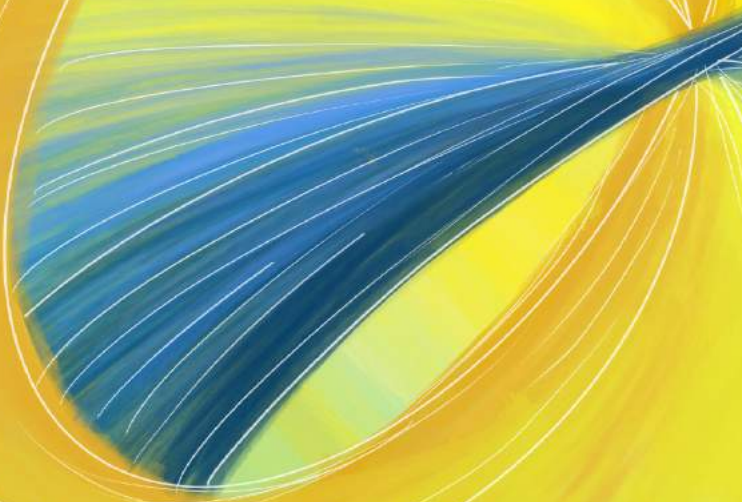
PI-álgebras: uma introdução à PI-teoria



Rafael Bezerra dos Santos
Ana Cristina Vieira

impa

33º Colóquio Brasileiro de Matemática

PI-álgebras: uma introdução à PI-teoria

PI-álgebras: uma introdução à PI-teoria
Primeira impressão, julho de 2021

Publicado no Brasil / Published in Brazil.

ISBN 978-65-89124-37-5
MSC (2020) Primary: 16R10, Secondary: 16P90, 20C30, 16D60, 16S50, 15A75

Coordenação Geral Carolina Araujo

Produção Books in Bytes **Capa** Izabella Freitas & Jack Salvador

Realização da Editora do IMPA
IMPA
Estrada Dona Castorina, 110
Jardim Botânico
22460-320 Rio de Janeiro RJ

www.impa.br
editora@impa.br

Sumário

Prefácio

Este livro é dedicado à introdução à teoria de álgebras com identidades polinomiais, conhecida como PI-teoria. Para isso, essencialmente consideraremos álgebras associativas sobre um corpo F de característica zero. Polinômios em variáveis não comutativas, se anulando sob avaliação de elementos em uma álgebra, são definidos como identidades polinomiais e foram considerados inicialmente nos trabalhos de Dehn (1922) e Wagner (1937).

Uma álgebra satisfazendo uma identidade polinomial não nula é denominada uma PI-álgebra. Qualquer álgebra comutativa é uma PI-álgebra, e um exemplo de uma PI-álgebra não comutativa é a álgebra UT_2, de matrizes triangulares superiores 2×2 sobre um corpo F. Em geral, álgebras de dimensão finita são exemplos de PI-álgebras, satisfazendo um polinômio especial, chamado polinômio standard[1]. Por outro lado, um excelente exemplo de uma PI-álgebra de dimensão infinita é a álgebra de Grassmann $\mathcal{G}$, ou álgebra exterior.

O desenvolvimento da PI-teoria teve início basicamente a partir do artigo de Kaplansky (1948), dedicado à descrição da estrutura de uma PI-álgebra primitiva. Dois anos após a publicação do Teorema de Kaplansky, Amitsur e Levitzki (1950) provaram que o polinômio standard de grau $2k$ é uma identidade de grau mínimo da álgebra de matrizes $M_k(F)$. Para provar o resultado, os autores usaram métodos puramente combinatoriais, introduzindo um novo tipo de abordagem na PI-teoria, cujo objetivo passou a ser a descrição das identidades satisfeitas por uma álgebra. Com isso, o interesse se tornou em determinar o conjunto $\mathrm{Id}(A)$ de todas as identidades polinomiais de uma dada álgebra A.

[1] Faremos a opção de não traduzir a palavra standard para o português.

O conjunto $\mathrm{Id}(A)$ é um T-ideal de $F\langle X\rangle$, a álgebra de polinômios em um conjunto enumerável X de variáveis não comutativas sobre F, isto é, é um ideal invariante sob todos os endomorfismos de $F\langle X\rangle$, e é chamado o T-ideal de A. Specht (1950) conjecturou que, sobre um corpo de característica zero, o T-ideal de uma álgebra associativa é finitamente gerado como um T-ideal.

A conjectura de Specht foi provada para alguns casos particulares nos anos seguintes, e a demonstração completa foi dada por Kemer (1988). Além disso, o T-ideal $\mathrm{Id}(A)$ é gerado por polinômios multilineares, ou seja, por polinômios cujas variáveis aparecem uma única vez em cada um de seus monômios. Mas mesmo diante dessas informações, é importante destacar que a descrição do T-ideal de uma álgebra é, em geral, um problema difícil. De fato, exemplificamos que, mesmo para a álgebra de matrizes $M_k(F)$, o T-ideal foi descrito somente para $k = 1$ e $k = 2$, até o presente momento. Na tentativa de minimizar a dificuldade encontrada na determinação do T-ideal de uma álgebra A, alguns invariantes numéricos associados à A foram introduzidos, para conhecer informações quantitativas sobre $\mathrm{Id}(A)$. Um invariante numérico muito útil é a chamada sequência de codimensões de uma álgebra A. Tal sequência, denotada $\{c_n(A)\}_{n\geq 1}$, foi introduzida por Regev (1972) e mede, de uma certa maneira, a taxa de crescimento das identidades polinomiais satisfeitas por A.

É bem compreendido que se A é uma PI-álgebra, então a sequência de codimensões cresce exponencialmente ou é limitada polinomialmente, isto é, existem constantes $a, k \geqslant 0$ tais que $c_n(A) \leqslant an^k$ para todo $n \geqslant 1$. Nesse último caso, dizemos que A tem crescimento polinomial.

A sequência de codimensões, além de ser uma importante ferramenta, tornou-se um dos principais objetos de investigação na PI-teoria e, nos últimos anos, tem sido estudada por diversos autores. A possibilidade de álgebras distintas possuírem o mesmo T-ideal nos leva a estudar a classe das álgebras que satisfaça todas as identidades de uma dada álgebra A, chamada de variedade gerada por A e denotada por $\mathrm{var}(A)$. Para uma variedade de álgebras $\mathcal{V} = \mathrm{var}(A)$, definimos $c_n(\mathcal{V}) = c_n(A)$. Um dos principais objetivos da PI-teoria tem sido caracterizar e classificar variedades de álgebras $\mathcal{V}$ por meio do comportamento assintótico da sequência $c_n(\mathcal{V})$. Em particular, nesse livro, temos interesse em variedades com crescimento polinomial da sequência de codimensões, isto é, variedades geradas por álgebras de crescimento polinomial.

O estudo das variedades de crescimento polinomial foi iniciado por Kemer (1979). Mais especificamente, ele mostrou que $\mathrm{var}(A)$ tem crescimento polinomial se, e somente se, $\mathcal{G}$ e $UT_2(F) \notin \mathrm{var}(A)$. Como consequência dessa caracterização, segue que $\mathrm{var}(\mathcal{G})$ e $\mathrm{var}(UT_2(F))$ são as únicas variedades de crescimento quase

polinomial, isto é, as sequências de codimensões de $\mathcal{G}$ e de $UT_2(F)$ crescem exponencialmente, mas qualquer subvariedade própria de $\text{var}(\mathcal{G})$ e de $\text{var}(UT_2(F))$ tem crescimento polinomial.

Este livro foi escrito com o objetivo de motivar estudantes interessados na área de álgebra a conhecer resultados clássicos e também recentes da PI-teoria, necessários para apresentar uma demonstração moderna do Teorema de Kemer e fornecer outras caracterizações de variedades de álgebras de crescimento polinomial.

Ao escrever o livro, nossa preocupação foi deixar um bom registro dos principais resultados em álgebra não comutativa, importantes ferramentas no desenvolvimento da PI-teoria. Fizemos a opção de detalhar o conteúdo de tais tópicos, não apenas para servir de apoio aos estudantes interessados no estudo de PI-álgebras, mas também para que os colegas possam utilizar o primeiro capítulo do livro em seus cursos básicos de teoria de anéis e módulos.

Dessa forma, no Capítulo 1, apresentamos as noções de anéis e módulos, seguidos de diversos resultados importantes sobre esses objetos. Introduzimos o conceito de produto tensorial de módulos e provamos o Teorema de Wedderburn–Artin, que caracteriza os anéis artinianos semissimples. Provamos também o Teorema de Wedderburn, que apresenta a estrutura de anéis semissimples. Definimos o radical de Jacobson de um anel e provamos suas propriedades. Por fim, dedicamos a última seção ao estudo das álgebras, objeto principal de estudo deste livro, e provamos o Teorema de Wedderburn–Malcev. Este capítulo pode ser dispensado por estudantes que tenham conhecimento básico dos resultados citados.

No Capítulo 2, nos preocupamos em explicitar os resultados essenciais a respeito de representações e caracteres de um grupo finito, tendo como foco o grupo simétrico S_n. Esse grupo tem participação especial no estudo do crescimento da sequência de codimensões de uma PI-álgebra, devido à sua ação sobre o espaço dos polinômios multilineares de grau n. Destacamos os resultados essenciais da teoria desenvolvida por A. Young para o estudo dos caracteres irredutíveis de S_n.

O Capítulo 3 tem como foco a introdução aos objetos principais deste livro, os polinômios na álgebra livre $F\langle X\rangle$ e as PI-álgebras. Provamos propriedades importantes sobre os geradores do T-ideal de uma PI-álgebra e demonstramos o processo de multilinearização, que permite obter uma identidade multilinear a partir de uma identidade qualquer de uma álgebra. Na seção final, demonstraremos o célebre Teorema de Amitsur–Levitzki.

No Capítulo 4, definimos as variedades de álgebras, apresentamos resultados destacados a respeito e damos exemplos de álgebras PI-equivalentes, isto é, que geram a mesma variedade. Definimos, ainda, a sequência de codimensões de uma

álgebra e o significado de crescimento polinomial e exponencial. Damos exemplos de álgebras de crescimento polinomial e calculamos a sequência de codimensões das álgebras $\mathcal{G}$ e UT_2, mostrando que estas têm crescimento exponencial. Introduzimos, também, os conceitos de superálgebra e de PI-expoente.

Iniciamos o Capítulo 5 estabelecendo um resultado que fornece uma condição necessária e suficiente para que uma variedade seja gerada por uma álgebra de dimensão finita e provamos o célebre Teorema de Kemer, que caracteriza variedades de crescimento polinomial das codimensões via exclusão de $\mathcal{G}$ e UT_2 da variedade. Além disso, introduzimos a sequência de cocaracteres $\{\chi_n(A)\}_{n\geq 1}$ de uma álgebra e demonstramos o resultado que caracteriza as variedades de crescimento polinomial por meio da decomposição de $\chi_n(A)$. Ao final, apresentamos mais um resultado de caracterização, provando que uma álgebra A tem crescimento polinomial se, e somente se, $\mathrm{var}(A) = \mathrm{var}(B)$, onde B é uma álgebra de dimensão finita, que tem uma decomposição explícita como soma direta de subálgebras com propriedades particulares.

O Capítulo 6 foi preparado com a intenção de atrair os interessados na área de álgebra a se aprofundar em resultados de pesquisa recentemente desenvolvidos na PI-teoria. Este capítulo não contém as demonstrações dos resultados apresentados, pois o objetivo é motivar o leitor a estudar os artigos onde foram publicados. Nele, destacamos a importância das variedades minimais de crescimento polinomial e introduzimos as φ-álgebras, que são as álgebras com estrutura adicional. Apresentamos a extensão das noções de identidades e codimensões para φ-álgebras, os teoremas de caracterização de φ-variedades de crescimento polinomial e resultados de classificação em diversos aspectos. Ao final, consideramos as superálgebras com involução graduada, objeto recente de estudo na PI-teoria, e apresentamos o teorema de caracterização de variedades de crescimento polinomial correspondente, junto com resultados de classificação já provados.

Convém ressaltar que, no decorrer dos capítulos, foram inseridos diversos exercícios interessantes com importantes informações sobre o assunto em desenvolvimento no texto. Também, ao fim da cada uma das seções dos Capítulos 1 a 5, sugerimos uma lista de sentenças afirmativas sobre o conteúdo descrito, para que os leitores possam decidir se são verdadeiras ou falsas, o que chamamos Exercícios V ou F da seção correspondente.

A redação deste livro é uma importante contribuição para a motivação de novos estudiosos em PI-teoria no Brasil, pela escassez de literatura em português sobre o assunto. Os primeiros livros dedicados à PI-teoria foram publicados nos anos 1970 e 1980, como, por exemplo, os livros de Procesi (1973), Jacobson (1975) e Rowen (1980). A prova da conjectura de Specht pode ser consultada na importante

monografia de Kemer (1991). Diversos livros dedicam algumas seções ao tratamento de álgebras com identidades polinomiais tais como os de Herstein (1968), Passman (1977), Rowen (1991) e Formanek (1991). Aos leitores interessados em se aprofundar de modo mais geral na PI-teoria, indicamos as literaturas mais atualizadas de Drensky (2000), Giambruno e Zaicev (2005) e Aljadeff et al. (2020). Por fim, um interessante material com resultados recentes de pesquisa em PI-teoria é o livro editado por Di Vincenzo e Giambruno (2021), que pode ser consultado pelo leitor interessado na área.

Queremos deixar registrado aqui, nossos agradecimentos àqueles que contribuíram para uma melhor qualidade deste livro. Aos nossos orientandos Maralice Assis e Wesley Quaresma, e a Dafne Bessades e a Maria Luiza Santos, doutoras recentemente formadas em PI-teoria sob nossa orientação, pela revisão dos termos matemáticos e pela sugestão de exercícios para as seções. Aos nossos estudantes que colaboraram com discussões durante os seminários sobre os assuntos deste livro. Aos colegas: Thiago Castilho de Mello e Luís Felipe Gonçalves Fonseca, pelas sugestões e empréstimo de material para a elaboração deste texto. Por fim, agradecemos à organização do 33^{0} Colóquio Brasileiro de Matemática pela oportunidade de divulgar a PI-teoria e pelo apoio constante de edição durante a elaboração do texto.

Belo Horizonte, maio de 2021

Rafael Bezerra dos Santos e Ana Cristina Vieira

1 Álgebras associativas

Este capítulo inicial contém os resultados que julgamos importantes para uma boa compreensão de todos os demais. Na Seção 1.1, fazemos uma pequena revisão sobre teoria de anéis, fixando a notação que será utilizada em todo o livro. Na Seção 1.2, estudamos o conceito de módulos e provamos suas principais propriedades. Finalizamos a seção definindo o produto tensorial, com a finalidade de estudar a extensão de escalares de um espaço vetorial. A Seção 1.3 é uma seção central do capítulo, onde estudamos a semissimplicidade de anéis e módulos. Definimos a noção de anéis e módulos artinianos e noetherianos e provamos o Teorema de Wedderburn–Artin, que caracteriza os anéis artinianos semissimples. É nesta seção que definimos o radical de Jacobson de um anel, um ideal em destaque na teoria de anéis. Por fim, na Seção 1.4, introduzimos o conceito de álgebras sobre um corpo, o principal objeto de estudo deste livro, e construímos a seção com o objetivo de demonstrar um dos principais teoremas utilizados neste livro: o Teorema de Wedderburn–Malcev.

Este capítulo contém resultados clássicos em álgebra não comutativa, podendo ser dispensado pelo leitor mais avançado. No final do capítulo, faremos um resumo com os principais resultados sobre álgebras utilizados nos capítulos seguintes.

1.1 Anéis

Esta seção é introdutória e pode ser dispensada aos leitores que já tem conhecimento básico sobre teoria de anéis. Aqui, faremos uma breve revisão dos resultados necessários para o desenvolvimento deste livro.

Definição 1.1.1. Um anel R é um conjunto não vazio munido de duas operações binárias, $+ : R \times R \to R$ e $\cdot : R \times R \to R$, que chamaremos de adição e multiplicação, respectivamente, tais que para todos $a, b, c \in R$, as seguintes propriedades são válidas:

1. $a + b = b + a$;
2. $a + (b + c) = (a + b) + c$;
3. Existe um elemento neutro aditivo $0 \in R$ tal que $a + 0 = a$;
4. Existe um inverso aditivo $-a \in R$ tal que $a + (-a) = 0$;
5. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
6. $a \cdot (b + c) = a \cdot b + a \cdot c$;
7. $(a + b) \cdot c = a \cdot c + b \cdot c$.

As propriedades 1, 2, 3 e 4 dizem que o conjunto R munido da operação $+$ é um grupo abeliano[1], e escreveremos $(R, +)$. A partir de agora, iremos omitir o ponto no produto de dois elementos de um anel R e escreveremos $a \cdot b = ab$.

Neste livro, não exigimos a comutatividade da multiplicação em um anel. Por isso, definiremos esse fato isoladamente.

Dizemos que um anel R é comutativo se $ab = ba$, para quaisquer $a, b \in R$. Um anel R é um domínio, se $ab = 0$ implica que ou $a = 0$ ou $b = 0$. Elementos não nulos $a, b \in R$ tais que $ab = 0$ são chamados de divisores de zero. Assim, um domínio é um anel sem divisores de zero.

Definição 1.1.2. Um anel R contendo um elemento $1 \neq 0$ tal que

$$1a = a1 = a, \text{ para todo } a \in R$$

é chamado de anel com unidade. Um domínio comutativo com unidade é chamado de domínio de integridade.

[1] O leitor interessado deve ver no Capítulo 2 uma definição geral de grupo.

Definição 1.1.3. Um elemento a em um anel com unidade R é dito ser invertível, se existe um elemento, que denotaremos por $a^{-1} \in R$ e chamado de inverso de a, tal que

$$aa^{-1} = a^{-1}a = 1.$$

Em um anel com unidade, consideramos o conjunto

$$\mathcal{U}(R) = \{a \in R : a \text{ é invertível}\}$$

chamado de grupo das unidades de R. Um anel com unidade tal que todos os elementos diferentes de 0 são invertíveis, isto é, $\mathcal{U}(R) = R - \{0\}$, é chamado de anel de divisão. Um anel de divisão comutativo é chamado de corpo.

Como exemplos básicos de domínios de integridade, temos os conjuntos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ dos números inteiros, racionais, reais e complexos, respectivamente, com operações de adição e multiplicação usuais.

Recordemos que $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$. Logo, $\mathbb{Z}$ não é um corpo, enquanto $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são exemplos de corpos.

Exemplo 1.1.4. O anel $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ da classe dos restos módulo m é um anel comutativo com unidade que é um corpo se, e somente se, m é primo.

Percebemos, então, que temos exemplos de corpos infinitos e de corpos finitos. Neste livro, conforme veremos, temos um interesse maior por resultados sobre corpos infinitos.

Exemplo 1.1.5. O conjunto $M_n(R)$ de todas as matrizes $n \times n$ com entradas em um anel R, com as operações de adição e multiplicação usuais, é um anel.

Em geral, o anel $M_n(R)$ não é um anel comutativo. Além disso, se R possui unidade, então $M_n(R)$ também possui unidade. Neste caso, denotamos por

$$1 = I_n = (a_{ij}) = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}$$

e I_n é chamada de matriz identidade $n \times n$.

Se R é um anel com unidade, denotamos por e_{ij} a matriz que possui o elemento 1 na entrada (i, j) e 0 nas demais.

As matrizes e_{ij}, $i, j \in \{1, \ldots, n\}$, são chamadas de matrizes elementares. Note que $I_n = \sum_{i=1}^{n} e_{ii}$ e que $e_{ij}e_{kl} = \delta_{jk}e_{il}$, onde

$$\delta_{jk} = \begin{cases} 1, & \text{se } j = k \\ 0, & \text{se } j \neq k \end{cases}$$

denota o delta de Kronecker. Observe que se $n \geqslant 2$, então as matrizes elementares são divisores de zero em $M_n(R)$.

Se R é um anel, então o conjunto

$$UT_n(R) = \{(a_{ij}) \in M_n(R) : a_{ij} = 0 \text{ se } i > j\} \subset M_n(R) \tag{1.1}$$

é um anel, com as operações de soma e multiplicação usuais de matrizes, chamado de anel das matrizes triangulares superiores $n \times n$ com entradas em R. Quando $R = F$ for um corpo, denotaremos o anel $UT_n(F)$ simplesmente por UT_n.

Em seguida, veremos mais alguns exemplos de anéis.

Exemplo 1.1.6. Sejam i, j, k símbolos e denote por

$$\mathbb{H} = \{x_0 + x_1 i + x_2 j + x_3 k : x_0, x_1, x_2, x_3 \in \mathbb{R}\}.$$

Vamos dar uma estrutura de anel ao conjunto $\mathbb{H}$, definindo a adição de dois elementos $\alpha = x_0 + x_1 i + x_2 j + x_3 k$ e $\beta = y_0 + y_1 i + y_2 j + y_3 k$ por

$$\alpha + \beta = (x_0 + y_0) + (x_1 + y_1)i + (x_2 + y_2)j + (x_3 + y_3)k$$

e a multiplicação é definida distributivamente, com a multiplicação entre os símbolos i, j, k dada da seguinte maneira:

$$\begin{gathered} i^2 = j^2 = k^2 = -1 \\ ij = k = -ji \\ jk = i = -kj \\ ki = j = -ik. \end{gathered}$$

O conjunto $\mathbb{H}$ com as operações acima é chamado de anel dos quatérnios reais. Dado um quatérnio $\alpha = x_0 + x_1 i + x_2 j + x_3 k \in \mathbb{H}$, definimos o conjugado $\overline{\alpha}$ de α por

$$\overline{\alpha} = x_0 - x_1 i - x_2 j - x_3 k.$$

A norma de α é definida por

$$||\alpha|| = \alpha\overline{\alpha} = x_0^2 + x_1^2 + x_2^2 + x_3^2$$

e observe que para todo $\alpha \in \mathbb{H}$, $||\alpha|| \geqslant 0$ e $||\alpha|| = 0$ se, e somente se, $\alpha = 0$. Agora, se $\alpha \in \mathbb{H}, \alpha \neq 0$, defina $\alpha' = \frac{\overline{\alpha}}{||\alpha||}$. Logo,

$$\alpha\alpha' = \alpha\frac{\overline{\alpha}}{||\alpha||} = \frac{||\alpha||}{||\alpha||} = 1.$$

De maneira análoga, pode-se verificar que $\alpha'\alpha = 1$. Com isso, $\alpha' = \alpha^{-1}$ e este argumento mostra que $\mathbb{H}$ é um anel de divisão.

Exemplo 1.1.7. Sejam R um anel e x uma variável. O conjunto $R[x]$ dos polinômios na variável x com coeficientes em R, com operações de soma e multiplicação usuais, é um anel, chamado de anel de polinômios na variável x. O anel $R[x]$:

1. tem unidade se, e somente se, R tem unidade;
2. é comutativo se, e somente se, R é comutativo;
3. é um domínio se, e somente se, R é um domínio.

Exemplo 1.1.8. Seja $\mathcal{C}^0([a,b]) = \{f : [a,b] \to \mathbb{R} : f \text{ é contínua}\}$. Dados $f, g \in \mathcal{C}^0([a,b])$, defina $(f+g)(x) = f(x) + g(x)$ e $(fg)(x) = f(x)g(x)$. Com essas operações, $\mathcal{C}^0([a,b])$ é um anel comutativo com unidade, chamado anel das funções contínuas no intervalo $[a,b]$.

Os exercícios a seguir apresentam algumas propriedades importantes sobre elementos de um anel.

Exercício 1.1.9. Seja R um anel. Mostre que:

(a) O elemento $0 \in R$, do item 3 da Definição 1.1.1, é único.

(b) O elemento $-a \in R$, do item 4 da Definição 1.1.1, é único.

(c) Se R tem unidade, então o elemento $1 \in R$, da Definição 1.1.2, é único.

(d) Se R tem unidade e $a \in R$ é invertível, então o elemento $a^{-1} \in R$, da Definição 1.1.3, é único.

Exercício 1.1.10 (Regra de sinais)**.** Sejam R um anel e $a, b \in R$. Mostre que:

(a) $(-a)b = -(ab) = a(-b)$.

(b) $-(-a) = a$.

(c) $(-a)(-b) = ab$.

Exercício 1.1.11. Mostre que, em um anel com unidade, elementos invertíveis não são divisores de zero. Conclua que todo anel de divisão é um domínio.

Exercício 1.1.12. Mostre que todo domínio de integridade finito é um corpo.

Dados dois anéis R_1 e R_2, podemos considerar o conjunto $R_1 \times R_2 = \{(r_1, r_2) : r_1 \in R_1, r_2 \in R_2\}$, que tem estrutura de anel definindo

1. $(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2')$;
2. $(r_1, r_2)(r_1', r_2') = (r_1 r_1', r_2 r_2')$

para todos $r_1, r_1' \in R_1, r_2, r_2' \in R_2$. O anel $R_1 \times R_2$ é chamado de produto direto dos anéis R_1 e R_2.

Exercício 1.1.13. Seja $R_1 \times R_2$ o produto direto dos anéis R_1 e R_2.

(a) Mostre que se R_1 e R_2 têm unidade (são comutativos), então $R_1 \times R_2$ tem unidade (é comutativo).

(b) Mostre que se $R_1, R_2 \neq \{0\}$, então $R_1 \times R_2$ possui divisores de zero.

(c) Generalize a construção do produto direto de uma quantidade arbitrária de anéis e mostre que os itens (a) e (b) continuam válidos neste anel.

Sejam R um anel, $a \in R$ e n um inteiro positivo. Definimos

$$na = \underbrace{a + a + \cdots + a}_{n \text{ vezes}}.$$

Se n é negativo, definimos $na = |n|(-a)$. Se $n = 0$, então definimos $na = 0$. Se existe um menor inteiro positivo tal que $na = 0$, para todo $a \in R$, então dizemos que R é um anel de característica n. Caso tal inteiro não exista, dizemos R é um anel de característica zero. Utilizaremos a notação $\text{char}(R) = n$ para dizer que R é um anel de característica n. Por exemplo, para todo $n \geqslant 2$, $\text{char}(\mathbb{Z}_n) = n$ e $\text{char}(\mathbb{Z}) = 0$.

Exercício 1.1.14. Seja R um anel com unidade de característica $n > 0$. Mostre que $\text{char}(R)$ é o menor inteiro positivo tal que $n1 = 0$. Conclua que se R é um domínio com unidade, então $\text{char}(R)$ é um número primo.

Como consequência do exercício anterior, para um corpo F, temos que $\text{char}(F) = 0$ ou $\text{char}(F) = p$, para algum primo p. Em grande parte dos resultados estudados neste livro, consideraremos um corpo F de característica zero.

Agora, veremos como construir corpos a partir de domínios de integridade.

Seja R um domínio de integridade e denote por $R^* = R - \{0\}$. Em $R \times R^*$, defina a seguinte relação:

$$(r, s) \sim (r', s') \text{ se, e somente se, } rs' = r's.$$

Exercício 1.1.15. Mostre que a relação acima é uma relação de equivalência.

A classe de equivalência de $(r, s) \in R \times R^*$ será denotada por r/s. Seja F_R o conjunto das classes de equivalência distintas, isto é,

$$F_R = \{r/s : r \in R, s \in R^*\}.$$

É rotina verificar que F_R com a adição e multiplicação definidas por

1. $r/s + r'/s' = (rs' + r's)/ss'$
2. $(r/s)(r'/s') = rr'/ss'$

para todos $r, s \in R$, $r', s' \in R^*$, é um corpo, chamado de corpo de frações do domínio de integridade R. Observe que se $R = \mathbb{Z}$, então $F_{\mathbb{Z}} = \mathbb{Q}$.

Exercício 1.1.16. Generalize a construção acima como segue. Sejam R um anel (possivelmente sem unidade) e S um subconjunto não vazio de R. Dizemos que S é um subconjunto multiplicativo de R se $r, s \in S$ implica que $rs \in S$. Seja R um anel comutativo. Mostre que:

(a) Se S é um subconjunto multiplicativo de R, então a relação em $R \times S$ definida por $(r, s) \sim (r', s')$ se, e somente se, $s_1(rs' - r's) = 0$, para algum $s_1 \in S$, é uma relação de equivalência. Além disso, se R é um domínio e $0 \notin S$, então $(r, s) \sim (r', s')$ se, e somente se, $rs' - r's = 0$.

(b) Denote por r/s a classe de equivalência de $(r, s) \in R \times S$ e por $S^{-1}R$ o conjunto das classes de equivalências distintas. Mostre que, com a adição e multiplicação definidas acima, $S^{-1}R$ é um anel comutativo. Se $0 \notin S$, então $S^{-1}R$ é um anel comutativo com unidade.

(c) Se $R \neq \{0\}$ é um domínio e $0 \notin S$, então $S^{-1}R$ é um domínio de integridade. Neste caso, conclua que se $S = R^*$, então $S^{-1}R$ é um corpo.

Se R é um anel e $\varnothing \neq S \subseteq R$, dizemos que S é um subanel de R, se é fechado sob as operações de R e é um anel com respeito a essas operações. O exercício a seguir apresenta uma maneira eficiente de garantir que um subconjunto de um anel R é um subanel.

Exercício 1.1.17. Sejam R um anel e S um subconjunto não vazio de R. Mostre que S é um subanel de R se, e somente se, para todos $x, y \in S$, temos $x - y \in S$ e $xy \in S$.

Obviamente, $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ é uma cadeia de subanéis de $\mathbb{C}$. Observamos também que se R um anel, então para todo $n \geqslant 2$, o anel $UT_n(R)$ definido na Equação (1.1) é um subanel de $M_n(R)$. Quando $R = F$ é um corpo, como dissemos, teremos UT_n um subanel de $M_n(F)$. Vejamos abaixo outros exemplos.

Exemplo 1.1.18. O conjunto $\mathbb{H}_{\mathbb{Z}} = \{x_0 + x_1 i + x_2 j + x_3 k : x_0, x_1, x_2, x_3 \in \mathbb{Z}\}$ é um subanel de $\mathbb{H}$. Observe que, apesar de $\mathbb{H}$ ser um anel de divisão, $\mathbb{H}_{\mathbb{Z}}$ não o é, pois $\mathcal{U}(\mathbb{H}_{\mathbb{Z}}) = \{\pm 1, \pm i, \pm j, \pm k\}$.

Exemplo 1.1.19. Dado $n \in \mathbb{Z}$, o conjunto $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$ é um subanel de $\mathbb{Z}$. Note que se $n \neq \pm 1$, então $n\mathbb{Z}$ não é um anel com unidade. Logo, subanéis de anéis com unidade não necessariamente possuem unidade.

Exemplo 1.1.20. Seja R um anel com unidade. O conjunto

$$\left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix} : a, b, c, d \in R \right\}$$

é um subanel de $M_3(R)$, possuindo unidade diferente da unidade de $M_3(R)$.

Exemplo 1.1.21. Dado $a \in (0, 1)$, o conjunto $S = \{f \in \mathcal{C}^0([0, 1]) : f(a) = 0\}$ é um subanel de $\mathcal{C}^0([0, 1])$ sem unidade.

Definimos o centro de um anel R como o conjunto dos elementos que comutam com todos os elementos de R, ou seja,

$$Z(R) = \{r \in R : rx = xr, \text{ para todo } x \in R\}.$$

Um elemento pertencente a $Z(R)$ será dito um elemento central. Observamos que o centro de R é um subanel de R. Além disso, um anel R é comutativo se, e somente se, $Z(R) = R$.

Exercício 1.1.22. Seja R um anel com unidade. Mostre que $Z(M_n(R)) = \{rI_n : r \in Z(R)\}$, para todo $n \geqslant 1$.

Dizemos que um elemento a em um anel R é nilpotente, se $a^n = 0$ para algum $n \geqslant 1$. Por exemplo, se R é um anel com unidade, para todo $n \geqslant 2$, os elementos $e_{ij} \in M_n(R)$, $i \neq j$, são nilpotentes.

Exercício 1.1.23. Mostre que, se R é um anel comutativo e $a, b \in R$ são nilpotentes, então $a + b$ é nilpotente. Mostre que o resultado pode ser falso se R não é comutativo. Conclua que se R é um anel comutativo, então o conjunto $N = \{a \in R : a \text{ é nilpotente}\}$ é um subanel de R.

Exercício 1.1.24. Mostre que, em um anel R, as seguintes condições são equivalentes:

(a) R não possui elementos nilpotentes não nulos.

(b) Se $a \in R$ e $a^2 = 0$, então $a = 0$.

Exercício 1.1.25. Seja a um elemento de um anel com unidade R. Mostre que:

(a) Se $a^n \in \mathcal{U}(R)$, então $a \in \mathcal{U}(R)$.

(b) Se a é nilpotente, então $1 \pm a \in \mathcal{U}(R)$. Neste caso, determine seu inverso.

Um elemento e em um anel R é dito idempotente se $e^2 = e$. Por exemplo, se R é um anel com unidade, para todo $n \geqslant 2$, os elementos da forma $e_{ii} + e_{ij} \in M_n(R)$, $i \neq j$, são idempotentes.

Exercício 1.1.26. Seja R um anel com unidade. Mostre que:

(a) Idempotentes não triviais em R são divisores de zero.

(b) Se R não possui elementos nilpotentes não triviais, então todo idempotente em R é central.

Exercício 1.1.27. Mostre que, se um anel R possui somente elementos idempotentes, então R é comutativo. Anéis com essa propriedade são chamados de anéis booleanos. Dê exemplos de anéis booleanos não nulos.

Seja I um subanel de um anel R. Dizemos que I é um:

1. ideal à esquerda de R, se para todo $r \in R, a \in I, ra \in I$.
2. ideal à direita de R, se para todo $r \in R, a \in I, ar \in I$.
3. ideal bilateral de R, se I é um ideal à direita e à esquerda de R.

Utilizaremos as notações $I \trianglelefteq_l R$, $I \trianglelefteq_r R$ e $I \trianglelefteq R$ para dizer que I é um ideal à esquerda, à direita, bilateral de R, respectivamente. Durante o texto, reservaremos a palavra "ideal" para nos referirmos a ideal bilateral. Observe que se R é um anel comutativo, então todo ideal à esquerda (à direita) de R é um ideal de R.

Observação 1.1.28. Se R é um anel com unidade e I é um ideal (à esquerda, à direita, bilateral) que contém um elemento invertível de R, então $I = R$.

Todo anel não nulo R possui pelos menos 2 ideais: $\{0\}$ e R, chamados de ideais triviais. Um ideal I (à esquerda, à direita, bilateral) de R tal que $I \neq \{0\}$ e $I \neq R$ é chamado de ideal (à esquerda, à direita, bilateral) próprio de R.

Como um exemplo, dado $n \in \mathbb{Z}$, o conjunto $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$. Reciprocamente, se $I \trianglelefteq \mathbb{Z}$, então existe $n \in \mathbb{Z}$ tal que $I = n\mathbb{Z}$.

Também vemos que o conjunto $S = \{f \in \mathcal{C}^0([0,1]) : f(a) = 0\}$, $a \in (0,1)$, é um ideal de $\mathcal{C}^0([0,1])$.

Exemplo 1.1.29. Seja R um anel. No anel das matrizes $M_n(R)$, dado $1 \leqslant k \leqslant n$, o conjunto $C_k = \{(a_{ij}) \in M_n(R) : a_{ij} = 0, \text{ se } j \neq k\}$ é um ideal à esquerda de $M_n(R)$, mas não é um ideal à direita. Analogamente, o conjunto $L_k = \{(a_{ij}) \in M_n(R) : a_{ij} = 0, \text{ se } i \neq k\}$ é um ideal à direita de $M_n(R)$, que não é um ideal à esquerda.

Se R é um anel e $a \in R$, então o conjunto $Ra = \{ra : r \in R\}$ é um ideal à esquerda de R. Analogamente, $aR = \{ar : r \in R\}$ é um ideal à direita de R. Observe que a pode não pertencer ao ideal à esquerda Ra ou ao ideal à direita aR.

Exercício 1.1.30. Seja $\{I_j : j \in \mathcal{I}\}$ uma família de ideais à esquerda de um anel R. Mostre que $\bigcap_{j\in\mathcal{I}} I_j$ também é um ideal à esquerda de R. Mostre que o resultado continua válido para ideais à direita e bilaterais de R.

Dado S um subconjunto de um anel R, podemos construir ideais laterais ou bilaterais a partir de S. Para isso, consideramos $\{I_j : j \in \mathcal{I}\}$ a família de todos os ideais à esquerda de R que contêm S. Então $\bigcap_{j\in\mathcal{I}} I_j$ é chamado de ideal à esquerda de R gerado por S, sendo denotado por $\langle S\rangle_L$. Analogamente, definimos o ideal à direita e o ideal bilateral gerado por S. Neste caso, $\langle S\rangle_R$ denota o ideal à direita gerado por S e $\langle S\rangle$ o ideal gerado por S. Se $S = \{a_1, \ldots, a_m\}$, então denotaremos por $\langle S\rangle_L = \langle a_1, \ldots, a_m\rangle_L$, $\langle S\rangle_R = \langle a_1, \ldots, a_m\rangle_R$ e $\langle S\rangle = \langle a_1, \ldots, a_m\rangle$.

Exercício 1.1.31. Sejam R um anel, $a \in R$ e $S \subset R$. Mostre que:

(a) $\langle a\rangle = \left\{ra + as + na + \sum_{i=1}^{m} r_i a s_i : r, s, r_i, s_i \in R, n \in \mathbb{Z}, m \geqslant 0\right\}$. Se R tem unidade, então $\langle a\rangle = \left\{\sum_{i=1}^{m} r_i a s_i : r_i, s_i \in R, m \geqslant 0\right\}$.

(b) Se R é um anel com unidade e $a \in Z(R)$, então $Ra = aR = \langle a\rangle$.

(c) Se R é um anel com unidade e $S \subset Z(R)$, então

$$\langle S \rangle = \left\{ \sum_{i=1}^{m} r_i a_i : r_i \in R, a_i \in S, m \geqslant 0 \right\}.$$

Observação 1.1.32. Por um abuso de linguagem, se R é um anel e $a \in R$, então diremos que Ra (aR) é o ideal à esquerda (à direita) de R gerado por a mesmo quando $a \notin Ra$ (aR).

Dados $S_1, \ldots, S_n$ subconjuntos de um anel R, denotamos por $S_1 + \cdots + S_n$ o conjunto

$$\{s_1 + \cdots + s_n : s_i \in S_i, i = 1, \ldots, n\}.$$

Além disso, denotamos por $S_1 S_2$ o conjunto de todas as somas finitas

$$\{s_1 s_1' + \cdots + s_n s_n' : s_i \in S_1, s_i' \in S_2, n \geqslant 1\}.$$

Mais geralmente, $S_1 S_2 \cdots S_n$ denota o conjunto de todas as somas finitas de elementos da forma $s_1 s_2 \cdots s_n$, $s_i \in S_i, i = 1, \ldots, n$. No caso particular em que $S_1 = S_2 = \cdots = S_n = S$, denotamos por $S_1 S_2 \cdots S_n = S^n$.

Exercício 1.1.33. Sejam $J_1, \ldots, J_n, I, J, K$ ideais à esquerda de um anel R. Mostre que:

(a) $J_1 + \cdots + J_n$ e $J_1 \cdots J_n$ são ideais à esquerda de R.

(b) $(I + J) + K = I + (J + K)$.

(c) $(IJ)K = IJK = I(JK)$.

(d) $I(J_1 + \cdots + J_n) = IJ_1 + \cdots + IJ_n$ e $(J_1 + \cdots + J_n)K = J_1 K + \cdots + J_n K$.

O exercício continua válido se tomarmos ideais à direita e ideias bilaterais de R.

Se $I \trianglelefteq_l R$, dizemos que I é um ideal à esquerda maximal de R, se $I \neq R$ e para todo ideal à esquerda J de R tal que $I \subset J \subset R$, então $J = I$ ou $J = R$. Analogamente, dizemos que I é um ideal à esquerda minimal de R, se $I \neq \{0\}$ e para todo ideal à esquerda J de R tal que $\{0\} \subset J \subset I$, então ou $J = \{0\}$ ou $J = I$. Da mesma forma, definimos ideais à direita e bilaterais maximais e minimais.

Como um exemplo, vemos que no anel $\mathbb{Z}$, $3\mathbb{Z}$ é um ideal maximal, mas $4\mathbb{Z}$ não o é, pois $4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$.

Exercício 1.1.34. Se D é um anel de divisão, utilizando a notação do Exemplo 1.1.29, mostre que C_k é um ideal à esquerda minimal de $M_n(D)$, para todo $k = 1, \ldots, n$.

Exercício 1.1.35. Mostre que $\mathbb{Z}$ não possui ideais minimais.

Definição 1.1.36. Um anel R é dito um anel simples, se $R^2 \neq \{0\}$ e os únicos ideais de R são $\{0\}$ e R.

Observamos que, se R é um anel com unidade, então a condição $R^2 \neq \{0\}$ é sempre satisfeita. Também, vemos que todo anel de divisão é um anel simples. Generalizando esse fato, temos o seguinte resultado.

Proposição 1.1.37. *Seja D um anel de divisão. Então, para todo $n \geqslant 1$, o anel das matrizes $M_n(D)$ é um anel simples.*

Demonstração. Já sabemos que o resultado vale para $n = 1$, então consideramos $n \geqslant 2$ e tomamos I um ideal de $M_n(D)$. Vamos mostrar que se $I \neq \{0\}$, então $I = M_n(D)$. De fato, se $I \neq \{0\}$, existe $a \in I$ tal que $a \neq 0$. Logo, alguma entrada de a, digamos a_{hk}, é diferente de zero.

Dado $i \in \{1, \ldots, n\}$, seja $b_i = e_{ih} a e_{ki} \in M_n(D)$. Temos que $b_i \in I$ e um cálculo direito nos mostra que $b_i = a_{hk} e_{ii}$. Como I é um ideal, temos que $b = b_1 + \cdots + b_n \in I$. Mas b é uma matriz diagonal, e todos os elementos na diagonal são iguais a $a_{hk} \neq 0$. Como D é um anel de divisão, a_{hk} é invertível e, assim, b é invertível. Portanto, $I = M_n(D)$. □

Exercício 1.1.38. Seja R um anel. Mostre que $I \trianglelefteq M_n(R)$ se, e somente se, existe $I_0 \trianglelefteq R$ tal que $I = M_n(I_0)$. Conclua que, se R é um anel simples, então $M_n(R)$ também o é.

Um conceito importante no estudo de anéis e ideais é o de anel quociente. Para definir esse conceito, inicialmente, para um ideal à esquerda I de um anel R e $a, b \in R$, definimos a relação

$$a \sim b \text{ se, e somente se, } a - b \in I.$$

Exercício 1.1.39. Mostre que a relação acima é uma relação de equivalência.

A classe de equivalência de $a \in R$ pela relação acima será denotada por $\overline{a} = a + I$. Considere o conjunto de todas as classes de equivalência distintas

$$R/I = \{\overline{a} : a \in R\}.$$

Dados $a, b \in R$, definimos a adição de classes em R/I por $\overline{a} + \overline{b} := \overline{a+b}$. Com a adição assim definida, $(R/I, +)$ é um grupo abeliano.

Agora, definimos também um produto de classes por $\overline{a}\overline{b} := \overline{ab}$, que dá uma estrutura de anel para R/I se, e somente se, I é um ideal de R. Neste caso, dizemos que R/I é o anel quociente de R por I.

Exercício 1.1.40. Sejam R um anel com unidade e $I \trianglelefteq R$. Mostre que:

(a) Se I é um ideal maximal e R é comutativo, então R/I é um corpo.

(b) Se R/I é um anel de divisão, então I é um ideal maximal.

(c) Mostre que, se R não tem unidade, então (a) é falso, e dê um exemplo de um anel não comutativo R que possui um ideal maximal I tal que R/I não é um anel de divisão.

Vamos apresentar mais duas definições importantes sobre um anel R. Dizemos que

- R é um anel nil, se todo elemento de R é nilpotente.
- R é um anel nilpotente, se existe $m \in \mathbb{N}$ tal que o produto de quaisquer m elementos em R é nulo, ou seja, $r_1 \cdots r_m = 0$ para quaisquer $r_1, \ldots, r_m \in R$.

Observe que em um anel nil R, para cada elemento $a \in R$, existe $n \in \mathbb{N}$ (que depende de a) tal que $a^n = 0$. Quando existe um natural s tal que $a^s = 0$ para todo $a \in R$, dizemos que R é nil de expoente limitado.

Quando R é um anel nilpotente, o menor natural m, nas condições do segundo item destacado acima, é dito o índice de nilpotência de R. Nesse caso, escrevemos $R^m = \{0\}$.

De modo análogo, um ideal $I \trianglelefteq R$ é dito nilpotente (resp. nil), se é um anel nilpotente (resp. nil). Claramente, todo ideal nilpotente é nil, mas a recíproca não é sempre verdadeira, como pode ser visto no exemplo abaixo.

Exemplo 1.1.41. Seja $\mathbb{Z}[x_1, x_2, \ldots]$ o anel de polinômios nas variáveis comutativas no conjunto $\{x_1, x_2, \ldots\}$ com coeficientes em $\mathbb{Z}$. No anel quociente

$$R = \frac{\mathbb{Z}[x_1, x_2, \ldots]}{\langle x_1^2, x_2^3, x_3^4, \ldots \rangle}$$

o ideal $I = \langle \overline{x}_1, \overline{x}_2, \ldots, \rangle$ é nil, mas não é nilpotente.

Um conceito que será extremamente importante será o de isomorfismo de anéis. Vamos começar definindo homomorfismos.

Definição 1.1.42. Sejam R e S anéis e $f : R \to S$ uma função. Dizemos que f é um homomorfismo (de anéis) se para quaisquer $a, b \in R$, temos que

1. $f(a + b) = f(a) + f(b)$;
2. $f(ab) = f(a)f(b)$.

Exercício 1.1.43. Mostre que, se R e S são anéis e $f : R \to S$ é um homomorfismo, então $f(0) = 0$ e $f(-a) = -f(a)$, para todo $a \in R$.

Se R e S são anéis com unidade 1_R e 1_S, respectivamente, e $f : R \to S$ é um homomorfismo, não necessariamente temos $f(1_R) = 1_S$.

Como um exemplo, vemos que se R é um anel com unidade, e definimos a aplicação $f : M_2(R) \to M_3(R)$ por

$$f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

temos que f é um homomorfismo de anéis, mas $f(I_2) \neq I_3$.

Em alguns casos $f(1_R) = 1_S$, como podemos ver no próximo exercício.

Exercício 1.1.44. Sejam R e S anéis com unidade 1_R e 1_S, respectivamente, e $f : R \to S$ um homomorfismo. Mostre que:

(a) se S é um domínio, então $f(1_R) = 1_S$.

(b) se f é sobrejetiva, então $f(1_R) = 1_S$.

Quando R e S são anéis e $f : R \to S$ é um homomorfismo, dizemos que f é um:

1. monomorfismo, se f é injetiva;
2. epimorfismo, se f é sobrejetiva;
3. isomorfismo, se f é bijetiva.

No caso em que f é um isomorfismo, dizemos que R e S são anéis isomorfos e escrevemos $R \cong S$. Além disso, um homomorfismo $f : R \to R$ é dito um endomorfismo de R e um isomorfismo $f : R \to R$ é dito um automorfismo de R.

Exercício 1.1.45. Seja R um anel e considere

$$End(R) = \{f : R \to R : f \text{ é um endomorfismo}\}.$$

Mostre que, com as operações $(f + g)(r) = f(r) + g(r)$ e $(fg)(r) = f(g(r))$ para todos $f, g \in End(R), r \in R$, $End(R)$ é um anel com unidade.

Dado um homomorfismo de anéis $f : R \to S$, a imagem de f é o conjunto

$$\text{Im}(f) = \{f(r) : r \in R\}$$

e o núcleo de f é o conjunto

$$\text{Ker}(f) = \{r \in R : f(r) = 0\}.$$

Exercício 1.1.46. Mostre que, se $f : R \to S$ é um homomorfismo de anéis, então $\text{Im}(f)$ é um subanel de S e $\text{Ker}(f)$ é um ideal de R. Além disso, mostre que f é um monomorfismo se, e somente se, $\text{Ker}(f) = \{0\}$.

Dados um anel R e $I \trianglelefteq R$, a aplicação

$$\pi : R \to R/I \text{ dada por } \pi(a) = \overline{a}$$

é um epimorfismo de anéis, chamado de projeção canônica (ao quociente). Em geral, se R é um anel e $I \trianglelefteq R$, então existe um anel S e um homomorfismo $f : R \to S$ tal que $I = \text{Ker}(f)$: basta tomarmos $S = R/I$ e $f = \pi$, a projeção canônica.

Exemplo 1.1.47. Se S é um subanel de um anel R, então a aplicação $i : S \to R$ dada por $i(s) = s$ é um monomorfismo, chamado inclusão (ou imersão) canônica.

Em geral, se R e S são anéis e $f : S \to R$ é um monomorfismo, então S pode ser visto como um subanel de R, identificando seus elementos com os elementos de $\text{Im}(f)$. Neste caso, dizemos que S está isomorficamente imerso em R.

Um importante resultado na teoria de anéis é o seguinte.

Teorema 1.1.48. *Todo anel R pode ser imerso em um anel S com unidade. O anel S (que não é único) pode ser escolhido para ter ou característica zero, ou a mesma característica de R.*

Demonstração. Seja $S = R \times \mathbb{Z}$. Em S, defina um novo produto dado por

$$(r_1, n_1) \circ (r_2, n_2) = (r_1 r_2 + n_2 r_1 + n_1 r_2, n_1 n_2)$$

para todo $r_i \in R, n_i \in \mathbb{Z}$. Não é difícil verificar que com esse produto S é um anel com unidade $(0, 1)$ e característica zero. Além disso, a aplicação $f : R \to S$ dada por $f(r) = (r, 0)$ é um monomorfismo de anéis. Se $\text{char}(R) = n > 0$, consideramos $S = R \times \mathbb{Z}_n$ e a multiplicação é dada por

$$(r_1, \overline{n}_1) \circ (r_2, \overline{n}_2) = (r_1 r_2 + n_2 r_1 + n_1 r_2, \overline{n}_1 \overline{n}_2)$$

onde $r_i \in R$ e $\overline{n}_i \in \mathbb{Z}_n$. De maneira análoga ao caso anterior, temos que R pode ser imerso em S e $\text{char}(S) = n$. □

A seguir, enunciaremos os chamados teoremas do isomorfismo de anéis, cujas demonstrações deixaremos a cargo do leitor.

Teorema 1.1.49. *Seja $f : R \to S$ um homomorfismo de anéis. Considere $\pi : R \to R/\text{Ker}(f)$ a projeção canônica, e $i : \text{Im}(f) \to S$ a inclusão canônica. Então existe um único homomorfismo $\bar{f} : R/\text{Ker}(f) \to \text{Im}(f)$ tal que $f = i \circ \bar{f} \circ \pi$. Mais ainda, $\bar{f}$ é um isomorfismo.*

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & S \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ R/\text{Ker}(f) & \xrightarrow[\bar{f}]{} & \text{Im}(f) \end{array}$$

Teorema 1.1.50. *Sejam I e J ideais de um anel R. Então*

$$I/(I \cap J) \cong (I + J)/J.$$

Teorema 1.1.51. *Se I e J são ideais de um anel R tais que $I \subseteq J$, então*

$$(R/I)/(J/I) \cong R/J.$$

Teorema 1.1.52. *Sejam I um ideal de um anel R e $\pi : R \to R/I$ a projeção canônica. Então:*

1. *para cada ideal (à esquerda, à direita, bilateral) J de R que contém I, $\pi(J) = J/I$ é um ideal (do mesmo tipo de J) de R/I.*

2. *Se $\mathcal{J} \trianglelefteq R/I$, então $\pi^{-1}(\mathcal{J}) = \{r \in R : \overline{r} \in \mathcal{J}\}$ é um ideal de R contendo I e $\mathcal{J} = J/I$, para algum $J \trianglelefteq R$ que contém I.*

Teorema 1.1.53. *Sejam R e S anéis e $f : R \to S$ um homomorfismo. Então existe uma correspondência biunívoca entre os ideais de S e os ideais de R que contêm* $\mathrm{Ker}(f)$.

Exercícios V ou F da Seção 1.1: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, R representa um anel.

(1) Se I é um ideal de R e R/I é anel comutativo, então R é comutativo.

(2) Um epimorfismo não nulo $\varphi : F \to R$, onde F é um corpo, é um isomorfismo.

(3) Se R tem unidade e o conjunto dos elementos não invertíveis de R é um ideal, então R admite um único ideal maximal.

(4) Se R é comutativo e I é um ideal de R, então o conjunto dado por $Rad(I) = \{r \in R \mid r^n \in I, \text{ para algum } n\}$ é um ideal de R.

(5) Para todo $m \in \mathbb{N}$, temos que os únicos idempotentes de $\mathbb{Z}_m$ são $\bar{0}$ e $\bar{1}$.

(6) Se F é um corpo, então para quaisquer $\alpha_1, \alpha_2, \alpha_3 \in F$, temos que $\alpha_1 e_{12} + \alpha_2 e_{13} + \alpha_3 e_{23}$ é um elemento nilpotente de $M_3(F)$.

(7) O conjunto $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in R \right\}$ é um ideal de $M_2(R)$.

(8) Para todo $n \in \mathbb{N}$, $M_n(R)$ está isomorficamente imerso em $M_{n+1}(R)$.

1.2 Módulos

É bem conhecido que o conceito de módulos sobre um anel generaliza o conceito de espaços vetoriais sobre um corpo. Nesta seção, apresentaremos os principais resultados sobre módulos que serão utilizados no decorrer do livro. Novamente, esta seção é dispensável aos leitores que tenham conhecimento sobre o assunto. Ao longo da seção, R denotará um anel.

Definição 1.2.1. Um grupo abeliano[2] $(M, +)$ é chamado de um R-módulo (à esquerda), se a cada $r \in R$ e a cada $m \in M$, está associado um elemento $rm \in M$, de modo que as seguintes condições são satisfeitas:

1. $(r_1 + r_2)m = r_1m + r_2m$;
2. $r(m_1 + m_2) = rm_1 + rm_2$;
3. $r_1(r_2m) = (r_1r_2)m$

para todos $r_1, r_2 \in R$, $m_1, m_2 \in M$. Se R é um anel com unidade, definimos

4. $1m = m$, para todo $m \in M$.

