maneira de obter os polinômios a partir de x^n e a solução foi concluída.

Nesta demonstração a associação será outra: os monômios multilineares usuais (ordinários) serão associados às permutações de S_{n+1} que consistem de apenas um ciclo, e serão considerados como um subconjunto de monômios multilineares generalizados (com traço). A construção fará com que um ideal verbal seja invariante sob a ação de S_{n+1} de ambos os lados. Nesse caso, os polinômios usados serão os geradores dos ideais bilaterais minimais. Além disso, essa construção terá a propriedade que um ideal verbal associado a um diagrama de Young é consequência de qualquer ideal verbal associado a um subdiagrama desse diagrama, o que permitirá que nós nos concentremos apenas em alguns diagramas, mais especificamente o diagrama com 1 linha com $n+1$ elementos e o diagrama com 1 coluna com $n+1$ elementos. Isso mostrará que $x_1 \cdots x_{n^2}$ é combinação de alguns polinômios generalizados, mas com mais um argumento obteremos uma combinação de alguns polinômios ordinários que são consequências de x^n.

Vamos começar definindo a álgebra dos polinômios generalizados.

Tome as variáveis x_1, x_2, ..., e defina uma função traço tr() formalmente. Primeiramente, vamos construir uma álgebra auxiliar, que denotaremos por G_0, de forma indutiva:

(1) Toda palavra de comprimento finito nas variáveis x_1, x_2, ..., está em G_0

(2) Se A e B são elementos de G_0, então AB também é

(3) Se a é uma palavra não vazia, e A e B são elementos de G_0, então $\mathrm{tr}(AaB)$, $\mathrm{tr}(aB)$ e $\mathrm{tr}(Aa)$ também são elementos de G_0

O item (2) define uma multiplicação por justaposição e transforma G_0 em um semigrupo. Note que expressões do tipo $\mathrm{tr}(\mathrm{tr}(\cdots))$ não são elementos de G_0.

Defina agora G como o semigrupo obtido de G_0 considerando as seguintes congruências:

$$\mathrm{tr}(A)B = B\,\mathrm{tr}(A) \tag{3.16}$$

$$\operatorname{tr}(AB) = \operatorname{tr}(BA) \tag{3.17}$$

$$\operatorname{tr}(A \operatorname{tr}(B)) = \operatorname{tr}(A) \operatorname{tr}(B) \tag{3.18}$$

em que A, $B \in G_0$. Note que, conforme essa definição, G é um semigrupo e é gerado pelos elementos da forma a e $\operatorname{tr}(b)$, em que a e b são palavras não vazias, e que todo elemento de G tem a forma

$$a_0 \operatorname{tr}(a_1) \operatorname{tr}(a_2) \cdots \operatorname{tr}(a_t)$$

em que os a_i são palavras e $a_1, \ldots, a_t$ são não vazias. Nesta forma a representação não é única, mas podemos tomar o elemento tal que a palavra $a_0 a_1 \cdots a_t$ é maximal em relação à ordenação lexicográfica para obtermos uma representação única. Chamaremos os elementos de G de monômios generalizados.

Agora a álgebra de polinômios generalizados sobre um corpo K é a álgebra sobre K do semigrupo G, que denotaremos por $\mathscr{G}$. Definimos o grau de um monômio em relação à variável x_i como o número de vezes que ele aparece na representação do monômio. Então podemos definir o multigrau de um monômio sobre as variáveis $x_1, \ldots, x_l$ como a l-upla $(r_1, \ldots, r_l)$ em que r_i é o grau desse monômio em relação à variável x_i. Um polinômio generalizado é dito homogêneo de multigrau $(r_1, \ldots, r_l)$ quando é uma combinação linear de monômios generalizados com esse mesmo multigrau. Por exemplo,

$$x_1 x_2 + x_2 x_1 + x_2 \operatorname{tr}(x_1) + \frac{1}{2} \operatorname{tr}(x_1 x_2)$$

é um polinômio generalizado homogêneo de multigrau $(1, 1)$ mas $\operatorname{tr}(x_1) + \operatorname{tr}(x_2)$ não é homogêneo. Um polinômio generalizado homogêneo $f(x_1, \ldots, x_l)$ é dito multilinear de grau l, quando é de multigrau $(1, \ldots, 1)$ (com l uns).

Também definimos a ação da função tr() sobre um polinômio

$$\operatorname{tr}(\sum \alpha_{a_0, a_1, \ldots, a_t} a_0 \operatorname{tr}(a_1) \cdots \operatorname{tr}(a_t)) = \sum \alpha_{a_0, a_1, \ldots, a_t} \operatorname{tr}(a_0) \operatorname{tr}(a_1) \cdots \operatorname{tr}(a_t))$$

quando o lado direito está bem definido, isto é, quando toda a_0 é não vazia. Para todo polinômio generalizado $g(x_1, \ldots, x_l) \in \mathscr{G}$ e quaisquer matrizes $B_1, \ldots, B_l \in M_n(K)$ podemos construir a expressão $g(B_1, \ldots, B_l)$ em que $\operatorname{tr}(B)$ é interpretada como a matriz escalar cujos elementos na diagonal são iguais ao traço usual da matriz B. Note que as propriedades do traço formal que citamos também valem para esta interpretação.

Definição 3.7.1. *Um polinômio generalizado $g(x_1, \ldots, x_l) \in \mathscr{G}$ é uma identidade com traço da álgebra das matrizes $M_n(K)$ se $g(B_1, \ldots, B_l) = 0$ para quaisquer matrizes $B_1, \ldots, B_l \in M_n(K)$.*

Faremos agora algumas definições importantes:

Definição 3.7.2. *Um ideal bilateral I da álgebra $\mathscr{G}$ é chamado de ideal verbal se para quaisquer polinômios generalizados $h_1, \ldots, h_l \in \mathscr{G}$ da forma*

$$\sum \alpha_{a_0,a_1,\ldots,a_t} a_0 \operatorname{tr}(a_1) \operatorname{tr}(a_2) \cdots \operatorname{tr}(a_t)$$

em que a_0 são palavras não vazias e para qualquer $g(x_1, \ldots, x_l) \in I$ temos que $g(h_1, \ldots, h_l) \in I$.

Definição 3.7.3. *Um polinômio generalizado g é consequência dos polinômios generalizados $g_1, \ldots, g_l$ se o ideal verbal gerado por $g_1, \ldots, g_l$ (isto é, o menor ideal verbal contendo $g_1, \ldots, g_l$) também contém g. Dois conjuntos de polinômios generalizados são equivalentes quando os ideais verbais gerados pelos dois conjuntos coincidem.*

Note que de forma similar ao processo de linearização dos polinômios ordinários podemos obter que todo ideal verbal é gerado por seus polinômios generalizados multilineares. Denotaremos por T_l o conjunto dos polinômios generalizados multilineares nas variáveis $x_1, \ldots, x_l$.

Lema 3.7.1. *A dimensão do espaço vetorial T_l é $(l+1)!$.*

Demonstração. Pela definição da álgebra dos polinômios generalizados, basta provar que o semigrupo G contém $(l+1)!$ monômios generalizados multilineares nas variáveis $x_1, \ldots, x_l$. Como observamos anteriormente todo elemento de $G \cap T_l$ pode ser escrito de forma única

$$a_0 \operatorname{tr}(a_1) \operatorname{tr}(a_2) \cdots \operatorname{tr}(a_t)$$

em que os a_i são palavras, $a_1, \ldots, a_t$ são não vazias e a palavra multilinear $a_0 a_1 \cdots a_t$ é maximal em relação à ordenação lexicográfica. Vamos provar por indução no número de variáveis. Para uma variável x_0 temos os $2! = 2$ monômios x_0 e $\operatorname{tr}(x_0)$. Se temos l variáveis, vamos dividir em dois casos:

(i) Se a_0 é não vazio, seja $a_0 = x_i a_0'$ em que x_i é a primeira letra de a_0. Por indução o número de monômios da forma $x_i a_0' \operatorname{tr}(a_1) \operatorname{tr}(a_2) \cdots \operatorname{tr}(a_t)$, em que fixamos x_i é igual ao número de monômios generalizados multilineares em $l-1$ variáveis, então $l!$ e portanto o número de monômios neste caso é igual a $l(l!)$.

(ii) Se a_0 é vazio, então necessariamente $a_1 = x_l a_l'$ pois por (3.17) cada $a_1, \ldots, a_t$ pode ser permutado ciclicamente e por (3.16) podemos permutar $a_1, \ldots, a_t$ entre si. Então o número de monômios generalizados multilineares neste caso será igual ao número de monômios da forma $a_l' \operatorname{tr}(a_2) \cdots \operatorname{tr}(a_t)$, que por indução é $l!$.

Portanto o número total de monômios generalizados multilineares é $(l+1)!$. □

Agora vamos definir a álgebra $\widetilde{\mathscr{G}}$. Seja K um corpo e $K(\gamma)$ o corpo de frações do anel de polinômios $K[\gamma]$ em uma variável γ. Denotaremos por $\widetilde{\mathscr{G}}$ a álgebra quociente da álgebra $\mathscr{G}(\gamma)$ de polinômios generalizados sobre o corpo $K(\gamma)$ a partir das relações a seguir:

$$x_i a x_i = \frac{x_i^2}{\gamma}\operatorname{tr}(a) \tag{3.19}$$

$$\operatorname{tr}(x_i a)x_i = \frac{x_i^2}{\gamma}a \tag{3.20}$$

$$[x_i^2, x_j] = 0, \quad \operatorname{tr}(x_i^2 a) = x_i^2 \operatorname{tr}(a), \quad \operatorname{tr}(x_i^2) = \gamma x_i^2 \tag{3.21}$$

$$w = 0 \tag{3.22}$$

em que $i, j = 1, 2, \ldots$, a é uma palavra qualquer e w é um polinômio generalizado com grau maior que 2 em relação à alguma variável. A estrutura da álgebra $\widetilde{\mathscr{G}}$ é descrita no lema a seguir.

Lema 3.7.2. *(a) A álgebra $\widetilde{\mathscr{G}}$ é gerada como um espaço vetorial pelos monômios generalizados de grau menor que 3 em relação a cada variável x_i.*

(b) Os conjuntos de polinômios multilineares das álgebras $\mathscr{G}(\gamma)$ e $\widetilde{\mathscr{G}}$ são isomorfos como espaços vetoriais.

(c) Todo polinômio homogêneo $f(x_{i_1}, \ldots, x_{i_s}, x_{j_1}, \ldots, x_{j_t})$ de grau 2 em relação às variáveis $x_{i_1}, \ldots, x_{i_s}$ e de grau 1 em relação às variáveis $x_{j_1}, \ldots, x_{j_t}$ podem ser representadas na forma

$$f = \frac{x_{i_1}^2}{\gamma} \cdots \frac{x_{i_s}^2}{\gamma} g(x_{j_1}, \ldots, x_{j_t}) \tag{3.23}$$

em que g é um polinômio generalizado multilinear.

(d) A representação (3.23) é única no seguinte sentido: se

$$f = \prod_{k=1}^{s} \frac{x_{i_k}^2}{\gamma} g_1$$

é outra representação, então $g = g_1$ em $\mathscr{G}(\gamma)$.