De maneira análoga definimos um R-módulo à direita. Ao longo do texto, utilizaremos a expressão R-módulo como uma abreviação de R-módulo à esquerda e todos os resultados feitos para R-módulos à esquerda são válidos para R-módulos à direita.

É fácil verificar que, em um R-módulo, $r0_M = 0_M$, para todo $r \in R$, e $0_Rm = 0_M$, onde 0_R e 0_M denotam os elementos neutros aditivos de R e M, respectivamente. Além disso, para todo $r \in R, m \in M$ e $a \in \mathbb{Z}$, temos

$$(-r)m = -(rm) = r(-m) \text{ e } a(rm) = r(am)$$

onde, am tem os mesmo significado como definido para anéis.

Obviamente, anéis e grupos abelianos são $\mathbb{Z}$-módulos e, quando R é um corpo, temos que os R-módulos são os espaços vetoriais sobre R.

Se S é um subanel de R, então R é um S-módulo, mas, em geral, S não é um R-módulo. No entanto, se $I \trianglelefteq_l R$, então I é um R-módulo. Em particular, R é um R-módulo sobre si próprio. Além disso, se $I \trianglelefteq_l R$, então R/I é um grupo abeliano e um R-módulo se definirmos $r\overline{r_1} = \overline{rr_1}$, para todos $r, r_1 \in R$.

Exemplo 1.2.2. Se $f : R \to S$ é um homomorfismo de anéis, então todo S-módulo M pode ser visto como um R-módulo, definindo $rm = f(r)m$, para todo $r \in R, m \in M$.

Exercício 1.2.3. Sejam R um anel comutativo e M um R-módulo à esquerda. Mostre que o produto dado por $mr := rm$, para todo $r \in R, m \in M$, dá uma estrutura de R-módulo à direita para M (e vice-versa).

[2]O leitor interessado deve ver no Capítulo 2 uma definição geral de grupo.

Definição 1.2.4. Sejam M um R-módulo e $\varnothing \neq N \subseteq M$. Dizemos que N é um R-submódulo de M se para todos $n_1, n_2 \in N$ e $r \in R$, temos que:

1. $n_1 + n_2 \in N$;
2. $rn_1 \in N$.

Utilizaremos a notação $N \leqslant M$ para indicar que N é um R-submódulo de M.

Note que os R-submódulos de um anel R são seus ideais à esquerda. Também, se R é um corpo e V é um R-espaço vetorial, então os R-submódulos de V são seus subespaços vetoriais.

A partir de dois R-submódulos N_1, N_2 de um R-módulo M, podemos construir o conjunto

$$N_1 + N_2 = \{n_1 + n_2 : n_1 \in N_1, n_2 \in N_2\}$$

que é um R-submódulo de M, chamado de soma de N_1 e N_2.

Exemplo 1.2.5. Sejam M um R-módulo e N um R-submódulo de M. Assim, como no caso de anéis, o conjunto quociente M/N tem estrutura de R-módulo, definindo $r\overline{m} = \overline{rm}$, para todo $r \in R$, $m \in M$. O R-módulo M/N é chamado de R-módulo quociente de M por N.

Exemplo 1.2.6. Sejam $I \trianglelefteq_l R$, M um R-módulo e N um subconjunto não vazio de M. Então

$$IN = \left\{ \sum_{i=1}^{m} r_i n_i : r_i \in I, n_i \in N, m \geqslant 1 \right\}$$

é um R-submódulo de M. Em particular, se $m \in M$, $Im = \{rm : r \in I\}$ é um R-submódulo de M.

Exercício 1.2.7. Sejam $I \trianglelefteq R$ e M um R-módulo. Mostre que M/IM tem estrutura de R/I-módulo, com produto dado por $(r + I)(m + IM) = rm + IM$.

Exemplo 1.2.8. Se $\{N_i : i \in \mathcal{I}\}$ é uma família de R-submódulos de um R-módulo M, então $\bigcap_{i \in \mathcal{I}} N_i$ é um R-submódulo de M.

Se X é um subconjunto não vazio de um R-módulo M, então a interseção de todos os R-submódulos de M que contêm X é chamado de R-submódulo gerado por X e é denotado por $\langle X \rangle$. Se X contém um único elemento $m \in M$, então o R-submódulo gerado por X é chamado de R-submódulo cíclico gerado por m, denotado por $\langle m \rangle$.

Assim como no caso de anéis, temos o seguinte exercício.

Exercício 1.2.9. Sejam M um R-módulo, X um subconjunto não vazio de M e $m \in M$. Mostre que:

(a) $\langle m \rangle = \{rm + nm : r \in R, n \in \mathbb{Z}\}$. Se R tem unidade, então $\langle m \rangle = Rm$.

(b) $\langle X \rangle = \left\{ \sum_{i=1}^{s} r_i m_i + \sum_{j=1}^{t} n_j m_j : m_i, m_j \in X, r_i \in R, n_j \in \mathbb{Z}, s, t \geqslant 1 \right\}$.

Se R tem unidade, então

$$\langle X \rangle := RX = \left\{ \sum_{i=1}^{s} r_i m_i : m_i \in X, r_i \in R, s \geqslant 1 \right\}.$$

Se X é um subconjunto não vazio de um R-módulo M tal que $M = \langle X \rangle$, então dizemos que X gera M. Se X é finito, então dizemos que M é um R-módulo finitamente gerado.

Assim, como no caso de anéis, se M é um R-módulo e $m \in M$, então Rm será chamado de R-módulo cíclico gerado por m, mesmo que $m \notin Rm$.

Como já observamos, se R é um corpo, então todo R-módulo V é um R-espaço vetorial. Neste caso, se X é um subconjunto não vazio de V, então utilizaremos a notação $\text{span}_R\{X\}$ para denotar o R-subespaço vetorial de V gerado por X.

Na Seção 1.1, definimos o conceito de homomorfismo de anéis. Agora vamos entender o significado de homomorfismo de R-módulos.

Definição 1.2.10. Seja $f : M \to N$ uma função entre dois R-módulos M e N. Dizemos que f é um homomorfismo de R-módulos (ou um R-homomorfismo), se para todos $m, n \in M$, $r \in R$, temos que:

1. $f(m + n) = f(m) + f(n)$;
2. $f(rm) = rf(m)$.

Observe que se R é um corpo, então um R-homomorfismo é uma aplicação linear entre espaços vetoriais.

Os conceitos de monomorfismo, epimorfismo, endomorfismo e isomorfismo são definidos analogamente como no caso de anéis, bem como os conceitos de $\text{Ker}(f)$, o núcleo de f, e $\text{Im}(f)$, a imagem de f. Também usaremos a notação $M \cong N$ para indicar que M e N são R-módulos isomorfos.

Exercício 1.2.11. Sejam M, N R-módulos e $f : M \to N$ um R-homomorfismo. Mostre que $\text{Ker}(f)$ é um R-submódulo de M e $\text{Im}(f)$ é um R-submódulo de N. Além disso, mostre que f é um monomorfismo se, e somente se, $\text{Ker}(f) = \{0\}$.

Ressaltamos que os Teoremas 1.1.49 a 1.1.53 são válidos para R-módulos, com as devidas alterações. Além disso, como no Exercício 1.1.45, o conjunto

$$End_R(M) = \{f : M \to M : f \text{ é um endomorfismo}\}$$

é um anel com unidade. Adicionalmente, dados $r \in R$ e $f \in End_R(M)$, definimos $(rf)(m) = rf(m)$, para todo $m \in M$. Nessas condições, $End_R(M)$ é um R-módulo.

Exercício 1.2.12. Sejam M, N R-módulos. Mostre que o conjunto

$$Hom_R(M, N) = \{f : M \to N : f \text{ é um } R\text{-homomorfismo}\}$$

é um R-módulo com as operações usuais. Em particular, quando $M = N$, temos $Hom_R(M, M) = End_R(M)$.

Exercício 1.2.13. Sejam V um espaço vetorial sobre um corpo R e $T \in End_R(V)$. Se $f(x) = \sum_{i=1}^{n} a_i x^i \in R[x]$, defina $f(T) = \sum_{i=1}^{n} a_i T^i \in End_R(V)$. Considere V como um $R[x]$-módulo com estrutura definida por $f(x)v = f(T)(v)$, para todo $v \in V$, $f(x) \in R[x]$. Mostre que os $R[x]$-submódulos de V são os subespaços de V que são T-invariantes, isto é, os subespaços W de V tais que $T(W) \subseteq W$.

Definição 1.2.14. Dizemos que um R-módulo M é um R-módulo simples, se $RM \neq \{0\}$ e os únicos R-submódulos de M são $\{0\}$ e M.

Observe que esta definição é parecida com a Definição 1.1.36, mas, quando vemos um anel R como um R-módulo sobre si mesmo, as noções são bem diferentes.

Exemplo 1.2.15. Vimos, na Proposição 1.1.37, que se D é um anel de divisão, então $M_n(D)$ é um anel simples. No entanto, $M_n(D)$ não é um $M_n(D)$-módulo simples, pois os conjuntos C_k, definidos no Exemplo 1.1.29, são $M_n(D)$-submódulos de $M_n(D)$.

A seguir, vamos caracterizar os R-módulos simples. Antes, precisamos da seguinte definição.

Definição 1.2.16. Um ideal à esquerda I de um anel R é regular (à esquerda) se existe $s \in R$ tal que $r - rs \in I$, para todo $r \in R$. Analogamente, definimos ideal regular à direita e ideal bilateral regular.

Observe que se R é um anel com unidade, então todo ideal (à esquerda, à direita, bilateral) de R é regular (basta tomar $s = 1_R$).

Proposição 1.2.17. *Seja M um R-módulo. São equivalentes:*

1. *M é simples;*
2. *M é cíclico e todo elemento não nulo gera M;*
3. *$M \cong R/I$, para algum ideal à esquerda maximal regular de R.*

Demonstração. [(1) $\Rightarrow$ (2)] Como M é simples, $RM \neq \{0\}$. Seja $m \in M, m \neq 0$, tal que $Rm \neq \{0\}$. Então Rm é um submódulo não nulo de M e como M é simples, devemos ter $M = Rm$.

[(2) $\Rightarrow$ (3)] Seja $m \in M, m \neq 0$, e seja $f : R \to M = Rm$ definida por $f(r) = rm$. Então f é um epimorfismo de R-módulos e $M \cong R/\mathrm{Ker}(f)$. Com isso, para todo $J \trianglelefteq_l R$ tal que $\mathrm{Ker}(f) \subset J$, $J/\mathrm{Ker}(f) \neq \{\bar{0}\}$ é um submódulo de M que, por hipótese, deve ser igual a M. Portanto $J = R$ e $\mathrm{Ker}(f)$ é maximal. Para ver que $\mathrm{Ker}(f)$ é regular, como $M = Rm$, $m = sm$, para algum $s \in R$. Consequentemente, para todo $r \in R$, $rm = r(sm) = (rs)m$. Logo, $r - rs \in \mathrm{Ker}(f)$, para todo $r \in R$ e, portanto, $\mathrm{Ker}(f)$ é regular.

[(3) $\Rightarrow$ (1)] Suponha que $M \cong R/I$, onde I é um ideal à esquerda maximal regular de R. Como I é regular, $R(R/I) \neq \{0\}$. De fato, se $R(R/I) = \{0\}$, então, para todo $r \in R$, $r\bar{s} = \bar{0}$ e, consequentemente, $rs \in I$. Como $r - rs \in I$, temos que $r \in I$ e, assim, $R = I$, contrariando a maximalidade de I. Seja N um R-submódulo não nulo de $M \cong R/I$. Então existe $J \trianglelefteq_l R, I \subset J$ tal que $N \cong J/I$. Como I é maximal, devemos ter $J = R$ e, portanto, $N = M$.

□

Exercício 1.2.18. Mostre que M é um $\mathbb{Z}$-módulo simples se, e somente se, M é finito e $|M| = p$, p primo. Conclua que se R é um anel tal que $R^2 = \{0\}$ e R não possui ideais não triviais, então R é um grupo abeliano com p elementos, onde o produto de quaisquer dois elementos de R é nulo.

A seguir, apresentamos um importante resultado sobre R-módulos simples, conhecido como Lema de Schur.

Lema 1.2.19 (Schur)**.** *Sejam M, N R-módulos simples. Então:*

1. *Todo R-homomorfismo não nulo $f : M \to N$ é um isomorfismo;*
2. *$End_R(M)$ é um anel de divisão.*

Demonstração. Para demonstrar o primeiro item, basta lembrarmos que $\mathrm{Ker}(f)$ é um R-submódulo de M e $\mathrm{Im}(f)$ é um R-submódulo de N. Com isso, como f é não nulo, $\mathrm{Ker}(f) \neq M$ e como M é simples, temos que $\mathrm{Ker}(f) = \{0\}$ e, assim, f é injetiva. Por outro lado, como $\mathrm{Im}(f) \neq \{0\}$, usando a simplicidade de N obtemos que $\mathrm{Im}(f) = N$ e, portanto, f é um isomorfismo. Para verificar que $End_R(M)$ é um anel divisão, basta observar que se $f \in End_R(M)$ é não nulo, utilizando a simplicidade de M e os argumentos acima, obtemos que f é invertível. □

Dados dois R-módulos M e N, podemos construir um novo R-módulo $M \times N$, definindo para todos $m_1, m_2, m \in M, n_1, n_2, n \in N$ e $r \in R$

1. $(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$;
2. $r(m, n) = (rm, rn)$.

Agora, seja $\{M_i\}_{i \in \mathcal{I}}$ uma família de R-módulos e consideremos

$$M = \prod_{i \in \mathcal{I}} M_i = \{(m_i)_{i \in \mathcal{I}} : m_i \in M_i\}.$$

Em M, definimos

1. $(m_i)_{i \in \mathcal{I}} + (m_i')_{i \in \mathcal{I}} = (m_i + m_i')_{i \in \mathcal{I}}$;
2. $r(m_i)_{i \in \mathcal{I}} = (rm_i)_{i \in \mathcal{I}}, r \in R$.

Com as operações assim definidas, M é um R-módulo, chamado de produto direto (externo) da família $\{M_i\}_{i \in \mathcal{I}}$.

Agora, sejam $\{M_i\}_{i \in \mathcal{I}}$ uma família de R-módulos e $M = \prod_{i \in \mathcal{I}} M_i$. Uma sequência $(m_i)_{i \in \mathcal{I}} \in M$ tal que $m_i = 0$, exceto para um número finito de índices, é chamada de sequência quase nula. O conjunto de todas as sequências quase nulas de M é chamado de soma direta (externa) da família $\{M_i\}_{i \in \mathcal{I}}$ e é denotada por $\bigoplus_{i \in \mathcal{I}} M_i$. Quando $\mathcal{I} = \{1, 2, \ldots, k\}$ é finito, a soma e o produto direto da família $\{M_i\}_{i \in \mathcal{I}}$ coincidem e escreveremos $M_1 \oplus \cdots \oplus M_k$. Se na soma direta $M_1 \oplus \cdots \oplus M_k$ os R-módulos M_i são iguais a um R-módulo fixo M, então denotaremos $M_1 \oplus \cdots \oplus M_k$ por $M^{(n)}$.

Exercício 1.2.20. Sejam $\{M_i\}_{i \in \mathcal{I}}$ uma família de R-módulos, $\prod_{i \in \mathcal{I}} M_i$ e $\bigoplus_{i \in \mathcal{I}} M_i$ o produto direto e a soma direta desta família, respectivamente. Mostre que:

(a) $\bigoplus_{i\in\mathcal{I}} M_i$ é um R-submódulo de $\prod_{i\in\mathcal{I}} M_i$.

(b) Para cada $k \in \mathcal{I}$, a projeção canônica $\pi_k \colon \prod_{i\in\mathcal{I}} M_i \to M_k$ é um epimorfismo de R-módulos.

(c) Para cada $k \in \mathcal{I}$, a imersão canônica $i_k \colon M_k \to \bigoplus_{i\in\mathcal{I}} M_i$ é um monomorfismo de R-módulos.

Exercício 1.2.21. Consideremos $M, M_1, \ldots, M_k$ como R-módulos. Mostre que $M \cong M_1 \oplus \cdots \oplus M_k$ se, e somente se, para cada $j = 1, \ldots, k$, existem R-homomorfismos $\pi_j \colon M \to M_j$ e $i_j \colon M_j \to M$ tais que:

(a) $\pi_j \circ i_j = id_{M_j}$, para $j = 1, 2, \ldots, k$.

(b) $\pi_j \circ i_l = 0$, se $j \neq l$.

(c) $i_1 \circ \pi_1 + \cdots + i_k \circ \pi_k = id_M$.

Se $\{M_i\}_{i\in\mathcal{I}}$ é uma família de R-módulos, o R-módulo gerado por esta família é chamado de soma dos módulos M_i e é denotado por $\sum_{i\in\mathcal{I}} M_i$. Quando $\mathcal{I} = \{1, 2, \ldots, k\}$ é finito, denotamos esta soma por $M_1 + \cdots + M_k$. É fácil verificar que $\sum_{i\in\mathcal{I}} M_i$ consiste de todas as somas finitas $m_{i_1} + \cdots + m_{i_k}$, onde $m_{i_j} \in M_{i_j}$.

A próxima proposição caracteriza a soma direta de R-módulos.

Proposição 1.2.22. *Seja $\{M_i\}_{i\in\mathcal{I}}$ uma família de R-submódulos de um R-módulo M. São equivalentes:*

1. *Todo elemento $m \in M$ se escreve de modo único na forma $m = \sum_{i\in\mathcal{I}} m_i$, onde $m_i \in M_i$, para todo $i \in \mathcal{I}$, e a sequência $(m_i)_{i\in\mathcal{I}}$ é quase nula;*
2. *$M = \sum_{i\in\mathcal{I}} M_i$ e se $\sum_{i\in\mathcal{I}} m_i = 0$, então $m_i = 0$, para todo $i \in \mathcal{I}$;*
3. *$M = \sum_{i\in\mathcal{I}} M_i$ e $M_j \cap \left(\sum_{i\neq j} M_i\right) = \{0\}$, para todo $j \in \mathcal{I}$.*

Um R-módulo M que satisfaz uma das condições acima (e portanto, todas) é chamado de soma direta (interna) da família $\{M_i\}_{i\in\mathcal{I}}$. Nas condições acima, temos que $M \cong \bigoplus_{i\in\mathcal{I}} M_i$.

Demonstração. É imediato que (1) $\Rightarrow$ (2). Para mostrar que (2) $\Rightarrow$ (3), seja $m \in M_j \cap \left(\sum_{i \neq j} M_i \right)$. Então $m \in M_j$ e $m \in \sum_{i \neq j} M_i$. Logo, $\sum_{i \neq j} m_i - m = 0$ e portanto $m = 0$. Para verificar que (3) $\Rightarrow$ (1), como $M = \sum_{i \in \mathcal{I}} M_i$, dado $m \in M$, existe uma sequência quase nula $(m_i)_{i \in \mathcal{I}}$ tal que $m = \sum m_i$. Suponha que $m = \sum m'_i$, onde $(m'_i)_{i \in \mathcal{I}}$ é outra sequência quase nula. Então, para todo $j \in \mathcal{I}, m_j - m'_j = \sum_{i \neq j} (m_i - m'_i) \in M_j \cap \left(\sum_{i \neq j} M_i \right) = \{0\}$. Portanto $m_j = m'_j$, para todo $j \in \mathcal{I}$, e a escrita é única. Com isso, o isomorfismo $M \cong \bigoplus_{i \in \mathcal{I}} M_i$ é claro. □

Observamos que para todo R-módulo M, temos $M = M \oplus \{0\}$.

Como um exemplo de soma direta de R-submódulos, consideremos o $\mathbb{Z}$-módulo $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \ldots, \overline{5}\}$. Os conjuntos $M_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $M_2 = \{\overline{0}, \overline{3}\}$ são $\mathbb{Z}$-submódulos de $\mathbb{Z}_6$ tais que $M_1 \cap M_2 = \{\overline{0}\}$ e $\mathbb{Z}_6 = M_1 + M_2$. Portanto, $\mathbb{Z}_6 = M_1 \oplus M_2$.

Em geral, deixamos como exercício o seguinte resultado.

Exercício 1.2.23. Mostre que, se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ é a fatoração em primos de um inteiro positivo n, então $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{\alpha_k}}$ como $\mathbb{Z}$-módulos.

Exercício 1.2.24. Com a notação do Exemplo 1.1.29, mostre que $M_n(R) = C_1 \oplus \cdots \oplus C_n$ como $M_n(R)$-módulos.

Exercício 1.2.25. Sejam $\{M_i\}_{i \in \mathcal{I}}$ uma família de R-módulos e N um R-módulo. Mostre que:

(a) $Hom_R \left(\bigoplus_{i \in \mathcal{I}} M_i, N \right) \cong \prod_{i \in \mathcal{I}} Hom_R(M_i, N)$;

(b) $Hom_R \left(N, \prod_{i \in \mathcal{I}} M_i \right) \cong \prod_{i \in \mathcal{I}} Hom_R(N, M_i)$.

Observação 1.2.26. Tudo que fizemos até agora com relação a somas e produtos diretos de R-módulos pode ser estendido para a classe dos anéis de maneira natural. Se $\{R_i\}_{i \in \mathcal{I}}$ é uma família de anéis, então o conjunto $R = \prod_{i \in \mathcal{I}} R_i$ é um anel, com produto dado por $(r_i)_{i \in \mathcal{I}}(r'_i)_{i \in \mathcal{I}} = (r_i r'_i)_{i \in \mathcal{I}}$ e adição definida como no caso de R-módulos. Da mesma forma, definimos a soma direta da família $\{R_i\}_{i \in \mathcal{I}}$ e, com as devidas alterações, os resultados exibidos são válidos na classe dos anéis.

Seja $N_1 \leqslant M$, onde M é um R-módulo. Dizemos que N_1 é um somando direto de M se existe $N_2 \leqslant M$ tal que $M = N_1 \oplus N_2$.

Lema 1.2.27. *Sejam M um R-módulo, $N_1, N_2 \leqslant M$, e suponha que $M = N_1 \oplus N_2$. Então $M/N_1 \cong N_2$.*

Demonstração. Como $M = N_1 \oplus N_2$, dado $m \in M$, existem $n_1 \in N_1, n_2 \in N_2$ tais que $m = n_1 + n_2$. Defina $f : M \to N_2$ por $f(n_1 + n_2) = n_2$. Então f é um epimorfismo com $\mathrm{Ker}(f) = N_1$. □

Corolário 1.2.28. *$\mathbb{Z}$, como $\mathbb{Z}$-módulo, não possui somandos diretos não triviais.*

Demonstração. Como sabemos, os $\mathbb{Z}$-submódulos de $\mathbb{Z}$ são cíclicos. Logo, suponha que $\mathbb{Z} = \langle m \rangle \oplus N$, para algum $N \leqslant \mathbb{Z}$. Assim, $N \cong \mathbb{Z}/\langle m \rangle = \mathbb{Z}_m$, mas, como $\mathbb{Z}$ não possui submódulos finitos, chegamos em um absurdo. □

Corolário 1.2.29. *Sejam M um R-módulo e $N \leqslant M$. Se $N_1, N_2 \leqslant M$ são tais que $M = N \oplus N_1 = N \oplus N_2$, então $N_1 \cong N_2$.*

A seguir, daremos uma caracterização de somandos diretos em um R-módulo M.

Proposição 1.2.30. *Sejam M um R-módulo e $N \leqslant M$. Então N é um somando direto de M se, e somente se, existe $f \in End_R(M)$ tal que $f^2 = f$ e $\mathrm{Im}(f) = N$.*

Demonstração. Suponha que N é um somando direto de M. Então $M = N \oplus N'$, para algum $N' \leqslant M$. Consideremos

$$f : M = N \oplus N' \to N$$

dada por $f(n + n') = n$. Claramente, $\mathrm{Im}(f) = N$ e $f(f(n + n')) = f(n) = f(n + n')$.

Reciprocamente, seja $f \in End_R(M)$ tal que $f^2 = f$ e $\mathrm{Im}(f) = N$. Afirmamos que $M = \mathrm{Ker}(f) \oplus \mathrm{Im}(f)$. De fato, primeiramente observe que $m = (m - f(m)) + f(m)$ e que $m - f(m) \in \mathrm{Ker}(f)$, já que $f^2 = f$.

Agora, se $m \in \mathrm{Ker}(f) \cap \mathrm{Im}(f)$, então $f(m) = 0$ e existe $m' \in M$ tal que $f(m') = m$. Como $f^2 = f$, temos que $m = f(m') = f(f(m')) = f(m) = 0$. Com isso $m = 0$ e $M = \mathrm{Ker}(f) \oplus \mathrm{Im}(f)$, conforme afirmamos. Portanto, $\mathrm{Im}(f) = N$ é um somando direto de M. □

Agora, queremos estender a noção familiar de base de um espaço vetorial para a classe dos módulos sobre um anel.

Definição 1.2.31. Um conjunto $S = \{m_i\}_{i\in\mathcal{I}}$ de elementos de um R-módulo M é chamado de linearmente independente (ou R-livre), se para toda combinação linear finita de elementos de S com coeficiente em R

$$r_{i_1}m_{i_1} + \cdots + r_{i_t}m_{i_t} = 0$$

implica que $r_{i_1} = \cdots = r_{i_t} = 0$.

Definição 1.2.32. Um conjunto $S = \{m_i\}_{i\in\mathcal{I}}$ de elementos de um R-módulo M é chamado de base de M sobre R (ou uma R-base de M), se é linearmente independente e gera M. Se um R-módulo M possui uma R-base, então dizemos que M é livre. Dizemos que M é livre de posto finito, se M possui uma R-base finita.

Nem todo R-módulo possui uma R-base. Como um exemplo, consideremos $\mathbb{Z}_n$ como $\mathbb{Z}$-módulo. Para todo $\overline{r} \in \mathbb{Z}_n$, temos que $n\overline{r} = \overline{0}$ e $n \neq 0$ em $\mathbb{Z}$. Isto nos diz que nenhum subconjunto de $\mathbb{Z}_n$ é linearmente independente sobre $\mathbb{Z}$ e, portanto, $\mathbb{Z}_n$ não possui uma $\mathbb{Z}$-base.

Exemplo 1.2.33. Se R é uma anel com unidade, então $R \oplus R$ é livre. De fato, o conjunto $\{(1,0),(0,1)\}$ é uma R base de $R \oplus R$. Em geral, se $\mathcal{I}$ é um conjunto arbitrário de índices, denote por $R^{(\mathcal{I})}$ a soma direta de $|\mathcal{I}|$ cópias de R, isto é, $R^{(\mathcal{I})} = \bigoplus_{i\in\mathcal{I}} R_i$, onde $R_i = R$, para todo $i \in \mathcal{I}$. Então $R^{(\mathcal{I})}$ é livre, com R-base dada por $\{e_i : i \in \mathcal{I}\}$, onde, $e_j = (r_i)_{i\in\mathcal{I}}$ são tais que $r_j = 1$ e $r_i = 0$, se $i \neq j$.

O exemplo anterior pode ser generalizado como no seguinte teorema.

Teorema 1.2.34. *Sejam R um anel com unidade e M um R-módulo. Então M é livre se, e somente se, M é soma direta de uma família de R-módulos cíclicos, sendo cada um deles isomorfo a R como R-módulo.*

Demonstração. Suponha que M é livre e seja $\mathcal{B}$ uma R-base de M. Dado $m \in \mathcal{B}$, a aplicação $f : R \to Rm$ dada por $f(r) = rm$ é um epimorfismo de R-módulos. Como $\mathcal{B}$ é linearmente independente, se $rm = 0$, então $r = 0$. Logo, f é injetiva e $R \cong Rm$, como R-módulos. Portanto, como $\mathcal{B}$ é uma R-base de M, pela Proposição 1.2.22, $M \cong \bigoplus_{m\in\mathcal{B}} Rm$.

Reciprocamente, suponha que $M \cong R^{(\mathcal{I})}$, para algum conjunto $\mathcal{I}$. Pelo Exemplo 1.2.33, $\{e_i : i \in \mathcal{I}\}$ é uma R-base de $R^{(\mathcal{I})}$. Utilizando o isomorfismo $M \cong R^{(\mathcal{I})}$ obtemos uma R-base de M. Portanto, M é livre. □

Observação 1.2.35. Se R é um anel com unidade, a demonstração do teorema anterior nos mostra como construir um R-módulo livre a partir de um conjunto X. De fato, seja $M = R^{(X)}$. Na notação da demonstração, $\{e_x : x \in X\}$ é uma base de M e, então, $M \cong \bigoplus_{x \in X} Re_x$. Identificando e_x com x, M pode ser escrito como $\bigoplus_{x \in X} Rx$ e, com essa identificação, X é uma R-base de M. Neste caso, dizemos que M é o R-módulo livremente gerado por X.

No exercício a seguir, o leitor pode verificar algumas diferenças entre R-módulos livres e espaços vetoriais.

Exercício 1.2.36. Dê exemplos de:

(a) Um conjunto gerador de um R-módulo M, que não contém uma base de M.

(b) Um conjunto linearmente independente de elementos de um R-módulo M, que não está contido em uma base de M.

(c) Um R-submódulo de um R-módulo livre, que não é livre.

Exercício 1.2.37. Seja R um anel com unidade. Mostre que todo R-módulo é isomorfo ao quociente de algum R-módulo livre.

Agora, vamos introduzir o conceito de produto tensorial de R-módulos. Para isso, vamos dar uma motivação considerando V um espaço vetorial de dimensão finita sobre um corpo F e K um corpo que contém F. Vamos estender V a um espaço vetorial sobre K da seguinte maneira: seja $\{v_1, \ldots, v_n\}$ uma base de V sobre F. Então $V^K = \text{span}_K\{v_1, \ldots, v_n\}$ é um espaço vetorial sobre K que contém V. Esse processo depende da base escolhida de V sobre F. Além disso, esse processo não pode ser estendido à classe dos R-módulos, pois um R-módulo pode não possuir uma base. A seguir, iremos fornecer uma construção que generaliza o processo acima.

No que segue, utilizaremos a seguinte notação: ${}_RM$ denotará um R-módulo à esquerda e M_R denotará um R-módulo à direita.

Observação 1.2.38. Como vimos no Exercício 1.2.3, se R é um anel comutativo, então todo R-módulo à esquerda é um R-módulo à direita. A partir de agora, todo módulo M sobre um anel comutativo R será um R-módulo à direita e à esquerda via $rm = mr$, para todo $m \in M, r \in R$.

Definição 1.2.39. Sejam M_R e ${}_RN$ R-módulos e L o $\mathbb{Z}$-módulo livremente gerado pelo conjunto $M \times N$. Seja W o $\mathbb{Z}$-submódulo de L gerado pelos elementos

1. $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$;
2. $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$;
3. $(mr, n) - (m, rn)$,

para todo $m_1, m_2, m \in M$, $n_1, n_2, n \in N$, $r \in R$. O $\mathbb{Z}$-módulo quociente $T = L/W$ é chamado de produto tensorial de M e N e é denotado por $M \otimes_R N$. A classe $\overline{(m,n)} \in T$ é denotada por $m \otimes n$ e a classe $\overline{(0,0)} \in T$ é denotada por 0.

Assim, os geradores $m \otimes n$ de $M \otimes_R N$ satisfazem as seguintes relações:

1. $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$;
2. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$;
3. $mr \otimes n = m \otimes rn$

para todo $m_1, m_2, m \in M$, $n_1, n_2, n \in N$, $r \in R$. Como consequência da relação 3 acima, temos que, para todo $m \in M$ e $n \in N$,

$$m \otimes 0 = 0 \otimes n = 0 \otimes 0 = 0.$$

Um elemento típico de L é a soma $\sum_{i=1}^{n} \alpha_i (m_i, n_i)$, $\alpha_i \in \mathbb{Z}, m_i \in M, n_i \in N$. Assim, uma classe em T é da forma $\sum_{i=1}^{n} \alpha_i (m_i \otimes n_i)$. Com isso, deve ficar claro que um elemento de $M \otimes_R N$ não necessariamente é da forma $m \otimes n$, $m \in M, n \in N$. Como estamos trabalhando com classes, é possível que $m \otimes n = m' \otimes n'$ em $M \otimes_R N$, mas $m \neq m'$ e $n \neq n'$: basta observar que, como acima, 0 pode ser escrito de várias maneiras diferentes. Além disso, é possível que $M \otimes_R N = \{0\}$, mesmo que $M \neq \{0\}$ e $N \neq \{0\}$.

Exemplo 1.2.40. Se $m \geqslant 2$, então $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_m = \{0\}$. De fato, seja $\frac{a}{b} \otimes \overline{n}$ um gerador de $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_m$. Então

$$\frac{a}{b} \otimes \overline{n} = \frac{a}{bm} m \otimes \overline{n} = \frac{a}{bm} \otimes m\overline{n} = \frac{a}{bm} \otimes \overline{0} = 0.$$

Exercício 1.2.41. Mostre que se $R = \mathbb{Z}$, então a condição 3, da Definição 1.2.39, é consequência das condições 1 e 2.

Exercício 1.2.42. Mostre que se $m, n \in \mathbb{Z}$ são tais que $mdc(m,n) = 1$, então $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}$.

Agora, vamos mostrar a unicidade do produto tensorial. Para isso, precisamos da seguinte definição.

Definição 1.2.43. Sejam M_R e ${}_RN$ R-módulos e P um $\mathbb{Z}$-módulo. Dizemos que uma aplicação $f : M \times N \to P$ é uma aplicação balanceada se satisfaz:

1. $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$;
2. $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$;
3. $f(mr, n) = f(m, rn)$

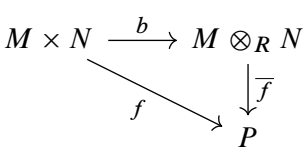
para todo $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ e $r \in R$.

É fácil verificar que $b : M \times N \to M \otimes_R N$ dada por $b(m,n) = m \otimes n$ é uma aplicação balanceada, chamada de aplicação balanceada canônica. Considerando os R-módulos M_R e ${}_RN$ e um $\mathbb{Z}$-módulo P, a importância dessa aplicação é dada no próximo teorema.

Teorema 1.2.44. *Se $f : M \times N \to P$ é uma aplicação balanceada, então existe um único $\mathbb{Z}$-homomorfismo $\bar{f} : M \otimes_R N \to P$ tal que $\bar{f} \circ b = f$. Além disso, o produto tensorial $M \otimes_R N$ é unicamente determinado, a menos de isomorfismos, por esta propriedade.*

Demonstração. Sejam L e W como na Definição 1.2.39. Como $M \times N$ é uma $\mathbb{Z}$-base de L, a aplicação $f : M \times N \to P$ se estende a um único $\mathbb{Z}$-homomorfismo $f' : L \to P$. Como f é balanceada, temos que $W \subseteq \mathrm{Ker}(f')$.

Afirmamos que a aplicação $\bar{f} : L/W = M \otimes_R N \to P$ dada por $\bar{f}(m \otimes n) = f'(m,n)$ é um $\mathbb{Z}$-homomorfismo bem definido.



De fato, se $m \otimes n = m' \otimes n'$, então $(m,n) - (m',n') \in W$. Como $W \subseteq \mathrm{Ker}(f')$, $f'(m,n) = f'(m',n')$ e, portanto, $\bar{f}(m \otimes n) = \bar{f}(m' \otimes n')$.

Com isso, $(\bar{f} \circ b)(m,n) = \bar{f}(m \otimes n) = f'(m,n) = f(m,n)$, para todo $(m,n) \in M \times N$. Portanto, $\bar{f} \circ b = f$.

Agora, seja $g\colon M \otimes_R N \to P$ outro $\mathbb{Z}$-homomorfismo tal que $g \circ b = f$. Então

$$g(m \otimes n) = g(b(m,n)) = f(m,n) = \bar{f}(b(m,n)) = \bar{f}(m \otimes n).$$

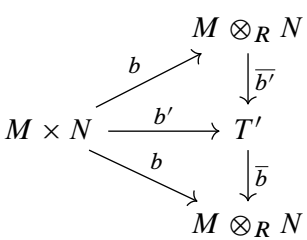
Assim, $g = \bar{f}$.

Observe que aplicando o resultado para b, temos que existe um único $\mathbb{Z}$-homomorfismo $\bar{b}$ tal que $\bar{b} \circ b = b$. Como $id_{M \otimes_R N} \circ b = b$, da unicidade temos que $\bar{b} = id_{M \otimes_R N}$.

Agora, suponha que T' seja outro $\mathbb{Z}$-módulo junto com uma aplicação balanceada $b'\colon M \times N \to T'$ que satisfaz as condições do teorema, isto é, que para qualquer aplicação balanceada $f\colon M \times N \to P$, existe um único $\mathbb{Z}$-homomorfismo $\bar{f}\colon T' \to P$ tal que $\bar{f} \circ b' = f$. Vamos mostrar que $T' \cong M \otimes_R N$ como $\mathbb{Z}$-módulos.

Ao considerar o exposto acima para a aplicação b, temos que existe um único $\mathbb{Z}$-homomorfismo $\bar{b}\colon T' \to M \otimes_R N$ tal que $\bar{b} \circ b' = b$.

Da mesma forma, como $M \otimes_R N$ e b satisfazem as condições do teorema, existe um único $\mathbb{Z}$-homomorfismo $\bar{b'}\colon M \otimes_R N \to T'$ tal que $\bar{b'} \circ b = b'$.



Logo,

$$(\bar{b} \circ \bar{b'}) \circ b = b \quad \text{e} \quad (\bar{b'} \circ \bar{b}) \circ b' = b'.$$

Da unicidade, devemos ter $\bar{b} \circ \bar{b'} = id_{T'}$ e $\bar{b'} \circ \bar{b} = id_{M \otimes_R N}$. Portanto, $\bar{b}$ é um isomorfismo de $\mathbb{Z}$-módulos e, assim, $T' \cong M \otimes_R N$. □

O teorema acima é chamado de propriedade universal do produto tensorial. O teorema nos diz que de certa forma o produto tensorial "lineariza" aplicações balanceadas. Vejamos uma aplicação dessa propriedade.

Lema 1.2.45. *Sejam $M_R, M'_R, {}_R N, {}_R N'$ R-módulos e $f\colon M \to M'$, $g\colon N \to N'$ R-homomorfismos. Então existe um único $\mathbb{Z}$-homomorfismo $h\colon M \otimes_R N \to M' \otimes_R N'$ tal que $h(m \otimes n) = f(m) \otimes g(n)$.*

Demonstração. Pela definição de produto tensorial, a aplicação $h' \colon M \times N \to M' \otimes_R N'$ dada por $h'(m,n) = f(m) \otimes g(n)$ é balanceada. Pelo Teorema 1.2.44, existe um único $\mathbb{Z}$-homomorfismo $h \colon M \otimes_R N \to M' \otimes_R N'$ tal que $h \circ b = h'$. Portanto, $h(m \otimes n) = h(b(m,n)) = h'(m,n) = f(m) \otimes g(n)$. □

Observe que, até agora, $M \otimes_R N$ é apenas um $\mathbb{Z}$-módulo. Com a propriedade universal do produto tensorial, podemos dar uma estrutura de R-módulo para $M \otimes_R N$. Antes, precisamos da seguinte definição.

Definição 1.2.46. Sejam R e S anéis e $(M, +)$ um grupo abeliano. Dizemos que M é um (R,S)-bimódulo se M é simultaneamente um R-módulo à esquerda e um S-módulo à direita e, para todo $r \in R, s \in S$ e $m \in M$, $(rm)s = r(ms)$. Se $R = S$, dizemos simplesmente que M é um R-bimódulo. Utilizaremos a notação ${}_R M_S$ para dizer que M é um (R,S)-bimódulo. Se M e N são (R,S)-bimódulos, dizemos que $f \colon M \to N$ é um homomorfismo de (R,S)-bimódulos se é um R-homomorfismo e um S-homomorfismo.

Note que, pela Observação 1.2.38, se R é um anel comutativo, então todo R-módulo é um R-bimódulo.

Teorema 1.2.47. *Sejam R e S anéis e ${}_S M_R, {}_R N_S$ bimódulos como indicado. Então:*

1. *$M \otimes_R N$ é um S-módulo tal que $s(m \otimes n) = sm \otimes n$, para todo $s \in S, m \in M, n \in N$;*
2. *se $f \colon M \to M'$ é um homomorfismo de (S,R)-bimódulos e $g \in N \to N'$ é um R-homomorfismo, então $f \otimes g \colon M \otimes_R N \to M' \otimes_R N'$ dada por $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$ é um S-homomorfismo.*

Demonstração. Para mostrar o item 1, para cada $s \in S$, defina

$$f_s \colon M \times N \to M \otimes_R N \quad \text{por} \quad f_s(m,n) = sm \otimes n.$$

Pela definição do produto tensorial, f_s é balanceada e, pelo Teorema 1.2.44, existe um único $\mathbb{Z}$-homomorfismo

$$\bar{f_s} \colon M \otimes_R N \to M \otimes_R N \quad \text{tal que} \quad \bar{f_s}(m \otimes n) = sm \otimes n.$$

Para cada $x = \sum_{i=1}^{k} m_i \otimes n_i$, defina sx como o elemento $\bar{f_s}(x) = \sum_{i=1}^{k} \bar{f_s}(m_i \otimes n_i) = \sum_{i=1}^{k} sm_i \otimes n_i$. Como $\bar{f_s}$ é um $\mathbb{Z}$-homomorfismo, sx não depende da forma

como x é escrito como a soma de geradores. Agora, é fácil verificar que $M \otimes_R N$ é um S-módulo. O item 2 será deixado como exercício. □

Nesse ponto, deve estar clara a importância da propriedade universal do produto tensorial. No teorema anterior, poderíamos ter definido diretamente $s(m \otimes n) = sm \otimes n$, mas como $M \otimes_R N$ é um conjunto de classes de equivalência, esse produto poderia não estar bem definido. A propriedade universal do produto tensorial nos permite dar uma estrutura de S-módulo bem definida a $M \otimes_R N$.

Vejamos mais alguns exemplos da aplicação da propriedade universal do produto tensorial.

Exemplo 1.2.48. Se R é um anel com unidade e M é um R-módulo, então

$$R \otimes_R M \cong M.$$

De fato, como R é um R-bimódulo, $R \otimes_R M$ é um R-módulo. É fácil ver que a aplicação $f\colon R \times M \to M$, dada por $f(r,m) = rm$, é balanceada. Logo, pelo Teorema 1.2.44, existe um único $\mathbb{Z}$-homomorfismo

$$\bar{f}\colon R \otimes_R M \to M \text{ tal que } \bar{f}(r \otimes m) = rm.$$

Note que se $r' \in R$, então $\bar{f}(r'(r \otimes m)) = \bar{f}(r'r \otimes m) = r'(rm) = r'\bar{f}(r \otimes m)$ e, assim, $\bar{f}$ é um R-homomorfismo. Seja $g\colon M \to R \otimes_R M$ dado por $g(m) = 1 \otimes m$.

Dado $r \in R$, temos que $g(rm) = 1 \otimes rm = r \otimes m = r(1 \otimes m) = rg(m)$. Logo, g é um R-homomorfismo, $\bar{f}(g(m)) = \bar{f}(1 \otimes m) = m$ e $g(\bar{f}(r \otimes m)) = g(rm) = 1 \otimes rm = r \otimes m$. Portanto, $\bar{f}$ é um R-isomorfismo e $R \otimes_R M \cong M$.

Proposição 1.2.49. *Sejam ${}_RM_1, {}_RM_2, N_R$ R-módulos. Então*

$$N \otimes_R (M_1 \oplus M_2) \cong (N \otimes_R M_1) \oplus (N \otimes_R M_2).$$

Demonstração. De fato, considere a aplicação

$$f\colon N \times (M_1 \oplus M_2) \to (N \otimes_R M_1) \oplus (N \otimes_R M_2)$$

dada por $f(n,(m_1,m_2)) = (n \otimes m_1, n \otimes m_2)$. Temos que f é balanceada e, pelo Teorema 1.2.44, induz um R-homomorfismo

$$\bar{f}\colon N \otimes_R (M_1 \oplus M_2) \to (N \otimes_R M_1) \oplus (N \otimes_R M_2)$$

dado por $\bar{f}(n \otimes (m_1,m_2)) = (n \otimes m_1, n \otimes m_2)$. Vamos construir a inversa de $\bar{f}$.

Sejam $i_j : M_j \to M_1 \oplus M_2$, $j = 1, 2$ as imersões canônicas. As aplicações $g_j : N \times M_j \to N \otimes_R (M_1 \oplus M_2)$ dadas por $g_j(n, m_j) = n \otimes i_j(m_j)$ são balanceadas. Pelo Teorema 1.2.44, as aplicações g_j induzem R-homomorfismos $\bar{g}_j : N \otimes_R M_j \to N \otimes_R (M_1 \oplus M_2)$ que, novamente pelo Teorema 1.2.44, induzem um R-homomorfismo

$$g : (N \otimes_R M_1) \otimes_R (N \otimes_R M_2) \to N \otimes_R (M_1 \oplus M_2)$$

dado por $g(n_1 \otimes m_1, n_2 \otimes m_2) = n_1 \otimes (m_1, 0) + n_2 \otimes (0, m_2)$. Agora, temos que

$$\begin{aligned}(\bar{f} \circ g)(n_1 \otimes m_1, n_2 \otimes m_2) &= \bar{f}(n_1 \otimes (m_1, 0) + n_2 \otimes (0, m_2)) \\ &= (n_1 \otimes m_1, 0) + (0, n_2 \otimes m_2) \\ &= (n_1 \otimes m_1, n_2 \otimes m_2)\end{aligned}$$

e

$$\begin{aligned}(g \circ \bar{f})(n \otimes (m_1, m_2)) &= g(n \otimes m_1, n \otimes m_2) \\ &= n \otimes (m_1, 0) + n \otimes (0, m_2) \\ &= n \otimes (m_1, m_2).\end{aligned}$$

Portanto, $\bar{f}$ é um R-isomorfismo.

□

Exercício 1.2.50. Sejam $\{{}_R M_i : i \in \mathcal{I}\}$ uma família de R-módulos e N_R um R-módulo. Mostre que $N \otimes_R \left(\bigoplus_{i \in \mathcal{I}} M_i \right) \cong \bigoplus_{i \in \mathcal{I}} (N \otimes_R M_i)$.

Exercício 1.2.51. Sejam R e S anéis e $M_{R,R} L_{,R} N_S$ (bi)módulos como indicado. Mostre que $M \otimes_R (N \otimes_S L) \cong (M \otimes_R N) \otimes_S L$. Com isso, escreveremos $M \otimes_R N \otimes_S L$. Generalize a construção do produto tensorial de n (bi)módulos.

Exercício 1.2.52. Sejam M, N R-bimódulos. Mostre que $M \otimes_R N \cong N \otimes_R M$.

Exercício 1.2.53. Sejam R um anel com unidade, $I \trianglelefteq_r R$ e ${}_R M$ um R-módulo. Mostre que:

(a) $R/I \otimes_R M \cong M/IM$ como $\mathbb{Z}$-módulos.

(b) Conclua que se $J \trianglelefteq_l R$, então $R/I \otimes_R R/J \cong R/(I + J)$ como $\mathbb{Z}$-módulos. Além disso, se R é comutativo e I, J são ideais de R, então o isomorfismo é de R-módulos.

Exercício 1.2.54. Mostre que $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n \cong \mathbb{Z}_d$, onde $d = mdc(m,n)$.

Exercício 1.2.55. Seja D um anel de divisão. Mostre que vale o isomorfismo $M_n(D) \otimes_R M_m(D) \cong M_{nm}(D)$.

Exercício 1.2.56. Sejam R um anel e $I \trianglelefteq R$. Mostre que $R \otimes_R I[x] \cong R[x]$.

Seja R um anel comutativo. Como mencionamos anteriormente, um R-módulo M tem estrutura natural de R-bimódulo. Com isso, pelo Teorema 1.2.47, se N também é um R-módulo, então $M \otimes_R N$ é um R-bimódulo e

$$r(m \otimes n) = rm \otimes m = mr \otimes n = m \otimes rn = m \otimes nr = (m \otimes n)r.$$

Sejam R um anel comutativo e M, N e P R-(bi)módulos. Uma aplicação $f : M \times N \to P$ é dita uma aplicação bilinear se para todo $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N, r \in R$:

1. $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$;
2. $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$;
3. $f(rm, n) = rf(m, n) = f(m, rn)$.

Assim, toda aplicação bilinear é uma aplicação balanceada. Além disso, se R é comutativo, então $b : M \times N \to M \otimes_R N$, a aplicação balanceada canônica, é uma aplicação bilinear. Neste contexto, b é chamada de aplicação bilinear canônica. Com isso, temos uma extensão do Teorema 1.2.44, para o caso em que R é um anel comutativo.

Teorema 1.2.57. *Considere os R-módulos M, N e P, onde R é um anel comutativo. Se $f : M \times N \to P$ é uma aplicação bilinear, então existe um único R-homomorfismo $\bar{f} : M \otimes_R N \to P$ tal que $\bar{f} \circ b = f$. Além disso, o R-módulo $M \otimes_R N$ é unicamente determinado, a menos de isomorfismos, por esta propriedade.*

Nosso próximo objetivo é mostrar que o produto tensorial de R-módulos livres é livre. Para isso, mostraremos o seguinte.

Teorema 1.2.58. *Seja R um anel com unidade. Se M_R é um R-módulo e ${}_RN$ é um R-módulo livre com R-base Y, então todo elemento x de $M \otimes_R N$ pode ser escrito de maneira única na forma $x = \sum_{i=1}^{k} m_i \otimes y_i$, onde os $y_i's$ são elementos distintos de Y.*

Antes de apresentar a demonstração, vamos explicar o significado de "maneira única" no enunciado do teorema anterior. Se $x = \sum_{i=1}^{k} m_i \otimes y_i$ e $x' = \sum_{j=1}^{t} m_j \otimes z_j$, com $m_i, m_j \in M$ e $y_i, z_j \in Y$, podemos, se necessário, inserir termos $0 \otimes y$, $y \in Y$, nas somas e assumir que $x = \sum_{i=1}^{k} m_i \otimes y_i$ e $x' = \sum_{i=1}^{k} m'_i \otimes y_i$. Assim, dizer que x pode ser escrito de maneira única como $x = \sum_{i=1}^{k} m_i \otimes y_i$ significa afirmar que se $\sum_{i=1}^{k} m_i \otimes y_i = \sum_{i=1}^{k} m'_i \otimes y_i$, então $m_i = m'_i$ para todo $i = 1, \ldots, k$. Em particular, se $x = \sum_{i=1}^{k} m_i \otimes y_i = 0$, então $m_i = 0$ para todo $i = 1, \ldots, k$.

Demonstração. Para cada $y \in Y$, seja M_y uma cópia de M e considere $\bigoplus_{y \in Y} M_y$. Como Y é linearmente independente, para cada $y \in Y$, temos um R-isomorfismo $f_y \colon R \to Ry$ dado por $f_y(r) = ry$. Logo, para cada $y \in Y$, temos um R-isomorfismo

$$id_M \otimes f_y^{-1} \colon M \otimes_R Ry \to M \otimes_R R \cong M = M_y$$

dado por $(id_M \otimes f_y^{-1})(m \otimes ry) = mr$. Assim, temos um R-isomorfismo f:

$$M \otimes_R N \cong M \otimes_R \left(\bigoplus_{y \in Y} Ry \right) \cong \bigoplus_{y \in Y} (M \otimes_R Ry) \cong \bigoplus_{y \in Y} M_y$$

e para todo $m \in M, z \in Y$, $f(m \otimes z) = (m_y)_{y \in Y} \in \bigoplus_{y \in Y} M_y$, onde $m_z = m$ e $m_y = 0$, se $y \neq z$, ou seja, $f(m \otimes z) = i_z(m)$, onde $i_z \colon M_z \to \bigoplus_{y \in Y} M_y$ é a imersão canônica. Agora, todo elemento $u \in \bigoplus_{y \in Y} M_y$ é escrito como uma soma finita $i_{y_1}(m_1) + \cdots + i_{y_k}(m_k) = f(m_1 \otimes y_1) + \cdots + f(m_k \otimes y_k)$, onde os y'_is são distintos e os m'_is são elementos não nulos unicamente determinados de M. Como todo elemento de $M \otimes_R N$ é da forma $f^{-1}(u)$, para algum $u \in \bigoplus_{y \in Y} M_y$, o teorema está mostrado. □

A seguir, apresentamos dois importantes corolários desse teorema.

Corolário 1.2.59. *Sejam R um anel com unidade e $M_R, {}_R N$ R-módulos livres com R-bases X e Y, respectivamente. Então $M \otimes_R N$ é um R-módulo (à direita) livre com base $W = \{x \otimes y : x \in X, y \in Y\}$ de cardinalidade $|X||Y|$.*

Corolário 1.2.60. *Sejam R um anel com unidade e S um subanel de R que contém 1_R. Se M é um S-módulo livre com S-base X, então $R \otimes_S M$ é um R-módulo livre com base $\{1_R \otimes x : x \in X\}$ de cardinalidade $|X|$.*

Neste livro, estaremos interessados no produto tensorial de R-módulos quando R é um corpo, isto é, no produto tensorial de espaços vetoriais.

Dado um espaço vetorial V sobre um corpo F, denotamos a dimensão de V sobre F por $\dim_F(V)$. Se K é um corpo que contém F, claramente K é um espaço vetorial sobre F. Assim, podemos formar o produto tensorial $V^K = V \otimes_F K$, o espaço vetorial sobre K obtido a partir de V através da extensão de escalares. Como consequência do corolário anterior, temos o seguinte.

Corolário 1.2.61. *Sejam F um corpo, K um corpo que contém F e V um F-espaço vetorial. Então o K-espaço vetorial $V^K = V \otimes_F K$ possui uma base $B^K = \{v \otimes 1 : v \in B\}$, onde B é uma F-base de V e $\dim_F(V) = \dim_K(V^K)$.*

Terminamos a seção informando que, em algumas situações, ao trabalhar com módulos M e N sobre um mesmo anel R, omitiremos o índice na notação do produto tensorial obtido, ou seja, usaremos simplesmente $M \otimes N$ no lugar de $M \otimes_R N$.

Exercícios V ou F da Seção 1.2: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, R representa um anel e A, B e C são R-módulos.

(1) Seja $f : A \to B$ um homomorfismo de R-módulos. Se C é R-submódulo de B, então $f^{-1}(C) = \{a \in A : f(a) \in C\}$ é R-submódulo de A.

(2) Se R é um domínio de integridade e M um R-módulo, então o conjunto $\mathcal{T}(M) = \{m \in M : am = 0, \text{ para algum } a \in R\}$ é um R-submódulo de M.

(3) Se A é um R-submódulo de B e B é livre, então A é livre.

(4) Se A e B são R-módulos simples, então $Hom_R(A, B) = \{0\}$.

(5) Se $A \otimes_R B \cong A \otimes_R C$, então $B \cong C$.

(6) Seja M um R-módulo e considere $A \subseteq B$ submódulos de M. Se $M/A \cong M/B$, então $A = B$.

(7) Se V e U são F-espaços vetoriais de dimensão finita, então

$$\dim_F(V \otimes_F U) = \dim_F(V) + \dim_F(U).$$

1.3 Anéis semissimples

Nesta seção, vamos demonstrar o Teorema de Wedderburn–Artin, que caracteriza os anéis artinianos semissimples. Existem basicamente duas definições de anéis artinianos semissimples, que são equivalentes. Utilizamos cada uma das definições dependendo se o anel tem unidade ou não.

Recordemos que, durante este livro, os anéis não necessariamente possuem unidade, mas optamos por estudar a semissimplicidade de anéis com unidade, pois a exposição dos resultados é mais intuitiva e de maior familiaridade para o leitor menos avançado. Por outro lado, informamos que é possível fazer o estudo de anéis artinianos semissimples sem unidade e indicamos o livro de Herstein (1968) para uma exposição desse assunto. Com isso em mente, durante essa seção, R denotará um anel com unidade.

Antes de apresentar a definição de R-módulos semissimples, iremos relembrar o Lema de Zorn e definir anéis artinianos. Para isso, consideremos X um conjunto e $\leqslant$ uma relação em X, isto é, um subconjunto de $X \times X$. Dizemos que $(X, \leqslant)$ é parcialmente ordenado se para todos $a, b, c \in X$,

1. $a \leqslant a$ (reflexividade);
2. se $a \leqslant b$ e $b \leqslant a$, então $a = b$ (antissimetria);
3. se $a \leqslant b$ e $b \leqslant c$, então $a \leqslant c$ (transitividade).

Dizemos que $a, b \in (X, \leqslant)$ são comparáveis se $a \leqslant b$ ou $b \leqslant a$. É fácil encontrar exemplos de conjuntos parcialmente ordenados, onde dois elementos não são comparáveis.

Exemplo 1.3.1. Seja X o conjunto formado pelas partes de $\{1, 2, 3, 4\}$. Defina $A \leqslant B$ se, e somente se, $A \subset B$. Então X é parcialmente ordenado, mas os elementos $\{1, 2\}$ e $\{3, 4\}$ não são comparáveis.

Dizemos que $(X, \leqslant)$ é totalmente ordenado, se é parcialmente ordenado e quaisquer dois elementos de X são comparáveis.

Exemplo 1.3.2. O conjunto $\mathbb{Z}$ com a ordem usual é um conjunto totalmente ordenado.

Sejam $(X, \leqslant)$ um conjunto parcialmente ordenado e $x \in X$. Dizemos que x é um elemento maximal em X, se para todo $y \in X$ que é comparável a x, temos $y \leqslant x$. Observe que, se x é maximal, então não necessariamente $y \leqslant x$, para todo $y \in X$, pois podem existir elementos em X que não são comparáveis a x. Além disso, um conjunto parcialmente ordenado pode possuir infinitos elementos maximais ou não possuir elemento maximal.

Exemplo 1.3.3. Dê exemplo de um conjunto parcialmente ordenado nas condições abaixo:

(a) possui infinitos elementos maximais;

(b) não possui elemento maximal.

De maneira análoga definimos elemento minimal em um conjunto parcialmente ordenado.

Dizemos que $Y \subseteq X$ é uma cadeia se $(Y, \leqslant)$ é totalmente ordenado. Uma cota superior, em uma cadeia $Y \subseteq X$, é um elemento $x \in X$ tal que $y \leqslant x$, para todo $y \in Y$. Assim, estamos prontos para enunciar o Lema de Zorn.

Lema 1.3.4 (Zorn)**.** *Se $(X, \leqslant)$ é um conjunto parcialmente ordenado tal que toda cadeia em X possui uma cota superior em X, então X contém (pelo menos) um elemento maximal.*

No que segue, se R é um anel e M é um R-módulo, vamos considerar o conjunto dos R-submódulos de M parcialmente ordenado pela inclusão.

Nas Seções 1.1 e 1.2, utilizamos o conceito de ideal maximal sem garantir sua existência. Com o Lema de Zorn, estamos aptos para demonstrar esse fato.

Lema 1.3.5. *Se R é um anel, então R possui um ideal maximal à esquerda (à direita, bilateral).*

Demonstração. Seja $X = \{I \subseteq R : I \trianglelefteq_l R, I \neq R\}$. Temos que $X \neq \varnothing$, pois $\{0\} \in X$. Seja Y uma cadeia em X. Então $J = \bigcup_{I \in Y} I$ é um ideal à esquerda de R e $R \neq J$, pois $1 \notin I$, para todo $I \in Y$. Logo, $J \in X$ é uma cota superior de Y em X e, pelo Lema 1.3.4, X possui um elemento maximal. □

Exercício 1.3.6. Sejam R um anel e $I \trianglelefteq_l R$. Mostre que existe $I' \trianglelefteq_l R$ maximal tal que $I \subseteq I'$. Conclua que todo elemento não invertível em R pertence a algum ideal maximal à esquerda de R.

Exercício 1.3.7. Sabemos que $\mathbb{Z}$ não possui ideais minimais. Explique por que não podemos utilizar o Lema de Zorn para garantir a existência de ideais minimais em um anel.

Dizemos que um R-módulo M é noetheriano (à esquerda), se toda cadeia ascendente de R-submódulos de M é estacionária, isto é, se

$$M_1 \subset M_2 \subset \cdots$$

é uma cadeia de R-submódulos de M, então existe $r \in \mathbb{N}$ tal que $M_i = M_r$, para todo $i \geqslant r$. Analogamente, dizemos que um R-módulo é artiniano (à esquerda), se toda cadeia descendente de R-submódulos de M é estacionária. Dizemos que um anel R é noetheriano (artiniano) se R é noetheriano (artiniano) à direita e à esquerda como R-módulo.

Exemplo 1.3.8. Todo espaço vetorial de dimensão finita é noetheriano e artiniano.

Exemplo 1.3.9. O anel $\mathbb{Z}$ é noetheriano, mas não é artiniano. De fato, se $n\mathbb{Z}$ e $m\mathbb{Z}$ são ideais de $\mathbb{Z}$ tais que $n\mathbb{Z} \subset m\mathbb{Z}$, então m é um divisor de n. Como a quantidade de divisores de um inteiro é finita, temos que toda cadeia ascendente de ideais de $\mathbb{Z}$ é estacionária e $\mathbb{Z}$ é noetheriano. Agora, a cadeia de ideais $2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots \supset 2^n\mathbb{Z} \supset \cdots$ não estaciona. Portanto, $\mathbb{Z}$ não é artiniano.

Exercício 1.3.10. Sejam p um primo, $\mathbb{Z}_{(p)} = \left\{\frac{a}{p^m} : a \in \mathbb{Z}, m \geqslant 0\right\}$, e $M = \mathbb{Z}_{(p)}/\mathbb{Z}$. Mostre que M é um $\mathbb{Z}$-módulo artiniano, mas não é noetheriano.

Exercício 1.3.11. Mostre que o anel $R = \begin{pmatrix} \mathbb{R} & \mathbb{R} \\ 0 & \mathbb{Q} \end{pmatrix}$ é artiniano à esquerda, noetheriano à esquerda, mas não é artiniano à direita e nem noetheriano à direita.

Exercício 1.3.12. Mostre que todo domínio de integridade artiniano é um corpo.

Agora, vamos utilizar o Lema de Zorn para caracterizar os R-módulos noetherianos e artinianos.

Teorema 1.3.13. *Seja M um R-módulo. São equivalentes:*

1. *Toda família não vazia de R-submódulos de M contém um elemento maximal;*

2. *Todo R-submódulo de M é finitamente gerado;*

3. *M é noetheriano.*

Demonstração. [(1) $\Rightarrow$ (2)] Suponha que existe $N \leqslant M$ que não é finitamente gerado. Considere a família $\mathcal{F} = \{S \subset M : S \leqslant N, S \text{ é finitamente gerado}\}$. Note que $\mathcal{F}$ é não vazio, pois $\{0\} \in \mathcal{F}$. Tome N_0 um elemento maximal de $\mathcal{F}$, que existe por hipótese. Então N_0 é finitamente gerado e $N_0 \neq N$, pois N não é finitamente gerado. Logo, existe $a \in N - N_0$ e $N_1 = N_0 + Ra$ é um R-submódulo finitamente gerado de N tal que $N_0 \subset N_1$ e $N_0 \neq N_1$. Dessa maneira, chegamos a um absurdo, pois N_0 é maximal.

[(2) $\Rightarrow$ (3)] Seja $M_1 \subset M_2 \subset \cdots$ uma cadeia ascendente de R-submódulos de M. Então $N = \bigcup_{i \geqslant 1} M_i$ é um R-submódulo de M que, por hipótese, é finitamente gerado. Seja $\{n_1, n_2, \ldots, n_t\}$ um conjunto gerador de N. Então, para cada $i = 1, \ldots, t$, existe j_i tal que $n_i \in M_{j_i}$. Considerando $k = \max\{j_1, \ldots, j_t\}$, temos $n_i \in M_k$ para todo $i = 1, \ldots, t$. Logo, $N \subseteq M_k$ e $M_i \subseteq M_k$, para todo $i \geqslant 1$. Com isso, segue que $M_i = M_k$ para todo $i \geqslant k$. Isso mostra que a cadeia estaciona e, portanto, M é noetheriano.

[(3) $\Rightarrow$ (1)] Seja $\mathcal{F} = \{N \subseteq M : N \leqslant M\}$. Como M é noetheriano, toda cadeia ascendente de R-submódulos de M possui cota superior, caso contrário existiria uma cadeia não estacionária. Pelo Lema 1.3.4, $\mathcal{F}$ contém um elemento maximal. □

Com uma demonstração análoga, temos o seguinte teorema.

Teorema 1.3.14. *Seja M um R-módulo. São equivalentes:*

1. *Toda família não vazia de R-submódulos de M possui um elemento minimal;*

2. *M é artiniano.*

Um critério útil para determinar se um R-módulo é noetheriano (artiniano) é dado no próximo lema.

Lema 1.3.15. *Sejam M um R-módulo e $N \leqslant M$. Então M é noetheriano (artiniano) se, e somente se, N e M/N são ambos noetherianos (artinianos).*

Demonstração. Vamos demonstrar o resultado para o caso noetheriano, já que o caso artiniano segue de modo análogo. Suponha que M seja noetheriano e seja $N \leqslant M$. Então todo R-submódulo de N é um R-submódulo de M e, portanto, toda cadeia ascendente de R-submódulos de N estaciona. Logo, N é noetheriano. Agora, como todo R-submódulo de M/N é da forma N'/N, onde $N' \leqslant M$ e $N \subseteq N'$, como no caso anterior, podemos mostrar que M/N é noetheriano.

Reciprocamente, suponha N e M/N são noetherianos e seja $M_1 \subset M_2 \subset \cdots$ uma cadeia de R-submódulos de M. Considere as seguintes cadeias:

$$M_1 \cap N \subset M_2 \cap N \subset \cdots$$

e

$$(M_1 + N)/N \subset (M_2 + N)/N \subset \cdots .$$

Como N e M/N são noetherianos, é possível determinar $k \geqslant 1$ tal que $M_i \cap N = M_k \cap N$ e $M_i + N = M_k + N$, para todo $i \geqslant k$.

Por hipótese, já temos que $M_k \subseteq M_i$, para todo $i \geqslant k$. Agora, vamos mostrar que $M_i \subseteq M_k$. Seja $x \in M_i$. Então existe $y \in M_k$ tal que $x + N = y + N$. Logo, $x - y \in N$. Como $M_k \subseteq M_i$, temos $x - y \in M_i \cap N = M_k \cap N$. Logo, $x - y \in M_k$ e, assim, $x \in M_k$. □

Como consequência do lema anterior, temos os seguintes corolários.

Corolário 1.3.16. *Seja M um R-módulo tal que $M = M_1 + \cdots + M_n$, onde cada $M_i \leqslant M$, $i = 1, \ldots, n$. Então M é noetheriano (artiniano) se, e somente se, cada M_i, $i = 1, \ldots, n$ é noetheriano (artiniano).*

Demonstração. Novamente, vamos mostrar somente o caso noetheriano. Se M é noetheriano, então cada $M_i, i = 1, \ldots, n$ é noetheriano. Reciprocamente, suponha que $M = M_1 + M_2$, onde M_1 e M_2 são noetherianos. Então $M/M_1 = (M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$, que é noetheriano, pois M_2 é noetheriano. Portanto, M é noetheriano. O caso geral segue utilizando o princípio da indução finita. □

Corolário 1.3.17. *Se R é um anel noetheriano (artiniano), então todo R-módulo finitamente gerado é noetheriano (artiniano).*

Demonstração. Seja $\{m_1, \ldots, m_k\}$ um conjunto gerador de M como R-módulo. Então $M = \sum_{i=1}^{k} Rm_i$ e, para todo $i = 1, \ldots, k$, a aplicação $f_i \colon R \to Rm_i$ dada por $f_i(r) = rm_i$ é um epimorfismo de R-módulos e $Rm_i \cong R/\mathrm{Ker}(f_i)$.

Como R é noetheriano (artiniano), Rm_i também o é. Portanto, M é noetheriano (artiniano). □

Exercício 1.3.18. Dê um exemplo de um R-módulo finitamente gerado, que possui um R-submódulo que não é finitamente gerado.

Exercício 1.3.19. Seja M um R-módulo. Uma série de composição de M é a menor cadeia finita de R-submódulos $\{0\} \subset M_1 \subset M_2 \subset \cdots \subset M_{n-1} \subset M_n = M$ tal que cada módulo quociente M_{i+1}/M_i é simples, $0 \leqslant i \leqslant n-1$. Se um R-módulo M possui uma série de composição, então dizemos que M tem comprimento finito. Mostre que um R-módulo tem comprimento finito se, e somente se, é noetheriano e artiniano.

Exercício 1.3.20. Se D é um anel de divisão, então mostre que, para todo $n \geqslant 1$, $M_n(D)$ é um anel artiniano e noetheriano.

Agora, vamos introduzir o principal conceito desta seção.

Definição 1.3.21. Um R-módulo M é semissimples, se todo R-submódulo de R é um somando direto. Um anel R é semissimples, se ${}_RR$ é um R-módulo semissimples.

Exemplo 1.3.22. Se V é um espaço vetorial de dimensão finita n sobre um corpo F, então V é um F-módulo semissimples. De fato, seja W um subespaço não nulo de V. Então toda F-base de W pode ser estendida a uma F-base de V. Com isso, se $\{w_1, \ldots, w_k\}$ é uma F-base de W e $\{w_1, \ldots, w_k, w_{k+1}, \ldots, w_n\}$ é uma F-base de V, então $W' = \text{span}_F\{w_{k+1}, \ldots, w_n\}$ é um somando direto de W.

Exemplo 1.3.23. Como vimos no Corolário 1.2.28, $\mathbb{Z}$ não é um anel semissimples, pois os únicos somandos diretos de $\mathbb{Z}$ são os triviais.

O próximo lema mostra que os R-submódulos não nulos de um R-módulo semissimples também são semissimples. Mais do que isto, esses possuem um R-submódulo simples.

Lema 1.3.24. *Sejam M um R-módulo semissimples e $\{0\} \neq N \leqslant M$. Então N é um R-módulo semissimples e possui um R-submódulo simples.*

Demonstração. Se $S \leqslant N$, então $S \leqslant M$ e, como M é semissimples, existe $S' \leqslant M$ tal que $M = S \oplus S'$. Afirmamos que $N = S \oplus (S' \cap N)$. De fato, dado $n \in N$, existem $s \in S, s' \in S'$ tais que $n = s + s'$. Logo, $n - s = s' \in S'$ e como $S \leqslant N$, $s' \in S' \cap N$. Com isso, $N = S + (S' \cap N)$. Agora, como $S \cap (S' \cap N) = \{0\} \cap N = \{0\}$, a afirmação está provada.

Para mostrar que N possui um R-submódulo simples, tomamos $n \in N, n \neq 0$, e consideramos

$$\mathcal{F} = \{N' \subset N : N' \leqslant N, n \notin N'\}.$$

Temos que $\mathcal{F}$ é não vazio, pois $\{0\} \in \mathcal{F}$ e toda cadeia em $\mathcal{F}$ possui elemento maximal: a união de todos os R-submódulos nesta cadeia. Pelo Lema 1.3.4, $\mathcal{F}$ possui um elemento maximal N_1. Como N é semissimples, existe $N_2 \leqslant N$ tal que $N = N_1 \oplus N_2$. Afirmamos que N_2 é simples. De fato, se não fosse, existiria $N_3 \leqslant N_2$ e como N_2 é semissimples, $N_2 = N_3 \oplus N_4$, para algum $N_4 \leqslant N_2$. Logo $N = N_1 \oplus N_3 \oplus N_4$ e $N_1 = (N_1 + N_3) \cap (N_1 + N_4)$, já que $N_1 \cap N_2 = \{0\}$. Como $n \notin N_1$, temos que ou $n \notin N_1 + N_3$, ou $n \notin N_1 + N_4$, contrariando a maximalidade de N_1. Portanto N_2 é simples. □

Corolário 1.3.25. *Se M é um R-módulo semissimples e $N \leqslant M$, então M/N é semissimples.*

Demonstração. Como M é semissimples, existe $N' \leqslant N$ tal que $M = N \oplus N'$. Pelo Lema 1.2.27, $M/N \cong N'$ e pelo lema anterior, N' é semissimples. Portanto, M/N é semissimples. □

Exercício 1.3.26. Mostre que o $\mathbb{Z}$-módulo $\mathbb{Q}$ não é semissimples e não possui um quociente simples.

A seguir, apresentaremos uma caracterização de módulos semissimples.

Teorema 1.3.27. *Seja M um R-módulo. São equivalentes:*

1. *M é semissimples;*
2. *M é soma direta de R-submódulos simples;*
3. *M é soma de R-submódulos simples.*

Demonstração. [(1) $\Rightarrow$ (2)] Seja

$$\mathcal{F} = \left\{ N \subset M : N \leqslant M, N = \bigoplus_{i \in \mathcal{I}} N_i, N_i \leqslant N \text{ simples, para todo } i \in \mathcal{I} \right\}.$$

Pelo Lema 1.3.24, $\mathcal{F} \neq \varnothing$. Vamos definir uma ordem parcial em $\mathcal{F}$ como segue: $\bigoplus_{i\in\mathcal{I}} N_i \leqslant \bigoplus_{j\in\mathcal{J}} N_j$ se, e somente se, $\mathcal{I} \subset \mathcal{J}$. Com a ordem assim definida, toda cadeia em $\mathcal{F}$ possui elemento maximal. Logo, pelo Lema 1.3.4, $\mathcal{F}$ possui um elemento maximal $N_0 = \bigoplus_{i\in\mathcal{I}} N_i$, $N_i \leqslant N$ simples, para todo $i \in \mathcal{I}$. Afirmamos que $N_0 = M$. De fato, suponha que $N_0 \neq M$. Como M é semissimples, existe $N' \leqslant M$ tal que $M = N_0 \oplus N'$. Mas, pelo Lema 1.3.24, N' possui um R-submódulo simples S e $N_0 \subset \bigoplus_{i\in\mathcal{I}} N_i \oplus S \in \mathcal{F}$, o que contraria a maximalidade de N_0.

[(2) $\Rightarrow$ (3)] Óbvio.

[(3) $\Rightarrow$ (1)] Suponha que $M = \sum_{i\in\mathcal{I}} M_i$, onde cada M_i é um R-submódulo simples de M, para todo $i \in \mathcal{I}$, e seja $N \leqslant M$.

Vamos mostrar N é um somando direto de M. Seja

$$\mathcal{F} = \left\{ \sum_{j\in\mathcal{J}} M_j : \mathcal{J} \subset \mathcal{I}, \left(\sum_{j\in\mathcal{J}} M_j \right) \cap N = \{0\} \right\} \subseteq M.$$

Como $N \neq M$, deve existir $i \in \mathcal{I}$ tal que $M_i \cap N = \{0\}$, caso contrário, como M_i é simples, $M_i \cap N = M_i$ e $M_i \subset N$. Portanto, $\mathcal{F} \neq \varnothing$ e, pelo Lema 1.3.4, $\mathcal{F}$ possui um elemento maximal $M_0 = \sum_{j\in\mathcal{J}'} M_j$, para algum $\mathcal{J}' \subset \mathcal{I}$.

Como $M_0 \cap N = \{0\}$, para finalizar a demonstração, basta mostrar que $M = M_0 + N$. Se para todo $i \in \mathcal{I}$, $M_i \subset M_0 + N$, então $M \subset M_0 + N$ e não há nada mais para ser feito. Caso contrário, existe $i \in \mathcal{I}$ tal que $M_i \not\subset M_0 + N$. Como M_i é simples, necessariamente devemos ter $M_i \cap (M_0 + N) = \{0\}$ e, portanto, $(M_i + M_0) \cap N \subset (M_i \cap N) + (M_0 \cap N) = \{0\}$, o que contraria a maximalidade de M_0. Portanto, N é um somando direto de M e M é semissimples. □

Corolário 1.3.28. *A soma direta de R-módulos semissimples é semissimples.*

Corolário 1.3.29. *Seja $M = \bigoplus_{i\in\mathcal{I}} M_i$ a decomposição de um R-módulo semissimples como soma direta de R-módulos simples. Se $N \leqslant M$, então existe $\mathcal{J} \subseteq \mathcal{I}$ tal que $N = \bigoplus_{i\in\mathcal{J}} M_i$.*

Demonstração. Como na demonstração do teorema anterior, dado $N \leqslant M$, é possível encontrar um conjunto de índices $\mathcal{J}'$ tal que $M = N \oplus N'$, onde $N' = \bigoplus_{i\in\mathcal{J}'} M_i$. Logo, $N \cong M/N' \cong \bigoplus_{i\in\mathcal{I}-\mathcal{J}'} M_i$. □

Ao fazer o próximo exercício, o leitor verá que a recíproca do Corolário 1.3.25 não é verdadeira.

Exercício 1.3.30. Dê um exemplo de um R-módulo M, que possui um R-submódulo N tal que N e M/N são semissimples, mas M não o é.

Exercício 1.3.31. Seja M um R-módulo semissimples. Mostre que as seguintes afirmações são equivalentes:

1. M é finitamente gerado;
2. M é a soma direta de um número finito de R-módulos simples;
3. M tem comprimento finito;
4. M é noetheriano e artiniano.

Exercício 1.3.32. Mostre que um R-módulo M é semissimples se, e somente se, todo R-submódulo cíclico de M é semissimples.

Exercício 1.3.33. Mostre que o $\mathbb{Z}$-módulo $\mathbb{Z}_n$ é semissimples se, e somente se, n é livre de quadrados.

Agora, vamos estudar os anéis semissimples. Começamos com o seguinte teorema.

Teorema 1.3.34. *Seja R um anel. As seguintes afirmações são equivalentes:*

1. *Todo R-módulo é semissimples;*
2. *R é um anel semissimples;*
3. *R é a soma direta finita de ideais minimais à esquerda.*

Demonstração. Como [(1) $\Rightarrow$ (2)] e [(3) $\Rightarrow$ (2)], basta mostrarmos as implicações abaixo.

[(2) $\Rightarrow$ (1)] Considerando M um R-módulo, notamos que sempre podemos tomar $X = M$ como um conjunto gerador de M. Assim, vamos considerar um conjunto gerador qualquer $X = \{m_i : i \in \mathcal{I}\}$ de M. A aplicação $f : R^{(\mathcal{I})} \to M$ dada por $f((r_i)_{i\in\mathcal{I}}) = \sum_{i\in\mathcal{I}} r_i m_i$ é um epimorfismo de R-módulos. Como R é semissimples, pelo Corolário 1.3.28, $R^{(\mathcal{I})}$ é semissimples. Portanto, M é semissimples.

[(2) $\Rightarrow$ (3)] Os R-submódulos simples de R são seus ideais minimais à esquerda. Logo, pelo Teorema 1.3.27, $R = \bigoplus_{i \in \mathcal{I}} L_i$, onde cada L_i é um ideal minimal à esquerda de R. Vamos mostrar que a soma é finita. Como R é um anel com unidade, temos

$$1 = r_{i_1} + r_{i_2} + \cdots + r_{i_n}$$

onde $r_{i_j} \in L_{i_j}$, $j = 1, \ldots, n$. Logo, dado $r' \in R$, temos

$$r' = r'r_{i_1} + r'r_{i_2} + \cdots + r'r_{i_n} \in L_{i_1} \oplus \cdots \oplus L_{i_n}.$$

Com isso, $R \subseteq L_{i_1} \oplus \cdots \oplus L_{i_n}$ e, portanto, $R = L_{i_1} \oplus \cdots \oplus L_{i_n}$. □

Corolário 1.3.35. *Seja $R = L_1 \oplus \cdots \oplus L_n$ a decomposição de um anel semissimples como a soma direta de ideais minimais à esquerda. Se M é um R-módulo simples, então $M \cong L_i$, para algum $i = 1, \ldots, n$. Em particular, a menos de isomorfismos, existe apenas uma quantidade finita de R-módulos simples.*

Demonstração. Como R tem unidade, $RM \neq \{0\}$. Por hipótese, temos que $R = L_1 \oplus \cdots \oplus L_n$. Logo, existe $i \in \{1, \ldots, n\}$ tal que $L_i M \neq \{0\}$. Mas $L_i M \leqslant M$ e pela simplicidade de M, obtemos que $L_i M = M$. Assim, a aplicação $f : L_i \to M$, dada por $f(r_i) = r_i m$, é um epimorfismo, cujo núcleo é um R-submódulo de L_i. Da minimalidade de L_i, obtemos que $\mathrm{Ker}(f) = \{0\}$ e, portanto, f é um isomorfismo. □

Como consequência do Exercício 1.3.31, também temos o seguinte corolário.

Corolário 1.3.36. *Todo anel semissimples é noetheriano e artiniano.*

Dizemos que um R-módulo M é homogêneo se $M = M_1 \oplus \cdots \oplus M_n$, onde cada M_i, $i = 1, \ldots, n$, é um R-módulo simples isomorfo a um R-módulo simples fixo M'. Seja $R = L_1 \oplus \cdots \oplus L_n$ a decomposição de um anel semissimples como a soma direta de ideais minimais à esquerda. Coletando os ideais minimais à esquerda isomorfos na decomposição acima, concluímos que um anel R é semissimples se, e somente se, R é a soma direta de anéis homogêneos. Em particular, se R é um anel semissimples e homogêneo, então todos os R-módulos simples são isomorfos.

Exemplo 1.3.37. Todo anel de divisão é semissimples, pois não possui ideais à esquerda próprios.

Exemplo 1.3.38. Se D é um anel de divisão, então $M_n(D)$ é um anel semissimples, para todo $n \geqslant 1$, pois, pelo Exercício 1.2.24, $M_n(D) = C_1 \oplus \cdots \oplus C_n$ e cada C_i é um ideal minimal à esquerda de $M_n(D)$.

Exemplo 1.3.39. Se F é um corpo, então o anel de polinômios $F[x]$ não é semissimples. De fato, se $F[x]$ fosse semissimples, então seria um anel artiniano e, evidentemente, a cadeia $\langle x \rangle \supset \langle x^2 \rangle \cdots$ não é estacionária.

Para continuar nosso estudo, vamos determinar a estrutura do anel $End_R(M)$, onde M é um R-módulo.

É bem conhecido que se V é um espaço vetorial sobre um corpo F de dimensão finita n, então $End_F(V) \cong M_n(F)$. Em particular, $End_F(F) \cong F$. Sabemos que se $\{v_1, \ldots, v_n\}$ é uma F-base de V, então $V = \bigoplus_{i=1}^{n} Fv_i$.

Além disso, as aplicações $f_i : F \to Fv_i$ dadas por $f_i(\alpha) = \alpha v_i$ são isomorfismos de espaços vetoriais, já que F é um F-módulo simples. Portanto,

$$V \cong \underbrace{F \oplus \cdots \oplus F}_{n \text{ vezes}} = F^{(n)}$$

e $End_F(F^{(n)}) \cong M_n(F) \cong M_n(End_F(F))$.

Deixamos como exercício o próximo resultado.

Lema 1.3.40. *Se M é um R-módulo e n é um inteiro positivo, então temos $End_R(M^{(n)}) \cong M_n(End_R(M))$.*

Com esse resultado, estamos aptos a demonstrar a próxima proposição.

Proposição 1.3.41. *Seja M um R-módulo semissimples de comprimento finito. Então $End_R(M)$ é isomorfo a uma soma direta finita de anéis de matrizes sobre anéis de divisão.*

Demonstração. Escreva $M = \bigoplus_{i=1}^{n} M_i$, onde cada M_i é um R-módulo simples. Agrupando os módulos isomorfos, podemos escrever

$$M = \bigoplus_{i=1}^{k} M_i^{(n_i)}, \text{ onde } M_i \ncong M_j, \text{ se } i \neq j.$$

Como cada M_i é um R-módulo simples, pelo Lema de Schur, temos que $Hom_R(M_i, M_j) = \{0\}$, se $i \neq j$. Logo, se $i \neq j$, $Hom_R(M_i^{(n_i)}, M_j^{(n_j)}) =$

$\{0\}$ e, assim, um endomorfismo de M deve levar $M_i^{(n_i)}$ nele mesmo. Com isso, temos que

$$End_R(M) = End_R\left(\bigoplus_{i=1}^{k} M_i^{(n_i)}\right) \cong \bigoplus_{i=1}^{k} M_{n_i}(End_R(M_i)).$$

Pelo Lema 1.2.19, o resultado está provado. □

A seguir, introduzimos a noção de anel oposto de um anel.

Definição 1.3.42. O anel oposto de um anel R, denotado por R^{op}, é definido como segue: como conjunto, os elementos de R^{op} são os elementos de R e a adição em R^{op} coincide com a adição em R. A multiplicação em R^{op} é dada por $a \circ b = ba$, para todos $a, b \in R$, onde ba denota a multiplicação em R.

Algumas propriedades de R^{op} estão listadas abaixo.

Exercício 1.3.43. Seja R um anel. Mostre que:

(a) R tem unidade se, e somente se, R^{op} tem unidade.

(b) R é um anel de divisão se, e somente se, R^{op} também o é.

(c) $(R^{op})^{op} = R$.

(d) Se S é um anel, então $R \cong S$ se, e somente se, $R^{op} \cong S^{op}$.

Exercício 1.3.44. Mostre que se R é um anel, então $M_n(R)^{op} \cong M_n(R^{op})$. Em particular, se R é comutativo, então $M_n(R)^{op} \cong M_n(R)$. Dê um exemplo de anel tal que $R^{op} \ncong R$.

Dados um anel R e $r \in R$, seja $f_r : R \to R$ definida por $f_r(x) = rx$. Observe que se R não é comutativo, então f_r não é um R-homomorfismo. Por outro lado, se definirmos $f_r(x) = xr$, então obtemos um R-homomorfismo que induz uma aplicação $g : R \to End_R(R)$ dada por $g(r) = f_r$, que não é um homomorfismo de anéis, pois dados $r, s \in R$, $f_{rs}(x) = x(rs) = (xr)s = (f_s \circ f_r)(x)$.

Logo, se considerarmos $g : R^{op} \to End_R(R)$, g é um homomorfismo de anéis. Observe que g é injetiva, pois se $f_r = f_s$, então $r = f_r(1) = f_s(1) = s$. Além disso, g é sobrejetiva, pois dado $h \in End_R(R)$, $h(x) = h(x1) = xh(1) = f_{h(1)}(x)$. Com isso, concluímos o seguinte.

Lema 1.3.45. *Se R é um anel, então $R^{op} \cong End_R(R)$.*

Podemos exibir mais uma classe de anéis semissimples.

Exemplo 1.3.46. Se D é um anel de divisão e V é um D-módulo livre de posto finito, então $End_D(V)$ é um anel semissimples. De fato, $V \cong D^{(n)}$, para algum $n \geqslant 1$, e $End_D(V) \cong End_D(D^{(n)}) \cong M_n(End_D(D)) \cong M_n(D^{op})$. Como D é um anel de divisão, D^{op} também o é. Portanto, $End_D(V)$ é semissimples.

Estamos prontos para exibir o resultado que apresenta a estrutura de anéis semissimples, conhecido como Teorema (estrutural) de Wedderburn.

Teorema 1.3.47 (Wedderburn)**.** *Todo anel semissimples é isomorfo a uma soma direta finita de anéis de matrizes sobre anéis de divisão.*

Demonstração. Seja R um anel semissimples. Pelo Teorema 1.3.34, R tem comprimento finito e, assim, pela Proposição 1.3.41, $End_R(R) \cong \bigoplus_{i=1}^{k} M_{n_i}(D_i)$, onde cada D_i, $i = 1, \ldots, k$, é um anel divisão. Pelo Lema 1.3.45, $R^{op} \cong End_R(R)$. Portanto,

$$R = (R^{op})^{op} \cong \bigoplus_{i=1}^{k} M_{n_i}(D_i)^{op} \cong \bigoplus_{i=1}^{k} M_{n_i}(D_i^{op}).$$

□

Corolário 1.3.48. *Todo anel semissimples é isomorfo a uma soma direta finita de anéis simples.*

Corolário 1.3.49. *Se R é um anel semissimples comutativo, então R é isomorfo a uma soma direta finita de corpos.*

Exercício 1.3.50. Mostre a unicidade da decomposição de um anel semissimples, isto é, mostre que se $R \cong \bigoplus_{i=1}^{k} M_{n_i}(D_i) \cong \bigoplus_{i=1}^{r} M_{m_i}(D_i')$, então $k = r$ e, após uma possível permutação dos índices, $n_i = m_i$ e $D_i \cong D_i'$.

Exercício 1.3.51. Seja R um anel. Mostre que se R é semissimples, então $M_n(R)$ também o é.

Exercício 1.3.52. Seja R um domínio. Mostre que se $M_n(R)$ é semissimples, então R é um anel de divisão.

A decomposição $R \cong R_1 \oplus \cdots \oplus R_n$ de um anel semissimples como a soma direta de anéis simples é chamada de decomposição de Wedderburn de R. Nessa decomposição, cada R_i pode ser visto como $\{0\} \oplus \cdots \oplus R_i \oplus \cdots \{0\}$ em $R_1 \oplus \cdots \oplus R_n$. Com isso, cada R_i é um ideal de R e $R_i R_j = \{0\}$, se $i \neq j$.

Exercício 1.3.53. Seja $R \cong R_1 \oplus \cdots \oplus R_n$ a decomposição de Wedderburn de um anel semissimples. Mostre que cada R_i é um ideal minimal de R.

Exercício 1.3.54. Seja R um anel. Mostre que R é semissimples se, e somente se, todo ideal à esquerda de R é gerado por um idempotente, isto é, se $L \trianglelefteq_l R$, então existe $e \in R$ idempotente tal que $L = Re$. Conclua que se $R \cong R_1 \oplus \cdots \oplus R_n$ é a decomposição de Wedderburn de um anel semissimples, então existe um conjunto $\{e_1, \ldots, e_n\}$ de idempotentes de R tal que:

1. cada e_i é um idempotente central, isto é, $e_i \in Z(R)$, $i = 1, \ldots, n$;
2. $e_i e_j = 0$, se $i \neq j$, isto é, os idempotentes são ortogonais;
3. $1 = e_1 + \cdots + e_n$;
4. cada e_i não pode ser escrito como $e_i = e_i' + e_i''$, onde e_i', e_i'' são idempotentes centrais ortogonais de R.

Além disso, cada e_i é a unidade do anel R_i, $i = 1, \ldots, n$.

Nosso objetivo agora é estudar a estrutura de anéis artinianos simples.

Seja V um espaço vetorial de dimensão finita sobre um corpo F. Como V possui uma F-base, então se $\alpha \in F$ e $v \in V$, $\alpha v = 0$ se, e somente se, $\alpha = 0$. Neste caso, dizemos que V é um F-módulo fiel. De modo geral, temos a seguinte definição.

Definição 1.3.55. Dizemos que um R-módulo M é fiel se

$$\{r \in R : rm = 0, \text{para todo } m \in M\} = \{0\}.$$

O conjunto $\{r \in R : rm = 0, \text{para todo } m \in M\}$ é chamado de anulador de M, denotado por $Ann(M)$. Com isso, um R-módulo M é fiel se, e somente se, $Ann(M) = \{0\}$.

Exercício 1.3.56. Sejam M um R-módulo e $I \trianglelefteq R$ tal que $I \subseteq Ann(M)$. Mostre que $\bar{r}m = rm$, para todos $\bar{r} \in R/I, m \in M$, fornece uma estrutura de (R/I)-módulo a M e os (R/I)-submódulos de M coincidem com os R-módulos de M.

Temos o seguinte resultado.

Lema 1.3.57. *Se M é um R-módulo, então $Ann(M) \trianglelefteq R$ e temos que M é um $(R/Ann(M))$-módulo fiel. Em particular, se R é um anel simples, então M é fiel.*

Demonstração. É claro que se $r, s \in Ann(M)$, então $r+s, rs \in Ann(M)$. Agora, sejam $r \in R$ e $a \in Ann(M)$. Então $(ra)m = r(am) = 0$ e $(ar)m = a(rm) = 0$, já que $rm \in M$. Portanto, $Ann(M) \trianglelefteq R$ e M é um $(R/Ann(M))$-módulo. Logo, se $\bar{r}m = 0$, para todo $m \in M$, então $r \in Ann(M)$ e, portanto, $\bar{r} = \bar{0}$. □

A seguir, apresentamos o teorema que estabelece a estrutura dos anéis artinianos simples, chamado por alguns autores de Teorema de Wedderburn–Artin.

Teorema 1.3.58 (Wedderburn–Artin)**.** *Seja R um anel. São equivalentes:*

1. *R é um anel artiniano simples;*
2. *R é isomorfo a um anel de matrizes com entradas em um anel de divisão;*
3. *R é semissimples e todos os R-módulos simples são isomorfos;*
4. *R é homogêneo;*
5. *R é artiniano e existe um R-módulo simples fiel.*

Demonstração. [(5) $\Rightarrow$ (4)] Seja M um R-módulo simples fiel. Considere, para cada $t \geqslant 1$, $S_t = Hom_R(R, M^{(t)})$. Então a família de todos os núcleos dos R-homomorfismos $f \in S_t$, para todo $t \geqslant 1$, é não vazia e, como R artiniano, existe $n \geqslant 1$ e $f \in S_n$ tal que $\mathrm{Ker}(f)$ é minimal.

Vamos mostrar que $\mathrm{Ker}(f) = \{0\}$ e, com isso, teremos que R é isomorfo a um R-submódulo de um R-módulo homogêneo e, assim, pelo Corolário 1.3.29, concluiremos que R é homogêneo.

Suponha que $f(r) = 0$, com $r \neq 0$. Como M é fiel, existe $m \in M$ tal que $rm \neq 0$. Como M é simples, $M = Rm$. Considere a aplicação $g\colon R \to M^{(n)} \oplus M$ dada por $g(x) = (f(x), xm)$. Então g é um R-homomorfismo e possui núcleo menor que $\mathrm{Ker}(f)$, contrariando a minimalidade de $\mathrm{Ker}(f)$. Portanto, $\mathrm{Ker}(f) = \{0\}$.

[(4) $\Rightarrow$ (3)] Corolário 1.3.35.

[(3) $\Rightarrow$ (2)] Proposição 1.3.41.

[(2) $\Rightarrow$ (1)] Pela Proposição 1.1.37, $M_n(D)$ é simples e, como $M_n(D)$ é semissimples, é um anel artiniano.

[(1) $\Rightarrow$ (5)] Como R é artiniano, R possui um ideal à esquerda minimal I, que é um R-módulo simples. Como R é um anel simples, pelo Lema 1.3.57, I é fiel. □

Observemos que se R é um anel artiniano semissimples, então R tem comprimento finito e, assim, é a soma direta finita de anéis homogêneos. Pelo Teorema de Wedderburn–Artin, cada um desses anéis homogêneos é simples e isomorfo a um anel de matrizes com entradas em um anel de divisão. Com isso, temos o Teorema de Wedderburn para anéis artinianos semissimples.

Assim, terminamos o estudo sobre a estrutura de anéis artinianos semissimples. Uma pergunta natural é a seguinte: existe algum "critério" que nos permite decidir se um anel artiniano é semissimples? A resposta é sim e, para exibi-lo, iremos definir o chamado radical de Jacobson de um anel.

Definição 1.3.59. Seja R um anel. O radical de Jacobson de R, denotado por $J(R)$, é a interseção dos anuladores dos R-módulos simples, isto é,

$$J(R) = \bigcap_{M\ simples} Ann(M).$$

Note que, pelo Lema 1.3.57, $J(R) \trianglelefteq R$ e, como R tem unidade, $J(R) \neq R$. Seja M um R-módulo simples. Então o núcleo do R-homomorfismo $f : R \to M$ dado por $f(r) = rm$ é exatamente $Ann(M)$, que, pela Proposição 1.2.17, é um ideal maximal à esquerda de R. Além disso, um ideal maximal à esquerda I de R é o anulador de algum R-módulo simples, a saber, R/I. Com isso, temos uma definição intrínseca do radical de Jacobson de um anel dada por

$$J(R) = \bigcap_{I \trianglelefteq_l R\, max} I.$$

Observação 1.3.60. Se R é um anel sem unidade, então não é possível garantir a existência de ideais maximais à esquerda de R. Neste caso, definimos $J(R) = R$.

Exemplo 1.3.61. Se R é um anel simples, então $J(R) = \{0\}$.

Exemplo 1.3.62. Os ideais maximais de $\mathbb{Z}$ são da forma $p\mathbb{Z}$, p primo. Portanto, $J(\mathbb{Z}) = \{0\}$.

Exemplo 1.3.63. $J(R/J(R)) = \{0\}$. De fato, todo ideal maximal à esquerda de $R/J(R)$ é da forma $I/J(R)$, onde I é um ideal maximal à esquerda de R. Logo, como $J(R)$ está contido em todo ideal maximal à esquerda de R, $J(R/J(R)) = \cap(I/J(R)) = (\cap I)/(J(R)) = J(R)/J(R) = \{0\}$.

Alguns autores definem que um anel R é semissimples se $J(R) = \{0\}$. Claramente essa definição não concorda com a nossa, pois $J(\mathbb{Z}) = \{0\}$, mas $\mathbb{Z}$ não é semissimples com a nossa definição. O nosso objetivo é mostrar que se R é artiniano e $J(R) = \{0\}$, então R é semissimples.

Exercício 1.3.64. Seja $I \trianglelefteq R$. Mostre que se $J(R/I) = \{0\}$, então $J(R) \subseteq I$. Em particular, se $I \subseteq J(R)$ e $J(R/I) = \{0\}$, então $I = J(R)$.

Exercício 1.3.65. Seja $f : R \to S$ um epimorfismo de anéis. Mostre que $f(J(R)) \subseteq J(S)$. Dê um exemplo onde a inclusão é estrita.

A seguir, vamos mostrar algumas propriedades do radical de Jacobson que nos permitirão exibir mais exemplos.

Dizemos que um elemento x em um anel com unidade R possui inverso à esquerda, se existe $y \in R$ tal que $yx = 1$. Analogamente, definimos o inverso à direita de x. Note que, se y é um inverso à esquerda de x e y' é um inverso à direita de x, então $y = y'$ e, portanto, x é invertível.

Lema 1.3.66. *Sejam R um anel e $x \in R$. Então $x \in J(R)$ se, e somente se, $1 + rx$ possui inverso à esquerda, para todo $r \in R$.*

Demonstração. Se $x \in J(R)$, então $rx \in J(R)$, para todo $r \in R$. Logo, rx pertence a todo ideal maximal à esquerda de R. Com isso, $1 + rx$ não pertence a nenhum ideal maximal à esquerda de R. Logo, $R(1 + rx) = R$ e, portanto, existe $s \in R$ tal que $s(1 + rx) = 1$.

Reciprocamente, se $x \notin J(R)$, então existe $I \trianglelefteq_l R$ maximal tal que $x \notin I$. Como I é maximal, $R = I + Rx$, caso contrário $I + Rx$ seria um ideal à esquerda que contém I. Em particular, $1 = s + rx$, para alguns $s \in I, r \in R$. Logo, $1 - rx = s \in I$ não possui inverso à esquerda, pois se possuísse, então $1 = r's \in I$, para algum $r' \in R$, contrariando a hipótese que $I \neq R$. □

Proposição 1.3.67. *Sejam R um anel e $x \in R$. Se $x \in J(R)$, então $1 + x$ é invertível. Além disso, $J(R)$ é o maior ideal de R com essa propriedade.*

Demonstração. Pelo lema anterior, se $x \in J(R)$, então $1 + x$ possui inverso à esquerda, digamos y. Então $y + yx = 1$ e $y - 1 = -yx \in J(R)$. Escrevendo $z = -yx$, temos que $y = 1 + z, z \in J(R)$ e, novamente pelo lema anterior, $1 + z$ possui inverso à esquerda. Mas, $1 + x$ é um inverso à direita de y. Portanto, $1 + x$ é invertível.

Agora, seja $I \trianglelefteq R$ tal que $1 + x$ é invertível para todo $x \in I$. Então, para todos $r \in R, x \in I$, temos que $1 + rx$ possui inverso à esquerda. Pelo lema anterior, $x \in J(R)$ e, portanto, $I \subseteq J(R)$. □

Corolário 1.3.68. *Seja I um ideal nil de um anel R. Então $I \subseteq J(R)$.*

Demonstração. Se $r \in I$, então $r^n = 0$ para algum $n \in \mathbb{N}$. Assim, pelo Exercício 1.1.25, $1 + r$ é invertível. Pela proposição anterior, temos $I \subseteq J(R)$. □

Estamos em condições para apresentar o seguinte exemplo.

Exemplo 1.3.69. Para todo anel R, $J(M_n(R)) = M_n(J(R))$. Para mostrar que $M_n(J(R)) \subseteq J(M_n(R))$, basta mostrar que $r \in J(R)$ implica que $x = re_{ij} \in J(M_n(R))$, para todo $i, j \in \{1, \ldots, n\}$, isto é, basta mostrar que para todo $y \in M_n(R)$, $z = I_n - yx$ possui inverso à esquerda. Escreva $y = \sum r_{kl}e_{kl}, r_{kl} \in R$. Então

$$z = I_n - yx = I_n - \sum_k r_{ki}re_{kj} = I_n - r_{ji}re_{jj} - \sum_{k \neq j} r_{ki}re_{kj}.$$

Como $r \in J(R)$, $1 - r_{ji}r$ possui inverso à esquerda $1 - s, s \in R$. Logo $I_n - se_{jj}$ é um inverso à esquerda de $I_n - r_{ji}re_{jj}$ e

$$(I_n - se_{jj})z = I_n - \sum_{k \neq j} r_{ki}re_{kj}.$$

Agora, observe que $I_n - \sum_{k \neq j} r_{ki}re_{kj}$ é invertível, com inverso $I_n + \sum_{k \neq j} r_{ki}re_{kj}$. Portanto, z possui inverso à esquerda.

Para mostrar a inclusão inversa, observe que, como $J(M_n(R)) \lhd M_n(R)$, pelo Exercício 1.1.38, podemos escrever $J(M_n(R)) = M_n(I)$, onde $I \trianglelefteq R$. Para todo $r \in I$, $rI_n \in J(M_n(R))$ e, assim, $I_n - srI_n = (1 - sr)I_n$ possui inverso à esquerda, para todo $s \in R$. Isto implica que $1 - sr$ possui inverso à esquerda, para todo $s \in R$ e, portanto, $I \subseteq J(R)$.

Exercício 1.3.70. Seja R um anel e considere $UT_2(R) = \begin{pmatrix} R & R \\ 0 & R \end{pmatrix}$. Mostre que $J(UT_2(R)) = \begin{pmatrix} J(R) & R \\ 0 & J(R) \end{pmatrix}$. Generalize.

Exercício 1.3.71. Sejam R um anel e $x \in R$. Mostre que x é invertível em R se, e somente se, $\bar{x}$ é invertível em $R/J(R)$.

Exercício 1.3.72. Seja R um anel. Mostre que se $e \in R$ é um idempotente tal que $e \in J(R)$, então $e = 0$.

Exercício 1.3.73. Seja $\{R_i\}_{i\in\mathcal{I}}$ uma família de anéis. Mostre que $J\left(\prod_{i\in\mathcal{I}} R_i\right) = \prod_{i\in\mathcal{I}} J(R_i)$. Conclua que, se R é um anel semissimples, então $J(R) = \{0\}$.

Exercício 1.3.74. Um elemento r em um anel R é chamado de não gerador de R, se para todo subconjunto $S \subseteq R$ tal que $S \cup \{r\}$ gera R, então S gera R. Mostre que $J(R)$ é o conjunto dos não geradores de R.

Teorema 1.3.75. *Todo ideal nilpotente de um anel R está contido em $J(R)$. Se R é artiniano, então $J(R)$ é nilpotente e, assim, é o maior ideal nilpotente de R.*

Demonstração. Seja $I \trianglelefteq R$ nilpotente, $I^n = \{0\}$. Vamos mostrar que $IM = \{0\}$, para todo R-módulo simples M. Se $IM \neq \{0\}$, da simplicidade de M, temos que $IM = M$. Com isso, $IM = I^2M = M$ e, assim, $M = I^nM = \{0\}$, absurdo. Portanto, $I \subseteq J(R)$.

Agora, supondo que R seja artiniano e, escrevendo $J = J(R)$, temos que a cadeia $J \supset J^2 \supset \cdots$ estaciona. Logo, existe $n \geqslant 1$ tal que $J^n = J^{n+i}$, para todo $i \geqslant 1$.

Seja $J' = J^n$. Se $J' = \{0\}$, não há nada mais para ser feito. Caso contrário, considere $\mathcal{F} = \{L : L \trianglelefteq_l R, J'L \neq \{0\}\}$ e observe que $\mathcal{F} \neq \varnothing$, já que $J \in \mathcal{F}$.

Como R é artiniano, podemos tomar $L_0 \in \mathcal{F}$ minimal. Como $J'L_0 \neq \{0\}$, tome $r \in L_0$ tal que $J'r \neq \{0\}$. Como $J'r \subseteq L_0$ e $J'(J'r) = J'r \neq \{0\}$, da minimalidade de L_0, temos que $L_0 = J'r$. Com isso, existe $s \in J'$ tal que $sr = r$ e, assim, $(1-s)r = 0$. Mas, como $s \in J$, temos que $1-s$ é invertível e, portanto, temos $r = 0$, o que é uma contradição. Portanto $J^n = \{0\}$ e $J(R)$ é nilpotente. Agora, se $I \trianglelefteq R$ é nilpotente, então em particular I é nil e, pelo Corolário 1.3.68, $I \subseteq J(R)$. □

Corolário 1.3.76. *Em um anel artiniano, todo ideal nil é nilpotente.*

Vamos a mais um exemplo.

Exemplo 1.3.77. Vamos calcular o radical de Jacobson do anel $R = \mathbb{Z}_{p^n}$, p primo. Como R é finito, R é artiniano. Agora, observe que todo ideal de R é da forma $\bar{p}^i R$, $i = 1, \ldots, n$, e para cada i, $\bar{p}^i R$ é um ideal nilpotente, sendo $\bar{p}R$ o maior deles. Portanto, pelo teorema anterior, $J(\mathbb{Z}_{p^n}) = \bar{p}\mathbb{Z}_{p^n}$. Note que se $n \geqslant 2$, então $J(\mathbb{Z}_{p^n}) \neq \{0\}$. Se $n = 1$, como $\mathbb{Z}_p$ é um corpo, temos que $J(\mathbb{Z}_p) = \{0\}$.

Agora, vamos caracterizar os anéis artinianos semissimples. Antes, precisamos do seguinte lema.

Lema 1.3.78. *Se R é um anel artiniano, então existe uma família finita de ideais maximais à esquerda de R $\{L_1, \ldots, L_n\}$ tal que $J(R) = \bigcap_{i=1}^{n} L_i$.*

Demonstração. Seja $\mathcal{F} = \{\bigcap L_i : L_i \trianglelefteq_l R \text{ maximal}, \{L_i\} \text{ finita}\}$. Claramente $\mathcal{F} \neq \varnothing$. Como R é artiniano, seja L um elemento minimal em $\mathcal{F}$. É claro que $J(R) \subseteq L$. Se $I \trianglelefteq_l R$ maximal, então $I \cap L \subseteq L$ e, como L é minimal em $\mathcal{F}$, devemos ter $I \cap L = L$. Logo, $L \subseteq I$ para todo $I \trianglelefteq_l R$ maximal e, assim, $L \subseteq J(R)$. Portanto, $L = J(R)$. □

Teorema 1.3.79. *Seja R um anel. Então R é semissimples se, e somente se, R é artiniano e $J(R) = \{0\}$.*

Demonstração. Se R é semissimples, já sabemos que R é artiniano e $J(R) = \{0\}$. Reciprocamente, suponha que R seja artiniano e $J(R) = \{0\}$. Pelo lema anterior, existe uma família finita de ideais maximais à esquerda $\{L_1, \ldots, L_n\}$ de R tal que $J(R) = \bigcap_{i=1}^{n} L_i = \{0\}$.

Logo, a aplicação canônica $f : R \to \bigoplus_{i=1}^{n} R/L_i$ dada por

$$f(r) = (r + L_1, \ldots, r + L_n)$$

é um monomorfismo de R-módulos. Como cada L_i é maximal, temos que R/L_i é um R-módulo simples, $i = 1, \ldots, n$. Com isso, $\bigoplus_{i=1}^{n} R/L_i$ é semissimples e, portanto, R é semissimples. □

Corolário 1.3.80. *Se R é artiniano, então $R/J(R)$ é semissimples.*

Uma consequência interessante do teorema anterior é o chamado Teorema de Hopkins–Levitzki. Antes, precisamos do seguinte resultado.