Demonstração. O primeiro item é verdade por causa de (3.22), o segundo por causa que todas as relações (3.19) a (3.22) são de grau pelo menos 2 em alguma variável. O terceiro item pode ser obtido ao usar as relações (3.16) a (3.22). Por fim, para a unicidade, podemos verificar diretamente que a ordem das variáveis que usamos para reduzir o polinômio para

a forma (3.23) não altera o resultado (e para isto basta mostrar que para duas variáveis a ordem não importa). Por exemplo, por um lado:

$$ax_ibx_jcx_idx_je = \frac{x_i^2}{\gamma}adx_je\,\mathrm{tr}(bx_jc) = \frac{x_i^2}{\gamma}ad\,\mathrm{tr}(x_jcb)x_je = \frac{x_i^2}{\gamma}\frac{x_j^2}{\gamma}adcbe$$

e por outro lado:

$$ax_ibx_jcx_idx_je = \frac{x_j^2}{\gamma}ax_ibe\,\mathrm{tr}(cx_id) = \frac{x_j^2}{\gamma}a\,\mathrm{tr}(x_idc)x_ibe = \frac{x_i^2}{\gamma}\frac{x_j^2}{\gamma}adcbe.$$

□

Uma igualdade importante em $\widetilde{\mathscr{G}}$ pode ser obtida da seguinte forma: Sejam $a, h, h_1, h_2 \in \widetilde{\mathscr{G}}$, então de (3.19) e (3.16) temos:

$$x_iahx_i = \frac{x_i^2}{\gamma}\,\mathrm{tr}(ah) = \frac{x_i^2}{\gamma}\,\mathrm{tr}(ha) = x_ihax_i.$$

De (3.19), (3.16) e (3.17) temos:

$$\mathrm{tr}(h_1x_iah_2)x_i = \mathrm{tr}(x_iah_2h_1)x_i = \frac{x_i^2}{\gamma}ah_2h_1 = a\,\mathrm{tr}(x_ih_2h_1)x_i = \mathrm{tr}(h_1x_ih_2)ax_i.$$

Logo obtemos que para quaisquer f, g polinômios generalizados multilineares em $x_1, \ldots, x_l$

$$f|_{x_i=x_ia} \cdot g = f \cdot g|_{x_i=ax_i}$$

e consequentemente

$$f(x_1a_1, x_2a_2, \ldots, x_la_l)g(x_1, x_2, \ldots, x_l) = f(x_1, x_2, \ldots, x_l)g(a_1x_1, a_2x_2, \ldots, a_lx_l). \quad (3.24)$$

De forma análoga podemos provar que

$$f(a_1x_1, a_2x_2, \ldots, a_lx_l)g(x_1, x_2, \ldots, x_l) = f(x_1, x_2, \ldots, x_l)g(x_1a_1, x_2a_2, \ldots, x_la_l). \quad (3.25)$$

Vamos denotar por T_l e $T_l(\gamma)$ os espaços dos polinômios multilineares nas variáveis $x_1, \ldots, x_l$ em $\mathscr{G}$ e $\widetilde{\mathscr{G}}$. Suponha que f e g são os mesmos da Equação 3.23. Vamos definir a função π de forma que $\pi(f) = g$. Com essas definições vamos dar uma estrutura de álgebra ao conjunto T_l.

Lema 3.7.3. *Suponha que a operação $\circ$ é definida no conjunto T_l da seguinte maneira:*

$$f \circ h = \pi(f(x_1, \ldots, x_l) \cdot h|_{\substack{x_1=y_1x_1 \\ \cdots\cdots \\ x_l=y_lx_l}})|_{\substack{y_1=x_1 \\ \cdots\cdots \\ y_l=x_l}} = \pi(f|_{\substack{x_1=x_1y_1 \\ \cdots\cdots \\ x_l=x_ly_l}} \cdot h(x_1, \ldots, x_l))|_{\substack{y_1=x_1 \\ \cdots\cdots \\ y_l=x_l}} \quad (3.26)$$

em que f, $h \in T_l$ e $x_1, \ldots, x_l, y_1, \ldots, y_l$ são variáveis distintas. Então essa operação é bem definida, o conjunto de monômios generalizados $G \cap T_l$ forma um grupo com respeito

à operação $\circ$*, e o espaço vetorial* T_l *se torna a álgebra de grupo do grupo* $G \cap T_l$*. Além disso, os elementos*

$$D_i = x_i \prod_{j=1, j\neq i}^{l} \operatorname{tr}(x_j)$$

em que $i = 1, \ldots, l$*, são os geradores desse grupo, e o monômio generalizado* $e = \prod_{j=1}^{l} \operatorname{tr}(x_j)$ *é o seu elemento neutro.*

Demonstração. A segunda igualdade em (3.26) é verdadeira por causa de (3.24) e do item (d) do Lema 3.7.2. As partes (c) e (d) do mesmo lema garantem a validade da definição (3.26) em T_l. Para mostrarmos que $\circ$ é associativa, observe que, para $f, g, h \in T_l(\gamma)$:

$$\begin{aligned}
(f \circ g) \circ h &= \pi(f \cdot g|_{\substack{x_1=y_1x_1 \\ \cdots\cdots \\ x_l=y_lx_l}} \cdot h|_{\substack{x_1=z_1y_1 \\ \cdots\cdots \\ x_l=z_ly_l}})|_{\substack{z_1=x_1 \\ \cdots\cdots \\ z_l=x_l}} \\
&= \pi(f \cdot g|_{\substack{x_1=y_1 \\ \cdots\cdots \\ x_l=y_l}} \cdot h|_{\substack{x_1=z_1x_1y_1 \\ \cdots\cdots \\ x_l=z_lx_ly_l}})|_{\substack{z_1=x_1 \\ \cdots\cdots \\ z_l=x_l}} \\
&= \pi(f \cdot (g|_{\substack{x_1=y_1 \\ \cdots\cdots \\ x_l=y_l}} \cdot h|_{\substack{x_1=x_1y_1 \\ \cdots\cdots \\ x_l=x_ly_l}})|_{\substack{x_1=z_1x_1 \\ \cdots\cdots \\ x_l=z_lx_l}})|_{\substack{z_1=x_1 \\ \cdots\cdots \\ z_l=x_l}} \\
&= f \circ (g \circ h).
\end{aligned}$$