Lema 1.3.81. *Seja M um R-módulo artiniano e semissimples. Então M é finitamente gerado.*

Demonstração. Suponha que M não seja finitamente gerado e considere

$$\mathcal{F} = \{N : N \leqslant M, N \text{ não é finitamente gerado}\}.$$

Como $M \in \mathcal{F}$, temos $\mathcal{F} \neq \varnothing$. Logo, como M é artiniano, $\mathcal{F}$ possui um elemento minimal N_0. Com isso, se $N' \leqslant N_0$, então N' é finitamente gerado e

como M é semissimples, N_0 é semissimples. Assim, existe $N'' \leqslant N_0$ tal que $N_0 = N' \oplus N''$ e N_0 é finitamente gerado, o que é um absurdo. Portanto, M é finitamente gerado. □

Teorema 1.3.82 (Hopkins–Levitzki)**.** *Todo anel artiniano é noetheriano.*

Demonstração. Considerando R um anel artiniano, vamos mostrar que R tem comprimento finito. Pelo Teorema 1.3.75, existe $n \geqslant 1$ tal que $J(R)^n = \{0\}$. Para cada $0 \leqslant i \leqslant n-1$, sejam $L_0 = R$ e $L_i = J(R)^i$. Assim,

$$L_0 \supset L_1 \supset \cdots \supset L_{n-1} \supset \{0\}.$$

Como $J(R)L_i \subseteq L_{i+1}$, cada L_i/L_{i+1} admite uma estrutura de $(R/J(R))$-módulo. Assim, para demonstrar o teorema, pelo Lema 1.3.15, basta mostrar que cada L_i/L_{i+1} é um R-módulo de comprimento finito. Desde que R é artiniano, pelo Corolário 1.3.80, $R/J(R)$ é semissimples e, pelo Teorema 1.3.34, cada L_i/L_{i+1} é um $(R/J(R))$-módulo semissimples e artiniano.

Pelo lema anterior, L_i/L_{i+1} é finitamente gerado e, consequentemente, de comprimento finito. Com isso, cada L_i/L_{i+1} é escrito como a soma direta finita de $(R/J(R))$-módulos simples, que, por sua vez, são R-módulos simples. Portanto, R é noetheriano. □

Exercícios V ou F da Seção 1.3: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, R representa um anel com unidade e F é um corpo.

(1) Se M é um R-módulo finitamente gerado e N é R-submódulo de M, então N é finitamente gerado.

(2) Se $f\colon M \to N$ é um epimorfismo de R-módulos e M é semissimples, então N também o é.

(3) O anel dos quatérnios reais $\mathbb{H}$ é semissimples.

(4) Se $x \in R$ e $1 + x$ é invertível, então $x \in J(R)$.

(5) Para todo $n \geqslant 2$, temos $J(UT_n) = \{0\}$.

(6) Para todo $n \geqslant 2$, temos $J(M_n(F)) = \{0\}$.

(7) Para todo $n \geqslant 1$, temos $M_n(F)^{op} \cong M_n(F)$.

1.4 Álgebras

Nosso objetivo nesta seção é introduzir o objeto principal de estudo deste livro, que são as álgebras sobre um corpo F. Começamos definindo o significado de álgebra sobre um anel comutativo R, apresentando resultados gerais a respeito. Além disso, vamos estudar as principais propriedades de uma álgebra e demonstrar o Teorema de Wedderburn–Malcev, que será uma importante ferramenta no estudo de PI-álgebras.

Na Seção 1.2, apresentamos a definição de aplicação bilinear, que agora trataremos em uma situação particular. Recordemos que se R é um anel comutativo e M é um R-módulo, então uma aplicação $f : M \times M \to M$ é denominada bilinear se para todo $m, m_1, m_2 \in M$, $r \in R$:

1. $f(m_1 + m_2, m) = f(m_1, m) + f(m_2, m)$;
2. $f(m, m_1 + m_2) = f(m, m_1) + f(m, m_2)$;
3. $f(rm_1, m_2) = rf(m_1, m_2) = f(m_1, rm_2)$.

Neste caso, podemos ver uma aplicação bilinear f como uma operação em M e denotando por $f(m_1, m_2) := m_1 * m_2$, para todos $m, m_1, m_2 \in M$, $r \in R$, temos que essa operação satisfaz:

1. $(m_1 + m_2) * m = m_1 * m + m_2 * m$;
2. $m * (m_1 + m_2) = m * m_1 + m * m_2$;
3. $(rm_1) * m_2 = m_1 * (rm_2) = r(m_1 * m_2)$.

Agora, damos a nossa definição de álgebra.

Definição 1.4.1. Seja R um anel comutativo. Um R-módulo A munido de uma aplicação bilinear $f : A \times A \to A$ é chamado de R-álgebra (ou álgebra sobre R).

Como R é um anel comutativo, observamos que uma R-álgebra A é um R-bimódulo, com ação definida por $ar = ra$ para todos $a \in A$, $r \in R$.

Por exemplo, todo anel é uma $\mathbb{Z}$-álgebra. Se D é um anel de divisão, então $Z(D)$ é um corpo e, assim, D é uma $Z(D)$-álgebra. Em geral, se R é um anel e F é um subanel de $Z(R)$, então R é uma F-álgebra, com estrutura de F-módulo dada pela multiplicação em R. Em particular, todo anel comutativo R é uma R-álgebra.

Neste livro, estaremos interessados no estudo de álgebras sobre um corpo. Com isso, a partir de agora, usaremos F para denotar um corpo.

Uma F-álgebra A é um F-espaço vetorial junto de uma aplicação bilinear. Salvo menção ao contrário, todas as álgebras daqui em diante serão F-espaços vetoriais. Uma F-base de A é uma F-base de A como espaço vetorial, e a dimensão de uma F-álgebra A é sua dimensão como F-espaço vetorial.

Exemplo 1.4.2. $\mathbb{C}$ é uma álgebra de dimensão 2 sobre $\mathbb{R}$, com base $\{1, i\}$.

Exemplo 1.4.3. O anel das matrizes $M_n(F)$ é uma F-álgebra de dimensão n^2. Uma base dessa álgebra é composta pelas matrizes elementares $\{e_{ij}\}_{i,j=1}^{n}$.

No que segue, se A é uma F-álgebra e $f : A \times A \to A$ é a aplicação bilinear associada, denotaremos $f(a, b) = a * b$, para todo $a, b \in A$. Definimos $a^1 = a$, $a^2 = a * a$ e $a^n = a^{n-1} * a$, para todo $a \in A, n \geqslant 2$.

Definição 1.4.4. Seja A uma F-álgebra. Dizemos que A é:

1. unitária, se existe $1 \in A$ tal que $a * 1 = 1 * a = a$;
2. associativa, se $a * (b * c) = (a * b) * c$;
3. de Lie, se $a * a = 0$ e $(a * b) * c + (b * c) * a + (c * a) * b = 0$;
4. de Jordan, se $a * b = b * a$ e $(a^2 * b) * a = a^2 * (b * a)$

para todos $a, b, c \in A$.

Se A é uma F-álgebra associativa, então A é um F-espaço vetorial munido de uma estrutura de anel. Neste caso, denotaremos por $a * b = ab$, para todo $a, b \in A$, onde ab denota o produto do anel A.

Em uma F-álgebra de Lie L, é usual denotar $a * b := [a, b]$. Assim, em uma álgebra de Lie L, é válido que, para todos $a, b, c \in L$, $[a, a] = 0$ e

$$[[a, b], c] + [[b, c], a] + [[c, a], b] = 0.$$

Esta relação é usualmente chamada de identidade de Jacobi.

Exemplo 1.4.5. O $\mathbb{R}$-espaço vetorial $\mathbb{R}^3$ com produto dado pelo produto vetorial entre vetores é uma álgebra de Lie de dimensão 3 sobre $\mathbb{R}$.

Exemplo 1.4.6. O anel de polinômios $F[x]$, com adição e multiplicação usuais, é uma F-álgebra associativa de dimensão infinita sobre F.

Exercício 1.4.7. Seja L uma F-álgebra de Lie. Mostre que, para todos $a, b \in L$, $[a, b] = -[b, a]$. Mostre que se $\text{char}(F) \neq 2$, então esta propriedade é equivalente a $[a, a] = 0$, para todo $a \in L$.

Exercício 1.4.8. Seja A uma F-álgebra associativa. Mostre que:

(a) o produto $[a, b] = ab - ba$, para todos $a, b \in A$, fornece uma estrutura de álgebra de Lie para A.

(b) se $\text{char}(F) \neq 2$, o produto $a \circ b = \frac{1}{2}(ab + ba)$, para todos $a, b \in A$, fornece uma estrutura de álgebra de Jordan para A.

Sejam A uma F-álgebra e $B = \{a_i : i \in \mathcal{I}\}$ uma base de A. Uma multiplicação em A é totalmente determinada pela multiplicação entre os elementos de B. Dados $a_i, a_j \in B$, temos que

$$a_i * a_j = \sum_{k \in \mathcal{I}} \alpha_{ij}^k a_k$$

onde $\alpha_{ij}^k \in F$ e, fixados i e j, apenas um número finito de α_{ij}^k são não nulos. Os elementos $\alpha_{ij}^k \in F$ são chamados de constantes estruturais da álgebra A.

No decorrer deste livro, a palavra "álgebra" será sinônimo de álgebra associativa. Logo, uma F-álgebra A é um anel, com estrutura de F-espaço vetorial, de tal maneira que as operações no anel A são compatíveis com a ação de F sobre o espaço vetorial A. Além disso, ao dizer que A é uma álgebra, estará implícito que A está sendo tomada sobre um corpo F, e todas as álgebras, salvo menção ao contrário, serão tomadas sobre o mesmo corpo base F.

Dessa maneira, temos também as seguintes definições.

Definição 1.4.9. Dizemos que uma F-álgebra A é comutativa (nil, nilpotente, de divisão), se A é um anel comutativo (nil, nilpotente, de divisão).

Agora, iremos traduzir os conceitos estabelecidos nas seções anteriores para a linguagem de álgebras.

Uma subálgebra de uma álgebra A é um subanel de A que também é um subespaço vetorial de A. Um ideal (à esquerda, à direita, bilateral) de A é um ideal (à esquerda, à direita, bilateral) de A que também é um subespaço vetorial de A. Como antes, a palavra ideal será sinônimo de ideal bilateral. As noções de ideal minimal e maximal são definidas analogamente.

Exemplo 1.4.10. O anel de matrizes triangulares superiores UT_n com entradas em F é uma subálgebra de $M_n(F)$.

Observação 1.4.11. Se A é uma álgebra, então um ideal do anel A não necessariamente é um ideal da álgebra A. De fato, seja $A = \text{span}_{\mathbb{Q}}\{v\}$, $v \neq 0$, um espaço vetorial unidimensional sobre $\mathbb{Q}$. Se definirmos $ab = 0$, para todos $a, b \in A$, então A é uma $\mathbb{Q}$-álgebra. Se R é um subanel próprio de $\mathbb{Q}$, então o conjunto Rv é um ideal do anel A, mas não é um ideal da $\mathbb{Q}$-álgebra A.

Apesar da observação acima, se A é uma F-álgebra unitária, para todos $\alpha \in F$ e $a \in A$, temos:

$$\alpha a = \alpha(1_A a) = (\alpha 1_A)a \quad \text{e} \quad \alpha a = (\alpha a)1_A = a(\alpha 1_A).$$

Logo, se I é um ideal à esquerda (direita) do anel A, temos:

$$\alpha I = (\alpha 1_A)I \subseteq I \quad (\alpha I = I(\alpha 1_A) \subseteq I).$$

Portanto, se A é unitária, então todo ideal (à esquerda, à direita, bilateral) do anel A é também um ideal (à esquerda, à direita, bilateral) da álgebra A. A álgebra quociente de uma álgebra A por um ideal I é definida de maneira análoga ao caso de anéis e módulos.

Exercício 1.4.12. Seja A uma F-álgebra. Mostre que um subconjunto I de A é um ideal maximal regular à esquerda da álgebra A (Definição 1.2.16) se, e somente se, I é um ideal maximal regular à esquerda do anel A.

Uma aplicação $f : A \to A'$, entre duas F-álgebras A e A', é chamado um homomorfismo (de álgebras) se, para todos $a, b \in A, \alpha \in F$, temos

1. $f(\alpha a) = \alpha f(a)$;
2. $f(a + b) = f(a) + f(b)$;
3. $f(ab) = f(a)f(b)$.

Em outras palavras, um homomorfismo de álgebras é um homomorfismo de anéis F-linear. Com isso, o núcleo e imagem de f são definidos assim como no caso de módulos. As noções de monomorfismos, epimorfismos, endomorfismos e isomorfismos de álgebras são claras. Além disso, os teoremas do isomorfismo continuam válidos na classe das álgebras.

Exercício 1.4.13. O centro $Z(A)$ de uma F-álgebra A é definido como sendo o centro do anel A. Mostre que $Z(A)$ é uma subálgebra de A. Além disso, se A é uma F-álgebra unitária, mostre que $Z(A)$ contém um corpo isomorfo a F.

Exercício 1.4.14. Mostre que se A é uma F-álgebra, então $End_F(A)$ também o é. Além disso, se A tem dimensão finita n sobre F, então $End_F(A) \cong M_n(F)$.

Se $\{A_i\}_{i\in\mathcal{I}}$ é uma família de F-álgebras, então o produto direto $\prod_{i\in\mathcal{I}} A_i$ e a soma direta $\bigoplus_{i\in\mathcal{I}} A_i$ são definidos como no caso de anéis e módulos.

Observação 1.4.15. Como uma álgebra possui estrutura de anel e de espaço vetorial, utilizaremos símbolos diferentes para denotar a soma direta como anel e como espaço vetorial. Se A, A' são álgebras, então $A \dot{+} A'$ denotará a soma direta como espaços vetoriais, enquanto $A \oplus A'$ denotará a soma direta como anéis.

Por exemplo, se A é uma álgebra e B, C, D são subálgebras de A, então a notação $A = (B \oplus C) \dot{+} D$ diz que A se escreve como uma soma direta dos espaços vetoriais $B \oplus C$ e D, onde $B \oplus C$ é uma soma direta de anéis.

Exemplo 1.4.16. Como $\{e_{11}, e_{22}, e_{12}\}$ é uma F-base da F-álgebra UT_2, temos que $UT_2 = (Fe_{11} \dot{+} Fe_{22}) \dot{+} Fe_{12}$. Mas a soma $Fe_{11} \dot{+} Fe_{22}$ também é direta como anéis. Logo, escreveremos $UT_2 = Fe_{11} \oplus Fe_{22} \dot{+} Fe_{12}$. Observe que essa soma não é direta como anéis, somente como espaços vetoriais.

A seguir, apresentamos uma definição que será utilizada até o fim da seção.

Definição 1.4.17. Sejam A uma F-álgebra e M um F-módulo. Dizemos que M é um A-módulo à esquerda, A vista como álgebra, se M é módulo à esquerda sobre o anel A e $\alpha(am) = a(\alpha m) = (\alpha a)m$, para todos $\alpha \in F$, $a \in A$ e $m \in M$. Analogamente, definimos A-módulo à direita, A-submódulos, A-módulos simples e A-bimódulos. Daqui em diante, sempre que A for uma F-álgebra, a noção de A-módulo será de acordo com essa definição. Uma aplicação $f : M \to N$ de A-módulos é um A-homomorfismo, se é uma aplicação F-linear e um A-homomorfismo de módulos.

Exercício 1.4.18. Mostre que o Lema de Schur é válido para a classe dos A-módulos, isto é, mostre que, se M é um A-módulo simples, então $D = End_A(M)$ é uma F-álgebra de divisão, onde $End_A(M)$ denota o conjunto de todos os A-endomorfismos de M.

Temos o seguinte resultado.

Proposição 1.4.19. *Seja A uma F-álgebra. Todo A-módulo simples é um módulo simples sobre o anel A. Reciprocamente, a todo módulo simples M sobre o anel A, pode ser dado uma única estrutura de F-espaço vetorial tal que M é um A-módulo simples.*

Demonstração. Seja M um A-módulo simples. Logo, $AM \neq \{0\}$. Se M' um submódulo sobre o anel A de M, então AM' é um A-submódulo de M e, como M é um A-módulo simples, $AM' = M$ ou $AM' = \{0\}$. No primeiro caso, $M' = M$. Se $AM' = \{0\}$, então $M' \subseteq N = \{m \in M : Am = 0\}$. Mas N é um A-submódulo de M e $N \neq M$, já que $AM \neq \{0\}$. Com isso, $N = \{0\}$ e, concluímos, $M' = \{0\}$. Logo, M não possui submódulos sobre o anel A e, portanto, M é um módulo simples sobre o anel A.

Agora, se M um módulo simples sobre o anel A, então $M = Am$, para algum $m \in M$, $m \neq 0$. Para todos $\alpha \in F, a \in A, m \in M$, defina $\alpha(am) = (\alpha a)m$. Como $\alpha a \in A$, $(\alpha a)m \in M$. Para mostrar que essa ação de F sobre M está bem definida, precisamos mostrar que se $am = a_1 m$, então $(\alpha a)m = (\alpha a_1)m$, para todos $a, a_1 \in A$, $m \in M$ e $\alpha \in F$. Logo, é suficiente mostrar que se $am = 0$, então $(\alpha a)m = 0$.

Pela Proposição 1.2.17, $M = Am \cong A/I$, para algum ideal à esquerda maximal regular do anel A, e I é o núcleo da aplicação $f : A \to M$ dada por $f(a) = am$. Consequentemente, $am = 0$ implica que $a \in I$. Mas, pelo Exercício 1.4.12, I é um ideal da álgebra A e, assim, $\alpha a \in I$. Logo, $(\alpha a)m = 0$ e a ação de F sobre M é bem definida. A verificação que, com a ação assim definida, M é um F-espaço vetorial e um A-módulo é deixada como exercício. Além disso, essa estrutura em $M = Am$ é unicamente determinada, já que todo A-módulo necessariamente satisfaz $\alpha(am) = (\alpha a)m$, para todos $\alpha \in F, a \in A$. □

As noções de álgebras simples, semissimples e o radical de Jacobson de uma álgebra são definidas da mesma forma como no caso de anéis. Pela Proposição 1.4.19, toda álgebra simples é um anel simples. Além disso, álgebras artinianas e noetherianas são definidas analogamente ao caso de anéis e módulo. Neste caso, uma álgebra artiniana pode não ser um anel artiniano. Por exemplo, a $\mathbb{Q}$-álgebra $A = \text{span}_{\mathbb{Q}}\{v\}$ definida anteriormente é uma álgebra artiniana, mas não é um anel artiniano. Toda álgebra de dimensão finita é artiniana e noetheriana.

Exercício 1.4.20. Mostre que o radical de Jacobson de uma álgebra A coincide com o radical de Jacobson do anel A.

O exercício anterior nos permite estender todas as propriedades do radical de

Jacobson de um anel, vistas na Seção 1.3, para o radical de Jacobson de uma álgebra.

Sejam A uma álgebra e $X \subseteq A$. Se $A = \langle X \rangle$, então dizemos que X gera A, como álgebra. Se X é finito, então dizemos que A é uma álgebra finitamente gerada. Como toda álgebra de dimensão finita é noetheriana, então toda álgebra de dimensão finita é finitamente gerada, mas a recíproca não é verdadeira.

Com todos os resultados apresentados até aqui, deixamos como exercício a demonstração do Teorema de Wedderburn–Artin para álgebras.

Teorema 1.4.21 (Wedderburn–Artin)**.** *Seja A uma F-álgebra. Então A é uma álgebra artiniana semissimples se, e somente se, existe um isomorfismo de F-álgebras*

$$A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_t}(D_t)$$

onde cada n_i é um inteiro positivo e cada D_i é uma álgebra de divisão sobre F.

Corolário 1.4.22. *Toda F-álgebra artiniana semissimples é um anel semissimples.*

Neste ponto, antes de continuarmos o estudo das álgebras, convém fazer uma pequena revisão sobre extensões de corpos, úteis no decorrer desse livro.

Ao longo dessa revisão, K e F denotarão corpos, e assumiremos que o leitor possui conhecimentos básicos sobre anéis de polinômios. Sugerimos o livro de Gonçalves (1979) para a consulta das demonstrações.

Recordemos que K é uma extensão de F se F é um subcorpo de K, isto é, F é um subconjunto de K e, com as operações de K, é um corpo. Se K é uma extensão de F, então K pode ser visto como uma F-álgebra, e a dimensão de K sobre F é chamada de grau da extensão e denotada por $[K : F]$. A extensão é finita se $[K : F] < \infty$, sendo denominada infinita caso contrário. É fácil verificar que se K é uma extensão de F, então $1_K = 1_F$.

Por exemplo, temos uma cadeia de extensões de corpos $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, onde $[\mathbb{C} : \mathbb{R}] = 2$, enquanto $[\mathbb{R} : \mathbb{Q}] = \infty$.

Considerando K uma extensão de F e $\Gamma \subset K$, definimos o subcorpo (subanel) de K gerado por Γ como a interseção de todos os subcorpos (subanéis) de K que contém Γ. Além disso, o subcorpo (subanel) de K gerado por $F \cup \Gamma$ é chamado de subcorpo (subanel) gerado por Γ sobre F, sendo denotado por $F(\Gamma)$ ($F[\Gamma]$). Observe que $F[\Gamma]$ é necessariamente um domínio de integridade. Quando $\Gamma = \{\alpha_1, \ldots, \alpha_n\}$ é finito, denotamos $F(\Gamma) = F(\alpha_1, \ldots, \alpha_n)$ ($F[\Gamma] = F[\alpha_1, \ldots, \alpha_n]$). Particularmente, se $\Gamma = \{\alpha\}$, então dizemos que $F(\alpha)$ é uma extensão simples de F.

Observação 1.4.23. O anel $F[\Gamma]$ é formado por todos os elementos da forma $h(u_1, \ldots, u_n)$, onde $u_i \in \Gamma$, $i = 1, \ldots, n$, e $h(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$, o anel de polinômios com coeficientes em F nas variáveis $x_1, \ldots, x_n$. Já o corpo $F(\Gamma)$ consiste de todos os elementos da forma $h_1(u_1, \ldots, u_n)h_2(u_1, \ldots, u_n)^{-1}$, onde $u_1, \ldots, u_n \in \Gamma$ e $h_1(x_1, \ldots, x_n), h_2(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$.

Se K é uma extensão de F e $u \in K$, dizemos que u é algébrico sobre F se u é raiz de algum polinômio $f(x) \in F[x]$. Caso contrário, dizemos que u é transcendente. Se $u \in K$ é algébrico sobre F, então existe um polinômio mônico irredutível $g(x) \in F[x]$ tal que $g(u) = 0$. Tal polinômio é chamado de polinômio minimal de u.

Algumas extensões são de tipos particulares, como na próxima definição.

Definição 1.4.24. Dizemos que K é uma extensão algébrica de F, se todo elemento de K é algébrico sobre F. Além disso, K é uma extensão transcendente de F, se pelo menos um elemento de K é transcendente sobre F.

Por exemplo, $i \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$ e, consequentemente, sobre $\mathbb{R}$. Temos que $\mathbb{C}$ é uma extensão algébrica de $\mathbb{R}$, pois $\mathbb{C} = \mathbb{R}(i)$. Por outro lado, $\mathbb{R}$ é uma extensão transcendente de $\mathbb{Q}$, pois, por exemplo, os elementos π e e são transcendentes sobre $\mathbb{Q}$.

Se K é uma extensão de F e $u \in K$ é algébrico sobre F, então $F(u) = F[u]$ e $[F(u) : F] = n$, onde n é o grau do polinômio minimal $f(x)$ de u. Além disso, $\{1, u, \ldots, u^{n-1}\}$ é uma base de $F(u)$ sobre F e $F(u) \cong F[x]/\langle f(x)\rangle$. Reciprocamente, se K é uma extensão finita de F, então K é uma extensão algébrica de F.

Se $f(x) \in F[x]$, dizemos que $f(x)$ cinde sobre F se $f(x)$ pode ser escrito na forma

$$f(x) = u_0(x - u_1) \cdots (x - u_n)$$

onde cada $u_i \in F, i = 0, \ldots, n$. Uma extensão K de F é um corpo de decomposição de um polinômio $f(x) \in F[x]$, se $f(x)$ cinde sobre K e $K = F(u_1, \ldots, u_n)$, onde $u_1, \ldots, u_n$ são as raízes de $f(x)$ em K. Todo polinômio $f(x) \in F[x]$ de grau $n \geqslant 1$ possui um corpo de decomposição K sobre F e $[K : F] \leqslant n!$.

Por exemplo, as únicas raízes de $x^2 - 5$ sobre $\mathbb{Q}$ são $\pm\sqrt{5}$, e temos $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$. Logo, $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sqrt{5}, -\sqrt{5})$ é um corpo de decomposição de $x^2 - 5$ sobre $\mathbb{Q}$. Observe que se u é uma raiz real de $f(x) = x^3 - 5$, então $\mathbb{Q}(u) \subset \mathbb{R}$ e, assim, $\mathbb{Q}(u)$ não é um corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$, pois não contém todas as raízes de $f(x)$.

Definição 1.4.25. Seja $f \in F[x]$ um polinômio irredutível sobre F.

1. Dizemos que f é separável se em algum corpo de decomposição de f sobre F toda raiz de f é simples.

2. Se K é uma extensão de F e $u \in K$ é algébrico sobre F, dizemos que u é separável sobre F se seu polinômio minimal é separável.

3. Se todo elemento de K é separável sobre F, então K é chamado de uma extensão separável de F.

O resultado a seguir é conhecido como teorema do elemento primitivo.

Teorema 1.4.26. *Se K é uma extensão finita e separável de F, então existe $u \in K$ tal que $K = F(u)$.*

Por exemplo, o polinômio $x^2 + 1 \in \mathbb{Q}[x]$ é separável, pois temos $x^2 + 1 = (x - i)(x + i) \in \mathbb{C}[x]$. Por outro lado, $x^2 + 1 \in \mathbb{Z}_2[x]$ não é separável, pois não é irredutível e $x^2 + 1 = (x + 1)^2$ em $\mathbb{Z}_2[x]$.

Observação 1.4.27. Um polinômio irredutível $f(x) \in F[x]$ é separável se, e somente se, $f'(x) \neq 0$, onde $f'(x)$ denota a derivada formal de $f(x)$. Com isso, se $\text{char}(F) = 0$, todo polinômio irredutível é separável e, portanto, toda extensão algébrica de F é separável.

Se F é um corpo, então as seguintes afirmações são equivalentes:

1. todo polinômio não constante $f \in F[x]$ possui uma raiz em F;

2. todo polinômio não constante $f \in F[x]$ cinde sobre F;

3. todo polinômio irredutível em $F[x]$ tem grau 1;

4. se K é uma extensão algébrica de F, então $K = F$;

5. existe um subcorpo F' de F tal que F é uma extensão algébrica de F' e todo polinômio em $F'[x]$ cinde sobre F.

Um corpo que satisfaz uma das condições equivalentes acima é denominado algebricamente fechado. Por exemplo, $\mathbb{C}$ é um corpo algebricamente fechado.

Se K é uma extensão de F, então dizemos que K é um fecho algébrico de F se K é uma extensão algébrica de F e K é algebricamente fechado. De maneira equivalente, K é o fecho algébrico de F se K é o corpo de decomposição de todos os polinômios em $F[x]$. Todo corpo F possui um fecho algébrico, e quaisquer dois fechos algébricos de F são isomorfos como espaços vetoriais sobre F. Por exemplo, $\mathbb{C}$ é o fecho algébrico de $\mathbb{R}$, mas $\mathbb{R}$ não é o fecho algébrico de $\mathbb{Q}$.

Exercício 1.4.28. Dizemos que um corpo é primo se ele não possui subcorpos próprios. Mostre que $\mathbb{Q}$ e $\mathbb{Z}_p$, p primo, são corpos primos.

Exercício 1.4.29. Seja F um corpo. Mostre que a interseção P de todos os subcorpos de F é um corpo. Além disso, mostre que P é um corpo primo.

Exercício 1.4.30. Sejam F um corpo e P seu corpo primo. Mostre que $P \cong \mathbb{Q}$ ou $P \cong \mathbb{Z}_p$, p primo, de acordo com a característica de F seja 0 ou p, respectivamente. Conclua que $\mathbb{Q}$ e $\mathbb{Z}_p$ são, a menos de isomorfismos, os únicos corpos primos.

Agora vamos continuar nosso estudo sobre álgebras. A seguir, vamos mostrar que o produto tensorial de duas álgebras é uma álgebra.

Teorema 1.4.31. *Se M, N são F-álgebras, então $M \otimes_F N$ é uma F-álgebra com multiplicação dada por*

$$\left(\sum_i m_i \otimes n_i\right)\left(\sum_j m_j \otimes n_j\right) = \sum_{i,j} m_i m_j \otimes n_i n_j.$$

Demonstração. Para cada $m \in M$ e $n \in N$, seja $f_{mn}\colon M \times N \to M \otimes_F N$ definida por $f_{mn}(x, y) = mx \otimes ny$. Temos que f_{mn} é uma aplicação balanceada e, pelo Teorema 1.2.57, existe uma única aplicação F-linear $\bar{f}_{mn}\colon M \otimes_F N \to M \otimes_F N$ tal que $\bar{f}_{mn}(x \otimes y) = mx \otimes ny$, para todo $x \otimes y \in M \otimes_F N$.

Agora, seja

$$\mathcal{B}(M \otimes_F N) = \{f : M \times N \to M \otimes_F N : f \text{ é balanceada}\}.$$

É fácil verificar que $\mathcal{B}(M \otimes_F N)$ é um F-espaço vetorial e a aplicação $g\colon M \times N \to \mathcal{B}(M \otimes_F N)$ dada por $g(m, n) = f_{mn}$ é balanceada. Novamente, pelo Teorema 1.2.57, existe uma única aplicação F-linear $\bar{g}\colon M \otimes_F N \to \mathcal{B}(M \otimes_F N)$ tal que $\bar{g}(m \otimes n) = f_{mn}$.

Finalmente, dados $x = \sum_i m_i \otimes n_i$, $y = \sum_j m_j \otimes n_j \in M \otimes_F N$, defina $xy := \bar{g}(x)(y)$ e verifique que $M \otimes_F N$ com esse produto é uma F-álgebra. Para finalizar a demonstração, basta mostrar que esse produto coincide com o produto do enunciado.

Temos que:

$$\begin{aligned} xy &= \bar{g}(x)(y) \\ &= \bar{g}\left(\sum_i m_i \otimes n_i\right)\left(\sum_j m_j \otimes n_j\right) \\ &= \sum_i \bar{g}(m_i \otimes n_i)\left(\sum_j m_j \otimes n_j\right) \\ &= \sum_i f_{m_i n_i}\left(\sum_j m_j \otimes n_j\right) \\ &= \sum_{i,j} f_{m_i n_i}(m_j \otimes n_j) \\ &= \sum_{i,j} m_i m_j \otimes n_i n_j. \end{aligned}$$

□

Como consequência dos Corolários 1.2.59 e 1.2.61, temos os seguintes corolários.

Corolário 1.4.32. *Se M, N são F-álgebras de dimensão finita, então $M \otimes_F N$ é uma F-álgebra de dimensão finita e* $\dim_F(M \otimes_F N) = \dim_F(M)\dim_F(N)$.

Corolário 1.4.33. *Sejam A uma F-álgebra e K uma extensão de F. Então $A \otimes_F K$ é uma K-álgebra e* $\dim_K(A \otimes_F K) = \dim_F(A)$.

Dizemos que a K-álgebra $A \otimes_F K$ do corolário anterior foi obtida através de A por meio da extensão dos escalares.

Se M, N são F-álgebras unitárias, então $M \otimes_F N$ também o é e $1_{M\otimes_F N} = 1_M \otimes 1_N$. As aplicações $i : M \to M \otimes_F N$ e $j : N \to M \otimes_F N$ dadas por $i(m) = m \otimes 1_N$ e $j(n) = 1_M \otimes n$, respectivamente, são monomorfismos de álgebras. Com isso, podemos identificar M e N como subálgebras de $M \otimes_F N$ e, com essa identificação,

$$mn = (m \otimes 1_N)(1_M \otimes n) = m \otimes n = (1_M \otimes n)(m \otimes 1_N) = nm.$$

Assim, M e N são subálgebras que comutam em $M \otimes_F N$. A partir de agora, se no produto tensorial $M \otimes_F N$, temos que M, ou N, é unitária, sempre faremos essa identificação.

Exercício 1.4.34. Se A_1, A_2 e A são F-álgebras, mostre que $(A_1 \oplus A_2) \otimes_F A \cong (A_1 \otimes_F A) \oplus (A_2 \otimes_F A)$. Generalize.

Exercício 1.4.35. Se A e B são F-álgebras, mostre que vale $Z(A \otimes_F B) = Z(A) \otimes_F Z(B)$.

Definição 1.4.36. Dizemos que uma F-álgebra A unitária é central simples se A é uma álgebra simples e $Z(A) \cong F$.

Por exemplo, para todo $n \geqslant 1$, $M_n(F)$ é uma F-álgebra central simples. Também, o anel dos quatérnios reais $\mathbb{H}$ é uma $\mathbb{R}$-álgebra central simples. Por outro lado, se K é uma extensão própria de F, então K não é uma F-álgebra central simples, pois $Z(K) = K \neq F$.

Exercício 1.4.37. Seja A uma F-álgebra central simples de dimensão finita n. Mostre que $A \otimes_F A^{op} \cong M_n(F)$.

Lema 1.4.38. *Sejam A uma F-álgebra central simples e B uma F-álgebra unitária simples. Então $A \otimes_F B$ é simples.*

Demonstração. Seja $I \trianglelefteq A \otimes_F B$. Primeiro, suponha que existe $a \otimes b \in I$, $a \otimes b \neq 0$. Como A é simples, $\langle a \rangle = A$ e existem $a_i, a_i' \in A$ tais que $\sum_{i=1}^{n} a_i a a_i' = 1_A$. Logo, $1_A \otimes b = \sum_{i=1}^{n} (a_i \otimes 1_B)(a \otimes b)(a_i' \otimes 1_B) \in I$. Como B é simples, $B = \langle b \rangle$ e temos que $B \subseteq I$. Com isso, $1_A \otimes 1_B \in I$ e, portanto, $I = A \otimes_F B$.

No caso geral, seja $x = a_1 \otimes b_1 + \cdots + a_n \otimes b_n \in I$, com n o menor possível. Podemos assumir que $\{a_i\}_{i=1}^n$ é linearmente independente sobre F, pois, caso contrário, poderíamos escrever x como uma combinação linear de menos parcelas. Pelo mesmo motivo, podemos assumir que $\{b_i\}_{i=1}^n$ é linearmente independente sobre F. Além disso, pela situação anterior, podemos assumir que $a_1 = 1_A \in F$. Suponha que $n > 1$. Então $a_2 \notin F$, pois, caso contrário, a_1 e a_2 seriam linearmente dependentes, contrariando a minimalidade de n. Como $Z(A) = F$, existe $a \in A$ tal que $aa_2 \neq a_2 a$. Então o elemento

$$(a \otimes 1_B)x - x(a \otimes 1_B) = (aa_2 - a_2 a) \otimes b_2 + \cdots + (aa_n - a_n a) \otimes b_n \in I$$

e, como $\{b_i\}_{i=1}^n$ é linearmente independente sobre F e $aa_2 - a_2 a \neq 0$, esse elemento é não nulo, um absurdo, pois contraria a minimalidade de n. Portanto, $n = 1$ e pelo caso anterior o resultado está mostrado. □

Antes de demonstrar o próximo resultado, apresentaremos um lema técnico.

Lema 1.4.39. *Seja A uma F-álgebra simples de dimensão finita. Se M_1 e M_2 são A-módulos de mesma dimensão finita sobre F, então $M_1 \cong M_2$.*

Demonstração. Como A tem dimensão finita e é simples, A é artiniana e simples e, pelo Teorema de Wedderburn–Artin, possui um único A-módulo simples M. Assim, $M_1 \cong M^{n_1}$, $M_2 \cong M^{n_2}$, para alguns $n_1, n_2 \geqslant 1$. Como $\dim_F(M_i) = n_i \dim_F(M)$, $i = 1, 2$, se $\dim_F(M_1) = \dim_F(M_2)$, então $n_1 = n_2$. Portanto, $M_1 \cong M_2$. □

Os resultados anteriores nos permitem demonstrar o chamado Teorema de Skolem–Noether. Recorde que se A é uma F-álgebra, então um automorfismo $f : A \to A$ é chamado de automorfismo interno se existe $a \in \mathcal{U}(A)$ tal que $f(x) = axa^{-1}$ para todo $x \in A$.

Teorema 1.4.40 (Skolem–Noether)**.** *Sejam A uma F-álgebra central simples de dimensão finita e B uma F-álgebra simples. Se $f, g : B \to A$ são homomorfismos de álgebras não nulos, então existe um automorfismo interno $i : A \to A$ tal que $i \circ f = g$. Em particular, todo automorfismo de A é interno.*

Demonstração. Como A é simples e tem dimensão finita, A é artiniana e pelo Teorema de Wedderburn–Artin, temos

$$A \cong M_n(D) \cong End_D(V)$$

onde D é um anel de divisão, V é um D-módulo livre de posto n, $Z(A) \cong Z(D) \cong F$ e D tem dimensão finita sobre F.

Como $f, g : A \to B$ são homomorfismos não nulos, da simplicidade de A e de B, segue que f e g são isomorfismos. Logo, B tem dimensão finita sobre F. Além disso, V é um B-módulo via f e g, definindo $bv = f(b)(v)$, $bv = g(b)(v)$, para todos $b \in B, v \in V$, e

$$b(dv) = f(b)(dv) = df(b)(v) = d(bv) \tag{1.2}$$

para todos $b \in B, d \in D$ e $v \in V$.

Como a Equação (1.2) também é válida para g, temos que V é um espaço vetorial de dimensão finita sobre F e é um $(B \otimes_F D)$-módulo de duas maneiras diferentes: via $(b \otimes d)v = df(b)(v)$ e via $(b \otimes d)v = dg(b)(v)$. Mas, pelo Lema 1.4.38, $B \otimes_F D$ é simples e tem dimensão finita sobre F. Pelo lema anterior, essas duas estruturas de $(B \otimes_F D)$-módulo de V são isomorfas.

Logo, existe um isomorfismo $h : V \to V$ tal que $h(f(b)(v)) = g(b)(h(v))$ e $h(dv) = dh(v)$, para todo $b \in B, d \in D, v \in V$. Portanto, $h \in End_D(V) \cong A$ e $hf(b) = g(b)h$, para todo $b \in B$, isto é, $g(b) = hf(b)h^{-1}$. □

Corolário 1.4.41. *Se F é um corpo, então todo automorfismo de $M_n(F)$ é interno.*

Agora, queremos estudar a semissimplicidade do produto tensorial de álgebras. Começamos com o seguinte resultado.

Lema 1.4.42. *Seja L uma extensão finita de F. Então $L \otimes_F K$ é uma K-álgebra semissimples, para toda extensão K de F, se, e somente se, L é uma extensão separável de F.*

Demonstração. Suponha que L seja uma extensão finita e separável de F. Pelo Teorema 1.4.26, existe $u \in L$ tal que $L = F(u)$. Logo, o conjunto $\{1, u, \ldots, u^{n-1}\}$ é uma F-base de L, $[L : F] = n$, onde n é o grau do polinômio minimal f de u, e $L \cong F[x]/\langle f(x)\rangle$.

Agora, por um abuso de notação, pelo Corolário 1.2.61, $\{1, u, \ldots, u^{n-1}\}$ é uma K-base de $L \otimes_F K$ e, assim, $L \otimes_F K \cong K[x]/\langle f(x)\rangle$. Como f é separável, existem polinômios irredutíveis distintos $f_1(x), \ldots, f_n(x) \in K[x]$ tais que $f(x) = f_1(x) \cdots f_n(x)$. Como $mdc(f_i, f_j) = 1$, se $i \neq j$, temos que $K[x]/\langle f(x)\rangle \cong \bigoplus_{i=1}^{n} K[x]/\langle f_i(x)\rangle$, a soma direta de corpos. Portanto, $L \otimes_F K$ é semissimples.

Reciprocamente, suponha que L não seja uma extensão separável de F. Então existe $u \in L$ que não é separável, isto é, o polinômio minimal f de u não é polinômio separável. Logo, existe uma extensão K de L tal que f possui raízes múltiplas e, portanto, $F(u) \otimes_F K \cong K[x]/\langle f(x)\rangle$ possui elementos nilpotentes não nulos.

Como $F(u) \otimes_F K \subseteq L \otimes_F K$, temos que $L \otimes_F K$ também possui elementos nilpotentes não nulos. Como $L \otimes_F K$ é comutativo, isso nos diz que $L \otimes_F K$ possui ideais nil não nulos. Assim, $J(L \otimes_F K) \neq \{0\}$ e, portanto, $L \otimes_F K$ não é semissimples. □

Com isso, temos que o produto tensorial de duas extensões de F é semissimples se, e somente se, um dos fatores é uma extensão finita e separável de F.

Suponha que A seja uma F-álgebra simples de dimensão finita. Pelo Teorema de Wedderburn–Artin, $Z(A)$ é um corpo e, assim, A é uma $Z(A)$-álgebra central simples. Além disso, $A \otimes_F B \cong A \otimes_{Z(A)} (Z(A) \otimes_F B)$, para toda F-álgebra B.

Agora, suponha que A seja uma F-álgebra semissimples de dimensão finita. Então, pelo Teorema de Wedderburn–Artin, $A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_t}(D_t)$, onde cada D_i é uma F-álgebra de divisão. Logo, $Z(A) \cong Z(D_1) \oplus \cdots \oplus Z(D_t)$ é isomorfo a um produto de corpos. Nesse caso, dizemos que A é uma F-álgebra separável se cada $Z(D_i)$ é uma extensão separável de F.

Feitas essas considerações, temos o seguinte teorema.

Teorema 1.4.43. *Se A é uma F-álgebra separável, então $A \otimes_F K$ é uma K-álgebra semissimples, para toda extensão K de F.*

Demonstração. Pelo Exercício 1.4.34, podemos supor que A é simples e, assim, $Z(A)$ é uma extensão separável de F. Pelo Lema 1.4.42, $Z(A) \otimes_F K$ é semissimples, para toda extensão K de F e, portanto, isomorfo à uma soma direta de corpos, já que $Z(A) \otimes_F K$ é comutativa. Com isso,

$$A \otimes_F K \cong A \otimes_{Z(A)} (Z(A) \otimes_F K) \cong A \otimes_{Z(A)} \left(\bigoplus_{i=1}^{n} C_i \right) \cong \bigoplus_{i=1}^{n} A \otimes_{Z(A)} C_i$$

onde cada C_i é um corpo. Como A é uma $Z(A)$-álgebra central simples e C_i é simples, pelo Lema 1.4.38, temos que cada $A \otimes_{Z(A)} C_i$ é simples. Portanto, $A \otimes_F K$ é semissimples. □

Utilizando argumentos semelhantes, temos o seguinte teorema.

Teorema 1.4.44. *Se A e B são F-álgebras semissimples de dimensão finita tais que ou A ou B é separável, então $A \otimes_F B$ é semissimples.*

Como consequência desses teoremas, e da Observação 1.4.27, temos o seguinte corolário.

Corolário 1.4.45. *Seja A uma álgebra semissimples de dimensão finita sobre um corpo F de característica zero. Então, para toda extensão algébrica K de F, $A \otimes_F K$ é uma K-álgebra semissimples.*

Sejam A uma F-álgebra e K uma extensão de F. Dizemos que K é um corpo de decomposição de A se $A \otimes_F K \cong M_{n_1}(K) \oplus \cdots \oplus M_n(K)$. Com os resultados anteriores, temos o seguinte teorema.

Teorema 1.4.46. *Se A é uma F-álgebra separável, então A possui um corpo de decomposição.*

Exercício 1.4.47. Sejam A uma F-álgebra e K uma extensão de F. Mostre que:

(a) $A \cap J(A \otimes_F K) \subseteq J(A)$. Se K é uma extensão algébrica de F ou $\dim_F(A) < \infty$, então $A \cap J(A \otimes_F K) = J(A)$.

(b) Se $[K : F] = n$, então $(J(A \otimes_F K))^n \subseteq J(A) \otimes_F K$.

A demonstração do seguinte teorema pode ser encontrada no livro de Lam (1991).

Teorema 1.4.48. *Sejam A uma F-álgebra e K uma extensão algébrica separável de F. Então $J(A \otimes_F K) = J(A) \otimes_F K$.*

O teorema acima nos diz que se $\text{char}(F) = 0$ e K é uma extensão algébrica de F, então $J(A \otimes_F K) = J(A) \otimes_F K$. Além disso, se $J(A)$ é nilpotente, então $J(A \otimes_F K)$ também é nilpotente.

Agora, queremos demonstrar o Teorema de Wedderburn–Malcev, uma das principais ferramentas utilizadas neste livro no estudo de PI-álgebras.

Começamos com a seguinte definição.

Definição 1.4.49. Sejam A e B duas F-álgebras, com B de dimensão finita sobre F. Se existe $f : B \to A$ um epimorfismo de álgebras, com núcleo N, então dizemos que B (ou f) é uma extensão de A com núcleo N. Dizemos que a extensão cinde se existe um homomorfismo de álgebras $g : A \to B$ tal que $f \circ g = id_A$.

Por exemplo, se A e B são F-álgebras de dimensão finita, então $\pi : A \oplus B \to A$, a projeção em A, é uma extensão de A com núcleo B. Se A é uma F-álgebra e $I \trianglelefteq A$, então $\pi : A \to A/I$ é uma extensão de A/I com núcleo I, que em geral não cinde.

Determinar extensões que cindem de uma álgebra A em geral não é uma tarefa fácil. Temos o seguinte lema.

Lema 1.4.50. *Seja $f : B \to A$ uma extensão de A com núcleo N. Então a extensão cinde se, somente se, existe uma subálgebra B' de B, para a qual vale, $B = B' \dotplus N$.*

Demonstração. Suponha que a extensão cinde e seja $g : A \to B$ tal que $f \circ g = id_A$. Vamos mostrar que $B = \text{Im}(g) \dotplus N$. Seja $x \in N \cap \text{Im}(g)$. Então $f(x) = 0$ e existe $a \in A$ tal que $g(a) = x$. Logo, $0 = f(x) = f(g(a)) = a$. Portanto, $x = 0$.

Agora, dado $b \in B$, então $b = (b - g(f(b))) + g(f(b))$. Temos que $g(f(b)) \in \text{Im}(g)$ e $f(b - g(f(b))) = f(b) - f(b) = 0$. Portanto, $B = \text{Im}(g) \dotplus N$.

Reciprocamente, suponha que $B = B' \dotplus N$, para alguma subálgebra B' de B. Dado $a \in A$, existe $b \in B$ tal que $f(b) = a$. Mas, por hipótese, $b = b' + n$, com $b' \in B', n \in N$. Com isso, $f(b) = f(b') = a$ e $B' \cong \text{Im}(f) = A \cong B/N$. Portanto, basta considerar g como sendo o isomorfismo $\bar{f} : A \to B/N$. □

É importante ressaltar que, no lema anterior, B se escreve como uma soma direta de uma subálgebra B' e de um ideal N, como espaços vetoriais, mas não necessariamente temos que $B'N = \{0\}$ ou que B' é um ideal de B.

O Teorema de Wedderburn–Malcev diz que se A é uma F-álgebra de dimensão finita tal que $A/J(A)$ é separável, então a extensão $f: A \to A/J(A)$ cinde, isto é, existe uma subálgebra B semissimples de A tal que $A = B \dot{+} J(A)$. Além disso, se A é unitária, então a subálgebra semissimples B é única, a menos de isomorfismos. A primeira parte do teorema é devida a Wedderburn, enquanto a segunda parte é devida a Malcev.

Faremos a demonstração do Teorema de Wedderburn–Malcev por indução sobre a dimensão de A. O caso mais difícil na demonstração do teorema é quando $J(A)^2 = \{0\}$. Para demonstrar tal caso, vamos introduzir alguns conceitos.

Novamente, consideremos A e B duas F-álgebras, com B de dimensão finita sobre F e $f: B \to A$ uma extensão de A com núcleo N. Seja $g: A \to B$ uma aplicação F-linear tal que $f \circ g = id_A$. Tal aplicação existe, pois, como B tem dimensão finita, existe um subespaço U de B que complementa N. Com isso, basta construirmos tal aplicação como no lema anterior. Se g é um homomorfismo de álgebras, então a extensão cinde e, pelo lema anterior, $B = B' \dot{+} N$, com $B' \cong A$. Nosso objetivo é determinar condições sobre g e N para as quais a extensão cinde.

Se $a, b \in A$, então $g(ab) - g(a)g(b) \in N$, pois $f(g(ab) - g(a)g(b)) = ab - ab = 0$, já que f é um homomorfismo de álgebras. Com isso, a aplicação $h: A \times A \to N$ por

$$h(a,b) = g(ab) - g(a)g(b) \tag{1.3}$$

é bem definida e é F-bilinear, já que g é F-linear. A aplicação h mede até que ponto g falha em ser um homomorfismo de álgebras.

Agora, dados $a, b, c \in A$, temos que

$$g((ab)c) = g(ab)g(c) + h(ab,c) = g(a)g(b)g(c) + h(a,b)g(c) + h(ab,c)$$

e

$$g(a(bc)) = g(a)g(bc) + h(a,bc) = g(a)g(b)g(c) + g(a)h(b,c) + h(a,bc).$$

Como A é associativa, devemos ter

$$h(ab,c) - h(a,bc) + h(a,b)g(c) - g(a)h(b,c) = 0.$$

Antes de continuarmos, temos a seguinte definição.

Definição 1.4.51. Sejam A uma F-álgebra e B um A-bimódulo. Uma aplicação F-bilinear $h\colon A \times A \to B$ é chamada de fator de A se, para todos $a, b, c \in A$,

$$h(ab, c) - h(a, bc) + h(a, b)c - ah(b, c) = 0.$$

Dizemos que um fator h cinde se existe uma aplicação F-linear $g\colon A \to B$ tal que, para todos $a, b \in A$,

$$h(a, b) = ag(b) - g(ab) + g(a)b.$$

Agora, gostaríamos de dar uma estrutura de A-bimódulo para N com operações definidas por $na = ng(a)$ e $an = g(a)n$, para todos $a \in A$, $n \in N$. Em geral isso não acontece, mas se $N^2 = \{0\}$, temos, para todos $a, b \in A$, $n \in N$,

$$(na)b - n(ab) = (ng(a))g(b) - ng(ab) = -nh(a, b) = 0$$

já que $N^2 = \{0\}$. Assim, se $N^2 = \{0\}$, então N é um A-bimódulo e h é um fator de A.

A justificativa da definição anterior vem do seguinte resultado.

Lema 1.4.52. *Seja $f\colon B \to A$ uma extensão de A com núcleo N tal que $N^2 = \{0\}$. Seja h um fator de A como na Equação (1.3) associado a uma aplicação F-linear $g\colon A \to B$ tal que $f \circ g = id_A$. Então h cinde se, e somente se, a extensão cinde.*

Demonstração. Suponha que h cinde. Então existe uma aplicação F-linear $\bar{g}\colon A \to N$ tal que $h(a, b) = a\bar{g}(b) - \bar{g}(ab) + \bar{g}(a)b = g(a)\bar{g}(b) - \bar{g}(ab) + \bar{g}(a)g(b)$, para todos $a, b \in A$.

Defina $g'\colon A \to B$ por $g'(a) = g(a) + \bar{g}(a)$. É claro que g' é F-linear e, como $f \circ g = id_A$ e $Im(\bar{g}) \subseteq N$, temos que $f \circ g' = id_A$. Para mostrar que a extensão cinde, basta mostrarmos que g' é um homomorfismo de anéis. Temos que

$$\begin{aligned} g'(ab) &= g(ab) + \bar{g}(ab) \\ &= h(a, b) + g(a)g(b) + \bar{g}(ab) \\ &= g(a)\bar{g}(b) + \bar{g}(a)g(b) + g(a)g(b). \end{aligned}$$

Por outro lado,

$$\begin{aligned} g'(a)g'(b) &= (g(a) + \bar{g}(a))(g(b) + \bar{g}(b)) \\ &= g(a)g(b) + g(a)\bar{g}(b) + \bar{g}(a)g(b) + \bar{g}(a)\bar{g}(b) \\ &= g(a)g(b) + g(a)\bar{g}(b) + \bar{g}(a)g(b) \end{aligned}$$

pois $N^2 = \{0\}$. Portanto, a extensão cinde.

Reciprocamente, suponha que a extensão cinde. Então existe um homomorfismo de álgebras $\bar{g}\colon A \to B$ tal que $f \circ \bar{g} = id_A$. Defina $g'\colon A \to B$ por $g'(a) = \bar{g}(a) - g(a)$. Temos que g' é F-linear e, como $f \circ g = id_A$, temos que $f \circ g' = 0$. Logo, $Im(g') \subseteq N$. Para mostrar que $h(a,b) = ag'(b) - g'(ab) + g'(a)b = g(a)g'(b) - g'(ab) + g'(a)g(b)$, basta utilizar que $g'(a)g'(b) = 0$, para todos $a, b \in A$, já que $N^2 = \{0\}$ e efetuar os cálculos como no caso anterior. □

Antes de prosseguirmos, vamos enunciar um resultado cuja demonstração pode ser encontrada no livro de Curtis e Reiner (1966).

Teorema 1.4.53. *Seja A uma F-álgebra de dimensão finita. Se A é separável, então, para alguma F-base $\{a_1, \ldots, a_n\}$ de A, existem elementos $a'_1, \ldots, a'_n \in A$ com as seguintes propriedades:*

1. $\sum_{i=1}^{n} a'_i a_i = 1$;

2. *para todo $a \in A$, $a_i a = \sum_{j=1}^{n} \lambda_{ij}(a) a_j, \lambda_{ij}(a) \in F$, implica que $aa'_i = \sum_{j=1}^{n} \lambda_{ji}(a) a'_j$, $i = 1, \ldots, n$.*

Recorde que se $C^\infty(\mathbb{R})$ denota a $\mathbb{R}$-álgebra das funções reais de classe C^∞, então a aplicação derivada $\frac{d}{dx}\colon C^\infty(\mathbb{R}) \to C^\infty(\mathbb{R})$ dada por $\frac{d}{dx}(f) = \frac{df}{dx}$ é uma aplicação $\mathbb{R}$-linear que, satisfaz $\frac{d}{dx}(fg) = \frac{df}{dx}g + f\frac{dg}{dx}$ para todos $f, g \in C^\infty(\mathbb{R})$. Em geral, temos a seguinte definição.

Definição 1.4.54. Sejam A uma F-álgebra e B um A-bimódulo. Uma aplicação F-linear $f\colon A \to B$ é chamada de derivação generalizada se, para todos $a, b \in A$,

$$f(ab) = f(a)b + af(b).$$

Exercício 1.4.55. Sejam A uma F-álgebra e B um A-bimódulo. Fixado $b \in B$, mostre que a função $f\colon A \to B$ definida por $f(a) = ab - ba := [a, b]$ é uma derivação generalizada, chamada de derivação interna.