Utilizando (3.20) sucessivamente obtemos

$$\prod_{j=1}^{l} \operatorname{tr}(x_j) \circ f = \pi\left(\prod_{j=1}^{l} \operatorname{tr}(x_jy_j) \cdot f\right)|_{\substack{y_1=x_1 \\ \cdots\cdots \\ y_l=x_l}} = (f|_{\substack{x_1=y_1 \\ \cdots\cdots \\ x_l=y_l}})|_{\substack{y_1=x_1 \\ \cdots\cdots \\ y_l=x_l}} = f$$

e portanto $e = \prod_{j=1}^{l} \operatorname{tr}(x_j)$ é um elemento neutro pela esquerda. Analogamente podemos mostrar que e é um elemento neutro pela direita. De forma similar, obtemos

$$f \circ D_i = \pi(fy_ix_i)|_{y_1=x_i}. \tag{3.27}$$

Se $f = a_0 \prod_{j=1}^{t} \operatorname{tr}(a_j)$ é um monômio generalizado, então temos dois casos: $a_0 = a_0' x_i a_0''$ e $a_k = x_i a_k'$. Usando (3.19) e (3.20).

$$\left\{a_0 \prod_{j=1}^{t} \operatorname{tr}(a_j)\right\} \circ D_i = \begin{cases} a_0' \operatorname{tr}(x_i a_0'') \prod_{j=1}^{t} \operatorname{tr}(a_j) \\ a_0 x_i a_k' \prod_{j=1, j\neq k}^{t} \operatorname{tr}(a_j) \end{cases} \tag{3.28}$$

de onde obtemos que $G \cap T_l$ é invariante sob a multiplicação por D_i. Utilizando (3.28) podemos obter

$$D_i \circ D_i = e,$$

$$\left\{ g(x_1,\dots,x_k)\prod_{j=k+1}^{l}\operatorname{tr}(x_j)\right\}\circ D_{k+1} = g(x_1,\dots,x_k)x_{k+1}\prod_{j=k+2}^{l}\operatorname{tr}(x_j),$$

$$\begin{aligned}\left\{ g(x_1,\dots,x_k)\prod_{j=k+1}^{l}\operatorname{tr}(x_j)\right\}&\circ D_{k+1}\circ D_{k+2}\circ\cdots\circ D_{k+t}\circ D_{k+1}\\ &= g(x_1,\dots,x_k)\operatorname{tr}(x_{k+1}\cdots x_{k+t})\prod_{j=k+t+1}^{l}\operatorname{tr}(x_j),\end{aligned}$$

em que g é um monômio generalizado multilinear em x_1, …, x_k. Com isso obtemos que todo monômio generalizado em $G\cap T_l$ pode ser obtido a partir de e usando multiplicações por elementos D_i, e vice-versa. Logo $G\cap T_l$ é um grupo com os elementos D_i como geradores. Assim fica claro que T_l é a álgebra de grupo do grupo $G\cap T_l$ de monômios generalizados multilineares, e a operação $\circ$ está bem definida sobre T_l. □

Agora vamos finalmente construir o isomorfismo entre $G\cap T_l$ e S_{l+1}.

Lema 3.7.4. *O grupo $G\cap T_l$ é isomorfo ao grupo S_{l+1} através do isomorfismo*

$$\varphi(a_0\operatorname{tr}(a_1)\cdots\operatorname{tr}(a_t)) = (x_0a_0)(a_1)\cdots(a_t).$$

Demonstração. A função φ está bem definida pois os ciclos comutam entre si e também podemos permutar ciclicamente os elementos de cada a_1, …, a_t. Pelo Lema 3.7.1, φ é biunívoca. Então para provar o lema é suficiente provar que para todo $g\in G\cap T_l$

$$\varphi(g)\cdot\varphi(D_i) = \varphi(g\circ D_i),$$

mas como

$$(x_0a_0)(a_1)\cdots(a_t)\cdot(x_0x_i) = \begin{cases}(x_0a_0')(x_ia_0'')(a_1)\cdots(a_t), & \text{se } a_0 = a_0'x_ia_0''\\ (x_0a_0x_ia_k')(a_1)\cdots(a_{k-1})(a_{k+1})\cdots(a_t), & \text{se } a_k = x_ia_k',\end{cases}$$

comparando com (3.28) obtemos o que queríamos. □

Agora vamos relembrar os fatos da teoria das representações do grupo simétrico de que precisamos, que foram explorados na seção 1.8. Dizemos que um diagrama de Young é do tipo $(n_1,\dots,n_k)$ quando o número de caixas na i-ésima linha é igual a n_i, e $n_1\geqslant n_2\geqslant\cdots\geqslant n_k$. Uma tabela de Young é obtida ao preencher um diagrama de Young com os inteiros de 1 a $l+1 = n_1+\cdots+n_k$. Denotaremos por R_α e C_α os subgrupos do grupo simétrico S_{l+1} que preservam respectivamente as linhas e as colunas do diagrama de Young α.

Proposição 3.7.1. *Existe uma bijeção entre o conjunto dos diagramas de Young D do tipo $(n_1,\dots,n_k)$ em que $n_1+\cdots+n_k = l+1$ e o conjunto dos ideais bilaterais simples*

da álgebra de grupo KS_{l+1}. O ideal correspondente ao diagrama D é gerado como um ideal bilateral pelo elemento $e(\alpha) = R^*_\alpha \circ C^*_\alpha$ em que $R^*_\alpha = \sum_{\sigma \in R_\alpha} \sigma$ e $C^*_\alpha = \sum_{\tau \in C_\alpha} \operatorname{sgn}(\tau)\tau$ para algum diagrama α construído sobre D. Uma permutação $s \in S_{l+1}$ pode ser representada na forma $s = \sigma\tau$ em que $\sigma \in R_\alpha$ e $\tau \in C_\alpha$ se e somente se os elementos na mesma linha do diagrama α estão em colunas diferentes do diagrama αs, e essa representação é única. Para todo $x \in KS_{l+1}$ temos que $R^*_\alpha \circ x \circ C^*_\alpha = uR^*_\alpha C^*_\alpha$, em que u é um número que depende de x.

Lema 3.7.5. *Suponha que V é um ideal verbal gerado por um conjunto de polinômios generalizados de grau l, formando um ideal bilateral de T_l em relação à operação $\circ$. Suponha que $f \in T_l$ gera o ideal bilateral $V \cap T_l$. Então $V \cap T_{l+k}$ é um ideal bilateral de T_{l+k} para todo $k \geqslant 0$ e*

$$f(x_1, \ldots, x_l) \prod_{i=1}^{k} \operatorname{tr}(x_{l+i})$$

gera esse ideal bilateral.

Demonstração. Primeiramente vamos provar que $V \cap T_{l+k}$ é um ideal bilateral. É suficiente verificar que $V \cap T_{l+k}$ é estável em relação à multiplicação pelos geradores D_i. Note que

$$bf(a_1, \ldots, a_l) = f(a_1, \ldots, a_l)b + \sum_{i+1}^{l} f(a_1, \ldots, a_i b - ba_i, \ldots, a_l),$$

logo podemos afirmar que $V \cap T_{l+k}$ é gerado por elementos do tipo

$$g_1 = g(a_1, \ldots, a_l)a_{l+1} \prod_{j=1}^{r} \operatorname{tr}(b_j)$$

em que $g(x_1, \ldots, x_l) \in V \cap T_l$ e a_i e b_i são palavras. Usando (3.27), (3.24), (3.25) e (3.28) obtemos

$$\begin{aligned} g_1 \circ D_i &= \pi(g(a_1, \ldots, a_l)a_{l+1} \prod_{j=1}^{r} \operatorname{tr}(b_j)y_i x_i)|_{y_i = x_i} \\ &= \begin{cases} g(a_1, \ldots, a_l)a_{l+1}x_i b'_s \prod_{j=1}^{r} \operatorname{tr}(b_j), & \text{se } b_s = x_i b'_s \\ g(a_1, \ldots, a_l)a'_{l+1} \operatorname{tr}(x_i a''_{l+1}) \prod_{j=1}^{r} \operatorname{tr}(b_j), & \text{se } a_{l+1} = a'_{l+1}x_i a''_{l+1} \\ (g(x_1, \ldots, x_l) \circ D_s)|_{\substack{x_j = a_j (j \neq s) \\ x_s = a_{l+1}x_i a''_s}} a'_s \prod_{j=1}^{r} \operatorname{tr}(b_j), & \text{se } s \leqslant l, a_s = a'_s x_i a''_s \end{cases} \end{aligned}$$

o que implica que $V \cap T_{l+k}$ é um ideal à direita. De forma similar podemos mostrar que $V \cap T_{l+k}$ é um ideal à esquerda. Considerando o que foi dito acima é suficiente mostrar que

$$g_1 = g(a_1, \ldots, a_l) \prod_{j=1}^{r} \operatorname{tr}(x_{i_j})$$

em que $g(x_1,\dots,x_l)\in V\cap T_l$ pertence ao ideal bilateral gerado por

$$f_1 = f(x_1,\dots,x_l)\prod_{j=1}^{k}\operatorname{tr}(x_{l+j}).$$

Sabemos que, se $\sigma=(y_{11}\cdots y_{1r_1})(y_{21}\cdots y_{2r_2})\cdots(y_{m1}\cdots y_{mr_m})$ uma permutação $\sigma\in S_n$, então para qualquer permutação $\delta\in S_n$

$$\delta^{-1}\sigma\delta=(\delta(y_{11})\cdots\delta(y_{1r_1}))(\delta(y_{21})\cdots\delta(y_{2r_2}))\cdots(\delta(y_{m1})\cdots\delta(y_{mr_m})),$$

logo é possível, conjugando g_1 por um elemento adequado, obter

$$g_2 = g(a_1'x_1,\dots,a_l'x_l)\prod_{j=k+l-r}^{k+l}\operatorname{tr}(x_j)$$

Claramente temos que

$$g_3 = g(x_1,\dots,x_l)\prod_{j=1}^{k}\operatorname{tr}(x_{l+j})$$

está no ideal bilateral gerado por f_1. Tomando

$$s = x_1a_1'\cdots x_la_l'\prod_{j=k+l-r}^{k+l}\operatorname{tr}(x_j)$$

e usando (3.20), (3.24) e (3.25), teremos

$$\begin{aligned}
g_3\circ s &= \pi(g(x_1y_1,\dots,x_ly_l)\prod_{j=1}^{k}\operatorname{tr}(x_{l+j}y_{l+j})s)\Big|_{\substack{y_1=x_1\\ \cdots\cdots\\ y_{l+k}=x_{l+k}}}\\
&= \pi(g(x_1,\dots,x_l)y_1x_1a_1'\cdots y_lx_la_l'\prod_{j=k+l-r}^{k+l}\operatorname{tr}(x_j))\Big|_{\substack{y_1=x_1\\ \cdots\cdots\\ y_l=x_l}}\\
&= \pi(g(a_1'x_1,\cdots,a_l'x_l)\prod_{j=k+l-r}^{k+l}\operatorname{tr}(x_j)y_1x_1\cdots_l x_l)\Big|_{\substack{y_1=x_1\\ \cdots\cdots\\ y_l=x_l}} = g_2\circ t
\end{aligned}$$

em que $t=x_1\cdots x_l\operatorname{tr}(x_{l+1})\cdots\operatorname{tr}(x_{l+k})$. Então $g_2\circ t$ está no ideal bilateral gerado por f_1, e então os elementos $g_2=(g_2\circ t)\circ t^{-1}$ e g_1 estão no mesmo ideal. □