Exercício 1.4.56. Sejam A uma F-álgebra e B um A-bimódulo. Denote por $Der_F(A, B)$ o conjunto de todas as derivações generalizadas de A em B. Mostre que:

1. $Der_F(A,B)$ possui uma estrutura natural de F-espaço vetorial.
2. Em $Der_F(A,A) = Der_F(A)$, em geral, a composta de duas derivações generalizadas não é uma derivação generalizada.
3. Se $f, g \in Der_F(A)$, então $[f,g] := f \circ g - g \circ f \in Der_F(A)$.

Estamos aptos a demonstrar o seguinte teorema.

Teorema 1.4.57. *Seja A uma F-álgebra separável de dimensão finita. Então todo fator de A cinde e toda derivação generalizada é interna.*

Demonstração. De acordo com o Teorema 1.4.53, considere $\{a_1, \ldots, a_n\}$ uma F-base de A junto com um conjunto $\{a'_1, \ldots, a'_n\} \subset A$ tal que

1. $\sum_{i=1}^{n} a'_i a_i = 1$;
2. para todo $a \in A$, $a_i a = \sum_{j=1}^{n} \lambda_{ij}(a) a_j, \lambda_{ij}(a) \in F$, implica que $a a'_i = \sum_{j=1}^{n} \lambda_{ji}(a) a'_j, i = 1, \ldots, n$.

Sejam B um A-bimódulo e $h\colon A \times A \to B$ um fator de A. Defina $g\colon A \to B$ por $g(a) = \sum_{i=1}^{n} h(a, a'_i) a_i$. Como h é F-bilinear, g é F-linear. Temos que, utilizando as relações 1 e 2 acima, para todos $a, b \in A$,

$$\begin{aligned}
ag(b) - g(ab) + g(a)b &= \sum_{i=1}^{n} ah(b,a'_i)a_i - \sum_{i=1}^{n} h(ab,a'_i)a_i + \sum_{i=1}^{n} h(a,a'_i)a_i b \\
&= \sum_{i=1}^{n} ah(b,a'_i)a_i - \Bigg(\sum_{i=1}^{n} h(a,ba'_i)a_i - \sum_{i=1}^{n} h(a,b)a'_i a_i \\
&\quad + \sum_{i=1}^{n} ah(b,a'_i)a_i \Bigg) + \sum_{i=1}^{n} h(a,a'_i)a_i b \\
&= h(a,b) - \sum_{i=1}^{n} h(a,ba'_i)a_i + \sum_{i=1}^{n} h(a,a'_i)a_i b \\
&= h(a,b) + \sum_{i,j=1}^{n} (\lambda_{ij}(b) - \lambda_{ji}(b)) h(a,a'_i)a_j \\
&= h(a,b).
\end{aligned}$$

Portanto, h cinde.

Agora, sejam $f : A \to B$ uma derivação generalizada e $b = \sum_{i=1}^{n} a_i' f(a_i)$. Da mesma forma do caso anterior, temos, para todo $a \in A$,

$$\begin{aligned} ab - ba &= \sum_{i=1}^{n} aa_i' f(a_i) - \sum_{i=1}^{n} a_i' f(a_i)a \\ &= \sum_{i=1}^{n} aa_i' f(a_i) - \sum_{i=1}^{n} a_i' f(a_i a) + \sum_{i=1}^{n} a_i' a_i f(a) \\ &= f(a) + \sum_{i,j=1}^{n} (\lambda_{ij}(a) - \lambda_{ji}(a)) a_i' f(a_i) \\ &= f(a). \end{aligned}$$

Portanto, f é interna. □

Estamos em condições de demonstrar o teorema principal da seção.

Teorema 1.4.58 (Wedderburn–Malcev)**.** *Seja A uma F-álgebra de dimensão finita tal que $A/J(A)$ é separável. Então existe uma subálgebra semissimples B de A tal que*

$$A = B \dot{+} J(A).$$

Além disso, se A é unitária e B_1 e B_2 são subálgebras de A tais que

$$A = B_1 \dot{+} J(A) = B_2 \dot{+} J(A)$$

então existe $j \in J(A)$ tal que $B_1 = (1 - j)B_2(1 - j)^{-1}$.

Demonstração. Primeiramente, observe que a álgebra semissimples B do enunciado do teorema é isomorfa a $A/J(A)$. Com isso, para demonstrar o teorema, basta mostrar que A possui uma subálgebra isomorfa a $A/J(A)$. Observe também que, pelo Teorema de Wedderburn–Artin, o teorema é válido se $J(A) = \{0\}$ ou se $A = J(A)$. Consequentemente, o teorema é válido trivialmente se $\dim_F(A) = 1$. A demonstração do teorema é por indução sobre a dimensão de A. Suponha que o teorema seja verdadeiro para toda F-álgebra de dimensão menor do que a dimensão de A. Recorde que, como A tem dimensão finita, $J = J(A)$ é um ideal nilpotente de A.

Podemos assumir que $J^2 \neq \{0\}$, pois, caso contrário, $\pi : A \to A/J$ é uma extensão com núcleo $J^2 = \{0\}$ e, pelo Lema 1.4.52 e Teorema 1.4.57, temos o resultado desejado. Como $J^2 \neq \{0\}$, temos que $\dim_F(A/J^2) < \dim_F(A)$ e $J(A/J^2) = J/J^2$. Logo, J/J^2 é um ideal nilpotente de A/J^2 e $(A/J^2)/(J/J^2)$

$\cong A/J$, que é separável, por hipótese. Pela hipótese de indução, existe uma subálgebra semissimples B_1' de A/J^2 tal que $A/J^2 = B_1' \dot{+} J/J^2$. Portanto, existe uma subálgebra B_1 de A tal que $A = B_1 + J$, com $B_1 \cap J = J^2 = J(B_1)$.

Como $J^2 \neq J$, $B_1 \neq A$. Além disso,

$$A/J = (B_1 + J)/J \cong B_1/(B_1 \cap J) = B_1/J^2.$$

Logo, a hipótese de indução pode ser aplicada B_1, e existe uma subálgebra semissimples B de B_1 tal que $B_1 = B \dot{+} J^2$. Note que, como $B_1 \cap J = J^2$ e $B \cap J^2 = \{0\}$, então $B \cap J = \{0\}$. Portanto, $A = B_1 + J = (B \dot{+} J^2) + J = B \dot{+} J$. A primeira parte do teorema está provada.

Para demonstrar a segunda parte do teorema, suponha que

$$A = B_1 \dot{+} J(A) = B_2 \dot{+} J(A).$$

Então, pelo Lema 1.4.50, existem homomorfismos de álgebras $f_i : A/J(A) \to A$, $i = 1, 2$ tais que $\pi \circ f_i = id_{A/J(A)}$, onde $\pi : A \to A/J(A)$ é a projeção canônica. Recorde que $Im(f_i) = B_i$. Assim, $J(A)$ se torna um $(A/J(A))$-bimódulo se definirmos $\bar{a}\, j = f_1(\bar{a})\, j$ e $j\bar{a} = j f_2(\bar{a})$, para todos $j \in J, \bar{a} \in A/J(A)$.

Considere a função $f : A/J(A) \to A$ definida por $f(\bar{a}) = f_1(\bar{a}) - f_2(\bar{a})$. Como $\pi \circ f_i = id_{A/J(A)}, i = 1, 2, \pi \circ f = 0$ e $Im(f) \subseteq J(A)$. Agora,

$$\begin{aligned} f(\bar{a}\bar{b}) &= f_1(\bar{a}\bar{b}) - f_2(\bar{a}\bar{b}) \\ &= f_1(\bar{a})(f_1(\bar{b}) - f_2(\bar{b})) + (f_1(\bar{a}) - f_2(\bar{a}))\, f_2(\bar{b}) \\ &= \bar{a}\, f(\bar{b}) + f(\bar{a})\bar{b}. \end{aligned}$$

Logo, f é uma derivação generalizada e, pelo Teorema 1.4.57, existe $j \in J$ tal que

$$f(\bar{a}) = f_1(\bar{a}) - f_2(\bar{a}) = \bar{a}\, j - j\bar{a} = f_1(\bar{a})\, j - j f_2(\bar{a}).$$

Reescrevendo, obtemos que $f_1(\bar{a})(1 - j) = (1 - j)\, f_2(\bar{a})$. Como j é nilpotente, $1 - j$ é invertível. Portanto, $f_1(\bar{a}) = (1 - j)\, f_2(\bar{a})(1 - j)^{-1}$. Isto nos diz que $B_1 = (1 - j)B_2(1 - j)^{-1}$, o que demonstra o teorema. □

Nas condições do teorema anterior, a decomposição $A = B \dot{+} J(A)$ é chamada de decomposição de Wedderburn–Malcev de A.

Exemplo 1.4.59. Considere a álgebra UT_2 sobre um corpo de característica zero. Temos que $J(UT_2) = Fe_{12}$ e $UT_2/J(UT_2) = F\bar{e}_{11} \oplus F\bar{e}_{22}$. Portanto, $UT_2 = Fe_{11} \oplus Fe_{22} \dot{+} Fe_{12}$ é uma decomposição de Wedderburn–Malcev de UT_2.

Exercício 1.4.60. Mostre que o Teorema de Wedderburn–Malcev é equivalente ao seguinte: Seja A uma F-álgebra de dimensão finita e B' uma subálgebra separável de $A/J(A)$. Então A contém uma subálgebra B isomorfa a B'.

Exercício 1.4.61. Seja $A = B \dot{+} J(A)$ a decomposição de Wedderburn–Malcev de uma F-álgebra A, nas condições do Teorema 1.4.58. Mostre que B é uma subálgebra semissimples maximal de A, isto é, B não está contida propriamente em nenhuma subálgebra semissimples de B.

Finalizamos o capítulo informando que, ao longo desse texto, a maioria das álgebras serão tomadas sobre um corpo de característica zero. Assim, como mencionamos anteriormente, se F é um corpo de característica zero e K é uma extensão algébrica de F, então K é uma extensão separável. Portanto, todos os resultados dessa seção são automaticamente válidos para álgebras sobre corpos de característica zero. Com isso, para nossos propósitos, iremos enunciar o novamente o Teorema de Wedderburn–Malcev para o caso em que F tem característica zero.

Teorema 1.4.62 (Wedderburn–Malcev)**.** *Seja A uma álgebra de dimensão finita sobre um corpo F de característica zero. Então existe uma subálgebra semissimples B de A tal que*

$$A = B \dot{+} J(A).$$

Além disso, se A é unitária e B_1 e B_2 são subálgebras de A tais que

$$A = B_1 \dot{+} J(A) = B_2 \dot{+} J(A)$$

então existe $j \in J(A)$ tal que $B_1 = (1-j)B_2(1-j)^{-1}$.

Exercícios V ou F da Seção 1.4: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, A representa uma F-álgebra e F é um corpo de característica zero.

(1) A aplicação $f : M_2(F) \to UT_2$ definida por $f(e_{ij}) = 0$, para $i = j$ e $f(e_{ij}) = e_{ij}$, para $i \neq j$ é um homomorfismo de álgebras.

(2) É verdade que $M_2(F) = F(e_{11} + e_{22}) \oplus F(e_{11} - e_{22}) \oplus Fe_{12} \oplus Fe_{21}$.

(3) É verdade que $M_3(F) \otimes_F UT_2$ é uma álgebra de dimensão 6.

(4) A álgebra $M_2(F) \otimes_F M_3(F)$ é central simples.

(5) Se A é nilpotente e de dimensão finita, então $A = J(A)$ é uma decomposição de Wedderburn–Malcev de A.

(6) $M_2(F) = Fe_{11} \oplus Fe_{12} \oplus Fe_{21} \oplus Fe_{22}$ é uma decomposição de Wedderburn–Malcev de $M_2(F)$.

Resumo

Aqui faremos um pequeno resumo do capítulo, coletando os principais resultados que serão utilizados no decorrer do livro.

- Uma álgebra A é artiniana se toda cadeia descendente de ideais à esquerda de A é estacionária. Toda álgebra de dimensão finita é artiniana.

- Uma álgebra A é semissimples se todo ideal à esquerda de A é um somando direto. O Teorema de Wedderburn–Artin (Teorema 1.4.21) diz que A é uma F-álgebra artiniana semissimples se, e somente se, $A \cong A_1 \oplus \cdots \oplus A_n$, onde cada A_i é um F-álgebra simples isomorfa a uma álgebra de matrizes com coeficientes em um anel de divisão. Além disso, cada A_i é um ideal de A e $A_i A_j = \{0\}$, se $i \neq j$. Toda álgebra artiniana semissimples é um anel semissimples.

- O radical de Jacobson de uma álgebra A, denotado por $J(A)$, é a interseção dos anuladores de todos os A-módulos simples. Se não existem A-módulos simples, definimos $J(A) = A$. O radical de Jacobson de uma álgebra é um ideal da álgebra e se A é uma álgebra artiniana, então $J(A)$ é nilpotente e todo ideal nilpotente de A está contido em $J(A)$.

- Uma álgebra artiniana A é semissimples se, e somente se, $J(A) = \{0\}$.

- Se A é uma F-álgebra e K é uma extensão de F, então $A \otimes_F K$ é uma K-álgebra e $\dim_F(A) = \dim_K(A \otimes_F K)$. Se K é uma extensão separável de F, então $J(A \otimes_F K) = J(A) \otimes_F K$. Em particular, $J(A)$ é nilpotente se, e somente se, $J(A \otimes_K F)$ é nilpotente.

- Se F é um corpo de característica zero e K é uma extensão algébrica de F, então K é uma extensão separável de F. Com isso, se A é uma álgebra semissimples de dimensão finita sobre um corpo F de característica zero, então para toda extensão algébrica K de F, $A \otimes_F K$ é uma K-álgebra semissimples.

- Se A é uma álgebra de dimensão finita sobre um corpo de característica zero, então o Teorema de Wedderburn–Malcev (Teorema 1.4.62) afirma que $A = B \dot{+} J(A)$, onde B é uma subálgebra semissimples de A.

2 Grupos e representações

Neste capítulo, faremos uma breve revisão dos resultados principais em teoria dos grupos, necessários para o bom entendimento dos capítulos seguintes. Para algumas demonstrações omitidas, indicamos o livro de Robinson (1982).

Nosso foco principal será a respeito de representações e caracteres de grupos, principalmente no que diz respeito ao grupo simétrico de grau n. Temos particular interesse nesse grupo devido à sua participação nos resultados sobre a sequência de codimensões de uma PI-álgebra, que serão tratados no Capítulo 4.

2.1 Grupos simétricos

Ao longo do texto, usaremos algumas propriedades dos grupos simétricos que vamos destacar agora. Recordemos inicialmente que um grupo G é um conjunto não vazio com uma operação binária fechada

$$\begin{aligned} G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

que é associativa e que satisfaz as seguintes condições:

1. Existe um elemento 1 em G, dito elemento neutro, tal que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in G$.

2. Para cada $a \in G$, existe um elemento b em G, dito o inverso de a, tal que $a \cdot b = b \cdot a = 1$.

O exercício a seguir garante a unicidade dos elementos definidos nos itens 1 e 2 acima.

Exercício 2.1.1. Se G é um grupo, mostre que

(a) O elemento neutro de G é único.

(b) Cada elemento de G possui um único inverso.

Em geral, denotamos um grupo G com operação $\cdot$ por $(G, \cdot)$ e observe que a notação aqui utilizada é multiplicativa, mas em geral outras operações são permitidas, dependendo do conjunto definidor do grupo.

Por exemplo, o conjunto dos números inteiros $\mathbb{Z}$ é um grupo com respeito à adição usual de inteiros. Neste caso, o elemento neutro é 0 e o inverso de cada elemento $a \in \mathbb{Z}$ é o inteiro $-a$.

Daqui pra frente, vamos omitir o ponto $\cdot$ presente na definição dada acima e usaremos simplesmente ab para o resultado da operação de dois elementos a e b em G. Vamos também denotar o inverso de um elemento $a \in G$ por a^{-1}.

Diremos também que G é grupo abeliano[1] se a operação for comutativa. Desta forma, $\mathbb{Z}$ com a operação de adição é um exemplo de grupo abeliano. Dado um corpo F, os grupos $(F, +)$ e $(F^*, \cdot)$ também são exemplos de grupos abelianos.

Para um subconjunto $S \subset G$, denotaremos sua cardinalidade por $|S|$, e lembremos que $|G|$ é denominada a ordem do grupo G. A ordem de um elemento $a \in G$ é definida como o menor inteiro positivo n tal que

$$a^n := \underbrace{a \cdots a}_{n \text{ vezes}} = 1$$

e é denotada $o(a) = n$. Se não existir tal n, dizemos que a tem ordem infinita. Observemos que o único elemento de ordem 1 em um grupo G é o elemento neutro e, além disso, para um elemento $a \in G$, temos $o(a) = o(a^{-1})$. Claramente, se a é um elemento de ordem 2, teremos $a = a^{-1}$.

Dado um corpo F, temos que $(M_n(F), +)$ é um grupo abeliano, mas com relação à multiplicação de matrizes, devemos ter um pouco mais de cuidado. Veja o exemplo a seguir.

[1] A palavra *abeliano* é uma homenagem ao matemático N. Abel.

Exemplo 2.1.2. Um exemplo importante de grupo é o conjunto de matrizes invertíveis $n \times n$ com entradas em um corpo F, munido da multiplicação usual de matrizes. Usaremos a notação

$$GL_n(F) := \{M \in M_n(F) : \det(M) \neq 0\}$$

e este é chamado de grupo linear geral de grau n sobre F. Quando F é um corpo infinito, vemos que $GL_n(F)$ é um grupo infinito não abeliano, para $n \geqslant 2$.

Considerando Q um conjunto não vazio qualquer, podemos definir o conjunto

$$Sim(Q) = \{f : Q \to Q : f \text{ é bijetiva}\}$$

de todas as bijeções de Q. Munindo este conjunto da operação de composição de funções, temos que $Sim(Q)$ é um grupo. Note que o conjunto Q pode ser finito ou não. Particularmente, quando tomamos Q o conjunto dos n primeiros números naturais $\widehat{n} = \{1, \ldots, n\}$, para $n \geqslant 3$, temos a seguinte definição.

Definição 2.1.3. O grupo formado por todas as possíveis permutações dos elementos em $\widehat{n}$, com $n \geqslant 3$, é dito o grupo simétrico de grau n e é denotado por S_n.

Note que S_n é um grupo não abeliano de ordem $n!$. Uma forma de representar as permutações no grupo S_n é utilizando a notação em ciclos.

Definição 2.1.4. Dizemos que uma permutação $\sigma \in S_n$ é um r-ciclo de S_n, $r \geqslant 2$, se existem $i_1, i_2, \ldots, i_r$ elementos distintos de $\widehat{n}$ tais que:

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1 \text{ e}$$

$$\sigma(j) = j, \text{ para todo } j \in \widehat{n} - \{i_1, \ldots, i_r\}.$$

Na definição acima, usaremos a notação $\sigma = (i_1\ i_2\ \cdots\ i_r) \in S_n$ e dizemos também que σ é um ciclo de comprimento r. Um ciclo de comprimento 2 será chamado de transposição.

Também podemos considerar um ciclo de comprimento igual a 1, usado para denotar um elemento fixo por uma permutação. Por exemplo, a permutação $\sigma = (1\ 3\ 5\ 2) \in S_5$ deixa fixo o número natural 4 e, assim, podemos eventualmente escrever $\sigma = (1\ 3\ 5\ 2)(4)$.

Definição 2.1.5. Dois ciclos em S_n são ditos disjuntos se eles não movem elementos em comum.

Por exemplo, $\sigma = (2\ 5\ 3\ 7)$ e $\tau = (1\ 4\ 6)$ são ciclos disjuntos em S_7.

Exercício 2.1.6. Mostre que ciclos disjuntos comutam entre si.

No próximo exercício, vemos que existe uma maneira especial de escrever uma permutação de S_n.

Exercício 2.1.7. Mostre que toda permutação $\sigma \neq 1$ em S_n pode ser escrita de maneira única, a menos de ordenação, como um produto de ciclos disjuntos.

Ao escrever uma permutação $\sigma \in S_n$ como um produto de ciclos disjuntos, temos a chamada estrutura cíclica de σ. Usando a notação de ciclos, temos que

$$S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

e assim vemos que as estruturas cíclicas presentes em S_3 são os 2-ciclos e os 3-ciclos.

Observemos que o ciclo (7 9 6) é o mesmo que o ciclo (6 7 9). Em geral, isto significa que, podemos começar um ciclo com o menor natural que a ele pertence, respeitando a permutação definida por ele. Dessa forma, a permutação $\sigma = (7\ 9\ 6)(3\ 5\ 8\ 1)(4\ 2) \in S_9$ também pode ser escrita como $\sigma = (1\ 3\ 5\ 8)(6\ 7\ 9)(2\ 4)$, pois ciclos disjuntos permutam entre si.

De modo mais geral, ao escrever uma permutação em sua estrutura cíclica, sempre consideraremos os ciclos ordenados por comprimento do maior para o menor e, em cada ciclo, iniciamos com o menor número natural neste ciclo. Assim, observamos que, ao escrever uma permutação como um produto de ciclos disjuntos, temos estabelecida uma unicidade na representação e podemos associar à permutação uma partição de n. Vamos recordar este conceito a seguir.

Definição 2.1.8. Uma partição de um número natural n é uma s-upla de números naturais $(\lambda_1, \ldots, \lambda_s)$ tais que $n \geqslant \lambda_1 \geqslant \cdots \geqslant \lambda_s \geqslant 1$ com $\lambda_1 + \cdots + \lambda_s = n$. Vamos usar a notação $\lambda \vdash n$.

Exemplo 2.1.9. Por exemplo temos $(3, 3, 2, 1) \vdash 9$.

Desta forma, se $\sigma \in S_n$ tem estrutura cíclica $\sigma = c_{l_1} \cdots c_{l_m}$, onde os c_{l_i}'s são ciclos disjuntos de comprimento $l_i \geqslant 1$, com $l_1 \geqslant \cdots \geqslant l_m$, então associamos a partição $\lambda = (l_1, \ldots, l_m)$ à permutação σ.

Exemplo 2.1.10. Se $\sigma = (2\ 3\ 9)(1\ 6)(4\ 8) \in S_9$, podemos também escrever $\sigma = (2\ 3\ 9)(1\ 6)(4\ 8)(5)(7)$ e associamos a partição $\lambda = (3, 2, 2, 1, 1) \vdash 9$, já que os ciclos de comprimento 1 correspondem aos elementos fixos 5 e 7.

Lembremos que, em geral, dois elementos a e b de um dado grupo G são ditos conjugados se existe uma elemento $x \in G$ tal que $a = xbx^{-1}$ e denotamos xbx^{-1} por b^x, ou seja, a e b em G são ditos conjugados se $a = b^x$, para algum $x \in G$.

Exercício 2.1.11. Mostre que a seguinte relação em G é uma relação de equivalência, onde $a, b \in G$:

$$a \sim b \text{ se, e somente se, } a \text{ e } b \text{ são conjugados em } G.$$

Definição 2.1.12. A classe de equivalência de um elemento $a \in G$ pela relação acima é denominada a classe de conjugação de a e é denotada por $cl(a)$.

Assim, para $a \in G$, temos que

$$cl(a) = \{a^x : x \in G\}.$$

Observação 2.1.13. Note que se G é um grupo abeliano, então a classe de conjugação de cada elemento $a \in G$ é dada por $cl(a) = \{a\}$, pois $a^x = a$, para todo $x \in G$. Desta forma, a quantidade de classes de conjugação em um grupo abeliano finito G é igual a sua ordem.

Como um exemplo em um grupo não abeliano, vemos que as permutações (1 2 4 5) e (1 3 2 5) são conjugadas em S_5 pois (2 3 4)(1 2 4 5)(2 4 3) = (1 3 2 5), e temos que (2 4 3) é inversa de (2 3 4).

Mais geralmente, observe que se $\sigma = (i_1 \cdots i_k)$ e $\tau = (j_1 \cdots j_k)$ são k-ciclos em S_n, considerando a permutação α:

$$\alpha : i_1 \mapsto j_1, \ \ i_2 \mapsto j_2, \ \ldots, \ \ i_k \mapsto j_k$$

temos que $\sigma = \alpha\tau\alpha^{-1}$. Desta forma, dois k-ciclos são conjugados em S_n e o mesmo vale para uma quantidade qualquer de ciclos, ou seja, duas permutações com mesma estrutura cíclica são conjugadas em S_n. A recíproca é verdadeira e pode ser provada facilmente de modo mais geral no próximo exercício.

Exercício 2.1.14. Duas permutações α e β são conjugadas em S_n se, e somente se, α e β têm a mesma estrutura cíclica.

Por exemplo, S_3 tem 3 classes de conjugação que são

$$cl(1) = \{1\}, \ cl((1\ 2)) = \{(1\ 2), \ (1\ 3), (2\ 3)\} \text{ e } cl((1\ 2\ 3)) = \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

Exercício 2.1.15. Determine a classe de conjugação de $(1\ 2)(3\ 5)$ em S_5.

Exercício 2.1.16. Determine um representante para cada uma das classes de conjugação em S_4 e também para cada uma em S_5.

Pelo Exercício 2.1.14, a classe de conjugação de uma permutação $\sigma \in S_n$ é determinada pela estrutura cíclica de σ e, por este motivo, uma classe de conjugação de S_n será associada a uma partição que corresponde a esta estrutura. Neste caso, indexaremos a classe pela partição correspondente. Por exemplo, denotaremos a classe $cl((2\ 3\ 9)(1\ 6)(4\ 8))$ de S_9 por $cl_{(3,2,2,1,1)}$.

Corolário 2.1.17. *O número de classes de conjugação em S_n é igual ao número de partições de n.*

Recordemos que um subgrupo de um grupo G é um subconjunto não vazio H de G tal que H é um grupo com a mesma operação de G. Neste caso, denotamos $H \leqslant G$.

Exercício 2.1.18. Mostre que se $H, K \leqslant G$, então $H \cap K \leqslant G$. Em geral, mostre que se $\{H_i\}_{i\in\mathcal{I}}$ é uma família de subgrupos de um grupo G, então $\bigcap_{i\in\mathcal{I}} H_i \leqslant G$.

Exercício 2.1.19. Mostre que, sendo $H, K \leqslant G$, nem sempre é verdade que $H \cup K \leqslant G$.

Para um subgrupo H de um grupo G e um elemento $x \in G$, definimos o conjugado de H por x como o subgrupo

$$H^x = \{h^x : h \in H\}.$$

Por exemplo, um conjugado do subgrupo $H = \{1, (1\ 3)\}$ de S_3 é o subgrupo $H^{(2\ 3)} = \{1, (1\ 2)\}$. Os subgrupos normais de um grupo, que definiremos abaixo, têm um destaque especial.

Definição 2.1.20. Dado um subgrupo N de um grupo G, dizemos que N é normal em G se $N^x = N$ para todo $x \in G$. Usaremos a notação $N \lhd G$ para indicar que N é um subgrupo normal de G.

Pelo exemplo dado acima, temos que $H = \{1, (1\ 3)\}$ não é um subgrupo normal de S_3, mas temos $\{1, (1\ 2\ 3), (1\ 3\ 2)\} \lhd S_3$.

Muitas vezes, basta conhecer informações sobre os geradores de um grupo G para saber fatos sobre todos os elementos do grupo. Dado um subconjunto não

vazio $S \subset G$, definimos o subgrupo de G gerado por S como a interseção de todos os subgrupos de G que contêm S. Denotamos esse subgrupo por $\langle S \rangle$ e podemos observar que

$$\langle S \rangle = \{x_1^{\pm 1} x_2^{\pm 1} \cdots x_m^{\pm 1} : x_i \in S, m \geqslant 0\}$$

onde interpretamos a expressão com $m = 0$ como sendo 1.

Um conjunto gerador para um grupo G é um subconjunto $S \subset G$ tal que $G = \langle S \rangle$. Por exemplo, o grupo S_3 é gerado pelo conjunto $S = \{(1\ 2), (1\ 2\ 3)\}$, ou seja, qualquer elemento de S_3 pode ser escrito como um produto de potências de elementos de S e de seus inversos.

Particularmente, quando $S = \{x\} \subset G$, o subgrupo $\langle S \rangle$ é denotado por $\langle x \rangle$ e é dito subgrupo cíclico gerado por x. Quando x é um elemento de ordem finita n, escrevemos $\langle x : x^n = 1 \rangle$ para denotar o grupo cíclico de ordem n gerado por x. O grupo G é um grupo cíclico se $G = \langle x \rangle$, para algum $x \in G$.

A seguir, vamos definir o subgrupo derivado de um grupo G. Para isto, definimos o comutador entre dois elementos x e y em G como sendo o elemento $xyx^{-1}y^{-1}$ e denotaremos

$$(x, y) := xyx^{-1}y^{-1} = y^x y^{-1}.$$

Definição 2.1.21. Considere $C = \{(x, y) : x, y \in G\}$. Definimos os subgrupo derivado de G como $G' = \langle C \rangle$, ou seja, G' é o subgrupo gerado por todos os comutadores de elementos em G.

Note que $(x, y) = 1$ se, e somente se, x e y comutam em G. Portanto, G é abeliano se, e somente se, $G' = \{1\}$.

Exercício 2.1.22. Mostre que $G' \lhd G$.

Podemos reescrever uma permutação de S_n como um produto de ciclos disjuntos, usando somente ciclos de comprimento 2. Isto acontece pois podemos reescrever um ciclo de comprimento r da seguinte maneira

$$(i_1\ i_2\ i_3 \cdots i_r) = (i_1\ i_r) \cdots (i_1\ i_3)(i_1\ i_2). \tag{2.1}$$

Neste caso, não temos necessariamente que estas transposições são disjuntas. Como um exemplo, temos $(1\ 3\ 5\ 7)(2\ 6\ 4) = (1\ 7)(1\ 5)(1\ 3)(2\ 4)(2\ 6)$. Como consequência, temos o seguinte resultado.

Proposição 2.1.23. *O grupo S_n é gerado pelo conjunto de suas transposições.*

Observe que $(1\ 2\ 5\ 7)(3\ 4) = (1\ 7)(1\ 5)(1\ 2)(3\ 4)$ está escrita como um produto de uma quantidade par de transposições, enquanto que em $(1\ 3\ 5\ 7)(2\ 6\ 4) = (1\ 7)(1\ 5)(1\ 3)(2\ 4)(2\ 6)$ temos uma quantidade ímpar de transposições. A pergunta que podemos fazer é se podemos ter quantidades distintas em paridade para maneiras diferentes de escrever uma mesma permutação como produto de transposições.

Afirmamos que, ao escrever uma permutação de S_n como um produto de transposições, a quantidade delas sempre é par ou sempre é ímpar. Para provar isto, vamos considerar um polinômio em n variáveis comutativas $x_1, \ldots, x_n$ definido por

$$P = P(x_1, \ldots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j).$$

Dada uma permutação $\sigma \in S_n$, associamos o polinômio

$$P^\sigma = \prod_{1 \leqslant i < j \leqslant n} (x_{\sigma(i)} - x_{\sigma(j)})$$

e vemos que $P^\sigma = P$ ou $P^\sigma = -P$.

Por exemplo, para $P = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$ e $\sigma = (1\ 3)(2\ 4) \in S_4$, temos

$$P^\sigma = (x_3 - x_4)(x_3 - x_1)(x_3 - x_2)(x_4 - x_1)(x_4 - x_2)(x_1 - x_2)$$

e observamos que neste caso, $P^\sigma = P$. Por outro lado, se σ é uma transposição, temos claramente que $P^\sigma = -P$.

Concluímos que se uma permutação $\sigma \in S_n$ pode ser escrita como um produto de uma quantidade par de transposições, temos $P^\sigma = P$ e, então, qualquer outra maneira de escrever essa mesma permutação como um produto de transposições deve conter também uma quantidade par de transposições.

Desta forma, temos uma boa definição para permutações pares e ímpares.

Definição 2.1.24. Dizemos que uma permutação $\sigma \in S_n$ é par se ela pode ser escrita como um produto de um número par de transposições. Quando uma permutação não é par, ela é uma permutação ímpar.

Observemos que a permutação identidade é par, o inverso de uma permutação par é par e que o produto de permutações pares é par. Com isso, o conjunto A_n das permutações pares de S_n é um subgrupo de S_n.

Definição 2.1.25. O subgrupo A_n das permutações pares de S_n é chamado grupo alternado de grau n.

Note ainda que, fixada uma permutação ímpar $\alpha \in S_n$, podemos definir

$$\begin{array}{rccc} f: & A_n & \to & S_n \\ & \sigma & \mapsto & \alpha\sigma \end{array}$$

e vemos que essa é uma aplicação injetiva tal que $\mathrm{Im}(f)$ é o conjunto $S_n - A_n$ das permutações ímpares. Logo, $|A_n| = |S_n - A_n|$ e, desde que S_n é união disjunta de A_n e $S_n - A_n$, temos

$$|A_n| = \frac{n!}{2}. \tag{2.2}$$

Pelo que provamos acima, metade das permutações no grupo S_n são pares e metade delas são ímpares. Para cada permutação σ de S_n, definimos seu sinal $\mathrm{sgn}(\sigma)$ como sendo o valor 1 ou -1, dependendo de sua paridade:

$$\mathrm{sgn}(\sigma) = \begin{cases} 1, & \text{se } \sigma \text{ é par} \\ -1, & \text{se } \sigma \text{ é ímpar.} \end{cases}$$

Vamos agora apresentar novos conjuntos geradores para S_n. Refinando um pouco mais a Proposição 2.1.23, temos o seguinte resultado.

Proposição 2.1.26. *O conjunto* $\{(1\ 2), (2\ 3), \ldots, (n{-}1\ n)\}$ *é um conjunto gerador de* S_n.

Demonstração. Primeiramente, escrevemos uma permutação como produto de ciclos disjuntos e, em seguida, escrevemos cada ciclo como um produto de transposições como na Equação (2.1). Considerando uma transposição $(i\ j)$ com $i < j-1$, podemos escrever $(i\ j) = (j-1\ j)(i\ j-1)(j-1\ j)$. Repetindo o raciocínio, o resultado está provado. □

Exercício 2.1.27. Mostre que os seguintes conjuntos são conjuntos geradores de S_n:

$$\{(1\ 2), (1\ 3), \ldots, (1\ n)\} \quad \text{e} \quad \{(1\ 2), (1\ 2\ \cdots\ n)\}.$$

Antes de finalizar esta seção, chamamos a atenção para a importância de subgrupos normais em um grupo G. Primeiramente, definimos o conceito de classe lateral de um subgrupo H em G.

Definição 2.1.28. Dados $H \leqslant G$ e $x \in G$, o conjunto $Hx = \{hx : h \in H\}$ é dita uma classe lateral à direita de H em G. Analogamente, definimos uma classe lateral à esquerda de H em G como o conjunto $xH = \{xh : h \in H\}$.

Temos um motivo importante para definir os conjuntos acima. Na verdade, eles são classes de relações de equivalência que podemos definir quando temos H um subgrupo de G. Dados $x, y \in G$, definimos estas relações conforme abaixo:

$$x \equiv y \text{ se, e somente se, } xy^{-1} \in H \tag{2.3}$$

$$x \sim y \text{ se, e somente se, } x^{-1}y \in H. \tag{2.4}$$

Exercício 2.1.29. Sejam G um grupo e $H \leqslant G$.

(a) Mostre que as relações definidas em G, nas Equações (2.3) e (2.4), são relações de equivalência.

(b) Mostre que a classe de equivalência de um elemento $x \in G$ dada a partir da Equação (2.3) é a classe lateral à direita Hx, e que a classe de equivalência de x dada pela Equação (2.4) é a classe lateral à esquerda xH.

Observamos que se G é um grupo finito, então, para qualquer $x \in G$, temos $|Hx| = |xH| = |H|$, pois as aplicações

$$\begin{array}{ccc} H & \to & Hx \\ h & \mapsto & hx \end{array} \quad \text{e} \quad \begin{array}{ccc} H & \to & xH \\ h & \mapsto & xh \end{array}$$

são bijetivas. A partir disto, podemos provar o célebre Teorema de Lagrange.

Teorema 2.1.30. *Sejam G um grupo finito e $H \leqslant G$. Então $|H|$ é um divisor de $|G|$.*

Demonstração. Usando a relação definida pela Equação (2.3), temos que G pode ser escrito como uma união disjunta de classes laterais à direita $G = \bigcup_{x \in G} Hx$. Desta forma, usando o que foi observado acima, temos

$$|G| = \sum_{x \in G} |Hx| = \sum_{x \in G} |H| = m|H|$$

onde m é o número de classes laterais à direita distintas de H em G. □

Para provar o teorema acima, poderíamos ter usado a relação dada a partir da Equação (2.4) no lugar da relação dada pela Equação (2.3) e chegaríamos a mesma conclusão. Portanto, isto mostra que o número de classes laterais à esquerda e à direita de H em G são iguais. Esse número é denominado o índice de H em G, denotado por $[G : H]$. Assim, o Teorema de Lagrange informa que

$$|G| = [G : H]|H|.$$

Podemos observar que as classes laterais à direita e à esquerda não são necessariamente iguais. Como um exemplo, se $H = \{1, (1\ 2)\}$ e $x = (1\ 2\ 3) \in S_3$, temos $Hx = \{(1\ 2\ 3), (2\ 3)\}$ enquanto que $xH = \{(1\ 2\ 3), (1\ 3)\}$, mas para subgrupos normais, essa propriedade é garantida como pode ser provada no próximo exercício.

Exercício 2.1.31. Sejam G um grupo e $N \leqslant G$. Mostre que se $N \lhd G$, então $Nx = xN$ para todo $x \in G$.

Exercício 2.1.32. Sejam G um grupo e $N \leqslant G$ tal que $[G : N] = 2$. Mostre que $N \lhd G$.

Pela Equação (2.2), usando o Teorema de Lagrange, temos que $[S_n : A_n] = 2$. Portanto, pelo exercício acima, temos que $A_n \lhd S_n$.

Quando N é um subgrupo normal de G, consideramos o conjunto

$$G/N := \{Nx : x \in G\}$$

de todas as classes laterais à direita e definimos a operação de classes

$$Nx \cdot Ny := Nxy, \text{ para } Nx, Ny \in G/N.$$

Obviamente, o mesmo pode ser feito considerando classes laterais à esquerda de N em G, já que as classes são iguais.

Exercício 2.1.33. Mostre que G/N com a operação definida acima é um grupo.

O grupo G/N, com $N \lhd G$, é chamado grupo quociente de G por N. Por exemplo, pelo Exercício 2.1.22, temos $G' \lhd G$ e o grupo G/G' tem a seguinte propriedade que será deixada como exercício.

Exercício 2.1.34. Mostre que o grupo quociente G/G' é abeliano.

Exercício 2.1.35. Mostre que o subgrupo derivado de S_3 é seu subgrupo alternado, ou seja, $S_3' = A_3$.

Observação 2.1.36. Em geral, o subgrupo derivado do grupo simétrico S_n é o subgrupo alternado A_n dado na Definição 2.1.25. Como $[S_n : A_n] = 2$, temos que o grupo quociente S_n/A_n tem ordem 2.

Exercícios V ou F da Seção 2.1: Verifique se cada sentença abaixo é verdadeira ou falsa, justificando convenientemente.

(1) As permutações (1 3)(2 3 5) e (1 2)(3 4 5) são conjugadas em S_5.

(2) O grupo simétrico S_6 tem 8 classes de conjugação.

(3) Os subgrupos $\{1, (1\ 2\ 3), (1\ 3\ 2)\}$ e $\{1, (2\ 3\ 4), (2\ 4\ 3)\}$ são conjugados em S_4.

(4) O grupo alternado A_n é gerado pelos 3-ciclos da forma $(1\ 2\ k),\ 3 \leqslant k \leqslant n$.

(5) O grupo alternado A_4 é abeliano.

(6) O grupo alternado A_8 tem um elemento de ordem 15.

(7) Os únicos subgrupos normais de S_3 são $\{1\}$, A_3 e S_3.

2.2 Representações de um grupo

Nesta seção, vamos apresentar a definição de representação de um grupo G e, para este fim, consideraremos G um grupo finito. Em particular, vamos dar exemplos e resultados específicos para o grupo simétrico S_n. Antes disso, vamos recordar alguns conceitos a respeito de homomorfismos de grupos e a ação de um grupo sobre um conjunto.

Definição 2.2.1. Uma função $\varphi : G \to H$ entre dois grupos G e H é dita um homomorfismo (de grupos), se ela é compatível com a estrutura dos grupos, isto é, se

$$\varphi(ab) = \varphi(a)\varphi(b), \text{ para todos } a, b \in G.$$

Se φ for um homomorfismo bijetor, então φ é dito um isomorfismo entre G e H, e denotamos $G \cong H$. Particularmente, um isomorfismo $\varphi : G \to G$ é dito um automorfismo de G.

Exemplo 2.2.2. Se F é um corpo, então a aplicação $\varphi : GL_n(F) \to F^*$, dada por $\varphi(A) = \det(A)$, é um homomorfismo de grupos, pois $\det(AB) = \det(A)\det(B)$, para quaisquer $A, B \in GL_n(F)$.

Exemplo 2.2.3. Dado um elemento x de um grupo G, definimos a aplicação

$$\begin{aligned} \tau_x : \quad & G \to G \\ & g \mapsto g^x \end{aligned}$$

onde $g^x = xgx^{-1}$. Esta aplicação é um automorfismo de G, dito automorfismo interno induzido por x.

Dados dois grupos G e H, não faremos distinções entre seus elementos neutros, ou seja, denotaremos 1 para ambos. Neste caso, se $\varphi : G \to H$ é um homomorfismo, vemos que $\varphi(1) = 1$ e definimos o conjunto

$$\mathrm{Ker}(\varphi) := \{g \in G : \varphi(g) = 1\}$$

que é denominado núcleo do homomorfismo φ.

Obviamente, $\mathrm{Ker}(\varphi)$ é um subgrupo de G e, mais do que isto, temos o exercício a seguir com mais informações.

Exercício 2.2.4. Seja $\varphi : G \to H$ um homomorfismo. Mostre que

(a) O núcleo $\mathrm{Ker}(\varphi)$ é um subgrupo normal de G.

(b) O conjunto imagem $\mathrm{Im}(\varphi) = \{\varphi(g) : g \in G\}$ é um subgrupo de H.

A partir de um homomorfismo de grupos $\varphi : G \to H$, considerando seu núcleo $N = \mathrm{Ker}(\varphi)$, podemos definir uma aplicação do grupo quociente G/N no subgrupo $\mathrm{Im}(\varphi)$

$$\begin{aligned} \widetilde{\varphi}: \quad & G/N \to \mathrm{Im}(\varphi) \\ & gN \mapsto \varphi(g). \end{aligned}$$

Exercício 2.2.5. Mostre que a aplicação $\widetilde{\varphi}$ dada acima está bem definida e é um isomorfismo.

Usando o exercício anterior, temos demonstrado o resultado abaixo, conhecido como Teorema do Isomorfismo de Grupos.

Teorema 2.2.6. *Se $\varphi: G \to H$ é um homomorfismo com núcleo $N = \mathrm{Ker}(\varphi)$, então $G/N \cong \mathrm{Im}(\varphi)$.*

Vamos agora nos preparar para definir o que entendemos por uma representação de um grupo G. Para isto, lembremos que se V é um espaço vetorial de

dimensão finita n sobre um corpo F, então podemos considerar o conjunto de todas as transformações lineares $T: V \to V$. Vamos particularmente considerar tais transformações que são bijetivas e formar o conjunto:

$$GL(V) = \{T: V \to V : T \text{ bijetiva}\}. \tag{2.5}$$

O conjunto acima, munido da operação de composição de funções, é um grupo. Além disso, ao fixar uma base de V sobre F, podemos associar cada elemento T de $GL(V)$ a uma matriz invertível M_T, um elemento do grupo $GL_n(F)$.

Exercício 2.2.7. Mostre que os grupos $GL_n(F)$ e $GL(V)$ definidos respectivamente no Exemplo 2.1.2 e na Equação (2.5) são isomorfos.

A partir de agora vamos considerar V um espaço vetorial de dimensão finita n e abaixo vamos definir o significado de representação de um grupo finito G.

Definição 2.2.8. Uma representação linear de G é um homomorfismo de grupos de G em $GL(V)$, para algum F-espaço vetorial de dimensão finita V, ou seja, é um homomorfismo

$$\begin{array}{rccc} \varphi: & G & \to & GL(V) \\ & g & \mapsto & \varphi_g \end{array}$$

onde o grau da representação φ é definido como a dimensão n de V.

Nos referiremos a uma representação $\varphi: G \to GL(V)$ como uma representação de G sobre V.

Observação 2.2.9. Fixada uma base β de V sobre F, podemos associar a uma representação $\varphi: G \to GL(V)$, um homomorfismo $[\varphi]_\beta : G \to GL_n(F)$, que associa cada elemento g do grupo à matriz correspondente à transformação linear φ_g. Esse homomorfismo é chamado uma representação matricial de grau n de G sobre F.

Para os nossos propósitos, nos referiremos às representações lineares e matriciais de um grupo G simplesmente como representações de G e não faremos distinções entre elas por motivos óbvios.

A partir da observação acima, é claro que todo grupo possui uma representação de grau arbitrário $n \geqslant 1$, bastando para isso considerar a aplicação

$$\begin{array}{rccc} \varphi: & G & \to & GL_n(F) \\ & g & \mapsto & \varphi_g := I_n \end{array}$$

onde I_n denota a matriz identidade $n \times n$.

Particularmente, temos a seguinte definição.

Definição 2.2.10. O homomorfismo $\varphi\colon G \to F^*$ dado por $\varphi(g) = 1$, para todo $g \in G$, é um exemplo de representação de grau 1 de um grupo G, denominada representação trivial de G.

Para dar um exemplo de uma representação não trivial, consideramos um grupo cíclico $\mathcal{C}_3 = \langle g : g^3 = 1\rangle$ de ordem 3 e uma raiz cúbica primitiva da unidade $u = e^{\frac{2\pi i}{3}}$. Temos que

$$\begin{array}{rccc} \varphi\colon & \mathcal{C}_3 & \to & GL_2(\mathbb{C}) \\ & g & \mapsto & \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix} \end{array}$$

define uma representação de grau 2 de $\mathcal{C}_3$.

Para dar mais exemplos de representações, vamos recordar o conceito de ação de um grupo sobre um conjunto e ver que cada representação $\varphi\colon G \to GL(V)$ define uma ação de G sobre o espaço V.

Definição 2.2.11. Uma ação de um grupo G sobre um conjunto $Y \neq \varnothing$ é uma aplicação $G \times Y \to Y$, que toma um par $(g, x) \in G \times Y$ e tem como resposta um elemento $g \cdot x \in Y$, respeitando duas condições:

1. $1 \cdot x = x$, para todo $x \in Y$.
2. $(g_1 g_2) \cdot\ x = g_1 \cdot (g_2 \cdot x)$, para todos $g_1, g_2 \in G$ e para todo $x \in Y$.

Assim, uma ação de um grupo G sobre um conjunto $Y \neq \varnothing$ é uma maneira de produzir um novo elemento de Y, que escrevemos como $g \cdot x$ a partir de um elemento g de G e um elemento x de Y, respeitando as condições abaixo

1. o elemento neutro de $1 \in G$ tem ação trivial: $1 \cdot x = x$, para todo $x \in Y$.
2. a ação tem que respeitar a operação do grupo: $\underbrace{(g_1 g_2)}_{\in G} \cdot x = g_1 \cdot \underbrace{(g_2 \cdot x)}_{\in Y}$.

Como um exemplo, temos que o grupo simétrico S_n age naturalmente sobre o conjunto $\widehat{n} = \{1, \ldots, n\}$ por

$$\sigma \cdot i = \sigma(i), \text{ para } \sigma \in S_n \text{ e } i \in \widehat{n}. \tag{2.6}$$

Antes de avançar em novos exemplos, para um corpo F e um grupo G, vamos definir a álgebra de grupo FG de G sobre F. Conforme dado na Observação 1.2.35, FG é o espaço vetorial sobre F livremente gerado por G, cujos elementos são somas formais

$$\sum_{g \in G} \alpha_g g \text{ com } \alpha_g \in F$$

onde $\alpha_g \neq 0$ apenas para um número finito de elementos de G.

A operação de adição em FG é dada por

$$\sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$$

e além disso, definimos uma multiplicação em FG por

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) = \sum_{g,h\in G} \gamma_{gh} gh, \;\; \gamma_{gh} = \alpha_g \beta_h.$$

Com isso, FG é um anel e se $\lambda \in F$, definimos também,

$$\lambda \left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \lambda \alpha_g g.$$

Claramente, temos que FG é uma álgebra cuja dimensão sobre F é a ordem do grupo G. Por exemplo, $\mathbb{C}S_4$ é uma álgebra de dimensão 24 sobre $\mathbb{C}$.

Agora vamos compreender a importância da álgebra de grupo FG na teoria de representações de grupos. Considerando uma representação $\varphi : G \to GL(V)$, temos definida uma ação de G sobre V dada por:

$$\begin{aligned} G \times V &\to V \\ (g, v) &\mapsto g \cdot v := \varphi_g(v). \end{aligned}$$

Vamos omitir o ponto em $g \cdot v$ e escrever simplesmente gv. Como consequência, considerando $\alpha_i \in F$ e $g_i \in G$, podemos estender a ação dada para os elementos $\alpha_1 g_1 + \ldots + \alpha_s g_s$ da álgebra de grupo FG da seguinte maneira

$$(\alpha_1 g_1 + \cdots + \alpha_s g_s)v = \alpha_1(g_1 v) + \cdots + \alpha_s(g_s v) \in V$$

e temos que o espaço V é um FG-módulo, que chamaremos FG-módulo correspondente à representação φ.

Note que se $\varphi : V \to W$ é uma aplicação F-linear entre dois FG-módulos V e W, então, de acordo com a Definição 1.2.10, para verificar se φ é um FG-homomorfismo, basta verificarmos que $\varphi(gv) = g\varphi(v)$ para todo $g \in G$ e todo $v \in V$.

Observação 2.2.12. De fato, existe uma correspondência biunívoca entre os FG-módulos de dimensão n e as representações de grau n de G. Isto significa que dado um FG-módulo V, podemos definir uma representação de G sobre V.

Observamos que um FG-módulo V é um F-espaço vetorial invariante sob a ação dada acima. Neste caso, dizemos que V é G-invariante.

Já comentamos que o grupo S_n age sobre o conjunto $\widehat{n}$ como na Equação (2.6) e, a partir desta ação, podemos definir uma representação de S_n sobre um espaço vetorial V com base $B = \{v_1, \ldots, v_n\}$ dada por

$$\begin{array}{rccl} \varphi\colon & S_n & \to & GL(V) \\ & \sigma & \mapsto & \varphi_\sigma\colon V \to V \\ & & & \qquad v_i \mapsto v_{\sigma(i)}. \end{array}$$

Desta forma, temos que $V = \operatorname{span}_F\{v_1, \ldots, v_n\}$ é um FS_n-módulo e a representação acima é chamada representação permutacional de grau n de S_n com módulo permutacional V. Vamos exemplificar explicitando a representação permutacional de grau 3 do grupo simétrico S_3 por meio das matrizes que correspondem às transformações lineares φ_σ.

Observação 2.2.13. Observe que como uma representação $\varphi\colon G \to GL(V)$ é um homomorfismo de grupos, para que ela esteja completamente definida é suficiente conhecer as imagens φ_x dos elementos x que são geradores de G.

Exemplo 2.2.14. Considerando $a = (1\,2\,3), b = (1\,2)$ como geradores do grupo S_3, temos a seguinte descrição deste grupo com seus geradores e relações entre eles

$$S_3 = \langle a, b : a^3 = b^2 = (ab)^2 = 1\rangle.$$

Pelo que foi dito acima, temos uma ação de S_3 sobre um espaço vetorial V com F-base $\{v_1, v_2, v_3\}$ dada por $\sigma \cdot v_i = v_{\sigma(i)}, \sigma \in S_3$. Assim, temos a representação correspondente $\psi\colon S_3 \to GL_3(F)$ dada por

$$\psi_a = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{e} \quad \psi_b = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Definição 2.2.15. Uma representação $\varphi\colon G \to GL(V)$ é irredutível se V é um FG-módulo simples, ou seja, os únicos F-subespaços G-invariantes de V são $\{0\}$ e V.

Obviamente, qualquer representação de grau 1 de um grupo é irredutível. Notamos que, de modo geral, a representação permutacional de grau n de S_n não é irredutível, pois o subespaço $U = \text{span}_F\{v_1 + \cdots + v_n\}$ é S_n-invariante.

Exercício 2.2.16. Considere a representação ψ dada no Exemplo 2.2.14.

(a) Mostre que o subespaço $W = \text{span}_F\{v_1 - v_2, v_1 - v_3\}$ é S_3-invariante.

(b) Mostre que W não contém subespaços S_3-invariantes.

(c) Conclua que a restrição da representação ψ ao $\mathbb{C}S_3$-módulo W é uma representação irredutível de grau 2 de S_3.

Observação 2.2.17. De modo geral, considerando a representação permutacional de grau n de S_n, temos que o subespaço $W = \text{span}_F\{v_1 - v_2, \ldots, v_1 - v_n\}$ é S_n-invariante e, além disso, a restrição ao subespaço W é uma representação irredutível de grau $n-1$ de S_n.

Ao considerar o FG-módulo V correspondente a uma representação φ, um dos nossos interesses é saber quando V é um FG-módulo semissimples. Quando isto ocorre, dizemos que a representação φ associada ao FG-módulo V é completamente redutível.

Apresentaremos a seguir um resultado sobre a semissimplicidade de FG-módulos, conhecido como Teorema de Maschke, que tem papel fundamental na teoria de representações de grupos.

Observação 2.2.18. Antes de enunciar o Teorema de Maschke, observamos que, se a característica de um corpo F não é divisor da ordem de um grupo finito G, então $|G|$ é invertível em F. Isto significa que, se V é um FG-módulo e $v \in V$, então $\frac{1}{|G|}v \in V$.

Teorema 2.2.19 (Maschke)**.** *Se G é um grupo finito e F é um corpo cuja característica não divide a ordem de G, então todo FG-módulo V é semissimples.*

Demonstração. Consideremos U um FG-submódulo de V. Queremos mostrar que existe um FG-submódulo W de V tal que $V = U \oplus W$. Inicialmente, já sabemos que existe um F-subespaço W_0 de V tal que $V = U \dot{+} W_0$. Vamos usar esse subespaço para construir o FG-submódulo W de V procurado.