Lema 3.7.6. *Suponha que o diagrama de Young D_1 do tipo $(n_1,\dots,n_k)$ é um subdiagrama do diagrama de Young D_2 do tipo $(n_1',\dots,n_r')$, isto é, $n_i\leqslant n_i'$ para todo i, e sejam $l_1=n_1+\cdots+n_k$ e $l_2=n_1'+\cdots+n_r'$. Sejam V_{D_i} $(i=1,2)$ os ideais verbais da álgebra $\mathscr{G}$ gerados por um conjunto de polinômios generalizados multilineares de grau l_i formando um ideal bilateral de T_{l_i} correspondente ao diagrama de Young D_i. Então $V_{D_1}\supseteq V_{D_2}$.*

Demonstração. Preencha o diagrama D_2 com os inteiros de 1 a l_2 de modo que os inteiros de 1 a l_1 fiquem na subdiagrama D_1, obtendo assim as tabelas α_2 e α_1 respectivamente. Se $e(\alpha_i)=R_{\alpha_i}^*\circ C_{\alpha_i}^*$, $(i=1,2)$ como na Proposição 3.7.1, então $e(\alpha_i)$ gera o ideal bilateral

$V_{D_i} \cap T_{l_i}$. Podemos identificar o grupo S_{l_1+1} agindo sobre $\{x_0, \ldots, x_{l_1}\}$ com o subgrupo de S_{l_2+1} que age sobre $\{x_0, \ldots, x_{l_2}\}$ e fixa os elementos $x_{l_1+1}, \ldots, x_{l_2}$. Desta forma, $R_{\alpha_2} \supseteq R_{\alpha_1}$ e $C_{\alpha_2} \supseteq C_{\alpha_1}$. Trazendo isso para as álgebras de grupo, podemos tratar T_{l_1} como se estivesse contido em T_{l_2}. Nesse sentido, pelo Lema 3.7.5, o elemento $e(\alpha_1)$ gera $V_{D_1} \cap T_{l_2}$ como um ideal bilateral. Por outro lado,

$$\begin{aligned} R^*_{\alpha_2} \circ e(\alpha_1) \circ C^*_{\alpha_2} &= (R^*_{\alpha_2} \circ R^*_{\alpha_1}) \circ (C^*_{\alpha_1} \circ C^*_{\alpha_2}) = |R_{\alpha_1}|\ |C_{\alpha_1}|(R^*_{\alpha_2} \circ C^*_{\alpha_2}) \\ &= |R_{\alpha_1}|\ |C_{\alpha_1}|e(\alpha_2). \end{aligned}$$

Consequentemente, o gerador $e(\alpha_2)$ do ideal $V_{D_2} \cap T_{l_2}$ está no ideal $V_{D_1} \cap T_{l_2}$, e portanto $V_{D_1} \cap T_{l_2} \supseteq V_{D_2} \cap T_{l_2}$. Portanto $V_{D_1} \supseteq V_{D_2}$, e o lema está provado. □

Finalmente vamos provar o resultado que queríamos. Nesta demonstração optamos por trabalhar mais na álgebra KS_{n^2+1} e apenas no final transportar para polinômios com traço.

Teorema 3.7.1. *Em qualquer álgebra associativa sobre um corpo de característica* 0 *na qual a identidade* $x^n = 0$ *é válida, a identidade* $x_1 x_2 \cdots x_{n^2} = 0$ *também é válida.*

Demonstração. KS_{n^2+1} é completamente redutível, logo, em particular, $(x_0 x_1 \ldots x_{n^2})$ pode ser escrito como soma de termos provenientes dos ideais minimais de KS_{n^2+1}. Usando os fatos da teoria das representações do grupo simétrico, temos:

$$(x_0 x_1 \ldots x_{n^2}) = \sum c_d g_d e(T_d) h_d$$

em que g_d e h_d são permutações (em S_{n^2+1}), $c_d \in K$ e T_d são tabelas de Young (que podem aparecer repetidas vezes). Note que aqui, pelo Corolário 1.8.2, podemos exigir que as tabelas T_d tenham os valores de 0 a n na primeira linha ou na primeira coluna.

Usando a parte da demonstração do Lema 3.7.6 que acontece dentro das álgebras de grupo, isto é, que se α_1 é uma subtabela de α_2 (aqui removemos o $\circ$, para enfatizar que nos referimos ao produto dentro de KS_{n^2+1}, estendido da composição usual de permutações, e não a operação $\circ$ definida anteriormente):

$$\begin{aligned} R^*_{\alpha_2} e(\alpha_1) C^*_{\alpha_2} &= (R^*_{\alpha_2} R^*_{\alpha_1})(C^*_{\alpha_1} C^*_{\alpha_2}) = |R_{\alpha_1}|\ |C_{\alpha_1}|(R^*_{\alpha_2} C^*_{\alpha_2}) \\ &= |R_{\alpha_1}|\ |C_{\alpha_1}|e(\alpha_2) \end{aligned}$$

e portanto

$$e(\alpha_2) = \frac{R^*_{\alpha_2} e(\alpha_1) C^*_{\alpha_2}}{|R_{\alpha_1}|\ |C_{\alpha_1}|}.$$

Assim, podemos reescrever $(x_0 x_1 \ldots x_{n^2})$ como

$$(x_0 x_1 \ldots x_{n^2}) = \sum c_d g_d f_d h_d$$

em que g_d e h_d são permutações (em S_{n^2+1}), $c_d \in K$ e $f_d = \sum_{\tau \in S_{n+1}} \operatorname{sgn}(\tau)\tau$ ou $f_d = \sum_{\sigma \in S_{n+1}} \sigma$, que são geradores dos ideais correspondentes ao diagrama com 1 coluna de $n+1$ caixas e ao diagrama com 1 linha de $n+1$ caixas, respectivamente. Esses $f_d \in KS_{n^2+1}$ são iguais à soma de todas as permutações que permutam $\{x_0, \ldots, x_n\}$ e preservam $\{x_{n+1}, \ldots, x_{n^2}\}$, com ou sem a multiplicação pelo sinal da permutação.