Considerando $v \in V$, temos $v = u + w$, com $u \in U$ e $w \in W_0$ e podemos definir $f : V \to V$ por $f(v) = u$. Modificamos f criando um nova aplicação

$$\begin{array}{rccc} \widetilde{f}: & V & \longrightarrow & V \\ & v & \longmapsto & \frac{1}{|G|}\displaystyle\sum_{g\in G} g^{-1} f(gv). \end{array}$$

Primeiramente, notamos que $\mathrm{Im}(\widetilde{f}) \subset U$, pois $f(gv) \in U$ para qualquer $g \in G$ e qualquer $v \in V$ e U é um FG-submódulo de V. Agora, vamos mostrar que $\widetilde{f}$ é um FG-homomorfismo. Para ver isto, basta mostrar que $\widetilde{f}(hv) = h\widetilde{f}(v)$, para todo $h \in G$ e todo $v \in V$. Isto é claro, pois o valor de $\widetilde{f}(hv)$ é dado como segue abaixo

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G} g^{-1} f(\underbrace{gh}_{x} v) &= \frac{1}{|G|}\sum_{x\in G} hx^{-1} f(xv)\\ &= h\left(\frac{1}{|G|}\sum_{x\in G} x^{-1} f(xv)\right)\\ &= h\widetilde{f}(v).\end{aligned}$$

Além disso, note que dados $g \in G$ e $u \in U$, temos $gu \in U$, logo, $f(gu) = gu$. Assim,

$$\widetilde{f}(u) = \frac{1}{|G|}\sum_{g\in G} g^{-1} f(gu) = \frac{1}{|G|}\sum_{g\in G} u = u. \tag{2.7}$$

Agora, tomando $v \in V$, temos $\widetilde{f}(v) \in U$ e, portanto, pelo que foi visto acima temos

$$\widetilde{f}^2(v) = \widetilde{f}(\widetilde{f}(v)) = \widetilde{f}(v)$$

ou seja, $\widetilde{f}^2 = \widetilde{f}$. Note ainda que, pela Equação (2.7), temos $\mathrm{Im}(\widetilde{f}) = U$.

Desde que $\widetilde{f}$ é um FG-homomorfismo, de acordo com o que vimos na Proposição 1.2.30, considerando $W = \mathrm{Ker}(\widetilde{f})$, temos que W é um FG-submódulo de V e $V = U \oplus W$. Desta forma, o teorema está demonstrado. □

Com isso, nas condições do Teorema de Maschke, temos que toda representação de um grupo finito G é completamente redutível.

Como a álgebra de grupo FG é um FG-módulo, como consequência temos o seguinte.

Corolário 2.2.20. *Seja G um grupo finito e F um corpo cuja característica não divide a ordem de G. Então a álgebra de grupo FG é uma álgebra semissimples.*

É possível mostrar que vale a recíproca do Teorema de Maschke: se todo FG-módulo é semissimples, então G é um grupo finito e a a característica de F não divide a ordem de G.

O resultado a seguir é o Lema de Schur, que já provamos no Lema 1.2.19. Vamos repetir o enunciado aqui na linguagem de FG-módulos simples para usá-lo em seguida.

Lema 2.2.21. *Sejam M e N dois FG-módulos simples e $\phi\colon M \to N$ um FG-homomorfismo. Então ou $\phi = 0$ ou ϕ é um isomorfismo.*

Corolário 2.2.22. *Seja M um FG-módulos simples, onde F é um corpo algebricamente fechado. Se $\phi\colon M \to M$ é um FG-isomorfismo, então ϕ é um múltiplo escalar da aplicação identidade em M.*

Demonstração. De fato, ϕ é uma F-transformação linear de M e F é algebricamente fechado, logo ϕ possui um autovalor $\alpha \in F$. Portanto, existe um autovetor $v \in M$, o qual é um elemento não nulo tal que $\phi(v) = \alpha v$. Logo, $\mathrm{Ker}(\phi - \alpha id_M)$ é um FG-submódulo de M diferente de zero. Como M é simples, temos que $\mathrm{Ker}(\phi - \alpha id_M) = M$, de onde segue que $\phi = \alpha id_M$. □

Como consequência do corolário acima, temos que grupos abelianos têm uma particularidade em relação às suas representações irredutíveis que está apresentada no próximo resultado.

Corolário 2.2.23. *As representações irredutíveis de um grupo abeliano G sobre um corpo algebricamente fechado são todas de grau 1.*

Demonstração. Vamos considerar $\varphi\colon G \to GL(V)$ uma representação irredutível de V. Deste modo, o FG-módulo correspondente é simples. Vamos fixar um elemento $x \in G$ e definir uma aplicação $f : V \to V$ por $f(v) = xv$, onde $v \in V$. Note que essa aplicação é linear e desde que G é abeliano, se $g \in G$, temos

$$f(gv) = xgv = gxv = gf(v), \text{ para todo } v \in V.$$

Portanto, f é um FG-homomorfismo e, pelo Corolário 2.2.22, temos que $f = \lambda_x id_V$, para algum $\lambda_x \in F$. Isto mostra que $xv = \lambda_x v$ e desta forma, se U é um subespaço não nulo qualquer de V e $u \in U$, temos $xu = \lambda_x u \in U$. Como x foi tomado arbitrariamente em G, temos que U é G-invariante. Desde que V é simples, temos $U = V$ e, com isso, concluímos que a única possibilidade é que V tem dimensão 1, pois qualquer subespaço U de V é um FG-submódulo de V. Portanto, a representação irredutível inicial φ é de grau 1. □

O interesse da teoria de representações de grupos é determinar todas as representações de um dado grupo G ou, pelo menos, obter informações sobre elas. Como esta parece ser uma tarefa difícil, inicialmente devemos saber como distinguir duas representações de G que tenham o mesmo grau.

Definição 2.2.24. Duas representações $\varphi\colon G \to GL(V_1)$ e $\phi\colon G \to GL(V_2)$ são equivalentes se existe uma transformação linear bijetiva $T : V_1 \to V_2$ tal que $\varphi_g = T^{-1}\phi_g T$, para todo $g \in G$.

Observamos portanto, que representações equivalentes têm necessariamente o mesmo grau, e a definição acima indica que o seguinte diagrama é comutativo, para todo $g \in G$:

$$\begin{array}{ccc} V_1 & \xrightarrow{\varphi_g} & V_1 \\ {\scriptstyle T}\downarrow & & \downarrow{\scriptstyle T} \\ V_2 & \xrightarrow{\phi_g} & V_2 \end{array}$$

ou seja, $T\varphi_g = \phi_g T$.

Observação 2.2.25. Observemos que duas representações de grau 1 de um grupo G são equivalentes se, e somente se, são aplicações iguais.

A seguir enunciaremos dois teoremas que nos informam sobre o grau de uma representação irredutível de um grupo finito G e a quantidade de representações irredutíveis não equivalentes que esse grupo finito pode ter. Não daremos as demonstrações, que podem ser consultadas no livro de James e Liebeck (2001).

Teorema 2.2.26. *O grau de uma representação irredutível de um grupo finito G é divisor de $|G|$.*

Teorema 2.2.27. *O número total de representações irredutíveis não equivalentes de um grupo finito G sobre um corpo algebricamente fechado, cuja característica não divide $|G|$, é igual ao número de classes de conjugação de G.*

A partir do teorema acima e da Observação 2.1.13, temos o seguinte.

Corolário 2.2.28. *O número total de representações irredutíveis não equivalentes de um grupo abeliano finito G sobre $\mathbb{C}$ é igual a $|G|$.*

Uma representação muito importante de um grupo G é a chamada representação regular. Para defini-la, consideramos a álgebra de grupo FG que sabemos que é um espaço vetorial sobre F que tem G como base. Podemos definir um homomorfismo de G em $GL(FG)$, usando apenas a ação de G sobre os elementos da base de FG, ou seja, apenas sobre G e estendendo linearmente, como abaixo, onde $x \in G$

$$\begin{aligned} R\colon\ G &\to GL(FG) \\ g &\mapsto R_g : FG \to FG \\ & \qquad x \mapsto gx. \end{aligned}$$

Definição 2.2.29. A aplicação definida acima é dita representação regular de G.

Ao considerar F um corpo cuja característica não divide a ordem de G, pelo Teorema 2.2.19, temos que a representação regular R é completamente redutível, ou seja, FG é uma álgebra semissimples e FG se escreve como a soma direta de FG-módulos simples. Além disso, pelo Teorema 2.2.27, o número total de FG-módulos simples é igual à quantidade de classes de conjugação de G, digamos k.

Definição 2.2.30. Um conjunto $\{V_1, \ldots, V_k\}$ de representantes de FG-módulos simples não isomorfos é chamado um conjunto completo de FG-módulos simples.

Seja $\{V_1, \ldots, V_k\}$ um conjunto completo de FG-módulos simples. Então a álgebra de grupo FG se escreve como

$$FG \cong V_1^{(n_1)} \oplus \cdots \oplus V_k^{(n_k)} \tag{2.8}$$

onde $n_i \geqslant 1$, para todo $i = 1, \ldots, k$. Agora, pelo Teorema de Wedderburn–Artin, temos, para cada i, que $V_i^{(n_i)} \cong M_{n_i}(D_i)$, onde D_i é uma F-álgebra de divisão. Em particular, se F é um corpo algebricamente fechado, então $V_i^{(n_i)} \cong M_{n_i}(F)$. Como $\dim_F(M_{n_i}(F)) = n_i^2$, concluímos que $\dim_F(V_i) = n_i$, para todo $i = 1, \ldots, k$. Nessas condições, sumarizamos estas informações no próximo teorema.

Teorema 2.2.31. *Considere a decomposição de FG como soma direta de FG-submódulos simples. Na decomposição, cada FG-submódulo simples de FG aparece um número finito de vezes que é exatamente igual a sua dimensão sobre F.*

Consequentemente, nas condições acima, temos

$$FG \cong M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F). \tag{2.9}$$

Observe que se G é um grupo abeliano, pelo Corolário 2.2.28 e pelo que foi dito acima, temos

$$\mathbb{C}G \cong \mathbb{C} \oplus \cdots \oplus \mathbb{C}$$

onde na soma direta o número de componentes é igual a $|G|$.

Agora, vamos considerar M um FG-módulo qualquer sobre um corpo F de característica zero. Nessa situação, também podemos usar o Teorema 2.2.19 para decompor M como soma direta de FG-submódulos simples, e o Corolário 1.3.35 nos dá informações sobre esses submódulos simples. Abaixo, repetimos o resultado na linguagem de FG-módulos, onde consideramos $\{V_1, \ldots, V_k\}$ um conjunto completo de FG-módulos simples.

Teorema 2.2.32. *Cada FG-submódulo simples que aparece na decomposição de M como dito acima é isomorfo a algum FG-submódulo simples de FG, ou seja, cada um desses FG-submódulos é isomorfo a algum FG-módulo em $\{V_1, \ldots, V_k\}$.*

De acordo com o teorema anterior, podemos escrever

$$M \cong V_1^{(s_1)} \oplus \cdots \oplus V_k^{(s_k)}. \tag{2.10}$$

Para $i = 1, \ldots, k$, cada s_i é denominado a multiplicidade do FG-módulo V_i em M.

A seguir, verificaremos como determinar a quantidade de representações distintas de grau 1 de um grupo finito G. Para isso, consideremos G' o subgrupo derivado de G conforme a Definição 2.1.21. Vamos mostrar que existe uma correspondência biunívoca entre as distintas representações de grau 1 de G e as distintas representações de grau 1 de G/G'.

Note que se $\varphi\colon G \to F^*$ é uma representação de grau 1 de G, então, lembrando que $(x, y) = xyx^{-1}y^{-1}$ é o comutador de x e y, temos

$$\varphi((x, y)) = (\varphi(x), \varphi(y)) = 1.$$

Consequentemente, considerando a aplicação $\overline{\varphi}\colon G/G' \to F^*$ induzida por φ dada por

$$\overline{\varphi}(xG') = \varphi(x),\ x \in G \tag{2.11}$$

vemos que $\overline{\varphi}$ está bem definida, pois se $x, y \in G$ são tais que $xG' = yG'$, então pelo Exercício 2.1.29 temos $x^{-1}y \in G'$. Assim, $\varphi(x^{-1}y) = 1$, ou seja, $\varphi(x) = \varphi(y)$. Logo, $\overline{\varphi}(xG') = \overline{\varphi}(yG')$. Como claramente, temos que $\overline{\varphi}(xG'yG') = \overline{\varphi}(xG')\overline{\varphi}(yG')$, concluímos que é um homomorfismo e, portanto, é uma representação de grau 1 de G/G'.

Reciprocamente, começando com uma representação de grau 1

$$\overline{\varphi} : G/G' \to F^*$$

usamos a Equação (2.11) para definir uma representação de G e temos a correspondência biunívoca desejada.

Agora, lembremos que, pelo Exercício 2.1.34, temos que G/G' é um grupo abeliano e desta forma, pelo Corolário 2.2.23, toda representação irredutível de G/G' é de grau 1. Além disso, pelo Corolário 2.2.28, a quantidade de representações irredutíveis de um grupo abeliano é igual a sua ordem.

Chegamos a seguinte conclusão.

Proposição 2.2.33. *O número de representações de grau 1 de um grupo finito G é igual a ordem do grupo quociente G/G'.*

No caso em que $G = S_n$, pela Observação 2.1.36, temos $G' = A_n$ e $|S_n/A_n| = 2$. Então S_n possui exatamente duas representações de grau 1, que são dadas por

$$1 : \sigma \mapsto 1 \quad \text{e} \quad \text{sgn} : \sigma \mapsto \text{sgn}(\sigma), \ \text{ para todo } \sigma \in S_n$$

ou seja, temos respectivamente, a representação trivial e a representação sinal.

Abaixo, apresentamos exemplos de representantes de todas as representações irredutíveis não equivalentes de S_3 sobre o corpo dos números complexos $\mathbb{C}$. Recordamos inicialmente que S_3 tem 3 classes de conjugação e, portanto, possui 3 representações irredutíveis não equivalentes sobre $\mathbb{C}$.

Já sabemos que S_3 tem duas representações irredutíveis de grau 1, que são não equivalentes:

$$1 : \begin{cases} a & \mapsto & 1 \\ b & \mapsto & 1 \end{cases} \qquad \text{e} \qquad \text{sgn} : \begin{cases} a & \mapsto & 1 \\ b & \mapsto & -1. \end{cases} \tag{2.12}$$

Lembremos também que, pelo Exercício 2.2.16, temos que $W = \text{span}\{w_1, w_2\}$, onde $w_1 = v_1 - v_2$ e $w_2 = v_1 - v_3$, é um $\mathbb{C}S_3$-módulo simples e, assim, a representação correspondente $\widetilde{\psi} : S_3 \to GL(W)$ é irredutível de grau 2 e é dada por

$$a = (1\,2\,3) \mapsto \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{e} \qquad b = (1\,2) \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}. \tag{2.13}$$

Qualquer outra representação irredutível de grau 2 de S_3 é equivalente a representação $\widetilde{\psi}$. Desta forma, todas as representações irredutíveis não equivalentes de S_3 estão listadas acima.

Exercícios V ou F da Seção 2.2: Verifique se cada sentença abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, G representa um grupo e F é um corpo de característica zero.

(1) Se φ e ψ são representações de um grupo G e têm o mesmo grau, então φ e ψ são equivalentes.

(2) Se V é um FG-módulo, então o conjunto $V_0 = \{v \in V : gv = v, \ \forall g \in G\}$ é um FG-submódulo de V.

(3) Se φ é uma representação de grau 1 de um grupo G, então φ é a representação trivial.

(4) Se $\mathcal{C}_4$ é um grupo cíclico de ordem 4, é verdade que $\mathbb{C}\mathcal{C}_4 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$.

(5) Se G é um grupo de ordem 8 que tem exatamente 4 classes de conjugação, então $\mathbb{C}G \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$.

(6) Duas representações de S_3 com grau 2 são equivalentes.

(7) Para a representação de S_3 definida na Equação (2.13), temos $\widetilde{\psi}((1\ 3)) = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$.

(8) Considere $\mathcal{C}_3 = \langle a : a^3 = 1 \rangle$ um grupo cíclico de ordem 3. A aplicação $\theta : \mathcal{C}_3 \to GL_2(\mathbb{C})$ definida por

$$a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

é uma representação de $\mathcal{C}_3$.

2.3 Caracteres do grupo simétrico

Vamos agora introduzir o conceito de caracter de grupo e apresentar algumas informações sobre os caracteres do grupo simétrico S_n que serão importantes no estudo de PI-álgebras.

Antes disso, lembremos que dada uma matriz $a = (a_{ij}) \in M_n(F)$, com $1 \leqslant i, j \leqslant n$, definimos o seu traço $\mathrm{tr}(a)$ como a soma das entradas na diagonal, ou seja, $\mathrm{tr}(a) = \sum_{i=1}^{n} a_{ii}$. Lembremos ainda que, dadas $a, b \in M_n(F)$, temos as seguintes propriedades básicas para o traço da soma e do produto:

1. $\mathrm{tr}(a + b) = \mathrm{tr}(a) + \mathrm{tr}(b)$.
2. $\mathrm{tr}(ab) = \mathrm{tr}(ba)$.

Ao definirmos uma representação φ de grau n de um grupo finito G, a cada elemento $g \in G$ associamos uma matriz invertível $\varphi_g \in GL_n(F)$. O caracter do elemento g é definido como o traço $\mathrm{tr}(\varphi_g)$ da matriz φ_g. Vamos agora definir o que entendemos pelo caracter da representação.

Definição 2.3.1. Definimos o caracter de uma representação $\varphi : G \to GL_n(F)$ como a função $\chi_\varphi : G \to F$ dada por $\chi_\varphi(g) := \mathrm{tr}(\varphi_g)$, para $g \in G$. Se V é o G-módulo correspondente à representação, também dizemos que χ_φ é o caracter de V, denotado $\chi_\varphi(V)$.

Um caracter de G, ou um G-caracter, é o caracter de alguma representação de G. O grau do caracter é o grau da representação correspondente e o caracter é dito irredutível se a representação for irredutível. Note que $\varphi(1) = I_n$ para qualquer representação φ de grau n, logo $\chi_\varphi(1) = n$ é exatamente o grau de φ.

Exemplo 2.3.2. Considerando a representação $\widetilde{\psi} : S_3 \to GL(W)$, definida na Equação (2.13), temos que $\chi_{\widetilde{\psi}}((1\,2\,3)) = -1$ e $\chi_{\widetilde{\psi}}((1\,2)) = 0$.

Quando $\varphi : G \to GL_n$ e $\psi : G \to GL_n$ são duas representações equivalentes de um grupo G, sabemos que existe uma matriz $n \times n$ invertível T tal que $T^{-1}\varphi_g T = \psi_g$, para todo $g \in G$. Com isso, usando a propriedade do traço do produto, vemos que duas representações equivalentes têm o mesmo caracter:

$$\mathrm{tr}(\psi_g) = \mathrm{tr}(T^{-1}\varphi_g T) = \mathrm{tr}(T(T^{-1}\varphi_g)) = \mathrm{tr}(\varphi_g), \text{ para todo } g \in G.$$

Considerando os caracteres χ_φ e χ_ψ das representações φ e ψ, respectivamente, o que provamos acima é que $\chi_\psi(g) = \chi_\varphi(g)$, para todo $g \in G$.

Definição 2.3.3. Dois caracteres de um grupo G são ditos equivalentes se as representações correspondentes são equivalentes.

Proposição 2.3.4. *Um caracter χ de G é uma função de classe, isto é, se dois elementos g e h estão em uma mesma classe de conjugação de G, então $\chi(g) = \chi(h)$.*

Demonstração. De fato, se g e h são conjugados em G, então existe $x \in G$ tal que $h = g^x := xgx^{-1}$ e assim, temos

$$\chi(h) = \mathrm{tr}(\varphi_{xgx^{-1}}) = \mathrm{tr}(\varphi_x\varphi_g\varphi_{x^{-1}}) = \mathrm{tr}(\varphi_{x^{-1}}\varphi_x\varphi_g) = \mathrm{tr}(\varphi_g) = \chi(g).$$

□

Como consequência da proposição acima, dada uma representação de G, para conhecer os valores dos caracteres dos elementos de G por esta representação, é suficiente determinar o valor do caracter de um representante da cada classe de conjugação. Desta forma, para a representação no Exemplo 2.3.2, temos

$$\chi_{\widetilde{\psi}}(1) = 2, \quad \chi_{\widetilde{\psi}}((1\,2\,3)) = -1 \quad \text{e} \quad \chi_{\widetilde{\psi}}((1\,2)) = 0.$$

e consequentemente teremos

$$\chi_{\widetilde{\psi}}((1\ 3\ 2)) = -1 \ \text{ e } \ \chi_{\widetilde{\psi}}((1\ 3)) = \chi_{\widetilde{\psi}}((2\ 3)) = 0.$$

Além disso, como cada caracter irredutível é o caracter de uma representação irredutível e representações equivalentes têm o mesmo caracter, pelo Teorema 2.2.27, o número de caracteres irredutíveis não equivalentes de um grupo finito G sobre um corpo algebricamente fechado cuja característica não divide $|G|$ é igual ao número de classes de conjugação de G.

Definição 2.3.5. A tábua de caracteres de um grupo finito G é uma tabela, onde disponibilizamos os valores de todos os seus caracteres irredutíveis não equivalentes em representantes das classes de conjugação de G.

Considerando apenas os valores dos caracteres em cada elemento, a tábua de caracteres de G é uma matriz quadrada $k \times k$, onde k é o número de classes de conjugação de G.

Exemplo 2.3.6. Vamos construir a tábua de caracteres de S_3. Nas Equações (2.12) e (2.13), já vimos os exemplos de representantes para todas as representações irredutíveis de S_3. Assim, escolhendo 1, (1 2 3) e (1 2) como representantes das classes de conjugação em S_3 e χ_t, χ_s e $\chi_{\widetilde{\psi}}$ para denotar o caracter da representação trivial, da representação sinal e da representação $\widetilde{\psi}$, respectivamente, temos a seguinte tábua de caracteres

caracter	1	(1 2 3)	(1 2)
χ_t	1	1	1
χ_s	1	1	-1
$\chi_{\widetilde{\psi}}$	2	-1	0

Recordemos que cada classe de conjugação de S_n corresponde a uma partição de n de acordo com a estrutura cíclica do representante da classe. Por exemplo para $a = (1\ 2\ 3)$ e $b = (1\ 2)$ em S_3, temos as correspondências:

$$\begin{aligned} cl(1) &\leftrightarrow (1)(2)(3) \leftrightarrow (1,1,1) \vdash 3 \\ cl(a) &\leftrightarrow (1\ 2\ 3) \leftrightarrow (3) \vdash 3 \\ cl(b) &\leftrightarrow (1\ 2)(3) \leftrightarrow (2,1) \vdash 3. \end{aligned}$$

Como a quantidade de caracteres irredutíveis de S_n é igual ao seu número de classes de conjugação, também vamos indexar cada caracter irredutível de S_n por uma partição $\lambda \vdash n$. Por exemplo, para S_3 vamos denotar

$$\chi_t = \chi_{(3)}, \quad \chi_s = \chi_{(1,1,1)} \quad \text{e} \quad \chi_{\widetilde{\psi}} = \chi_{(2,1)}.$$

A escolha feita para cada partição acima determinada depende de uma série de fatores que não vamos enumerar aqui, pois é importante apenas ter em mente que tal associação pode ser feita de modo geral. A representação e o $\mathbb{C}S_n$-módulo correspondentes ao caracter também serão indexados pela mesma partição.

Assim, no exemplo acima, temos as representações $\varphi_{(3)}$ como a representação trivial, $\varphi_{(1,1,1)}$ como a representação sinal e $\varphi_{(2,1)}$ como uma representação irredutível de grau 2 de S_3. Podemos escrever os $\mathbb{C}S_3$-módulos correspondentes como $V_{(3)}$, $V_{(1,1,1)}$ e $V_{(2,1)}$, respectivamente. De acordo com a Equação (2.8), temos

$$\mathbb{C}S_3 \cong V_{(3)} \oplus V_{(1,1,1)} \oplus V_{(2,1)}^{(2)}$$

ou seja, pela Equação (2.9) temos

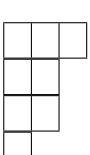
$$\mathbb{C}S_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}).$$

Para o grupo simétrico S_4, existem 5 caracteres irredutíveis não equivalentes que podem ser denotados $\chi_{(1,1,1,1)}$, $\chi_{(2,1,1)}$, $\chi_{(2,2)}$, $\chi_{(3,1)}$ e $\chi_{(4)}$. Para determinar a decomposição de $\mathbb{C}S_4$ em $\mathbb{C}S_4$-submódulos simples é necessário conhecer a multiplicidade de cada S_4-módulo simples, ou seja, precisamos conhecer o grau da representação correspondente.

Vamos agora descrever brevemente a teoria desenvolvida por A. Young para determinar o grau de cada representação irredutível de S_n. O leitor que desejar se aprofundar neste assunto, pode consultar o livro de Sagan (2001).

Primeiramente, ao considerarmos uma partição $\lambda = (\lambda_1, \ldots, \lambda_s) \vdash n$, vamos associar a ela um diagrama que consiste de n boxes $\square$ distribuídos da seguinte maneira: colocaremos λ_1 boxes na primeira linha, λ_2 boxes na segunda linha de modo que fiquem alinhados com os boxes da primeira linha desde a primeira coluna, e assim por diante até termos λ_s boxes na última linha. Este será dito o diagrama de Young do tipo λ.

Exemplo 2.3.7. O diagrama de Young do tipo λ, onde $\lambda = (3, 2, 2, 1) \vdash 8$, está ao lado.

$D_\lambda =$ 

Para uma partição fixa $\lambda \vdash n$, definimos uma tabela de Young do tipo λ como um completamento dos boxes do diagrama D_λ com naturais $1, 2, \ldots, n$.

Exemplo 2.3.8. Para $n = 3$, as tabelas de Young do tipo $\lambda = (2, 1)$ são:

$$\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array} \quad , \quad \begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array} \quad , \quad \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 3 \\ \cline{1-1}\end{array}$$

$$\begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 \\ \cline{1-1}\end{array} \quad , \quad \begin{array}{|c|c|}\hline 3 & 1 \\ \hline 2 \\ \cline{1-1}\end{array} \quad \text{e} \quad \begin{array}{|c|c|}\hline 3 & 2 \\ \hline 1 \\ \cline{1-1}\end{array} \quad .$$

Observe que para todo $n \geqslant 1$, existem $n!$ tabelas de Young do tipo λ. Algumas dessas tabelas têm destaque especial, como veremos a seguir.

Definição 2.3.9. Dizemos que uma tabela de Young T_λ do tipo λ é standard[2] se os inteiros em cada linha e em cada coluna de T_λ crescem da esquerda para direita e de cima para baixo, respectivamente.

Exemplo 2.3.10. Para $n = 5$, as tabelas standard do tipo $\lambda = (3, 2)$ são:

$$\begin{array}{|c|c|c|}\hline 1 & 3 & 5 \\ \hline 2 & 4 \\ \cline{1-2}\end{array} \quad , \quad \begin{array}{|c|c|c|}\hline 1 & 2 & 5 \\ \hline 3 & 4 \\ \cline{1-2}\end{array} \quad , \quad \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 & 5 \\ \cline{1-2}\end{array}$$

$$\begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 5 \\ \cline{1-2}\end{array} \quad \text{e} \quad \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 \\ \cline{1-2}\end{array} \quad .$$

O interesse pelas tabelas standard do tipo λ está exatamente no resultado a seguir, provado por A. Young, cuja demonstração pode ser vista no livro de James e Kerber (1981). Lembrando que cada representação irredutível de S_n está associada a uma partição λ de n, o resultado nos diz qual é o seu grau.

Teorema 2.3.11. *Seja φ_λ uma representação irredutível de S_n, onde $\lambda \vdash n$. Então, o grau d_λ de φ_λ é igual ao número de tabelas standard do tipo λ.*

Para poder estabelecer o resultado que nos informa sobre o valor do grau d_λ, precisamos de mais alguns conceitos. Dadas uma partição $\lambda \vdash n$ e um diagrama D_λ de Young do tipo λ, vamos denotar um box na posição (i, j), ou seja, localizado na linha i e coluna j, por b_{ij}. O gancho do box b_{ij} é dado pelo número de boxes a direita de b_{ij} mais o número de boxes abaixo de b_{ij} mais 1, denotado h_{ij}.

[2] A palavra standard pode ser traduzida para padrão em português, mas faremos a opção de não fazer a tradução e vamos manter a terminologia usada em inglês.

Exemplo 2.3.12. Ao lado, usando o diagrama do Exemplo 2.3.7, preenchemos cada box com o valor de seu gancho. Note que o produto dos ganchos é igual a $\prod h_{ij} = 6 \cdot 4 \cdot 4 \cdot 3 \cdot 2$.

6	4	1
4	2	
3	1	
1		

Existem diversas demonstrações dadas para o próximo teorema que estabelece o valor exato do grau d_λ de uma representação irredutível φ_λ de S_n. Não apresentaremos uma demonstração aqui, pois nenhuma delas é trivial e todas fogem do objetivo deste livro. O leitor interessado pode consultar o livro de Sagan (2001).

Teorema 2.3.13. *Para cada $\lambda \vdash n$, o número d_λ de tabelas standard do tipo λ é igual a*

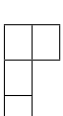
$$d_\lambda = \frac{n!}{\prod_{i,j} h_{ij}}. \tag{2.14}$$

A expressão dada na Equação (2.14) é conhecida como fórmula do gancho. Usando as informações dadas pela Equação (2.9) e pelo teorema anterior, para o grupo simétrico S_n, temos

$$\mathbb{C}S_n \cong \bigoplus_{\lambda \vdash n} M_{d_\lambda}(\mathbb{C}).$$

Exemplo 2.3.14. Vamos determinar os graus de todas as representações irredutíveis de S_4, ou seja, os graus de todos os S_4-caracteres irredutíveis. Consequentemente, vamos apresentar a decomposição de $\mathbb{C}S_4$ em submódulos simples. Para isso, consideremos abaixo os diagramas de Young de cada uma das partições de 4 e os ganchos referentes a cada box:

$D_{(1,1,1,1)} =$  ganchos : $h_{11} = 4,\ h_{21} = 3,\ h_{31} = 2,\ h_{41} = 1.$

$D_{(2,1,1)} =$  ganchos : $h_{11} = 4,\ h_{12} = 1,\ h_{21} = 2,\ h_{22} = 1.$

$D_{(2,2)} =$  ganchos : $h_{11} = 3,\ h_{12} = 2,\ h_{21} = 2,\ h_{22} = 1.$

$D_{(3,1)} =$  ganchos : $h_{11} = 4,\ h_{12} = 2,\ h_{13} = 1,\ h_{21} = 1.$

$D_{(4)} =$  ganchos : $h_{11} = 4,\ h_{12} = 3,\ h_{13} = 2,\ h_{14} = 1.$

Assim, pela fórmula do gancho dada na Equação (2.14), os graus das representações irredutíveis de S_4 são

$$d_{(1,1,1,1)} = 1, \quad d_{(2,1,1)} = 3, \quad d_{(2,2)} = 2, \quad d_{(3,1)} = 3 \quad \text{e} \quad d_{(4)} = 1$$

e portanto,

$$\mathbb{C}S_4 \cong \mathbb{C} \oplus \mathbb{C} \oplus M_3(\mathbb{C}) \oplus M_2(\mathbb{C}) \oplus M_3(\mathbb{C}). \tag{2.15}$$

Já sabemos que ao considerar um $\mathbb{C}G$-módulo M, podemos decompô-lo em $\mathbb{C}G$-submódulos simples e, de acordo com a Equação (2.10), temos

$$M \cong V_1^{(s_1)} \oplus \cdots \oplus V_k^{(s_k)}$$

onde $\{V_1, \ldots, V_k\}$ um conjunto completo de $\mathbb{C}G$-módulos simples. Considerando χ_i o caracter irredutível de G correspondente ao $\mathbb{C}G$-módulo simples V_i, temos o seguinte resultado, cuja demonstração pode ser vista no livro de James e Liebeck (2001).

Teorema 2.3.15. *Seja $\chi(M)$ o caracter correspondente ao $\mathbb{C}G$-módulo M, com a decomposição dada acima como soma de $\mathbb{C}G$-módulos simples. Então*

$$\chi(M) = s_1\chi_1 + \cdots + s_k\chi_k. \tag{2.16}$$

Na Equação (2.16), cada s_i é denominado a multiplicidade do caracter irredutível χ_i na decomposição do caracter de M, que também é a multiplicidade do $\mathbb{C}S_n$-módulo irredutível correspondente ao caracter χ_i, na decomposição de M, de acordo com a Equação (2.10).

Particularmente, o caracter $\chi_R(S_n)$, da representação regular de S_n, se escreve como

$$\chi_R(S_n) = \sum_{\lambda \vdash n} d_\lambda \chi_\lambda.$$

Exemplo 2.3.16. Conforme a Equação (2.15), se $\chi_R(S_4)$ é o caracter da representação regular de S_4, temos

$$\chi_R(S_4) = \chi_{(1,1,1,1)} + \chi_{(4)} + 3\chi_{(2,1,1)} + 2\chi_{(2,2)} + 3\chi_{(3,1)}. \tag{2.17}$$

Terminamos esta seção fazendo uma observação importante sobre os S_n-caracteres irredutíveis. Para isto, consideremos V um FS_n-módulo e $\overline{V} = V \otimes_F \overline{F}$, onde $\overline{F}$ é o fecho algébrico de F. Inicialmente, observemos que $\overline{V}$ é um $\overline{F}S_n$-módulo e, assim, temos a seguinte informação cuja demonstração pode ser vista no livro de Curtis e Reiner (1966).

Observação 2.3.17. Se V_λ é um FS_n-módulo irredutível que aparece na decomposição do FS_n-módulo V com multiplicidade não nula m_λ, então $\overline{V}_\lambda = V_\lambda \otimes_F \overline{F}$ também aparece na decomposição de $\overline{V}$ com multiplicidade m_λ.

Exercícios V ou F da Seção 2.3: Verifique se cada sentença abaixo é verdadeira ou falsa, justificando convenientemente.

(1) Se χ é um caracter de S_4, então $\chi((1\ 2\ 3\ 4)) = \chi((1\ 3\ 4\ 2)$.

(2) Para a representação de S_3 definida na Equação (2.13),temos que o valor do caracter $\chi_{\widetilde{\psi}}((1\ 3))$ é igual a zero.

(3) É verdade que $\mathbb{C}S_5 \cong \mathbb{C} \oplus \mathbb{C} \oplus M_4(\mathbb{C}) \oplus M_5(\mathbb{C})^{(2)} \oplus M_6(\mathbb{C})$.

(4) O grupo simétrico S_8 contém exatamente 16 caracteres irredutíveis não equivalentes.

(5) O grau do caracter irredutível χ_λ de S_5 correspondente à partição $\lambda = (2, 1, 1, 1)$ é igual a 4.

(6) O grau da representação irredutível de S_6 correspondente à partição $\lambda = (3, 1, 1, 1)$ é igual ao grau da representação irredutível de S_5 correspondente à partição $\lambda = (3, 2)$.

(7) Se χ_λ é um caracter irredutível de grau 3 de S_4, então $\lambda = (2, 1, 1)$.

2.4 A decomposição da álgebra do grupo simétrico

Nesta seção, faremos uma breve descrição da decomposição de Wedderburn da álgebra de grupo FS_n, F um corpo de característica zero. Os resultados apresentados aqui serão de grande importância no desenvolvimento do Capítulo 5. As demonstrações dos teoremas desta seção podem ser encontradas no livro de Curtis e Reiner (ibid.).

Como vimos na seção anterior, cada partição $\lambda \vdash n$ está associada a um S_n-caracter irredutível χ_λ. Como os caracteres irredutíveis estão associados a FS_n-módulos simples, podemos indexar cada um desses módulos por partições de n. Como foi feito na Seção 2.3, vamos considerar V_λ a soma dos FS_n-módulos simples isomorfos e, com isso, temos que FS_n possui a seguinte decomposição de Wedderburn

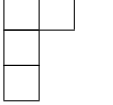
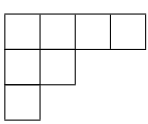
$$FS_n \cong \bigoplus_{\lambda \vdash n} V_\lambda.$$

Temos que cada V_λ é um ideal simples de FS_n. Agora, pelo Exercício 1.3.54, cada ideal simples V_λ é gerado por idempotente, isto é, existe $e_\lambda \in FS_n$ idempotente tal que $V_\lambda = FS_n e_\lambda$. Nosso objetivo é obter uma maneira de construir geradores para V_λ. Para isso, a seguir, vamos considerar a teoria desenvolvida por Young.

Para a partição $\lambda \vdash n$, definimos sua conjugada $\lambda' = (\lambda'_1, \ldots, \lambda'_r)$ como a partição de n, onde $\lambda'_1, \ldots, \lambda'_r$ são os comprimentos das colunas do diagrama D_λ.

Observemos que o diagrama de Young $D_{\lambda'}$ do tipo $\lambda' \vdash n$ é obtido de D_λ, trocando-se as linhas pelas colunas.

Exemplo 2.4.1. Se $\lambda = (3, 2, 1, 1)$, então sua partição conjugada é $\lambda' = (4, 2, 1)$. Além disso, os diagramas de Young associados a essas partições são, respectivamente:

D_λ :  e $D_{\lambda'}$: 

Fixada uma partição $\lambda = (\lambda_1, \ldots, \lambda_t)$ de n, consideramos uma tabela $T_\lambda = D_\lambda(a_{ij})$, obtida pelo preenchimento do diagrama D_λ com números naturais a_{ij} entre 1 e n, onde a_{ij} ocupa o box que está na i-ésima linha e na j-ésima coluna. Consideremos ainda $\lambda' = (\lambda'_1, \ldots, \lambda'_r)$ a partição conjugada de λ. Com essas considerações, definimos os subgrupos de S_n abaixo.

Definição 2.4.2. Sejam $\lambda = (\lambda_1, \ldots, \lambda_t) \vdash n$ e $T_\lambda = D_\lambda(a_{ij})$ uma tabela de Young do tipo λ.

1. O subgrupo estabilizador-linha de S_n da tabela T_λ é definido por

$$R_{T_\lambda} := S_{\lambda_1}(a_{11}, \cdots, a_{1\lambda_1}) \times \cdots \times S_{\lambda_t}(a_{t1}, \cdots, a_{t\lambda_t})$$

onde $S_{\lambda_i}(a_{i1}, \cdots, a_{i\lambda_i})$ denota o grupo simétrico, agindo sobre os inteiros $a_{i1}, \cdots, a_{i\lambda_i}$.

2. O subgrupo estabilizador-coluna de S_n da tabela T_λ é definido por

$$C_{T_\lambda} := S_{\lambda'_1}(a_{11}, \cdots, a_{\lambda'_1 1}) \times \cdots \times S_{\lambda'_r}(a_{1r}, \cdots, a_{\lambda'_r r})$$

onde $S_{\lambda'_j}(a_{1j}, \cdots, a_{\lambda'_j j})$ denota o grupo simétrico, agindo sobre os inteiros $a_{1j}, \cdots, a_{\lambda'_j j}$.

Exemplo 2.4.3. Para a tabela do tipo $\lambda = (2,2) \vdash 4$ ao lado, temos $R_{T_\lambda} = S_2(1,2) \times S_2(3,4)$ e $C_{T_\lambda} = S_2(2,3) \times S_2(1,4)$.

2	1
3	4

Ou seja,

$$R_{T_\lambda} = \{1, (1\ 2)\} \times \{1, (3\ 4)\} = \{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

$$\text{e } C_{T_\lambda} = \{1, (2\ 3)\} \times \{1, (1\ 4)\} = \{1, (2\ 3), (1\ 4), (1\ 4)(2\ 3)\}.$$

Finalmente, definimos o que é o idempotente essencial associado à tabela T_λ.

Definição 2.4.4. Dada uma tabela de Young T_λ, definimos o idempotente essencial associado a T_λ como o seguinte elemento de FS_n:

$$e_{T_\lambda} = \sum_{\substack{\rho \in R_{T_\lambda} \\ \sigma \in C_{T_\lambda}}} (\operatorname{sgn} \sigma) \rho\sigma.$$

A nomenclatura dada ao elemento e_{T_λ} é justificada pela proposição a seguir. A demonstração geral pode ser encontrada no trabalho de Henke e Regev (2003).

Proposição 2.4.5. *Seja T_λ uma tabela de Young. Para o idempotente essencial e_{T_λ} definido acima, existe $\gamma \in F$ tal que $e_{T_\lambda}^2 = \gamma e_{T_\lambda}$.*

É possível mostrar que $\gamma = \frac{n!}{d_\lambda} = \prod_{i,j} h_{ij}$, o produto dos ganchos da tabela T_λ, é um inteiro positivo. Além disso, temos que o elemento $\frac{e_{T_\lambda}}{\gamma}$ é um idempotente em FS_n.

Exemplo 2.4.6. Para a tabela ao lado, temos

$$\begin{aligned} e_{T_{(2,1)}} &= 1 - (2\ 3) + (1\ 2) - (1\ 2)(2\ 3) \\ &= 1 - (2\ 3) + (1\ 2) - (1\ 2\ 3). \end{aligned}$$

2	1
3	

Exercício 2.4.7. Considere e o idempotente essencial de FS_3 dado no Exemplo 2.4.6. Calcule e^2 e prove que $e^2 = 3e$.

A seguir, apresentamos um teorema que mostra a importância do idempotente essencial e_{T_λ}.

Teorema 2.4.8. *Para toda tabela de Young T_λ do tipo $\lambda \vdash n$, $FS_n e_{T_\lambda}$ é um ideal minimal à esquerda de FS_n com caracter χ_λ.*

Observe que como $e_{T_\lambda}^2 = \gamma e_{T_\lambda}$, onde γ é um inteiro, então $FS_n e_{T_\lambda} = FS_n \frac{e_{T_\lambda}}{\gamma}$.

As tabelas standard também têm um papel fundamental na decomposição de um ideal simples de FS_n. Lembrando que, para cada partição $\lambda \vdash n$, existem d_λ tabelas standard, temos o teorema a seguir.

Teorema 2.4.9. *Sejam $T_1, \ldots, T_{d_\lambda}$ todas as tabelas standard do tipo $\lambda \vdash n$. Se V_λ é o ideal simples de FS_n correspondente a partição λ, então*

$$V_\lambda = \bigoplus_{i=1}^{d_\lambda} FS_n e_{T_i}.$$

Com isso, concluímos que a álgebra de grupo FS_n pode ser escrita como a soma direta de ideais minimais à esquerda $FS_n e_{T_\lambda}$, onde T_λ é uma tabela standard do tipo $\lambda \vdash n$.

Agora, apresentaremos uma série de exemplos que serão úteis futuramente.

Exemplo 2.4.10. Para a tabela de Young do tipo $\lambda = (n-1, 1) \vdash n$ abaixo,

$$T_\lambda = \begin{array}{|c|c|c|c|} \hline 1 & 2 & \cdots & n-1 \\ \hline n \\ \cline{1-1} \end{array}$$

temos $R_{T_\lambda} = S_{n-1}$ e $C_{T_\lambda} = \{1, (1\ n)\}$. Assim,

$$e_{T_{(n-1,1)}} = \sum_{\rho \in S_{n-1}} (\rho - \rho(1\ n)).$$

Exemplo 2.4.11. Para a tabela de Young do tipo $\lambda = (n-2, 1, 1) \vdash n$ a seguir,

$$T_\lambda = \begin{array}{|c|c|c|c|} \hline 1 & 2 & \cdots & n-2 \\ \hline n-1 \\ \cline{1-1} n \\ \cline{1-1} \end{array}$$

temos $R_{T_\lambda} = S_{n-2}$ e $C_{T_\lambda} = \{1, (1\,n), (1\,n-1), (n-1\,n), (1\,n-1\,n), (1\,n\,n-1)\}$. Assim, o idempotente essencial $e_{T_{(n-1,1,1)}}$ é igual a

$$\sum_{\rho \in S_{n-2}} (\rho - \rho(1\,n) - \rho(1\,n-1) - \rho(n-1\,n) + \rho(1\,n-1\,n) + \rho(1\,n\,n-1)).$$

Exercício 2.4.12. Mostre que, para a tabela do Exemplo 2.4.3, temos

$$e_{T_\lambda} = 1 - (2\,3) - (1\,4) + (2\,3)(1\,4) + (1\,2) - (1\,2\,3) - (1\,4\,2) + (1\,4\,2\,3)$$
$$+(3\,4) - (2\,3\,4) - (1\,3\,4) + (1\,3\,2\,4) + (1\,2)(3\,4) - (1\,2\,4\,3) - (1\,3\,4\,2) + (1\,3)(2\,4).$$

Vamos denotar a partição $\lambda = (1, \ldots, 1) \vdash n$ por (1^n).

Não é difícil ver que para esta partição,

$$e_{T_{(1^n)}} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\sigma. \qquad (2.18)$$

$$T_{(1^n)} = \begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline \vdots \\ \hline n \\ \hline \end{array}$$

O idempotente essencial, $e_{T_{(1^n)}} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\sigma$, definido na Equação (2.18), será denotado daqui por diante por $e_{(1^n)}$. O próximo lema técnico mostra a importância de $e_{(1^n)}$.

Lema 2.4.13. *Seja $\Gamma = \{i_1, \ldots, i_k\} \subset \widehat{n}$. Considere o subgrupo*

$$S_k = S_k(i_1, \ldots, i_k) \subset S_n$$

que permuta os elementos de Γ e fixa os elementos de $\widehat{n} - \Gamma$. Consideremos

$$e = \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma)\sigma.$$

Então existe $\omega \in FS_n$ tal que $\omega e = e_{(1^n)}$.

Demonstração. Podemos supor, sem perda de generalidade, que $i_l = l$, para todo $l \in \{1, \ldots, k\}$, e vemos que, para os nossos propósitos, é suficiente provar o resultado para caso em que $k = n-1$, pois a situação geral segue por recursividade. Assim, temos $e = \sum_{\sigma \in S_{n-1}} \operatorname{sgn}(\sigma)\sigma$ e vamos considerar

$$\omega = 1 - (1\,n) - (2\,n) - \cdots - (n-1\,n) \in FS_n.$$

Mostraremos que esse é o elemento procurado na tese do lema. Notemos que ω é constituído pela soma de n permutações distintas de S_n, e o elemento e é formado pela soma de $(n-1)!$ permutações distintas de S_n.

O nosso primeiro objetivo será provar que o elemento ωe é constituído pela soma de $n!$ permutações distintas em S_n, cada uma delas precedida de algum coeficiente ± 1. Primeiramente, vemos que o elemento ωe possui $(n-1)!$ termos distintos que não movem n. Além disso, notemos que, se $(i\ n) \neq (j\ n)$ e α e τ são quaisquer permutações em $S_{n-1}(1,\ldots,n-1)$ entre aquelas que formam a soma do elemento e, temos que:

$$\alpha \neq \pm(i\ n)(j\ n)\tau. \tag{2.19}$$

Isto ocorre porque, do lado esquerdo da Equação (2.19), temos a permutação α que fixa n, enquanto do lado direito temos uma permutação que move n para j. Assim, $(i\ n)\alpha \neq \pm(j\ n)\tau$ e, portanto, existem $(n! - (n-1)!)$ termos distintos em ωe que movem n. Como o coeficiente que antecede cada permutação σ na soma do elemento e é justamente $\mathrm{sgn}(\sigma)$, ωe é formado pela soma das permutações de S_n, cada uma delas antecedidas pelo seu sinal. Assim, concluímos que $\omega e = e_{(1^n)}$. □

Exercícios V ou F da Seção 2.4: Verifique se cada sentença abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, F denota um corpo de característica zero.

(1) Para toda partição $\lambda \vdash n$ e toda tabela de Young T_λ, o elemento e_{T_λ} é um idempotente de FS_n.

(2) Para toda partição $\lambda \vdash n$ e toda tabela de Young T_λ, o elemento e_{T_λ} gera um ideal à esquerda minimal de FS_n.

(3) A partição conjugada de $\lambda = (4,3,2) \vdash 9$ é $\lambda' = (3,3,1,1,1)$.

(4) A partição conjugada de $\lambda = (3,3,2) \vdash 8$ é ela mesma.

(5) Pela Equação (2.18), é verdade que $e_{T_{(1^2)}} = 1 + (1\ 2)$.

(6) Pela Equação (2.18), é verdade que $e^2_{T_{(1^2)}} = 2(1\ 2)$.

3 Álgebras com identidades polinomiais

Neste capítulo, apresentamos as definições e resultados básicos sobre PI-álgebras associativas. Após definirmos a álgebra livre associativa, apresentamos o conceito de polinômios homogêneos com ênfase nos polinômios multilineares, que desempenham um papel central na PI-teoria. Em particular, os polinômios standard St_n de grau n e de Capelli Cap_n de posto n são definidos e suas principais propriedades são estudadas.

Após apresentarmos as propriedades essenciais dos polinômios, definiremos o principal objeto deste livro: as PI-álgebras. Exibimos diversos exemplos de PI-álgebras e apresentamos o processo de multilinearização. Finalizamos o capítulo apresentando uma demonstração do Teorema de Amitsur–Levitzki, que trata de identidades polinomiais em álgebras de matrizes.

Ao longo deste livro, todas as álgebras são consideradas sobre um mesmo corpo base F. Quando quisermos enfatizar sobre qual corpo uma álgebra está sendo considerada, utilizaremos o termo F-álgebra.

3.1 Polinômios

Dada uma classe de álgebras que são $\mathcal{P}$, onde $\mathcal{P}$ denota alguma propriedade (por exemplo, associativa, comutativa, de Lie, etc.), geralmente estamos interessados em um objeto universal que satisfaz a propriedade $\mathcal{P}$. A este objeto damos o nome de álgebra livre $\mathcal{P}$. O nosso objetivo é construir a álgebra livre associativa.

Seja $X = \{x_i : i \in I\}$ um conjunto. Os elementos do conjunto X serão chamados de variáveis e definimos uma palavra em X como sendo uma sequência $x_{i_1}x_{i_2}\cdots x_{i_n}$, com $n \in \mathbb{N}$ e $x_{i_j} \in X$, incluindo o 1 para ser a palavra vazia.

Considere $F\langle X\rangle$ como sendo o espaço vetorial sobre F com base formada por todas as palavras em X.

Podemos definir o produto de duas palavras por justaposição, isto é,

$$(x_{i_1}x_{i_2}\cdots x_{i_n})(x_{j_1}x_{j_2}\cdots x_{j_m}) = x_{i_1}x_{i_2}\cdots x_{i_n}x_{j_1}x_{j_2}\cdots x_{j_m}, x_{i_k}, x_{j_l} \in X.$$

O espaço $F\langle X\rangle$ munido deste produto é uma álgebra, chamada de álgebra livre associativa, livremente gerada por X sobre o corpo F. Um elemento f de $F\langle X\rangle$ é chamado de polinômio. Escrevendo $f = \sum \alpha_h h$, onde $\alpha_h \in F$ e h é uma palavra em X, chamamos α_h de coeficiente de h. Se $\alpha_h \neq 0$, então $\alpha_h h$ é dito um monômio de f e α_h é um coeficiente de f. Se em f aparecem somente as variáveis $x_1, \ldots, x_n$, então escrevemos $f = f(x_1, \ldots, x_n)$.

Exemplo 3.1.1. O elemento $f = f(x_1, x_2, x_3, x_4) = x_2x_1^2x_3 - 2x_4x_3x_1x_4$ é um polinômio de $F\langle X\rangle$ e seus monômios são $x_2x_1^2x_3$ e $-2x_4x_3x_1x_4$.

Note que $F\langle X\rangle$ é uma álgebra unitária. Frequentemente consideramos a álgebra livre não unitária $F^*\langle X\rangle$, a álgebra de todos os polinômios sem termo constante. O posto de $F\langle X\rangle$ é a cardinalidade do conjunto X.

Exercício 3.1.2 (Propriedade universal)**.** Sejam A uma álgebra unitária e $\varphi_0 : X \to A$ uma função. Mostre que existe um único homomorfismo $\varphi : F\langle X\rangle \to A$ que estende φ_0, i.e. $\varphi\,|_X = \varphi_0$.

Exercício 3.1.3. Mostre que o posto de $F\langle X\rangle$ é um invariante da álgebra, isto é, $F\langle X\rangle \cong F\langle Y\rangle$ se, e somente se, $|X| = |Y|$.

Exercício 3.1.4. Mostre que toda álgebra unitária A é isomorfa à um quociente da álgebra livre $F\langle X\rangle$, para algum conjunto X.

Exercício 3.1.5. De maneira análoga, construa a álgebra livre comutativa $F[X]$ e refaça os exercícios anteriores para a classe das álgebras comutativas unitárias.

A partir de agora, fixaremos um conjunto infinito enumerável $X = \{x_1, x_2, \ldots\}$ e, em alguns momentos, utilizaremos outros símbolos, por exemplo y, z, y_j, z_j, para denotar os elementos de X.

A seguir, vamos considerar alguns polinômios que serão importantes neste texto. Primeiramente, definimos o comutador de peso 2 (ou comutador duplo) como sendo o polinômio

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

Indutivamente, um comutador de peso $n \geqslant 3$ é definido como

$$[x_1, \ldots, x_n] := [[x_1, \ldots, x_{n-1}], x_n].$$

Pelo Exercício 1.4.8, valem as seguintes propriedades de comutadores:

(a) $[x_1, x_2] = -[x_2, x_1]$ (anticomutatividade);

(b) $[x_1, x_2, x_3] + [x_2, x_3, x_1] + [x_3, x_1, x_2] = 0$ (identidade de Jacobi).

De modo geral, dados $f, g \in F\langle X\rangle$, definimos

$$[f, g] := fg - gf$$

e se $f_1, \ldots, f_n \in F\langle X\rangle$, definimos

$$[f_1, \ldots, f_n] = [[f_1, \ldots, f_{n-1}], f_n].$$

Exercício 3.1.6. Mostre que para quaisquer $f, g, h \in F\langle X\rangle$,

$$[f, gh] = [f, g]h + g[f, h].$$

Definimos o produto de Jordan de duas variáveis x_1 e x_2 como sendo o polinômio

$$x_1 \circ x_2 := x_1x_2 + x_2x_1.$$

De modo geral, dados $f, g \in F\langle X\rangle$, definimos $f \circ g = fg + gf$.

O polinômio standard[1] de grau n tem um papel fundamental no estudo de PI-álgebras. Este é definido como

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

[1]Novamente, não traduziremos a palavra standard para português.

onde S_n é o grupo simétrico de grau n e $\mathrm{sgn}(\sigma)$ denota o sinal da permutação $\sigma \in S_n$, ou seja, este polinômio é formado por todos os monômios obtidos a partir das permutações das variáveis $x_1, \ldots, x_n$ cujo coeficiente é o sinal da permutação correspondente.

Em algumas situações durante o texto, vamos usar simplesmente a notação St_n para denotar o polinômio standard de grau n, omitindo as variáveis $x_1, \ldots, x_n$. Por exemplo, em alguns momentos denotaremos $St_2 = [x_1, x_2]$.

Exemplo 3.1.7. Observe que $St_3(x_1, x_3, x_2) = -St_3(x_1, x_2, x_3)$. Além disso, note também que

$$\begin{aligned} St_3(x_1, x_2, x_3) &= x_1[x_2, x_3] - x_2[x_1, x_3] + x_3[x_1, x_2] \\ &= x_1 St_2(x_2, x_3) - x_2 St_2(x_1, x_3) + x_3 St_2(x_1, x_2). \end{aligned}$$

O exemplo acima pode ser generalizado como no próximo exercício.

Exercício 3.1.8. Mostre que:

(*a*) $St_n(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = -St_n(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n)$, para quaisquer $i, j \in \{1, \ldots, n\}$, $i \neq j$.

(*b*) $St_{n+1}(x_1, \ldots, x_{n+1}) = \sum_{i=1}^{n+1} (-1)^{i+1} x_i St_n(x_1, \ldots, \hat{x}_i, \ldots, x_{n+1})$, onde o símbolo $\hat{x}_i$ denota a omissão da variável x_i.

Definição 3.1.9. Seja $m = m(x_1, \ldots, x_n) \in F\langle X \rangle$ um monômio. O grau de x_j em m, denotado por $\deg_{x_j}(m)$, é o número de ocorrências de x_j em m. O grau de m, denotado por $\deg(m)$, é o número total de todas as variáveis presentes em m, contadas as multiplicidades de cada variável.

Exemplo 3.1.10. Se $m = m(x_1, x_2, x_3) = 5x_1x_3^2x_2^3x_1x_3^5$, então $\deg_{x_1}(m) = 2$, $\deg_{x_2}(m) = 3$, $\deg_{x_3}(m) = 7$ e $\deg(m) = 12$.

Definição 3.1.11. Seja $f = f(x_1, \ldots, x_n) = \sum_{i=1}^{r} m_i$, onde para cada $i = 1, \ldots, r$, $m_i = m_i(x_1, \ldots, x_n)$ é um monômio. O grau em f da variável x_j, denotado por $\deg_{x_j}(f)$, é igual ao maior grau da variável x_j em seus monômios. O grau de f, denotado por $\deg(f)$, é o maior grau obtido entre seus monômios.

Exemplo 3.1.12. Se $f(x_1, x_2, x_3) = x_1^2x_2 + 2x_3x_1^3x_2^4 - x_3^5$, então $\deg_{x_1}(f) = 3$, $\deg_{x_2}(f) = 4$, $\deg_{x_3}(f) = 5$ e $\deg(f) = 8$.

No que segue, vamos definir os polinômios multi-homogêneos e multilineares. Vamos começar considerando $F_n = F\langle x_1, \ldots, x_n\rangle$ a álgebra livre de posto $n \geqslant 1$ sobre F. Se $F_n^{(j)}$ denota o subespaço vetorial de F_n gerado por todos os monômios de grau total j, então $F_n = \sum_{j\geqslant 1} F_n^{(j)}$. Note que esta soma é direta como espaços vetoriais.

Definição 3.1.13. Um polinômio $f^{(k)}$ pertencente a $F_n^{(k)}$, para algum $k \geqslant 1$, será dito homogêneo de grau k. Todo polinômio $f \in F\langle x_1, \ldots, x_n\rangle$ de grau m pode ser escrito como $f = f^{(1)} + \cdots + f^{(m)}$. Os polinômio não nulos $f^{(k)}$ que aparecem na decomposição de f são chamados de componentes homogêneas de f.

Exemplo 3.1.14. O polinômio $f(x_1, x_2, x_3) = x_1^4 + x_2^2x_3^2 + x_3x_1^2x_2$ é homogêneo de grau 4. No polinômio $g(x_1, x_2, x_3) = 3x_1 + 4x_2^2x_3^2 - x_2^3 - 5x_3^3$, as suas componentes homogêneas são $g^{(1)} = 3x_1$, $g^{(3)} = -x_2^3 - 5x_3^3$ e $g^{(4)} = 4x_2^2x_3^2$.

A decomposição acima ainda pode ser refinada como segue. Para cada $j \geqslant 1$, escreva $F_n^{(j)} = \sum_{i_1+\cdots+i_n=j} F_n^{(i_1,\ldots,i_n)}$, onde $F_n^{(i_1,\ldots,i_n)}$ é o subespaço gerado por todos os monômios de F_n de grau i_1 em $x_1, \ldots,$ grau i_n em x_n. Tais decomposições podem ser estendidas para $F\langle X\rangle$, com X infinito enumerável.

Com isso, se $f \in F_n^{(k)}$, então podemos sempre escrever

$$f = \sum_{i_1,\ldots,i_n\geqslant 0} f^{(i_1,\ldots,i_n)}$$

onde $f^{(i_1,\ldots,i_n)} \in F_n^{(i_1,\ldots,i_n)}$ é a soma de todos os monômios em f em que x_1 aparece com grau i_1, x_2 aparece com grau $i_2, \ldots,$ e x_n aparece com grau i_n, e $i_1 + \cdots + i_n = k$. Isto sugere a seguinte definição.

Definição 3.1.15. Dizemos que um polinômio f é homogêneo na variável x_i, se x_i aparece com o mesmo grau em todos os seus monômios, e que f é multi-homogêneo quando for homogêneo em todas as suas variáveis. Ainda, os polinômios $f^{(i_1,\ldots,i_n)} \in F_n^{(i_1,\ldots,i_n)}$ que são não nulos em f são chamados componentes multi-homogêneas de f de multigrau $(i_1, \ldots, i_n)$.

Exemplo 3.1.16. O polinômio $f(x_1, x_2, x_3, x_4) = x_1x_2^2x_3x_4^2x_2 + x_4x_2^2x_1x_3^2x_4$ é homogêneo nas variáveis x_1 e x_4, mas não é nas variáveis x_2 e x_3 enquanto que o polinômio $g(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4x_3x_2 + x_4x_2^2x_1x_3^2$ é multi-homogêneo de multigrau $(1, 2, 2, 1)$.

Dentre os polinômios multi-homogêneos, um papel importante é desempenhado por aqueles que são multilineares, os quais definiremos a seguir.

Definição 3.1.17. Um polinômio $f = f(x_1, \ldots, x_n) \in F\langle X\rangle$ é linear na variável x_i, se x_i ocorre com grau 1 em cada monômio de f.

Exemplo 3.1.18. O polinômio $x_1x_4x_3^2x_2 - x_4x_2^2x_3x_1$ é linear nas variáveis x_1 e x_4, mas não é linear nas variáveis x_2 e x_3.

É importante ressaltar que se $f = f(x_1, \ldots, x_n)$ é um polinômio linear, por exemplo, na variável x_1, então

$$f\left(\sum_{i=1}^{m} \alpha_i g_i, x_2, \ldots, x_n\right) = \sum_{i=1}^{m} \alpha_i f(g_i, x_2, \ldots, x_n)$$

para todos $\alpha_i \in F, g_i \in F\langle X\rangle$.

Definição 3.1.19. Um polinômio em $F\langle X\rangle$ que é linear em cada uma de suas variáveis é dito multilinear.

Exemplo 3.1.20. Os seguintes polinômios são multilineares.

(a) O polinômio standard $St_n(x_1, \ldots, x_n)$ de grau n.

(b) O polinômio comutador $[x_1, \ldots, x_n]$ de peso n.

(c) O polinômio $x_1 \circ x_2$.

(d) O polinômio $x_1x_2x_3 + 2x_2x_1x_3 - 4x_1x_3x_2$.

Note que um polinômio $f = f(x_1, \ldots, x_n) \in F\langle X\rangle$ é multilinear se ele é multi-homogêneo de multigrau $(1, 1, \ldots, 1)$. Neste caso, é sempre possível escrevê-lo na forma

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

onde $\alpha_\sigma \in F$ e $\sigma \in S_n$.

Exercício 3.1.21. Utilizando o Exercício 3.1.8, mostre que

$$St_n(x_1, \ldots, x_i, \ldots, x_i, \ldots, x_n) = 0.$$

Definição 3.1.22. Seja $f(x_1, \ldots, x_n, y_1, \ldots, y_m) \in F\langle X\rangle$ um polinômio linear nas variáveis $x_1, \ldots, x_n$. Dizemos que f é alternado nas variáveis $x_1, \ldots, x_n$ se para quaisquer $1 \leqslant i < j \leqslant n$, f se torna o polinômio nulo quando substituímos x_i no lugar de x_j.

Pela linearidade de f nas variáveis $x_1, \ldots, x_n$, temos que f é alternado nas variáveis $x_1, \ldots, x_n$ se

$$f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n, y_1, \ldots, y_m) = -f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n, y_1, \ldots, y_m).$$

Se $\mathrm{char}(F) \neq 2$, então essa propriedade é equivalente à definição de polinômio alternado nas variáveis $x_1, \ldots, x_n$.

Com isso, se $\sigma \in S_n$, e escrevendo σ como um produto de transposições, temos que se f é alternado nas variáveis $x_1, \ldots, x_n$, então

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}, y_1, \ldots, y_m) = \mathrm{sgn}(\sigma) f(x_1, \ldots, x_n, y_1, \ldots, y_m)$$

para todo $\sigma \in S_n$.

Definição 3.1.23. Um polinômio que é alternado em todas as suas variáveis é chamado simplesmente de polinômio alternado.

Observe que pelo Exercício 3.1.21, temos que $St_n(x_1, \ldots, x_n)$ é um polinômio alternado.

Um outro exemplo de polinômio alternado em um conjunto de variáveis é o chamado polinômio de Capelli de posto m que definiremos a seguir.

Definição 3.1.24. O polinômio

$$\mathrm{Cap}_m(x_1, \ldots, x_m, y_1, \ldots, y_{m+1}) = \sum_{\sigma \in S_m} \mathrm{sgn}(\sigma) y_1 x_{\sigma(1)} y_2 x_{\sigma(2)} \cdots y_m x_{\sigma(m)} y_{m+1}$$

é chamado de polinômio de Capelli de posto m.

Durante o texto, muitas vezes utilizaremos a notação Cap_m para denotar o polinômio de Capelli de posto m, omitindo as variáveis correspondentes. Observamos que o polinômio de Capelli $Cap_m(x_1, \ldots, x_m, y_1, \ldots, y_{m+1})$ é linear e alternado nas variáveis $x_1, \ldots, x_m$. Especializando as variáveis $y_i's$ por 1, obtemos que

$$Cap_m(x_1, \ldots, x_m, 1, \ldots, 1) = St_m(x_1, \ldots, x_m).$$

A proposição a seguir mostra como os polinômios de Capelli relacionam-se com os polinômios alternados.

Proposição 3.1.25. *Seja* $f = f(x_1, \ldots, x_m, y_1, \ldots, y_n) \in F\langle X\rangle$ *um polinômio alternado nas variáveis* $x_1, \ldots, x_m$. *Então*

$$f = \sum_{w_1,\ldots,w_{m+1}} \alpha_{w_1,\ldots,w_{m+1}} Cap_m(x_1, \ldots, x_m, w_1, \ldots, w_{m+1})$$

onde $\alpha_{w_1,\ldots,w_{m+1}} \in F$ *e cada* $w_i, i = 1, \ldots, m+1$, *é um monônio (eventualmente vazio) nas variáveis* $y_1, \ldots, y_n$.

Demonstração. Seja $\beta w_1 x_{i_1} w_2 x_{i_2} \cdots w_m x_{i_m} w_{m+1}$ um monômio qualquer de f, onde os $w_i's$ são monômios nas variáveis $y_1, \ldots, y_n$. Como f é alternado nas variáveis $x_1, \ldots, x_m$, temos que, para todo $\sigma \in S_m$, o monômio

$$w_1 x_{\sigma(i_1)} w_2 x_{\sigma(i_2)} \cdots w_m x_{\sigma(i_m)} w_{m+1}$$

é um monômio de f com coeficiente $\mathrm{sgn}(\sigma)\beta$. Portanto, o polinômio

$$Cap_m(x_1, \ldots, x_m, w_1, \ldots, w_{m+1})$$

é um somando de f com coeficiente $\pm\beta$ e isto conclui a demonstração. □

Como consequência direta da proposição anterior, temos o seguinte corolário.

Corolário 3.1.26. *Se* $f(x_1, \ldots, x_n)$ *é um polinômio multilinear e alternado de grau n, então* $f(x_1, \ldots, x_n) = \alpha St_n(x_1, \ldots, x_n)$, *para algum* $\alpha \in F$.

Definição 3.1.27. Seja $f(x_1, \ldots, x_n, y_1, \ldots, y_m) \in F\langle X\rangle$ um polinômio linear nas variáveis $x_1, \ldots, x_n$. Definimos o operador de alternância $\mathcal{A}_{x_1,\ldots,x_n}$ das variáveis $x_1, \ldots, x_n$ como

$$\mathcal{A}_{x_1,\ldots,x_n} f = \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}, y_1, \ldots, y_m).$$

Exemplo 3.1.28. Observe que

(a) $\mathcal{A}_{x_1,x_2} x_1 x_2 = \sum_{\sigma\in S_2} \mathrm{sgn}(\sigma) x_{\sigma(1)} x_{\sigma(2)} = St_2(x_1, x_2)$.

(b) $\mathcal{A}_{x_1,x_2} y_1 x_1 y_2 x_2 y_3 = \sum_{\sigma\in S_2} \mathrm{sgn}(\sigma) y_1 x_{\sigma(1)} y_2 x_{\sigma(2)} y_3 =$
$= Cap_2(x_1, x_2, y_1, y_2, y_3)$.

(c) $\mathcal{A}_{x_1,x_2,x_3,x_4}[x_1,x_2][x_3,x_4] = 4St_4(x_1,x_2,x_3,x_4)$.

Generalizamos o exemplo acima no próximo exercício.

Exercício 3.1.29. Verifique que:

(a) $\mathcal{A}_{x_1,\ldots,x_n} x_1 \cdots x_n = St_n(x_1,\ldots,x_n)$.

(b) $\mathcal{A}_{x_1,\ldots,x_n} y_1 x_1 y_2 \cdots y_n x_n y_{n+1} = Cap_n(x_1,\ldots,x_n,y_1,\ldots,y_{n+1})$.

(c) $\mathcal{A}_{x_1,\ldots,x_{2n}}[x_1,x_2]\cdots[x_{2n-1},x_{2n}] = 2^n St_{2n}(x_1,\ldots,x_{2n})$. (Dica: utilize o Corolário 3.1.26.)

Definição 3.1.30. Seja $f = f(x_1,\ldots,x_n,y_1,\ldots,y_m) \in F\langle X\rangle$ um polinômio linear nas variáveis $x_1,\ldots,x_n$. Dizemos que f é simétrico nas variáveis $x_1,\ldots,x_n$ se, para $\sigma \in S_n$, $f(x_{\sigma(1)},\ldots,x_{\sigma(n)},y_1,\ldots,y_m) = f(x_1,\ldots,x_n,y_1,\ldots,y_m)$. Um polinômio que é simétrico em todas as suas variáveis é chamado simplesmente de polinômio simétrico.

Exemplo 3.1.31. O polinômio $f(x_1,x_2) = x_1 \circ x_2 = x_1x_2 + x_2x_1$ é um polinômio simétrico. Em geral, o polinômio $f(x_1,\ldots,x_n) = \sum_{\sigma\in S_n} x_{\sigma(1)}\cdots x_{\sigma(n)}$ é um polinômio simétrico.

Exercício 3.1.32. Mostre que se $\mathrm{char}(F) \neq 2$ e $f = f(x_1,\ldots,x_n,y_1,\ldots,y_m) \in F\langle X\rangle$ é um polinômio linear nas variáveis $x_1,\ldots,x_n$ que é simultaneamente alternado e simétrico nas variáveis $x_1,\ldots,x_n$, então f é o polinômio nulo.

Finalizamos essa seção com um importante resultado que será utilizado no decorrer deste livro. Pela definição da álgebra livre $F\langle X\rangle$, temos que as palavras em X formam uma base de $F\langle X\rangle$ sobre F. O próximo resultado, conhecido como Teorema de Poincaré–Birkhoff–Witt, nos fornece uma base mais funcional de $F\langle X\rangle$. Uma demonstração deste teorema pode ser encontrada em Drensky (2000).

Teorema 3.1.33 (Poincaré–Birkhoff–Witt)**.** *Considere o conjunto ordenado B formado pelos seguintes elementos de $F\langle X\rangle$*

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

Então a álgebra livre $F\langle X\rangle$ possui uma base sobre F formada pelos elementos

$$x_{n_1}\cdots x_{n_p} c_{m_1}\cdots c_{m_k}$$

onde $n_1 \leqslant n_2 \leqslant \cdots \leqslant n_p$, $p \geqslant 0$, $c_{m_1}, \ldots, c_{m_k}$ *são comutadores de pesos arbitrários e* $c_{m_1} \leqslant c_{m_2} \leqslant \cdots \leqslant c_{m_k}$ *na ordem induzida de* B. *De maneira equivalente,* $F\langle X\rangle$ *possui uma base sobre* F *formada pelos elementos*

$$x_1^{\alpha_1} \cdots x_m^{\alpha_m} [x_{i_1}, x_{i_2}]^{\beta_1} \cdots [x_{j_1}, x_{j_2}, \ldots, x_{j_p}]^{\beta_k}$$

onde $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_k \geqslant 0$ *e* $[x_{i_1}, x_{i_2}] < \cdots < [x_{j_1}, x_{j_2}, \ldots, x_{j_p}]$ *na ordem induzida de* B.

A seguir, apresentamos a seguinte proposição que nos mostra uma maneira eficiente de reescrever polinômios multilineares da álgebra livre $F\langle X\rangle$.

Proposição 3.1.34. *Qualquer polinômio multilinear de grau n pode ser escrito como uma combinação linear de polinômios do tipo*

$$x_{i_1} \cdots x_{i_{s_1}} \underbrace{[x_{j_1}, \ldots, x_{j_{s_2}}]}_{c_1} \cdots \underbrace{[x_{l_1}, \ldots, x_{l_{s_m}}]}_{c_r}, \tag{3.1}$$

onde $i_1 < \cdots < i_{s_1}$, *os polinômios* $c_1, \ldots, c_r$ *são comutadores de pesos arbitrários (eventualmente vazios) nas demais variáveis distintas de* $x_{i_1}, \ldots, x_{i_{s_1}}$, *e* $\sum_{i=1}^{m} s_i = n$.

Exemplo 3.1.35. Observe que o polinômio $f = x_1x_3x_2x_4[x_6, x_5]$ não está escrito como indicado em Equação (3.1), pois as variáveis fora do comutador não estão ordenadas. Vamos reescrevê-lo, usando inicialmente que $x_3x_2 = [x_3, x_2] + x_2x_3$ e assim temos

$$f = x_1[x_3, x_2]x_4[x_6, x_5] + x_1x_2x_3x_4[x_6, x_5].$$

Note que o segundo polinômio acima já é um termo da combinação linear desejada. Agora, vamos organizar o primeiro polinômio usando novamente a definição de comutador, ou seja, vamos usar que $[x_3, x_2]x_4 = [x_3, x_2, x_4] + x_4[x_3, x_2]$ e portanto, temos

$$f = x_1[x_3, x_2, x_4][x_6, x_5] + x_1x_4[x_3, x_2][x_6, x_5] + x_1x_2x_3x_4[x_6, x_5]$$

como queríamos.

Exercícios V ou F da Seção 3.1: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente.

(1) Usando propriedades dos comutadores, temos que $[x_1^3, x_2] = x_1^2 \circ [x_1, x_2] + x_1[x_1, x_2]x_1$.

(2) $St_3(x_1, x_2, x_3) = St_2(x_1x_2, x_3) - St_2(x_2x_1, x_3) + St_2(x_3x_1, x_2)$.

(3) As componentes homogêneas do polinômio $f(x_1, x_2, x_3) = 4x_1x_2 + 2x_2^2x_3^2 + x_2^3 + x_3^3$ são $f^{(1)} = 4x_1x_2$, $f^{(2)} = 2x_2^2x_3^2$ e $f^{(3)} = x_2^3 + x_3^3$.

(4) O polinômio $x_1x_2 \circ x_3 + 2[x_2, x_1x_3] - 4x_1x_3x_2$ é multilinear.

(5) Se $f(x_1, x_2, x_3, x_4)$ é um polinômio alternado, então $f(x_3, x_1, x_4, x_2) = -f(x_1, x_2, x_3, x_4)$.

(6) O polinômio $x_1x_3x_2x_4 + x_2x_3x_1x_4$ é simétrico nas variáveis x_1 e x_2 e também é simétrico nas variáveis x_3 e x_4.

(7) O polinômio $x_2x_1x_4x_3 - x_2x_4x_1x_3 - x_3x_1x_4x_2 + x_3x_4x_1x_2$ é alternado e simétrico nas variáveis x_2 e x_3.

(8) O polinômio $\sum_{\sigma \in S_5} \operatorname{sgn}(\sigma) y_1 x_{\sigma(1)} y_2 x_{\sigma(2)} y_3 x_{\sigma(3)} y_4 x_{\sigma(4)} y_5$ é o polinômio de Capelli de posto 5.

3.2 PI-álgebras

Nesta seção vamos definir o objeto de estudo deste livro: as álgebras com identidades polinomiais. Para entender esse conceito, dada uma álgebra A e elementos $a_1, \ldots, a_n \in A$, para $f(x_1, \ldots, x_n) \in F\langle X \rangle$, denotaremos por $f(a_1, \ldots, a_n)$ o elemento de A obtido substituindo-se x_i por a_i, $i = 1, \ldots, n$, no polinômio f.

Definição 3.2.1. Sejam A uma álgebra e $f = f(x_1, \ldots, x_n) \in F\langle X \rangle$. Dizemos que f é uma identidade polinomial de A se

$$f(a_1, \ldots, a_n) = 0, \text{ para todos } a_1, \ldots, a_n \in A.$$

Neste caso, escrevemos simplesmente $f \equiv 0$ em A e dizemos que f é uma identidade de A ou que A satisfaz $f \equiv 0$.

É claro que o polinômio nulo é uma identidade polinomial para qualquer álgebra A. Por isso, temos a seguinte definição.

Definição 3.2.2. Dizemos que uma álgebra A é uma PI-álgebra[2] se A satisfaz uma identidade polinomial não nula.

Note que $f \in F\langle X\rangle$ é uma identidade polinomial para uma álgebra A se, e somente se, f pertence ao núcleo de todos os homomorfismos $F\langle X\rangle \to A$.

Observe que o termo constante de uma identidade polinomial f de uma álgebra A é nulo, já que $f(0,\ldots,0) = 0$. Logo, uma identidade polinomial de uma álgebra A pertence a $F^*\langle X\rangle$.

Vejamos alguns exemplos de PI-álgebras.

Exemplo 3.2.3. Toda álgebra comutativa é uma PI-álgebra, pois satisfaz o polinômio $[x_1, x_2] \equiv 0$.

Exemplo 3.2.4. Toda álgebra nilpotente, de índice de nilpotência n, é uma PI-álgebra, pois satisfaz o polinômio $x_1 \cdots x_n \equiv 0$.

Exemplo 3.2.5. Se A é uma álgebra nil de expoente limitado, então A é uma PI-álgebra. De fato, existe $n > 1$ tal que $a^n = 0$, para todo $a \in A$. Logo, A satisfaz a identidade $x^n \equiv 0$.

Exemplo 3.2.6. A álgebra UT_2, das matrizes triangulares superiores 2×2 sobre um corpo F, é uma PI-álgebra. De fato, ao considerar $a, b \in UT_2$, um simples cálculo mostra que existe $\alpha \in F$ tal que $[a, b] = \alpha e_{12}$. Com isso, para quaisquer $a, b, c, d \in UT_2$, $[a, b][c, d] = 0$ e portanto $[x_1, x_2][x_3, x_4] \equiv 0$ é uma identidade polinomial de UT_2.

O próximo exercício é uma generalização do exemplo anterior.

Exercício 3.2.7. Mostre que UT_n, a álgebra das matrizes triangulares superiores $n \times n$ sobre um corpo F, satisfaz o polinômio

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

Exemplo 3.2.8. O corpo $\mathbb{Z}/p\mathbb{Z}$, p primo, obviamente satisfaz $[x_1, x_2] \equiv 0$. Pelo Teorema de Fermat, $\mathbb{Z}/p\mathbb{Z}$ também satisfaz a identidade $x_1^p - x_1 \equiv 0$.

Com os exemplos apresentados até aqui vemos que a classe das PI-álgebras é grande. O próximo resultado nos ajudará a exibir mais exemplos de PI-álgebras e nos mostra uma particular vantagem de trabalhar com polinômios multilineares.

[2] PI, do inglês, *polynomial identity*.

Proposição 3.2.9. *Seja A uma álgebra que é gerada, como espaço vetorial, por um conjunto B sobre F. Se $f = f(x_1, \ldots, x_n)$ é um polinômio multilinear que se anula sob qualquer substituição de elementos em B, então f é uma identidade polinomial de A.*

Demonstração. Seja $\{b_i\}_{i \in \mathcal{I}}$ um conjunto gerador de A sobre F e consideremos $a_1, \ldots, a_n$ elementos quaisquer em A. Vamos mostrar que $f(a_1, \ldots, a_n) = 0$. Por hipótese, podemos escrever

$$a_1 = \sum \alpha_{1i} b_i, \ldots, a_n = \sum \alpha_{ni} b_i$$

onde os $b_i's$ são elementos de B e $\alpha_{ji} \in F$. Então, como f é linear em cada uma de suas variáveis, temos que

$$f(a_1, \ldots, a_n) = f\left(\sum \alpha_{1i} b_i, \ldots, \sum \alpha_{ni} b_i\right) = \sum \alpha_{1i_1} \ldots \alpha_{ni_n} f(b_{i_1}, \ldots, b_{i_n}).$$

Como, por hipótese, f se anula quando é avaliado em elementos de B, concluímos que $f \equiv 0$ em A, como queríamos. □

O resultado anterior nos diz que sempre que quisermos averiguar se um polinômio multilinear f é uma identidade polinomial de uma álgebra A, então basta avaliarmos f em uma base de A.

Exercício 3.2.10. Seja $f(x_1, \ldots, x_n, y_1, \ldots, y_m)$ um polinômio multilinear e alternado nas variáveis $x_1, \ldots, x_n$. Se $a_1, \ldots, a_n \in A$ são linearmente dependentes sobre F, então $f(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0$, para quaisquer $b_1, \ldots, b_m \in A$.

Como, para todo $n \geqslant 2$, o polinômio St_n é multilinear e alternado, temos, como consequência da Proposição 3.2.9 e do exercício anterior, o seguinte corolário.

Corolário 3.2.11. *Toda álgebra de dimensão n satisfaz o polinômio $St_{n+1} \equiv 0$.*

Assim, toda álgebra de dimensão finita é uma PI-álgebra.

Exercício 3.2.12. Dê um exemplo de uma álgebra de dimensão infinita que satisfaz St_n, para algum $n \geqslant 1$.

Mesmo para álgebras não unitárias, fazemos a seguinte definição.

Definição 3.2.13. Dizemos que uma álgebra A satisfaz o polinômio de Capelli de posto m se A satisfaz todos os polinômios da forma

$$Cap_m(x_1, \ldots, x_m, y_1, \ldots, y_{m+1})$$

eventualmente substituindo-se as variáveis y por 1. Observe que existem 2^{m+1} polinômios obtidos através da substituição das variáveis y por 1.

Segue também da Proposição 3.2.9 o seguinte corolário.

Corolário 3.2.14. *Se A é uma álgebra de dimensão n, então A satisfaz $Cap_{n+1} \equiv 0$.*

O nosso próximo objetivo é exibir identidades polinomiais para a álgebra de matrizes $M_2(F)$. Para isso, utilizaremos o seguinte fato que é deixado como exercício.

Exercício 3.2.15. Mostre que

$$St_4(x_1, x_2, x_3, x_4) = [x_1, x_2] \circ [x_3, x_4] + [x_1, x_3] \circ [x_4, x_2] + [x_1, x_4] \circ [x_2, x_3].$$

Exemplo 3.2.16. Vamos determinar duas importantes identidades da álgebra de matrizes $M_2(F)$. Como $\dim_F(M_2(F)) = 4$, temos, pelo Corolário 3.2.11, que $St_5 \equiv 0$ em $M_2(F)$. Vamos mostrar que

$$St_4(x_1, x_2, x_3, x_4) \equiv 0 \text{ em } M_2(F).$$

Pela Proposição 3.2.9, basta mostrarmos que St_4 se anula quando é avaliado em elementos de uma base de $M_2(F)$.

Seja $\{e_{11} + e_{22}, e_{11}, e_{12}, e_{21}\}$ uma base $M_2(F)$ sobre F. Ao avaliarmos St_4 nos elementos desta base, pelo Exercício 3.2.15, temos que $e_{11} + e_{22}$ aparece somente dentro de comutadores de peso 2. Portanto $St_4 \equiv 0$ em $M_2(F)$. Também, temos que St_3 não é uma identidade polinomial de $M_2(F)$. De fato, temos que $St_3(e_{11} + e_{22}, e_{11}, e_{12}) = e_{12} \neq 0$.

Agora, vamos exibir outra identidade polinomial de $M_2(F)$. Observamos que se $a, b \in M_2(F)$, ao calcular o comutador $[a, b] \in M_2(F)$ vemos que $[a, b]^2$ é uma matriz múltiplo escalar da matriz identidade e, portanto, comuta com todo elemento de $M_2(F)$. Assim,

$$[[x_1, x_2]^2, x_3] \equiv 0 \text{ em } M_2(F).$$

Como vimos no Corolário 3.2.11, toda álgebra de dimensão finita é uma PI-álgebra. A seguir, exibiremos um exemplo de PI-álgebra de dimensão infinita.

Exemplo 3.2.17. Na álgebra $F\langle X\rangle$, considere $I = \langle x_i x_j + x_j x_i : i, j \geqslant 1\rangle$. A álgebra $\mathcal{G} = F\langle X\rangle/I$ é chamada de álgebra de Grassmann (ou álgebra exterior) de dimensão infinita sobre F. Denotando por $e_i = x_i + I$, se $\mathrm{char}(F) \neq 2$, temos a seguinte apresentação para $\mathcal{G}$:

$$\mathcal{G} = \langle 1, e_1, e_2, \ldots : e_i e_j = -e_j e_i, \text{para todos } i, j \geqslant 1\rangle.$$

Como $e_i e_j = -e_j e_i$, segue que, se $\mathrm{char}(F) \neq 2$, $e_i^2 = 0$, para todo $i \geqslant 1$. Além disso, para todo $\sigma \in S_n$,

$$e_{\sigma(i_1)} \cdots e_{\sigma(i_n)} = \mathrm{sgn}(\sigma) e_{i_1} \cdots e_{i_n}.$$

Com isso, $B = \{e_{i_1} \cdots e_{i_n} : i_1 < i_2 < \cdots < i_n, n \geqslant 0\}$ gera $\mathcal{G}$ sobre F. Afirmamos que B é uma base de $\mathcal{G}$. De fato, suponha que $h = \sum_{i=1}^{n} \alpha_i g_i = 0, \alpha_i \in F, g_i \in B, i = 1, \ldots, n$, é uma relação com um número minimal de coeficientes α_i não nulos. Se um elemento e_j aparece em g_1, mas não em g_2, então $e_j g_1 = 0$ e $e_j h = \sum_{i=2}^{n} \alpha_i e_j g_i = 0$ é uma relação com um número menor de coeficientes não nulos, o que é uma contradição. Portanto, B é uma base de $\mathcal{G}$ sobre F.

A seguir, introduziremos dois subespaços importantes da álgebra de Grassmann:

$$\mathcal{G}^{(0)} = \mathrm{span}_F\{e_{i_1} \cdots e_{i_{2k}} : 1 \leqslant i_1 < \cdots < i_{2k}, k \geqslant 0\} \quad \text{e}$$

$$\mathcal{G}^{(1)} = \mathrm{span}_F\{e_{i_1} \cdots e_{i_{2k+1}} : 1 \leqslant i_1 < \cdots < i_{2k+1}, k \geqslant 0\}.$$

Pela definição, pode-se verificar que esses subespaços satisfazem as seguintes relações:

$$\mathcal{G}^{(0)}\mathcal{G}^{(0)} + \mathcal{G}^{(1)}\mathcal{G}^{(1)} \subseteq \mathcal{G}^{(0)} \quad \text{e} \quad \mathcal{G}^{(0)}\mathcal{G}^{(1)} + \mathcal{G}^{(1)}\mathcal{G}^{(0)} \subseteq \mathcal{G}^{(1)}.$$

Como consequência, a primeira relação nos diz que $\mathcal{G}^{(0)}$ é uma subálgebra de A. Desde que $\mathcal{G}^{(0)} \cap \mathcal{G}^{(1)} = \{0\}$ e todo elemento de $\mathcal{G}$ pode ser escrito como soma de elementos de $\mathcal{G}^{(0)}$ e $\mathcal{G}^{(1)}$, temos que $\mathcal{G} = \mathcal{G}^{(0)} \dotplus \mathcal{G}^{(1)}$.

Além disso, não é difícil verificar que todo elemento de $\mathcal{G}^{(0)}$ comuta com qualquer elemento de $\mathcal{G}$ e que, se w_1, w_2 são monômios em $\mathcal{G}^{(1)}$, então $w_1 w_2 =$

$-w_2w_1$. Com isso, segue que, para todo $a = a_0 + a_1, b = b_0 + b_1 \in \mathcal{G}$, com $a_0, b_0 \in \mathcal{G}^{(0)}$ e $a_1, b_1 \in \mathcal{G}^{(1)}$, temos

$$[a, b] = [a_1, b_1] + [a_0, b_0] + [a_1, b_0] + [a_0, b_1] = 2a_1b_1 \in \mathcal{G}^{(0)}.$$

Portanto, obtemos que $[x_1, x_2, x_3] \equiv 0$ em $\mathcal{G}$, ou seja, $\mathcal{G}$ é uma PI-álgebra.

Exercício 3.2.18. Mostre que a álgebra de Grassmann $\mathcal{G}$ não satisfaz St_n, para todo $n \geqslant 1$.

Nem toda álgebra é uma PI-álgebra, como veremos a seguir.

Exemplo 3.2.19. A álgebra livre $F\langle X\rangle$ não é uma PI-álgebra. De fato, seja f uma identidade polinomial de $F\langle X\rangle$. Como $x_1, \ldots, x_n \in F\langle X\rangle$, temos que $f(x_1, \ldots, x_n) = 0$ e, portanto, f é o polinômio nulo.

Exercícios V ou F da Seção 3.2: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente.

(1) A álgebra UT_2 satisfaz o polinômio $[x_1x_2, x_3][x_4, x_5x_6]$.

(2) Se A é uma álgebra de dimensão 3, então A satisfaz $St_3(x_1, x_2, x_3)$.

(3) A álgebra de Grassmann $\mathcal{G}$ satisfaz o polinômio $[x_1, x_2]^2$.

(4) Se A é uma álgebra não comutativa, então A não é PI-álgebra.

(5) Se e_1, e_2, e_3, e_4 são geradores da álgebra de Grassmann $\mathcal{G}$, então $e_4e_2e_1e_3 = -e_1e_2e_3e_4$.

(6) Se $w_1, w_2 \in \mathcal{G}^{(1)}$, então $w_1 \circ w_2 = 2w_1w_2$.

(7) Se A é uma álgebra de dimensão 6, então A satisfaz o polinômio de Capelli Cap_5 de posto 5.

3.3 T-ideais e o processo de multilinearização

Um dos interesses da PI-teoria é conhecer todas as identidades satisfeitas por uma dada F-álgebra A. Desta forma, consideraremos

$$\mathrm{Id}(A) = \{f \in F\langle X\rangle : f \equiv 0 \text{ em } A\}$$

o conjunto de todas as identidades polinomiais de uma álgebra A. É claro que uma álgebra A é uma PI-álgebra se, somente se, $\mathrm{Id}(A) \neq \{0\}$.

Por exemplo, considerando uma álgebra comutativa A, já sabemos que o comutador $[x_1, x_2] \in \mathrm{Id}(A)$. Mas, além desta identidade, podemos nos perguntar como se comportam os demais polinômios em $\mathrm{Id}(A)$.

As propriedades básicas de $\mathrm{Id}(A)$ estão listadas no próximo exercício.

Exercício 3.3.1. Mostre que:

(a) $\mathrm{Id}(A)$ é um ideal de $F\langle X\rangle$.

(b) Se $\varphi\colon F\langle X\rangle \to F\langle X\rangle$ é um endomorfismo e $f \in \mathrm{Id}(A)$, então $\varphi(f) \in \mathrm{Id}(A)$.

O Exercício 3.3.1 nos diz que $\mathrm{Id}(A)$ é um ideal invariante sob todos os endomorfismos de $F\langle X\rangle$. Vejamos alguns exemplos do uso desta propriedade.

Exemplo 3.3.2. Se os polinômios $x_3^2x_2x_1 \equiv 0$ e $[x_1, x_2^2] \equiv 0$ são identidades de uma álgebra A, então $[x_3x_4, x_1^4]x_2^6x_1^2x_3x_4 \equiv 0$ também é uma identidade de A. Para ver isso, basta aplicar o endomorfismo $x_1 \mapsto x_3x_4$, $x_2 \mapsto x_1^2$, $x_3 \mapsto x_2^3$ e utilizar o fato que $\mathrm{Id}(A)$ é um ideal de $F\langle X\rangle$.

Exercício 3.3.3. Seja A uma álgebra tal que $[x_1, x_2]x_3^2 \in \mathrm{Id}(A)$. Mostre que $[x_1x_3, x_4^2, x_5x_6^3]x_7^6 \in \mathrm{Id}(A)$.

Exemplo 3.3.4. O grupo simétrico S_n age sobre $\{x_1, \ldots, x_n\}$ permutando as variáveis:

$$\text{se } \sigma \in S_n, \text{ então } \sigma \cdot x_i = x_{\sigma(i)}.$$

Tal ação pode ser estendida a um automorfismo de $F\langle x_1, \ldots, x_n\rangle$, que continuaremos denotando por σ. Por exemplo, se $f(x_1, x_2, x_3) = x_1^2x_2 + x_3x_1x_2$ e $\sigma = (1\ 2\ 3) \in S_3$, então $\sigma \cdot f(x_1, x_2, x_3) = x_2^2x_3 + x_1x_2x_3$. Pelo Exercício 3.3.1, se $f = f(x_1, \ldots, x_n) \in \mathrm{Id}(A)$ e $\sigma \in S_n$, então $\sigma \cdot f \in \mathrm{Id}(A)$.

Motivados pela propriedade de invariância do ideal $\mathrm{Id}(A)$ em relação aos endomorfismos de $F\langle X\rangle$, apresentamos a seguinte definição mais geral.

Definição 3.3.5. Um ideal I de $F\langle X\rangle$ é um T-ideal se $\varphi(I) \subseteq I$ para todo endomorfismo φ de $F\langle X\rangle$.

Exercício 3.3.6. Prove que se I_1 e I_2 são T-ideais de $F\langle X\rangle$, então $I_1 \cap I_2$ é um T-ideal de $F\langle X\rangle$. Mais do que isto, mostre que a interseção de uma família arbitrária de T-ideais de $F\langle X\rangle$ é ainda um T-ideal de $F\langle X\rangle$.

Nosso próximo objetivo é verificar como pode ser a forma de um conjunto gerador para um T-ideal da álgebra livre $F\langle X\rangle$. Para fazer isto, dado um subconjunto S de $F\langle X\rangle$, definimos o T-ideal gerado por S, denotado por $\langle S\rangle_T$, como sendo a interseção de todos os T-ideais de $F\langle X\rangle$ que contêm S. Portanto, $\langle S\rangle_T$ é o menor T-ideal de $F\langle X\rangle$ que contém S e é dado por

$$\langle S\rangle_T = \operatorname{span}_F\{h_1 f(g_1,\ldots,g_n)h_2 : f \in S \text{ e } h_1,g_1,\ldots,g_n,h_2 \in F\langle X\rangle\}.$$

Desta forma, um T-ideal I é gerado, como T-ideal, por um conjunto $S \subset F\langle X\rangle$ se todo elemento de I pode ser escrito como uma combinação linear de elementos da forma

$$h_1 f(g_1,\ldots,g_n)h_2,$$

onde os polinômios $h_1,h_2,g_1,\ldots,g_n \in F\langle X\rangle$ e $f \in S$. Nesse caso, escrevemos $I = \langle S\rangle_T$ e ainda, escreveremos $\langle f_1,\ldots,f_m\rangle_T$ para indicar que I é gerado por um conjunto finito $S = \{f_1,\ldots,f_m\}$ como T-ideal.

Dizemos que um polinômio f é consequência dos polinômios em um subconjunto S de $F\langle X\rangle$ se $f \in \langle S\rangle_T$. Em particular, dados $f,g \in F\langle X\rangle$, dizemos que g é uma consequência de f se $g \in \langle f\rangle_T$. Nesse caso, escrevemos $f \rightsquigarrow g$ e caso contrário, escrevemos $f \not\rightsquigarrow g$. Por exemplo, é fácil ver que $[x_1,x_2] \rightsquigarrow [x_1,\ldots,x_n]$, para $n \geqslant 2$. Além disso, pelo Exercício 3.1.8, temos que $St_n(x_1,\ldots,x_n) \rightsquigarrow St_{n+1}(x_1,\ldots,x_{n+1})$, para todo $n \geqslant 2$.

Exercício 3.3.7. Mostre que $[x_2,x_1,x_1] \rightsquigarrow [x_1,x_3,[x_1,x_2]]$.

A partir do Exercício 3.3.1, temos que $\mathrm{Id}(A)$ é um T-ideal de $F\langle X\rangle$ e vamos denominá-lo de T-ideal da álgebra A. Esse abuso de linguagem é permitido a partir da próxima proposição que nos mostra que todo T-ideal de $F\langle X\rangle$ é o ideal das identidades polinomiais de alguma álgebra.

Proposição 3.3.8. *Se I é um T-ideal de $F\langle X\rangle$, então $I = \mathrm{Id}(F\langle X\rangle/I)$.*

Demonstração. Seja $A = F\langle X\rangle/I$. Vamos mostrar que $\mathrm{Id}(A) = I$.

Seja $f(x_1,\ldots,x_n) \in I$. Dados $h_1+I,\ldots,h_n+I \in A$, existe um endomorfismo ϕ de $F\langle X\rangle$ tal que $\phi(x_i) = h_i$, para todo $i = 1,\ldots,n$, e assim

$$f(h_1+I,\ldots,h_n+I) = f(h_1,\ldots,h_n)+I = \phi(f(x_1,\ldots,x_n))+I.$$

Como I é um T-ideal, temos que $\phi(f(x_1,\ldots,x_n)) \in I$. Portanto, fica claro que $f(h_1+I,\ldots,h_n+I) \in I$. Como os polinômios $h_1,\ldots,h_n$ foram tomados arbitrariamente em $F\langle X\rangle$, concluímos que $f \in \mathrm{Id}(A)$ e, portanto, $I \subset \mathrm{Id}(A)$.

Reciprocamente, seja $f = f(x_1, \ldots, x_n) \in \mathrm{Id}(A)$. Temos

$$f(x_1, \ldots, x_n) + I = f(x_1 + I, \ldots, x_n + I) = I.$$

Portanto, $f(x_1, \ldots, x_n) \in I$. Isto implica em $\mathrm{Id}(A) \subset I$, o que prova a proposição. □

Observação 3.3.9. Se I é um T-ideal próprio de $F\langle X\rangle$, então $F\langle X\rangle/I$ é uma álgebra unitária. Mas existem T-ideais que não são ideais de identidades de nenhuma álgebra unitária. Por exemplo, $I = \langle x_1 \cdots x_n\rangle_T$ não é o T-ideal de uma álgebra unitária A, pois $x_1 \cdots x_n \notin \mathrm{Id}(A)$. Para evitar mais definições e um excesso de notação, escreveremos como no enunciado da proposição anterior, ficando claro para o leitor quando estaremos trabalhando com a álgebra associativa livre com ou sem unidade.

Com isso, podemos fazer os seguintes questionamentos sobre uma dada PI-álgebra A:

- Questão 1: Existe um subconjunto finito S de $F\langle X\rangle$ tal que $\mathrm{Id}(A) = \langle S\rangle_T$?
- Questão 2: Se tal subconjunto S existe, como determiná-lo?

A Questão 1 foi primeiramente levantada por Specht (1950) e uma resposta positiva foi dada por Kemer (1988) no caso em que A é uma álgebra associativa sobre um corpo de característica zero. Nesta situação, dizemos que A possui a propriedade de Specht e um conjunto gerador encontrado é chamado de uma base de Specht para o T-ideal $\mathrm{Id}(A)$. No caso em que a característica de F é diferente de zero, existem exemplos de PI-álgebras cujo T-ideal $\mathrm{Id}(A)$ não é finitamente gerado como T-ideal (veja Belov (2000)).

Em geral, a Questão 2 não é simples de ser respondida. De fato, a demonstração da existência de uma base de Specht dada por Kemer não exibe um método construtivo para obtermos tal base. Como exemplo da dificuldade de encontrá-la, destacamos a álgebra de matrizes $M_n(F)$. Conhecemos uma base de Specht de $\mathrm{Id}(M_n(F))$ somente quando $n = 2$, conforme dado pelas informações a seguir.

No caso que a característica do corpo é zero, Razmyslov (1973) determinou uma base de Specht para $\mathrm{Id}(M_2(F))$ com 9 identidades de graus 4, 5 e 6. Posteriormente, Tki (1981) mostrou que $\mathrm{Id}(M_2(F))$ possui uma base de Specht com 4 elementos e, em seguida, Drensky (1981) mostrou que as duas identidades dadas no Exemplo 3.2.16, $[[x_1, x_2]^2, x_3]$ e $St_4(x_1, x_2, x_3, x_4)$, são suficientes para formar uma base de Specht de $\mathrm{Id}(M_2(F))$, ou seja, ele provou que

$$\mathrm{Id}(M_2(F)) = \left\langle [[x_1, x_2]^2, x_3],\, St_4(x_1, x_2, x_3, x_4)\right\rangle_T .$$

No caso em F é um corpo infinito de característica diferente de 2 e 3, Colombo e Koshlukov (2004) mostraram que as duas identidades acima formam uma base de Specht de $\mathrm{Id}(M_2(F))$. No caso em que $\mathrm{char}(F) = 3$, os autores mostraram que a identidade

$$f = f_1 - \frac{1}{8}(f_2 - f_3 - f_4 - f_5)$$

onde

$$\begin{aligned} f_1 &= [x_1, x_2] \circ ([x_3, x_4] \circ [x_5, x_6]) \\ f_2 &= [x_1, [x_3, x_4], [x_5, x_6], x_2] \\ f_3 &= [x_1, [x_5, x_6], [x_3, x_4], x_2] \\ f_4 &= [x_2, [x_3, x_4], x_1, [x_5, x_6]] \\ f_5 &= [x_2, [x_5, x_6], x_1, [x_3, x_4]] \end{aligned}$$

junto com as duas identidades dadas no Exemplo 3.2.16 formam uma base de Specht para $\mathrm{Id}(M_2(F))$ neste caso.

Finalmente, no caso em que F é um corpo finito de característica diferente de 2, Malcev e Kuzmin (1978) mostraram que $[[x_1, x_2]^2, x_3]$ e $St_4(x_1, x_2, x_3, x_4)$ formam uma base de Specht de $\mathrm{Id}(M_2(F))$.

Até o momento, não é conhecido se $\mathrm{Id}(M_2(F))$ possui uma base de Specht, quando F é um corpo de característica 2.

Nosso próximo objetivo é mostrar que podemos obter identidades de uma álgebra A a partir de uma identidade mais geral. Para isso, consideramos x_i uma variável de um polinômio $f = f(x_1, \ldots, x_n)$ tal que $\deg_{x_i}(f) = m$ e escrevemos $f = \sum_{j=0}^{m} f_j$, onde cada f_j é a componente de f que tem grau j em relação à variável x_i, ou seja, f_j é a parcela de f formada pela soma de todos monômios de grau j em relação à variável x_i. Com essa notação, temos o seguinte resultado.

Teorema 3.3.10. *Seja A uma F-álgebra, onde F é um corpo infinito, e considere $f(x_1, \ldots, x_n)$ uma identidade de A tal que $\deg_{x_i}(f) = m$. Se f_j é a componente de f tal que $\deg_{x_i}(f_j) = j$, $0 \leqslant j \leqslant m$, então f_j é uma identidade de A, para todo $j = 1, \ldots, m$.*

Demonstração. Temos por hipótese que $f = \sum_{j=0}^{m} f_j$. Observemos que para qualquer $\alpha \in F$, vale

$$f(x_1, \ldots, \alpha x_i, \ldots, x_n) = \sum_{j=0}^{m} \alpha^j f_j(x_1, \ldots, x_n).$$

Além disso, como f é uma identidade de A, para quaisquer $a_1, \ldots, a_n \in A$, temos que $f(a_1, \ldots, \alpha a_i, \ldots, a_n) = 0$.

Sendo F um corpo infinito, podemos considerar $\alpha_0, \ldots, \alpha_m \in F$ escalares distintos e, a partir da igualdade acima, ao substituirmos $f(a_1, \ldots, \alpha_j a_i, \ldots, a_n)$, obtemos um sistema com $m+1$ variáveis, $\widetilde{f_0} = f_0(a_1, \ldots, a_n), \ldots, \widetilde{f_m} = f_m(a_1, \ldots, a_n)$, dado por

$$\begin{cases} \widetilde{f_0} + \alpha_0 \widetilde{f_1} + \cdots + \alpha_0^m \widetilde{f_m} = 0 \\ \widetilde{f_0} + \alpha_1 \widetilde{f_1} + \cdots + \alpha_1^m \widetilde{f_m} = 0 \\ \quad \vdots \quad \quad \vdots \quad \quad \ddots \quad \quad \vdots \\ \widetilde{f_0} + \alpha_m \widetilde{f_1} + \cdots + \alpha_m^m \widetilde{f_m} = 0. \end{cases}$$

Para avaliar se esse sistema homogêneo tem solução não trivial, temos que verificar se o determinante da matriz abaixo é nulo

$$B = \begin{pmatrix} 1 & \alpha_0 & \cdots & \alpha_0^m \\ 1 & \alpha_1 & \cdots & \alpha_1^m \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_m & \cdots & \alpha_m^m \end{pmatrix}.$$

Notemos que matriz transposta B^t de B é uma matriz de Vandermonde, portanto seu determinante é dado por $\det(B^t) = \prod_{0 \leqslant i < j \leqslant m} (\alpha_j - \alpha_i) \neq 0$. Como $\det(B) = \det(B^t)$, concluímos que $f_0, \ldots, f_m$ são identidades da álgebra A. □

Observemos que se F é um corpo finito de cardinalidade q, então $x_1^q - x_1 \equiv 0$ em F. Com isso, $x_1^q - x_1 \equiv 0$ é uma identidade de F, mas suas componentes homogêneas não são, o que mostra que o teorema acima não é válido em geral quando o corpo é finito. Por outro lado, quando F é um corpo finito de cardinalidade $|F|$ tal que $|F| > \deg(f)$, o argumento dado na demonstração pode ser usado sob estas condições e, assim, o teorema é ainda válido.

A partir do Teorema 3.3.10, segue o corolário abaixo, que pode ser provado por indução sobre o número de variáveis nas quais o polinômio é não homogêneo.

Corolário 3.3.11. *Sejam F um corpo infinito e f uma identidade de uma F-álgebra A. Então qualquer componente multi-homogênea de f é uma identidade de A.*

Nosso próximo objetivo é apresentar o processo de multilinearização que tem como função obter uma identidade multilinear de grau menor ou igual a k, a partir de uma identidade polinomial arbitrária de grau k de uma álgebra A. Antes, vamos apresentar o processo por meio de um exemplo.

Exemplo 3.3.12. Suponha que uma álgebra A satisfaz a identidade $f(x_1, x_2) = [x_1, x_2]x_1 \equiv 0$. Note que f é linear na variável x_2, mas não o é na variável x_1. Considere o polinômio $h(y_1, y_2, x_2) = f(y_1 + y_2, x_2) - f(y_1, x_2) - f(y_2, x_2)$. Como $\mathrm{Id}(A)$ é um T-ideal, $h \in \mathrm{Id}(A)$ e $h(y_1, y_2, x_2) = [y_1 + y_2, x_2](y_1 + y_2) - [y_1, x_2]y_1 - [y_2, x_2]y_2 = [y_1, x_2]y_2 + [y_2, x_2]y_1$. Renomeando as variáveis, temos que o polinômio $h(x_1, x_2, x_3) = [x_1, x_2]x_3 + [x_3, x_2]x_1$ é uma identidade multilinear de A obtida a partir da identidade f. É claro que se fizermos $x_1 = x_3$ em h, então recuperamos a identidade f. Além disso, h é um polinômio simétrico nas variáveis $\{x_1, x_3\}$.

Teorema 3.3.13 (Processo de Multilinearização)**.** *Se uma álgebra A satisfaz uma identidade polinomial de grau k, então A satisfaz uma identidade multilinear de grau menor ou igual a k.*

Demonstração. Seja $f = f(x_1, \ldots, x_n) \in \mathrm{Id}(A)$ e suponhamos que $\deg_{x_i}(f) \leqslant 1$ para todo $i \in \{1, \ldots, n\}$. Veremos que é possível obter uma identidade multilinear de A a partir de f. Inicialmente, escreva f como

$$f = \sum_{j=1}^{m} \alpha_j u_j,\ \alpha_j \in F$$

onde os polinômios u_j são as componentes homogêneas de f de grau j.

Caso tenhamos, para todo $i \in \{1, \ldots, n\}$ e para todo $j \in \{1, \ldots, m\}$, $\deg_{x_i}(u_j) = 1$, não há nada para se fazer, pois nesse caso f já é multilinear. Suponhamos que f não seja multilinear.