Antes de voltar para polinômios com traço, vamos trabalhar um pouco mais sobre os termos $g_d f_d h_d$. Como uma conjugação de uma permutação escrita na forma de ciclos equivale a uma renomeação de variáveis (Proposição 1.1.1), ao trabalharmos com permutações podemos remover o termo g_d da esquerda de f_d. Assim, com um pouco de abuso de notação, podemos escrever $g_d f_d h_d = f_d(x_{i_{d0}}, x_{i_{d1}}, \ldots, x_{i_{dn}})h'_d$, em que $f_d(x_{i_{d0}}, \ldots x_{i_{dn}})$ é igual à soma de todas as permutações que permutam $\{x_{i_{d0}}, x_{i_{d1}}, \ldots, x_{i_{dn}}\}$ e preservam as outras variáveis, com ou sem a multiplicação pelo sinal da permutação. A partir daqui vamos omitir o d de i_{dk} e usar apenas i_k.

Agora considere h'_d escrita na forma de ciclos. O resultado da multiplicação de dois ciclos com apenas um elemento em comum é (lembramos que aqui estamos usando composição de permutações da esquerda para a direita):

$$(a_j x_j a'_j)(x_j b_j) = (a_j b_j x_j a'_j)$$

em que x_j é um elemento e a_j, a'_j e b_j são palavras. Então podemos interpretar esse produto por $(x_j b_j)$ como a substituição de x_j por $b_j x_j$. Falta contornar a situação em que existe mais de um elemento de $\{x_{i_0}, x_{i_1}, \ldots, x_{i_n}\}$ em um mesmo ciclo de h'_d. Para tanto, note que, por exemplo,

$$(b_i x_i b_j x_j b_k x_k) = (x_i x_j x_k)(b_i x_i)(b_j x_j)(b_k x_k)$$

em que x_i, x_j e x_k são elementos e b_i, b_j e b_k são palavras. Podemos fazer algo semelhante para cada ciclo, e como os ciclos originais de h'_d são disjuntos, é possível comutar os ciclos do tipo $(x_i x_j x_k)$ e levá-los para a esquerda do produto. Com isso é possível obter h'_i como um produto de uma permutação formada por ciclos contendo apenas $\{x_{i_0}, x_{i_1}, \ldots, x_{i_n}\}$ (e os outros termos não aparecem, isto é, estão sozinhos em ciclos de tamanho 1), outra permutação em que os elementos $\{x_{i_0}, x_{i_1}, \ldots, x_{i_n}\}$ aparecem em ciclos distintos e uma terceira permutação que permuta apenas os elementos que não estão na permutação anterior e nem em $\{x_{i_0}, x_{i_1}, \ldots, x_{i_n}\}$.

Note que ao aplicar uma permutação que permuta apenas $\{x_{i_0}, x_{i_1}, \ldots, x_{i_n}\}$ sobre $f_d(x_{i_0}, x_{i_1}, \ldots, x_{i_n})$ o resultado é o próprio $f_d(x_{i_0}, x_{i_1}, \ldots, x_{i_n})$ (pois vai continuar sendo a soma de todas as permutações dos elementos $\{x_{i_0}, x_{i_1}, \ldots, x_{i_n}\}$), exceto eventualmente por uma mudança de sinal, que ocorre se o f_d original era $\sum_{\tau \in S_{n+1}} \operatorname{sgn}(\tau)\tau$ e a permutação aplicada era ímpar. Concluímos então que é possível considerar que

h'_d é uma permutação em que os elementos $\{x_{i_0}, x_{i_1}, \ldots, x_{i_n}\}$ estão em ciclos distintos. Com mais um abuso de notação, podemos dizer que, se $h'_d = (x_{i_0}a_{i_0}) \cdots (x_{i_n}a_{i_n})$, então $f_d(x_{i_0}, x_{i_1}, \ldots, x_{i_n})h'_d = f_d(a_{i_0}x_{i_0}, a_{i_1}x_{i_1}, \ldots, a_{i_n}x_{i_n})$. Este último é igual à soma de todas as permutações de $n+1$ elementos, escritos na forma de ciclos, em que substituímos esses elementos pelos $a_{i_j}x_{i_j}$. Para simplificar um pouco a notação, seja $b_{i_k} = a_{i_k}x_{i_k}$. Logo

$$(x_0x_1 \ldots x_{n^2}) = \sum c'_d f_d(b_{i_0}, b_{i_1}, \ldots, b_{i_n})h''_d$$

em que c'_d é igual a c_d, eventualmente com um sinal diferente e h''_d é permutação que preserva todas as letras que estão nos b_{i_j}.

Então vamos começar a voltar para os polinômios com traço. A ideia é considerar apenas os termos sem traço, que, pelo isomorfismo definido no Lema 3.7.4 entre os monômios generalizados em n^2 variáveis e S_{n^2+1}, correspondem às permutações compostas por exatamente um ciclo (ou seja, todas as letras devem estar no mesmo ciclo). Note que se algum elemento não aparecer em $f_d(b_{i_0}, b_{i_1}, \ldots, b_{i_n})$, isto é, não estiver em nenhum dos b_{i_k}, todos os termos de f_d terão mais de um ciclo, logo não correspondem a monômios ordinários (sem traço). Nesse caso iremos ignorar tais termos do somatório, e portanto, os h''_d restantes têm que preservar todas as letras, logo devem ser a permutação trivial. Para verificar qual monômio ordinário é obtido a partir de um termo de $f_d(b_{i_0}, b_{i_1}, \ldots, b_{i_n})$, precisamos ter em consideração onde o elemento x_0 está. Sem perda de generalidade, suponha que x_0 está em b_{i_0}, e que $b_{i_0} = b'_{i_0}x_0b''_{i_0}$. Então os monômios ordinários são obtidos das permutações formadas por exatamente um ciclo $(b_{i_0}b_{i_{\sigma(1)}} \ldots b_{i_{\sigma(n)}})$ em que $\sigma \in S_n$ e portanto são iguais a $b''_{i_0}b_{i_{\sigma(1)}} \ldots b_{i_{\sigma(n)}}b'_{i_0}$. O σ percorre todas as permutações em S_n, logo os monômios ordinários obtidos de $f_d(b_{i_0}, b_{i_1}, \ldots, b_{i_n})$, somados, são iguais a $b''_{i_0}e_n(b_{i_1}, \ldots, b_{i_n})b'_{i_0}$, eventualmente com sinal negativo. Aqui é importante notar que um modo de obter a paridade de uma permutação é verificar a paridade do número de ciclos (incluindo os de tamanho 1) - se o número de ciclos e o número de termos têm mesma paridade então a permutação é par, caso contrário a permutação é ímpar. Assim a paridade das permutações formadas por exatamente um ciclo são todas iguais, e portanto o sinal associado também é igual.

Logo o somatório inicial se torna (aqui voltamos com o d omitido anteriormente):

$$x_1 \ldots x_{n^2} = \sum c''_d b''_{i_{d0}} e_n(b_{i_{d1}}, \ldots, b_{i_{dn}})b'_{i_{d0}}$$

em que c''_d é igual a c'_d, eventualmente com um sinal diferente. Concluímos que $x_1 \ldots x_{n^2}$ é consequência de e_n e portanto de x^n. □

Referências

1 CURTIS, C. W.; REINER, I. *Representation theory of finite groups and associative algebras*. Providence, RI: American Mathematical Society, 1962. v. 356.

2 DRENSKY, V. S. *Polynomial Identity Rings*. Basel: Birkhäuser, 2004. (Advanced Courses in Mathematics CRM Barcelona).

3 DRENSKY, V. S. *Free algebras and PI-algebras: graduate course in algebra*. Singapore: Springer, 2000.

4 HERSTEIN, I. N. *Noncommutative rings*. Singapore: Mathematical Association of America, 1968. (Carus Mathematical Monographs).

5 HERSTEIN, I. N. *Topics in algebra*. Wiley, 2006.

6 HIGMAN, G.; HALL, P. On a conjecture of Nagata. *Mathematical Proceedings of the Cambridge Philosophical Society*, Cambridge University Press, v. 52, n. 1, p. 1–4, 1956.

7 LAMBEK, J. *Lectures on rings and modules*. Providence, RI: American Mathematical Society, 1966.

8 NAGATA, M. On the nilpotency of nil-algebras. *Journal of the Mathematical Society of Japan*, Mathematical Society of Japan, v. 4, n. 3-4, p. 296–301, 12 1952.

9 RAZMYSLOV, Y. P. Trace identities of full matrix algebras over a field of characteristic zero. *Mathematics of the USSR-Izvestiya*, v. 8, n. 4, p. 727–760, 1974.

10 REGEV, A.; REGEV, A. The Golod-Shafarevich counterexample without Hilbert series. In: *Groups, rings and group rings*. Providence, RI: American Mathematical Society, 2009, (Contemporary Mathematics, v. 499). p. 257–264.

11 VAUGHAN-LEE, M. An algorithm for computing graded algebras. *Journal of Symbolic Computation*, v. 16, n. 4, p. 345–354, 1993.

12 ZHEVLAKOV, K. A.; SLIN'KO, A. M.; SHESTAKOV, I. P.; SHIRSHOV, A. I. *Rings that are nearly associative*. Tradução Harry F. Smith. New York: Academic Press, 1982. v. 104. (Pure and Applied Mathematics, v. 104).

Leitura extra:

13 AMITSUR, A. S.; LEVITZKI, J. Minimal identities for algebras. *Proceedings of the American Mathematical Society*, American Mathematical Society, v. 1, n. 4, p. 449–463, 8 1950.

14 DUBNOV, J.; IVANOV, V. Sur l'abaissement du degré des polynômes en affineurs. *CR (Doklady) Acad. Sci. USSR*, v. 41, p. 96–98, 1943.

15 KAPLANSKY, I. Rings with a polynomial identity. *Bulletin of the American Mathematical Society*, American Mathematical Society, v. 54, n. 6, p. 575–580, 6 1948.

16 KUZMIN, E. N. On the Nagata-Higman theorem. In: *Mathematical Structures, Computational Mathematics, Mathematical Modelling. Proc. Dedicated to the 60th Birthday of Acad. L. Iliev*. Sofia: [s.n.], 1975. p. 101–107.

17 LEVITZKI, J. A theorem of polynomial identities. *Proceedings of the American Mathematical Society*, American Mathematical Society, v. 1, n. 3, p. 334–341, 6 1950.

18 PROCESI, C. The invariant theory of n x n matrices. *Advances in Mathematics*, v. 19, n. 3, p. 306–381, 3 1976.

19 SHESTAKOV, I. P.; ZHUKAVETS, N. On associative algebras satisfying the identity $x^5 = 0$. *Algebra Discrete Math.*, n. 1, p. 112–120, 2004.