Assim, existem $i \in \{1, \ldots, n\}$ e $j, l \in \{1, \ldots, m\}$ tais que $\deg_{x_i}(u_j) = 0$ e $\deg_{x_i}(u_l) = 1$. Seja x_{i_1} uma variável de f com esta propriedade, e consideremos o seguinte endomorfismo de $F\langle X\rangle$

$$\begin{array}{rccl} \phi_{i_1}: & F\langle X\rangle & \to & F\langle X\rangle \\ & x_{i_1} & \mapsto & 0 \\ & x_j & \mapsto & x_j,\ j \neq i_1. \end{array}$$

Com isso, $\phi_{i_1}(f)$ é uma identidade de A, onde a variável x_{i_1} não aparece. Caso $\phi_{i_1}(f)$ seja multilinear, concluímos a demonstração nesse caso. Caso contrário,

existe uma variável x_{i_2}, com a propriedade que x_{i_1} tinha em f, e repetimos o procedimento anterior.

Como o número de variáveis de f é finito, esse algoritmo terminará em alguma etapa, e obteremos uma identidade multilinear a partir da identidade f.

Agora, consideremos o caso em que $\deg_{x_i}(f) = d > 1$, para algum $i \in \{1, \ldots, n\}$. Veremos que é possível obter uma identidade h de A onde

$$\deg_{y_i}(h(x_1, \ldots, \underbrace{y_i, y_{i+1}}_{\hat{x}_i}, \ldots, x_n)) = \\ = \deg_{y_{i+1}}(h(x_1, \ldots, \underbrace{y_i, y_{i+1}}_{\hat{x}_i}, \ldots, x_n)) = d - 1,$$

onde acima estamos indicando que a variável x_i é substituída por novas variáveis distintas y_i e y_{i+1}. Por simplicidade, vamos supor que $i = 1$.

Consideremos o seguinte polinômio

$$h(y_1, y_2, x_2, \ldots, x_n) = \\ = f(y_1 + y_2, x_2, \ldots, x_n) - f(y_1, x_2, \ldots, x_n) - f(y_2, x_2, \ldots, x_n)$$

e observe que $h \in \mathrm{Id}(A)$.

Se substituirmos y_1 e y_2 por x_1 na igualdade acima, temos

$$h(x_1, x_1, x_2, \ldots, x_n) = f(2x_1, x_2, \ldots, x_n) - 2f(x_1, \ldots, x_n).$$

Considerando f_i a componente de f de grau i na variável x_1, obtemos que

$$f(2x_1, \ldots, x_n) = \sum_{i=0}^{d} 2^i f_i.$$

Verificaremos agora que h é não nulo e, para isto, vamos supor que $h = 0$. Assim, temos

$$f(2x_1, x_2, \ldots, x_n) = \sum_{i=0}^{d} 2^i f_i = 2f(x_1, \ldots, x_n).$$

Logo,

$$f_0 = (2^2 - 2) f_2 + \cdots + (2^d - 2) f_d.$$

Sabemos que $\deg_{x_1}(f_0) = 0$, mas $\deg_{x_1}((2^2-2)f_2 + \cdots + (2^d-2)f_d) = d > 1$, o que é um absurdo. Assim, h é uma identidade não nula de A com a propriedade desejada, ou seja, $\deg_{y_i}(h) = d - 1 < \deg_{x_1}(f)$.

Utilizando um argumento indutivo, concluímos o teorema. □

Como consequência do Corolário 3.3.11, temos que qualquer T-ideal sobre um corpo infinito é consequência de polinômios multi-homogêneos. Mais do que isto, o teorema a seguir nos dá ainda mais informações sobre os geradores do T-ideal de uma álgebra A, quando ela é tomada sobre um corpo de característica zero.

Teorema 3.3.14. *Seja F um corpo de característica zero e considere um polinômio $f = f(x_1, \ldots, x_n) \in F\langle X\rangle$. Então f é uma consequência de um conjunto finito de polinômios multilineares.*

Demonstração. Consideremos o T-ideal $I = \langle f\rangle_T$. Sabemos que existe uma álgebra A tal que $\mathrm{Id}(A) = I$. Para simplificar a demonstração, podemos usar o Corolário 3.3.11 e supor que f é multi-homogêneo. Aplicamos o processo de multilinearização em f, e supondo que $\deg_{x_1}(f) = d > 1$, escrevemos o polinômio $h = h(y_1, y_2, x_2, \ldots, x_n)$ como

$$\begin{aligned} h &= f(y_1 + y_2, x_2, \ldots, x_n) - f(y_1, x_2, \ldots, x_n) - f(y_2, x_2, \ldots, x_n) \\ &= \sum_{i=0}^{d} g_i(y_1, y_2, x_2, \ldots, x_n) \end{aligned}$$

onde $\deg_{y_1}(g_i) = i$, $\deg_{y_2}(g_i) = d - i$ e $\deg_{x_t}(g_i) = \deg_{x_t}(h)$ para todo $t = 2, \ldots, n$.

Como f é uma identidade de A, h também é uma identidade de A. Além disso, $g_0, \ldots, g_d$ são as componentes multihomogêneas de h e novamente podemos usar o Corolário 3.3.11 para concluir que cada uma dessas componentes pertence a $\mathrm{Id}(A)$. Assim, $\langle g_1, \ldots, g_{d-1}\rangle_T \subset \langle f\rangle_T$. Notemos ainda que para todo i, temos

$$g_i(y_1, y_1, x_2, \ldots, x_n) = \binom{d}{i} f(y_1, x_2, \ldots, x_n).$$

Como a característica de F é zero, segue que $\binom{d}{i} \neq 0$. Portanto, $\langle f\rangle_T = \langle g_1, \ldots, g_{d-1}\rangle_T$. Para completar a demonstração, basta usar indução sobre o número de variáveis de f. □

Como consequência do teorema anterior e dos resultados de Kemer (1978), temos o seguinte corolário que será utilizado em todo o livro.

Corolário 3.3.15. *Seja A uma PI-álgebra sobre um corpo de característica zero. Então* $\mathrm{Id}(A)$ *é gerado, como T-ideal, por um conjunto finito de polinômios multilineares.*

Exercício 3.3.16. Determine a linearização completa dos seguintes polinômios:

(*a*) $[[x_1, x_2]^2, x_3]$.

(*b*) $x_1^2 x_2^3$.

(*c*) $x^n, n \geqslant 2$.

Denotamos por P_n o espaço dos polinômios multilineares de grau n nas variáveis $x_1, \ldots, x_n$. Assim,

$$P_n = \mathrm{span}_F\{x_{\sigma(1)} \cdots x_{\sigma(n)} : \sigma \in S_n\}.$$

Pelo corolário anterior, se A é uma álgebra sobre um corpo de característica zero, para estudarmos $\mathrm{Id}(A)$, basta estudarmos os espaços $P_n \cap \mathrm{Id}(A), n \geqslant 1$. Vejamos um exemplo.

Exemplo 3.3.17. Seja A uma álgebra comutativa unitária sobre um corpo de característica zero. Já sabemos que $[x_1, x_2] \equiv 0$ em A. Afirmamos que $\mathrm{Id}(A) = \langle [x_1, x_2] \rangle_T$. De fato, se $I = \langle [x_1, x_2] \rangle_T$, então $I \subseteq \mathrm{Id}(A)$. Vamos mostrar a inclusão inversa. Seja $f \in \mathrm{Id}(A)$. Para demonstrar a afirmação, basta mostrarmos que $f \equiv 0 \pmod{I}$. Pelo Corolário 3.3.15, podemos supor que f é um polinômio multilinear de grau, digamos, n. Além disso, pela Proposição 3.1.34, temos que f pode ser escrito como uma combinação linear de polinômios da forma

$$x_{i_1} \cdots x_{i_k} c_1 \cdots c_m$$

onde $i_1 < \cdots < i_k$ e cada $c_j, j = 1, \ldots, m$, é um comutador de peso arbitrário (eventualmente vazio).

Agora, como $[x_1, x_2] \equiv 0$ em A, então, para todo $k \geqslant 2$, $[x_1, \ldots, x_k] \equiv 0$ em A. Logo, módulo I, temos que

$$f = f(x_1, \ldots, x_n) = \alpha x_1 \cdots x_n$$

para algum $\alpha \in F$. Com isso, para mostrarmos que $f \in I$, basta mostrarmos que $\alpha = 0$. Como $f \in \mathrm{Id}(A)$, fazendo a avaliação $x_i = 1, i = 1, \ldots, n$, obtemos que

$$0 = f(1, \ldots, 1) = \alpha 1.$$

Portanto $\alpha = 0$ e concluímos que $\mathrm{Id}(A) = I$.

Exercício 3.3.18. Mostre que se A é uma álgebra comutativa e nilpotente de índice de nilpotência $n > 1$ sobre um corpo de característica zero, então $\mathrm{Id}(A) = \langle [x_1, x_2], x_1 \cdots x_n \rangle_T$.

Observação 3.3.19. Se A é uma álgebra nilpotente de índice de nilpotência 2, então A é comutativa, já que para quaisquer $a, b \in A, [a, b] = ab - ba = 0$. Como $x_1 x_2 \rightsquigarrow [x_1, x_2]$, no exercício anterior, temos que $\mathrm{Id}(A) = \langle x_1 x_2 \rangle_T$.

Exercícios V ou F da Seção 3.3: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente.

(1) É verdade que $[x_1, x_2, x_1] \rightsquigarrow [x_1, x_3, [x_1, x_2]]$.

(2) Quando multilinearizamos o polinômio $x_1^2 x_2$, obtemos $(x_1 \circ x_2)x_3$.

(3) Se $x_1^2 x_2 + x_1 x_2 x_3$ é identidade de uma álgebra A então $x_1^2 x_2 \in \mathrm{Id}(A)$.

(4) $[x_2, x_3]^2 x_1 x_4 - x_1 [x_2, x_3]^2 x_4 \in \mathrm{Id}(M_2(F))$.

(5) $St_5(x_1, x_2, x_3, x_4, x_5) \notin \mathrm{Id}(M_2(F))$.

(6) Se A é uma álgebra nilpotente de índice 2, então $x_1 \circ x_2 \in \mathrm{Id}(A)$.

(7) Os polinômios $[x_1, x_2, x_3]$ e $[x_1, x_2][x_3, x_4]$ são identidades da subálgebra $A = F(e_{11} + e_{22} + e_{33}) + Fe_{12} + Fe_{13} + Fe_{23}$ de UT_3.

3.4 O Teorema de Amitsur–Levitzki

Um problema importante na PI-teoria é determinar todas as identidades polinomiais de uma PI-álgebra A. Claramente, esse problema é difícil e está resolvido somente para algumas classes de álgebras. Determinar se um polinômio é uma identidade polinomial ou não de uma álgebra pode ser uma tarefa árdua e, com isso, se fez necessário desenvolver estratégias para obter identidades polinomiais em uma álgebra.

Um dos primeiros resultados provados nessa direção foi o célebre Teorema de Amitsur–Levitzki. Tal teorema é de suma importância na PI-teoria e foi um dos resultados que motivou o estudo de identidades polinomiais em uma álgebra.

Como vimos no Corolário 3.2.11, o polinômio $St_{k^2+1} \equiv 0$ é uma identidade polinomial da álgebra de matrizes $M_k(F)$. O Teorema de Amitsur–Levitzki diz que o menor grau de um polinômio standard que é identidade de $M_k(F)$ é $2k$. Além disso, se f é uma identidade polinomial de grau $2k$, então f é múltiplo escalar de St_{2k}.

Ao longo dos anos, várias demonstrações do Teorema de Amitsur–Levitzki foram apresentadas. A demonstração original dada por Amitsur e Levitzki (1950) é baseada em argumentos combinatórios. Kostant (1958) forneceu uma demonstração utilizando técnicas da cohomologia, Swan (1963) apresentou uma demonstração usando teoria de grafos e Razmyslov (1974) utilizou polinômios de traço para demonstrar o teorema.

O objetivo desta seção é fornecer uma demonstração "elementar" do teorema que utiliza ferramentas do Cálculo e Álgebra Linear baseada na demonstração de Rosset (1976).

Durante essa seção, vamos fixar F para ser um corpo de característica diferente de 2 e vamos iniciar estudando identidades em álgebras de matrizes.

Lema 3.4.1. *O polinômio de Capelli Cap_{k^2} não é uma identidade de $M_k(F)$, mas é uma identidade de qualquer subálgebra própria de $M_k(F)$.*

Demonstração. Para provar que $Cap_{k^2}(x_1, \ldots, x_{k^2}, y_1, \ldots, y_{k^2+1})$ é uma identidade de qualquer subálgebra própria B de $M_k(F)$, basta observar que temos $\dim_F(B) < k^2$ e utilizar a Proposição 3.2.9 e o fato que Cap_{k^2} é alternado em $x_1, \ldots, x_{k^2}$.

Agora, vamos fornecer uma avaliação que não anula o polinômio de Capelli $Cap_{k^2}(x_1, \ldots, x_{k^2}, y_1, \ldots, y_{k^2+1})$.

Primeiro, vamos determinar a avaliação nas variáveis x_i, escrevendo

$$\{x_1, \ldots, x_{k^2}\} = \bigcup_{i=1}^{k} X_i$$

como a união de k conjuntos com k variáveis $X_i = \{x_{ik-(k-1)}, x_{ik-(k-2)}, \ldots, x_{ik}\}$.

Nas variáveis de X_i, faça a avaliação

$$x_{ik-(k-1)} = e_{i1}, x_{ik-(k-2)} = e_{i2}, \ldots, x_{ik} = e_{ik}, \quad 1 \leqslant i \leqslant k.$$

Fixada essa avaliação, vamos determinar a avaliação nas variáveis y. Faça $y_1 = e_{11}, y_{k^2+1} = e_{k1}$ e nas outras variáveis y faça a única avaliação de elementos de $M_k(F)$ que faz o monômio $y_1x_1y_2x_2\cdots y_{k^2}x_{k^2}y_{k^2+1}$ não se anular. Como resultado dessa avaliação, temos que

$$Cap_{k^2}(e_{11},\ldots,e_{1k},\ldots,e_{k,k-1},e_{kk},e_{11},\ldots,e_{k1}) = e_{11} \neq 0.$$

Portanto, Cap_{k^2} não é uma identidade de $M_k(F)$. □

Lema 3.4.2. *$M_k(F)$ não satisfaz identidades de grau menor que $2k$.*

Demonstração. Seja $f \equiv 0$ uma identidade não nula de $M_k(F)$ de grau $d < 2k$, que podemos supor, pelo Teorema 3.3.13, que é multilinear. Como $\mathrm{Id}(M_k(F))$ é um T-ideal, multiplicando f por novas variáveis e renomeando-as, podemos assumir que $\deg(f) = 2k-1$ e

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

com $\alpha_\sigma \in F$. Além disso, como f é não nulo, existe pelo menos um α_σ tal que $\alpha_\sigma \neq 0$. Pelo Exemplo 3.3.4, $\sigma^{-1}\cdot f \in \mathrm{Id}(M_k(F))$. Com isso, podemos supor, sem perda de generalidade, que $\alpha_1 = 1$. Assim,

$$f(e_{11},e_{12},e_{22},e_{23},e_{33},\ldots,e_{k-1,k},e_{kk}) = e_{1k},$$

já que $x_1\cdots x_{2k-1}$ é o único monômio que não se anula nessa avaliação. Portanto, f não é uma identidade de $M_k(F)$. □

O resultado anterior nos diz que St_j, para todo $j \in \{1,\ldots,2k-1\}$, não é uma identidade de $M_k(F)$. Nosso objetivo agora é mostrar que $St_{2k} \equiv 0$ em $M_k(F)$. Mostrado isso, concluímos, em particular, que o grau mínimo de uma identidade standard de $M_k(F)$ é $2k$.

Além disso, o lema anterior nos permite exibir mais um exemplo de álgebra que não é uma PI-álgebra.

Exemplo 3.4.3. Seja V um espaço vetorial de dimensão infinita e considere $\mathrm{End}(V)$, a álgebra dos endomorfismos de V. Afirmamos que $\mathrm{End}(V)$ não é uma PI-álgebra. De fato, suponha que $\mathrm{End}(V)$ satisfaz uma identidade não nula f de grau k. Considere U um subespaço de V de dimensão k. Então $\mathrm{End}(U)$ é uma subálgebra de $\mathrm{End}(V)$ e, consequentemente, satisfaz $f \equiv 0$. Mas, fixada uma base de U, sabemos que $\mathrm{End}(U) \cong M_k(F)$ e assim, teríamos que $M_k(F)$ satisfaz uma identidade de grau k, o que é um absurdo pois, pelo Lema 3.4.2, $M_k(F)$ não satisfaz nenhuma identidade não nula de grau menor que $2k$.

Para demonstrar o Teorema de Amitsur–Levitzki, precisamos de vários resultados auxiliares. Começamos com seguinte lema.

Lema 3.4.4. *Se $St_{2k} \equiv 0$ em $M_k(\mathbb{Q})$, então $St_{2k} \equiv 0$ em $M_k(F)$, para qualquer corpo F.*

Demonstração. Seja $a_r = \sum_{i,j=1}^{k} \alpha_{ij}^r e_{ij} \in M_k(F)$, $r = 1, \ldots, 2k$, $\alpha_{ij}^r \in F$. Como St_{2k} é um polinômio multilinear, temos que $St_{2k}(a_1, \ldots, a_{2k})$ é uma combinação linear de $St_{2k}(e_{i_1 j_1} \ldots, e_{i_{2k} j_{2k}})$. Mas como $St_{2k}(e_{i_1 j_1} \ldots, e_{i_{2k} j_{2k}}) \in M_k(\mathbb{Z}) \subset M_k(\mathbb{Q})$ e por hipótese $St_{2k} \equiv 0$ em $M_k(\mathbb{Q})$, temos que $St_{2k} \equiv 0$ em $M_k(F)$. □

A seguir, iremos apresentar resultados sobre álgebras sobre o corpo dos racionais $\mathbb{Q}$ que serão utilizadas na demonstração do Teorema de Amitsur–Levitzki.

Consideremos $\mathbb{Q}[\xi_1, \ldots, \xi_n]$ a álgebra dos polinômios nas variáveis comutativas $\xi_1, \ldots, \xi_n$ sobre o corpo dos racionais $\mathbb{Q}$. Da mesma forma como no Exemplo 3.3.4, o grupo simétrico S_n age sobre $\{\xi_1, \ldots, \xi_n\}$ permutando as variáveis: se $\sigma \in S_n$, então $\sigma \cdot \xi_i = \xi_{\sigma(i)}$. Tal ação pode ser estendida naturalmente a um automorfismo em $\mathbb{Q}[\xi_1, \ldots, \xi_n]$, que continuaremos denotando por σ.

Um polinômio $f \in \mathbb{Q}[\xi_1, \ldots, \xi_n]$ é simétrico se $\sigma \cdot f = f$, para todo $\sigma \in S_n$.

Exemplo 3.4.5. Os polinômios $s_0 = 1$ e $s_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} \xi_{i_1} \cdots \xi_{i_k}$, $1 \leqslant k \leqslant n$, são polinômios simétricos, chamados de polinômios simétricos elementares nas variáveis $\xi_1, \ldots, \xi_n$. Se $n = 3$, então $s_1 = \xi_1 + \xi_2 + \xi_3$, $s_2 = \xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3$ e $s_3 = \xi_1\xi_2\xi_3$.

Exercício 3.4.6. Seja x uma variável. Mostre que, em $\mathbb{Q}[\xi_1, \ldots, \xi_n, x]$, temos que:

(a) $\prod_{i=1}^{n} (1 + \xi_i x) = \sum_{k=0}^{n} s_k x^k$.

(b) $\prod_{i=1}^{n} (x - \xi_i) = \sum_{k=0}^{n} (-1)^k s_k x^{n-k}$.

Exemplo 3.4.7. Os polinômios $p_k = \sum_{i=1}^{n} \xi_i^k$, $k \geqslant 1$, são polinômios simétricos nas variáveis $\xi_1, \ldots, \xi_n$. Se $n = 3$ e $k = 2$, então $p_2 = \xi_1^2 + \xi_2^2 + \xi_3^2$.

O próximo resultado, conhecido como Fórmula de Newton, relaciona os polinômios s_k e p_k.

Proposição 3.4.8. *Em* $\mathbb{Q}[\xi_1, \ldots, \xi_n]$, *para* $k = 1, \ldots, n$, *temos que*

$$ks_k = \sum_{r=1}^{k} (-1)^{r-1} p_r s_{k-r}.$$

Demonstração. Para a demonstração do resultado, vamos utilizar séries de potências. Seja x uma variável e considere $\sum_{r=1}^{\infty} (-1)^{r-1} p_r x^{r-1}$. Utilizando a definição de p_r, temos que

$$\sum_{r=1}^{\infty} (-1)^{r-1} p_r x^{r-1} = \sum_{i=1}^{n} \sum_{r=1}^{\infty} (-1)^{r-1} \xi_i^r x^{r-1}.$$

Agora, como $\sum_{r=0}^{\infty} x^r = \frac{1}{1-x}$, temos que

$$\sum_{r=1}^{\infty} (-1)^{r-1} p_r x^{r-1} = \sum_{i=1}^{n} \frac{\xi_i}{1+\xi_i x} = \sum_{i=1}^{n} \frac{d}{dx} \ln(1+\xi_i x) =$$

$$= \frac{d}{dx} \ln \left(\prod_{i=1}^{n} (1+\xi_i x) \right).$$

Pelo Exercício 3.4.6, $\prod_{i=1}^{n} (1+\xi_i x) = \sum_{k=0}^{n} s_k x^k$. Com isso,

$$\frac{d}{dx} \ln \left(\prod_{i=1}^{n} (1+\xi_i x) \right) = \frac{d}{dx} \ln \left(\sum_{k=0}^{n} s_k x^k \right) = \frac{\sum_{k=1}^{n} s_k k x^{k-1}}{\sum_{k=0}^{n} s_k x^k}.$$

Portanto,

$$\left(\sum_{r=1}^{\infty} (-1)^{r-1} p_r x^{r-1} \right) \left(\sum_{k=0}^{n} s_k x^k \right) = \sum_{k=1}^{n} s_k k x^{k-1}.$$

Comparando os coeficientes de $x^{k-1}, k = 1, \ldots, n$, obtemos o resultado. □

Proposição 3.4.9. *Sejam C uma álgebra comutativa sobre $\mathbb{Q}$ e $a \in M_k(C)$. Se $f_a(x) = x^k + \sum_{i=1}^{k} \alpha_i x^{k-i}$ é o polinômio característico de a, então, para todo $j = 1, \ldots, k$,*

$$\alpha_j = \sum_{\lambda=(\lambda_1,\ldots,\lambda_n)\vdash j} q_\lambda \operatorname{tr}(a^{\lambda_1}) \cdots \operatorname{tr}(a^{\lambda_n}),$$

para algum $q_\lambda \in \mathbb{Q}$ que não depende de a.

Demonstração. Primeiro, suponha que C é um domínio de integridade. Então $a \in M_n(F)$, onde F é o corpo de frações de C. Sejam $\varepsilon_1, \ldots, \varepsilon_k$ os autovalores de a em algum corpo de decomposição de $f_a(x)$. Pelo Exercício 3.4.6, temos que

$$f_a(x) = \prod_{i=1}^{k} (x - \varepsilon_i) = \sum_{i=0}^{k} (-1)^i s_i(\varepsilon_1, \ldots, \varepsilon_k) x^{k-i}.$$

Agora, para todo $j = 1, \ldots, k$, $\varepsilon_1^j, \ldots, \varepsilon_k^j$ são os autovalores de a^j. Assim, $\operatorname{tr}(a^j) = p_j(\varepsilon_1, \ldots, \varepsilon_k)$, para todo $j = 1, \ldots, k$, e, pela Proposição 3.4.8,

$$\begin{aligned} s_i(\varepsilon_1, \ldots, \varepsilon_k) &= \frac{1}{i} \sum_{j=1}^{i} (-1)^{j-1} p_j(\varepsilon_1, \ldots, \varepsilon_k) s_{i-j}(\varepsilon_1, \ldots, \varepsilon_k) \\ &= \frac{1}{i} \sum_{j=1}^{i} (-1)^{j-1} \operatorname{tr}(a^j) s_{i-j}(\varepsilon_1, \ldots, \varepsilon_k). \end{aligned}$$

Repetindo o processo para todos polinômios simétricos elementares presentes no somatório, temos o resultado neste caso. No caso geral, sabemos, pelo Exercício 3.1.5, que existe um epimorfismo $\varphi\colon \mathbb{Q}[X] \to C$, para algum conjunto X, e que $\mathbb{Q}[X]$ é um domínio de integridade. Esse epimorfismo induz um epimorfismo $\bar{\varphi}\colon M_k(\mathbb{Q}[X]) \to M_k(C)$ dado por $\bar{\varphi}(a_{ij}) = (\varphi(a_{ij}))$, para todo $(a_{ij}) \in M_k(\mathbb{Q}[X])$. Como $\operatorname{tr}(\bar{\varphi}(a)) = \varphi(\operatorname{tr}(a))$, para todo $a \in M_k(\mathbb{Q}[X])$, procedendo como no caso anterior, temos o resultado. □

Como consequência dessa proposição, temos o seguinte resultado.

Corolário 3.4.10. *Seja C uma álgebra comutativa sobre $\mathbb{Q}$. Se $a \in M_k(C)$ é tal que $\operatorname{tr}(a) = \operatorname{tr}(a^2) = \cdots = \operatorname{tr}(a^k) = 0$, então $a^k = 0$.*

Demonstração. Pela proposição anterior, $f_a(x) = x^k$ e pelo Teorema de Cayley–Hamilton, toda matriz é raiz do seu polinômio característico. □

Seja $\mathcal{G}$ a álgebra de Grassmann sobre $\mathbb{Q}$. Pelo Exemplo 3.2.17, podemos escrever $\mathcal{G} = \mathcal{G}^{(0)} \dotplus \mathcal{G}^{(1)}$, onde $\mathcal{G}^{(0)}$ (resp. $\mathcal{G}^{(1)}$) é o espaço vetorial gerado por todos os monômios nos elementos $e_1, e_2, \ldots$ de comprimento par (resp. ímpar). Além disso, $\mathcal{G}^{(0)}$ é uma subálgebra comutativa de $\mathcal{G}$ e, se w_1, w_2 são monômios em $\mathcal{G}^{(1)}$, então $w_1 w_2 = -w_2 w_1$.

Lema 3.4.11. *Se* $a, b \in M_k(\mathcal{G}^{(1)})$*, então* $\mathrm{tr}(ab) = -\mathrm{tr}(ba)$.

Demonstração. Escreva $a = \sum_i a_i w_i$ e $b = \sum_j b_j w_j$, onde, para todos i, j, temos $a_i, b_j \in M_k(\mathbb{Q})$ e $w_i, w_j \in \mathcal{G}^{(1)}$ são monômios de comprimento ímpar nos elementos $e_1, e_2, \ldots$. Temos que

$$\mathrm{tr}(ab) = \sum_{i,j} \mathrm{tr}(a_i b_j) w_i w_j = -\sum_{i,j} \mathrm{tr}(b_j a_i) w_j w_i = -\mathrm{tr}(ba).$$

□

Como consequência, temos o seguinte corolário.

Corolário 3.4.12. *Se* $a_1, \ldots, a_{2r} \in M_k(F)$*, então* $\mathrm{tr}(St_{2r}(a_1, \ldots, a_{2r})) = 0$.

Demonstração. Dados $a_1, \ldots, a_{2r} \in M_k(F)$, seja $a = \sum_{i=1}^{2r} a_i e_i \in M_k(\mathcal{G}^{(1)})$. Como, para todo $\sigma \in S_{2r}$, $e_{\sigma(1)} \cdots e_{\sigma(2r)} = \mathrm{sgn}(\sigma) e_1 \cdots e_{2r}$ e $e_i^2 = e_i$, para todo $i \in \{1, \ldots, 2r\}$, temos que

$$a^{2r} = \sum_{\sigma \in S_{2r}} \mathrm{sgn}(\sigma) a_{\sigma(1)} \cdots a_{\sigma(2r)} e_1 \cdots e_{2r} = St_{2r}(a_1, \ldots, a_{2r}) e_1 \cdots e_{2r}.$$

Agora, como $a, a^{2r-1} \in M_k(\mathcal{G}^{(1)})$ temos, pelo lema anterior, que $2\mathrm{tr}(a^{2r}) = 0$ e assim, $0 = \mathrm{tr}(a^{2r}) = \mathrm{tr}(St_{2r}(a_1, \ldots, a_{2r})) e_1 \cdots e_{2r}$. Portanto,

$$\mathrm{tr}(St_{2r}(a_1, \ldots, a_{2r})) = 0.$$

□

Com todos os resultados obtidos até aqui, estamos em condições de provar o teorema principal desta seção.

Teorema 3.4.13 (Amitsur–Levitzki)**.** *A álgebra $M_k(F)$ satisfaz o polinômio $St_{2k} \equiv 0$.*

Demonstração. Pelo Lema 3.4.4, basta mostrarmos que $St_{2k} \equiv 0$ em $M_k(\mathbb{Q})$. Sejam $a_1, \ldots, a_{2k} \in M_k(\mathbb{Q})$ e considere $a = \sum_{i=1}^{2k} a_i e_i \in M_k(\mathcal{G}^{(1)})$. Como no corolário anterior, temos que

$$a^{2k} = St_{2k}(a_1, \ldots, a_{2k}) e_1 \cdots e_{2k}.$$

Assim, para demonstrar o teorema, basta mostrar que $a^{2k} = 0$.

Para todo $i = 1, \ldots, k$, temos que $a, a^{2i-1} \in M_k(\mathcal{G}^{(1)})$. Mas, pelo Lema 3.4.11, aplicado aos elementos a, a^{2i-1}, temos que $\mathrm{tr}(a^{2i}) = 0$, para todo $i = 1, \ldots, k$. Como $a^2 \in M_k(\mathcal{G}^{(0)})$, $\mathrm{tr}(a^{2i}) = 0$, para todo $i = 1, \ldots, k$, e $\mathcal{G}^{(0)}$ é uma álgebra comutativa sobre $\mathbb{Q}$, pelo Corolário 3.4.10, temos que $a^{2k} = 0$. Isto conclui a demonstração. □

Assim, concluímos que o grau minimal de uma identidade polinomial para a álgebra de matrizes $M_k(F)$ é $2k$.

Agora, mostraremos que toda identidade de grau $2k$ de $M_k(F)$ é múltiplo escalar de St_{2k}.

Proposição 3.4.14. *Se f é uma identidade de $M_k(F)$ de grau $2k$, então $f = \alpha St_{2k}$, para algum $\alpha \in F$.*

Demonstração. Primeiramente, supomos que f seja multilinear e escrevemos

$$f = f(x_1, \ldots, x_{2k}) = \sum_{\sigma \in S_{2k}} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(2k)}.$$

Assim como no Lema 3.4.2, podemos supor, sem perda de generalidade, que o coeficiente de $x_1 \cdots x_{2k}$ seja $\alpha_1 = 1$. Vamos mostrar o resultado calculando os coeficientes α_σ em f e mostrando que $\alpha_\sigma = \mathrm{sgn}(\sigma)$, para todo $\sigma \in S_n$. Para isso, vamos fazer avaliações específicas em f e iniciamos verificando os coeficientes de transposições particulares.

Primeiro, consideremos a avaliação abaixo

$$f(e_{11}, e_{12}, e_{22}, e_{23}, \ldots, e_{i-1,i}, e_{ii}, e_{ii}, e_{i,i+1}, \ldots, e_{k-1,k}, e_{kk}) = (1 + \alpha_{(2i-1\ 2i)}) e_{1k}$$

cujo valor é nulo e assim, $\alpha_{(2i-1\ 2i)} = -1$, para todo $i = 1, \ldots, k$.

Agora, consideremos a seguinte avaliação:

$$f(e_{12}, e_{22}, \ldots, e_{i-1,i}, e_{ii}, e_{ii}, e_{i,i+1}, \ldots, e_{k-1,k}, e_{kk}, e_{k1}) = (1 + \alpha_{(2i-2\ 2i-1)})e_{11}$$

cujo resultado também é nulo e portanto, $\alpha_{(2i-2\ 2i-1)} = -1$, para todo $i = 2, \ldots, k$. Com isso, obtemos que para toda transposição do tipo $(i\ \ i+1)$, temos $\alpha_{(i\ i+1)} = -1 = \mathrm{sgn}(i\ \ i+1)$, onde $i = 1, \ldots, 2k-1$.

Recorde que o conjunto de transposições $\{(i\ \ i+1) : i = 1, \ldots, 2k-1\}$ gera S_{2k}. Desta forma, se para uma permutação qualquer $\tau \in S_{2k}$, mostrarmos que $\alpha_{\tau(i\ i+1)} = -\alpha_\tau$, usando um raciocínio recursivo, teremos provado que $\alpha_\tau = \mathrm{sgn}(\tau)$, para todo $\tau \in S_{2k}$.

Com isso, dado $\tau \in S_{2k}$, considere o polinômio $g_\tau = \tau \cdot f$, isto é,

$$g_\tau(x_1, \ldots, x_{2k}) = \sum_{\sigma \in S_{2k}} \alpha_\sigma x_{\tau\sigma(1)} \cdots x_{\tau\sigma(2k)} = \sum_{\pi \in S_{2k}} \alpha_{\tau^{-1}\pi} x_{\pi(1)} \cdots x_{\pi(2k)}.$$

Como $\mathrm{Id}(M_k(F))$ é um T-ideal, para todo $\tau \in S_{2k}$, g_τ é uma identidade multilinear de grau $2k$ de $M_k(F)$.

Considere $g_{\tau^{-1}}(x_1, \ldots, x_{2k}) = \sum_{\pi \in S_{2k}} \alpha_{\tau\pi} x_{\pi(1)} \cdots x_{\pi(2k)}$. Observe que o coeficiente do monômio $x_1 \cdots x_{2k}$ é igual a α_τ e no monômio $x_{\pi(1)} \cdots x_{\pi(2k)}$, obtido quando tomamos $\pi = (i\ \ i+1)$, o coeficiente é $\alpha_{\tau(i\ i+1)}$. Desta forma, a avaliação

$$g_{\tau^{-1}}(e_{11}, e_{12}, e_{22}, \ldots, e_{i-1,i}, e_{ii}, e_{ii}, e_{i,i+1}, \ldots, e_{k-1,k}, e_{kk}) = (\alpha_\tau + \alpha_{\tau(i\ i+1)})e_{1k},$$

é nula, ou seja, obtemos que $\alpha_{\tau(i\ i+1)} = -\alpha_\tau$. Como a permutação $\tau^{-1} \in S_{2k}$ foi tomada arbitrariamente, concluímos neste caso que $\alpha_\sigma = \mathrm{sgn}(\sigma)$, para todo $\sigma \in S_{2k}$.

No caso geral, seja h o polinômio multilinear obtido através de f pelo processo de multilinearização.

Note que, pelo Lema 3.4.2, $\deg(h) = 2k$. Além disso, pela forma que o polinômio h é obtido, temos que h é simétrico em pelo menos duas variáveis. Mas, pela primeira parte da demonstração, h é um múltiplo escalar de St_{2k} que, como sabemos, é um polinômio alternado. Como $\mathrm{char}(F) \neq 2$, um polinômio simultaneamente alternado e simétrico em pelo menos duas variáveis deve ser necessariamente nulo. Isso mostra que $M_k(F)$ não satisfaz identidades que não são multilineares de grau $2k$. A demonstração está completa. □

Como consequência da proposição anterior e do Teorema de Amitsur–Levitzki, temos o seguinte corolário.

Corolário 3.4.15. *A menos de uma constante, o polinômio St_{2k} é a única identidade polinomial de grau $2k$ de $M_k(F)$.*

Como sabemos, se F é um corpo de característica zero, então

$$\mathrm{Id}(M_2(F)) = \langle [[x_1, x_2]^2, x_3], St_4 \rangle_T .$$

Com isso, a identidade $[[x_1, x_2]^2, x_3]$, de grau 5, não é consequência de St_4. Logo, pelo Corolário 3.4.15, o grau mínimo de uma identidade polinomial de $M_2(F)$ que não é consequência de St_4 é 5. Um problema interessante na PI-teoria é determinar o grau mínimo de identidades polinomiais de $M_k(F)$, $k > 3$, que não são consequências de St_{2k}.

Leron (1973) mostrou que, para $k \geqslant 3$, todas as identidades de grau $2k+1$ de $M_k(F)$ são consequências de St_{2k}. Drensky e Kasparian (1983) mostraram que em $M_3(F)$ todas as identidades de grau $8 = 2 \cdot 3 + 2$ são consequências de St_6.

É possível mostrar que a álgebra $M_k(F)$ satisfaz a identidade

$$\begin{aligned} a_k(x, y_1, \ldots, y_k) &= \sum_{\sigma \in S_{k+1}} \mathrm{sgn}(\sigma) x^{\sigma(0)} y_1 x^{\sigma(1)} y_2 \cdots y_k x^{\sigma(k)} \\ &= Cap_{k+1}(1, x, x^2, \ldots, x^k, 1, y_1, \ldots, y_k, 1) \end{aligned}$$

chamada de identidade de algebricidade de posto $k+1$, onde S_{k+1} é o grupo de permutações de $\{0, 1, \ldots, k\}$. Além disso, temos que o polinômio a_k não é uma consequência de St_{2k}. Portanto, o grau mínimo de uma identidade de $M_3(F)$, que não é consequência de St_6, é 9.

Na busca por identidades polinomiais da álgebra de matrizes $M_k(F)$, os polinômios centrais têm um papel de destaque. Vamos definir este conceito a seguir, lembrando que $Z(A)$ denota o centro de uma álgebra A.

Definição 3.4.16. Dizemos que um polinômio não nulo $f = f(x_1, \ldots, x_n) \in F\langle X \rangle$ é um polinômio central para uma álgebra A se

1. $f \notin \mathrm{Id}(A)$;
2. f tem termo constante nulo, ou seja, $f \in F^*\langle X \rangle$;
3. $f(a_1, \ldots, a_n) \in Z(A)$, para todos $a_1, \ldots, a_n \in A$.

Por essa definição, podemos ver que $f \in F\langle X \rangle$ é um polinômio central para A se, e somente se, $[f, x] \in \mathrm{Id}(A)$, onde $x \in X$. Portanto, a partir de um polinômio central para a álgebra A, podemos construir uma identidade de A. Como

um exemplo, observamos que o comutador $[x_1, x_2]$ é um polinômio central para a álgebra de Grassmann $\mathcal{G}$.

Já sabemos que $[[x_1, x_2]^2, x_3] \in \mathrm{Id}(M_2(F))$ e de fato, o polinômio $[x_1, x_2]^2$ já aparece como polinômio central para $M_2(F)$ no trabalho de Wagner (1937). Esse polinômio ficou conhecido como polinômio de Wagner–Hall e, por muitos anos, foi o único polinômio central conhecido para álgebras de matrizes. No entanto, Kaplansky (1957) conjecturou a existência de polinômios centrais para $M_k(F)$, para qualquer $k \geqslant 1$, sendo essa conjectura provada independentemente por Formanek (1972) e Razmyslov (1973).

Teorema 3.4.17. *Para qualquer $k \geqslant 1$, existe um polinômio central para a álgebra $M_k(F)$.*

Como no caso de identidades polinomiais, podemos nos perguntar sobre o grau mínimo de um polinômio central para $M_k(F)$, especialmente para $\mathrm{char}(F) = 0$. O polinômio central dado por Formanek é de grau k^2, enquanto que o construído por Razmyslov tem grau maior. Porém, a partir do polinômio dado por Razmyslov, Halpin (1983) deduziu um outro polinômio central de grau k^2, indicando que k^2 seria o menor grau de um polinômio central para $M_k(F)$, onde $k \geqslant 3$. Mas, Drensky e Kasparian (1983) construíram um polinômio central de grau 8 para $M_3(F)$, mostrando que 3^2 não é o grau mínimo nesse caso.

Em seguida, Formanek (1991) conjecturou que o grau mínimo de um polinômio central para $M_k(F)$ é exatamente $\frac{1}{2}(k^2 + 3k - 2)$, para $k \geqslant 3$. Porém isso foi refutado por Drensky (1995), que construiu, para qualquer $k \geqslant 3$, um polinômio central de grau $(k-1)^2 + 4$ para $M_k(F)$ e, até o momento, esse é o menor grau de um polinômio central construído para álgebras de matrizes.

Finalizamos com uma importante observação a respeito de polinômios centrais na produção de identidades de álgebras de matrizes feita por Rowen (1980).

Proposição 3.4.18. *Se $f = f(x_1, \ldots, x_n)$ é um polinômio central para $M_k(F)$, então f é uma identidade de $M_{k-1}(F)$.*

Demonstração. Podemos imergir $M_{k-1}(F)$ em $M_k(F)$ da seguinte maneira: $(a_{ij}) \mapsto (b_{ks})$, onde $b_{ks} = a_{ks}$, para $1 \leqslant k, s \leqslant n-1$ e $b_{kn} = b_{nk} = 0$, para $1 \leqslant k \leqslant n$, ou seja, em $M_k(F)$ consideramos uma matriz com a última linha e a última coluna nulas, obtida de uma matriz de $M_{k-1}(F)$.

Sendo $f = f(x_1, \ldots, x_n)$ um polinômio central para $M_k(F)$, para quaisquer $a_1, \ldots, a_n \in M_{k-1}(F)$, temos $f(a_1, \ldots, a_n)$ está no centro de $M_k(F)$.

Portanto, essa é uma matriz múltiplo escalar da matriz identidade $k \times k$ e, ao mesmo tempo, a entrada (k, k) é nula. Portanto, $f(a_1, \ldots, a_n) = 0$ e, assim, f é uma identidade de $M_{k-1}(F)$. □

Exercícios V ou F da Seção 3.4: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente.

(1) $St_{2n+1} \in \mathrm{Id}(M_n(F))$.

(2) Cap_{n^2+1} é uma identidade de $M_n(F)$.

(3) O polinômio $St_2(x_1, x_2)x_1^4$ não é uma identidade da subálgebra $A = F(e_{11} + e_{22} + e_{33}) + Fe_{12} + Fe_{13} + Fe_{23}$ de UT_3.

(4) Se A satisfaz o polinômio $[x_1, x_2] \cdots [x_{2n-1}, x_{2n}]$, então A satisfaz St_{2n}.

(5) O grau minimal de uma identidade de $M_4(F)$ é 6.

(6) O polinômio $[x_1, x_2]^2$ é um polinômio central para $M_3(F)$.

(7) $St_2(x_1, x_2)$ é um polinômio central para UT_2.

4 Ideais de identidades e codimensões

Para descrever todas as identidades polinomiais satisfeitas por uma álgebra A, devemos encontrar um conjunto gerador de $\mathrm{Id}(A)$ como um T-ideal, conforme visto na Seção 3.3. Porém, nem sempre é simples determinar este conjunto gerador, como já comentamos anteriormente. Na tentativa de minimizar essa dificuldade, Regev (1972) introduziu a chamada sequência de codimensões de uma álgebra A, denotada por $\{c_n(A)\}_{n\geq 1}$, que, de uma certa maneira, controla o crescimento das identidades satisfeitas por A.

A sequência de codimensões, além de ser uma importante ferramenta para o estudo das identidades polinomiais satisfeitas por uma álgebra, se tornou um dos principais objetos de investigação na PI-teoria. A possibilidade de álgebras distintas possuírem o mesmo T-ideal favorece o estudo da classe das álgebras que satisfazem as identidades da álgebra A que será introduzida aqui, a chamada de variedade gerada por A e denotada por $\mathrm{var}(A)$.

Neste capítulo, vamos apresentar propriedades de T-ideais de identidades e construir geradores para T-ideais de algumas álgebras. Além disso, vamos dar as principais informações sobre a sequência de codimensões, com exemplos concretos do seu cálculo para particulares álgebras. Também daremos exemplos de álgebras geradoras de uma mesma variedade.

4.1 T-ideais e variedades

Um dos interesses da PI-teoria é conhecer todas as identidades satisfeitas por uma dada F-álgebra A. Por este motivo, consideraremos

$$\mathrm{Id}(A) = \{f \in F\langle X\rangle \ : \ f \equiv 0 \ \text{ em } \ A\}$$

como o T-ideal das identidades de A, definido na Seção 3.3.

Nessa seção, vamos inicialmente estabelecer algumas propriedades básicas de T-ideais de identidades e, em seguida, estudar álgebras que satisfazem as mesmas identidades.

Exercício 4.1.1. Mostre que se A e B são F-álgebras isomorfas então $\mathrm{Id}(A) = \mathrm{Id}(B)$.

Lema 4.1.2. *Se é A uma F-álgebra, então temos o seguinte.*

1. *Se B é subálgebra de A, então* $\mathrm{Id}(A) \subseteq \mathrm{Id}(B)$.
2. *Se I é ideal de A, então* $\mathrm{Id}(A) \subseteq \mathrm{Id}\left(A/I\right)$.
3. *Se B é uma F-álgebra isomorfa a uma subálgebra de A, então* $\mathrm{Id}(A) \subseteq \mathrm{Id}(B)$.

Demonstração. O primeiro item é óbvio, pois se $f \in \mathrm{Id}(A)$, então f se anula pela avaliação de quaisquer elementos de A e, portanto, se anula ao ser avaliado por quaisquer elementos de B. Para ver o segundo item, tomemos $f = f(x_1, \ldots, x_n) \in \mathrm{Id}(A)$ e $\overline{a}_1, \ldots, \overline{a}_n \in A/I$. Temos que

$$f(\bar{a}_1, \ldots, \bar{a}_n) = \overline{f(a_1, \ldots, a_n)} = \bar{0}.$$

Com isso, segue que $f \in \mathrm{Id}(A/I)$ e isto prova o item 2. O item 3 segue diretamente do item 1 e do Exercício 4.1.1. □

Lema 4.1.3. *Se A e B são álgebras, então* $\mathrm{Id}(A \oplus B) = \mathrm{Id}(A) \cap \mathrm{Id}(B)$.

Demonstração. Primeiramente, observe que $ab = 0$, para todo $a \in A, b \in B$, já que a soma $A \oplus B$ é direta. Logo, se $f(x_1, \ldots, x_n) \in F\langle X\rangle$, então

$$f(a_1 + b_1, \ldots, a_n + b_n) = f(a_1, \ldots, a_n) + f(b_1, \ldots, b_n)$$

para todos $a_i \in A, b_i \in B, i = 1, \ldots, n$.

Assim, se $f \in \mathrm{Id}(A \oplus B)$, então $0 = f(a_1+b_1, \ldots, a_n+b_n) = f(a_1, \ldots, a_n) + f(b_1, \ldots, b_n)$, para todos $a_i \in A, b_i \in B, i = 1, \ldots, n$. Como $A \cap B = \{0\}$, segue que $f \in \mathrm{Id}(A) \cap \mathrm{Id}(B)$. Reciprocamente, se $f \in \mathrm{Id}(A) \cap \mathrm{Id}(B)$, então $f(a_1 + b_1, \ldots, a_n + b_n) = f(a_1, \ldots, a_n) + f(b_1, \ldots, b_n) = 0$, para todos $a_i \in A, b_i \in B, i = 1, \ldots, n$. Portanto, $f \in \mathrm{Id}(A \oplus B)$. □

Durante este texto, estamos trabalhando com um corpo F com característica zero, mas não exigimos que o mesmo seja algebricamente fechado. Em algumas situações, esta será uma condição importante e, a seguir, vamos ver que quando estamos provando resultados a respeito da sequência de codimensões de uma álgebra, será possível assumir essa propriedade para o corpo.

Definição 4.1.4. Dizemos que uma identidade $f \in F\langle X\rangle$ de uma F-álgebra A é estável se f for uma identidade de $A \otimes C$, para qualquer F-álgebra comutativa C.

No próximo resultado, provaremos que, quando F é um corpo de característica zero, todas as identidades de A são estáveis.

Proposição 4.1.5. *Se A é uma F-álgebra e C é uma F-álgebra comutativa, então* $\mathrm{Id}(A) \subset \mathrm{Id}(A \otimes C)$.

Demonstração. Suponhamos que $f = f(x_1, \ldots, x_n)$ seja uma identidade de A que podemos supor multilinear, pois $\mathrm{char}(F) = 0$. Agora, devemos provar que, para quaisquer elementos $a_1 \otimes b_1, \ldots, a_n \otimes b_n \in A \otimes C$, com $a_i \in A$ e $b_i \in C$, $1 \leqslant i \leqslant n$, temos que

$$f(a_1 \otimes b_1, \ldots, a_n \otimes b_n) = 0.$$

Usando a multilinearidade de f e a comutatividade de C, temos

$$f(a_1 \otimes b_1, \ldots, a_n \otimes b_n) = f(a_1, \ldots, a_n) \otimes b_1 \cdots b_n = 0$$

pois $f(a_1, \ldots, a_n) = 0$. Assim, $f \in \mathrm{Id}(A \otimes C)$ e isto conclui a nossa prova. □

O T-ideal de uma F-álgebra A é definido como o conjunto de todos os polinômios de $F\langle X\rangle$ que são satisfeitos por A. Contudo, podem existir outras álgebras que satisfazem as mesmas identidades de A, e isto nos motiva a definir o conceito de variedade de álgebras, conforme faremos a seguir.

Inicialmente, consideremos $S \subset F\langle X\rangle$ um conjunto não vazio de polinômios e $\langle S\rangle_T$ o T-ideal gerado por este conjunto. A seguir temos a definição de variedade.

Definição 4.1.6. Definimos a variedade determinada pelo conjunto S, denotada por $\mathcal{V}(S)$, como a classe de todas as álgebras que satisfazem todas as identidades no conjunto S.

Observe que se $S = \{0\}$, então $\mathcal{V}(0)$ é a classe de todas as álgebras. Se $S = F\langle X\rangle$, então $\mathcal{V}(F\langle X\rangle)$ consiste apenas de $\{0\}$.

Exemplo 4.1.7. Se $S = \{[x_1, x_2]\}$, então $\mathcal{V}(S)$ é a classe de todas as álgebras comutativas.

Dizemos que uma variedade $\mathcal{V} = \mathcal{V}(S)$ é não trivial se $S \neq \{0\}$. A variedade é dita ser própria quando é não trivial e contém uma álgebra não nula. Por exemplo, para uma dado natural m, temos que $\mathcal{V}(x^m)$ é uma variedade própria, que é a classe de todas as álgebras nil de expoente limitado por m.

Observamos que $\mathcal{V}(S) = \mathcal{V}(\langle S\rangle_T)$ e $\langle S\rangle_T = \bigcap_{A\in\mathcal{V}} \mathrm{Id}(A)$. Vamos escrever $\mathrm{Id}(\mathcal{V}) = \langle S\rangle_T$ e desta forma, temos que cada variedade corresponde a um T-ideal de $F\langle X\rangle$. Reciprocamente, dado um T-ideal I de $F\langle X\rangle$, podemos considerar a variedade de todas as álgebras satisfazendo os polinômios em I.

Proposição 4.1.8. *A correspondência definida acima é biunívoca.*

Demonstração. Primeiramente, consideremos I_1 e I_2 dois T-ideais distintos de $F\langle X\rangle$. Podemos tomar, digamos, $f \in I_1$ tal que $f \notin I_2$. Mas note que no caso considerado, temos $A = F\langle X\rangle/I_2 \in \mathcal{V}(I_2)$ e, como A não satisfaz f, segue que $A \notin \mathcal{V}(I_1)$. Portanto, temos $\mathcal{V}(I_1) \neq \mathcal{V}(I_2)$.

Agora, consideremos $\mathcal{V}_1$ e $\mathcal{V}_2$ duas variedades distintas e digamos que $A \in \mathcal{V}_1$, mas $A \notin \mathcal{V}_2$. Isto significa que existe $f \in \mathrm{Id}(\mathcal{V}_2)$ tal que $f \notin \mathrm{Id}(A)$. Como $\mathrm{Id}(\mathcal{V}_1) \subset \mathrm{Id}(A)$, concluímos que $\mathrm{Id}(\mathcal{V}_1) \neq \mathrm{Id}(\mathcal{V}_2)$. □

Dada uma variedade $\mathcal{V}$, vimos na Proposição 3.3.8 que existe uma álgebra A tal que $\mathrm{Id}(A) = \mathrm{Id}(\mathcal{V})$. De fato, basta considerar $A = F\langle X\rangle/\mathrm{Id}(\mathcal{V})$. Porém, podem existir outras álgebras nessa mesma situação e, desta forma, para uma F-álgebra A tal que $\mathrm{Id}(A) = \mathrm{Id}(\mathcal{V})$, diremos que A gera a variedade $\mathcal{V}$ e escreveremos $\mathcal{V} = \mathrm{var}(A)$. Com isso, para uma uma álgebra B, temos

$$B \in \mathrm{var}(A) \text{ se, e somente se, } \mathrm{Id}(A) \subseteq \mathrm{Id}(B).$$

Definição 4.1.9. Se duas F-álgebras A e B são tais que $\mathrm{Id}(A) = \mathrm{Id}(B)$, então dizemos que A e B são álgebras PI-equivalentes.

É claro que se A e B são PI-equivalentes, temos $\mathrm{var}(A) = \mathrm{var}(B)$. A notação que utilizaremos nesta situação é $A \sim_{PI} B$.

Proposição 4.1.10. *Seja $\mathcal{V} = \mathrm{var}(A)$ uma variedade própria de álgebras.*

1. *Se B é uma subálgebra de A, então $B \in \mathcal{V}$.*
2. *Se I é um ideal de A, então $A/I \in \mathcal{V}$.*
3. *Se B está isomorficamente imersa em A, então $B \in \mathcal{V}$.*
4. *Se $\{A_i\}_{i\in\mathcal{I}}$ é uma família de subálgebras de A, então $\prod_{i\in\mathcal{I}} A_i \in \mathcal{V}$.*

Demonstração. Os item 1, 2 e 3 seguem diretamente do Lema 4.1.2. Para provar o item 4, dados $a^{(1)}, \ldots, a^{(n)} \in \prod_{i\in\mathcal{I}} A_i$, onde $a^{(j)} = (a_i^{(j)})_{i\in\mathcal{I}}$, $j = 1, \ldots, n$, e $f \in F\langle X\rangle$, temos que

$$f(a^{(1)}, \ldots, a^{(n)}) = (f(a_i^{(1)}, \ldots, a_i^{(n)}))_{i\in\mathcal{I}}.$$

Logo, se $f \in \mathrm{Id}(A)$, então $f(a_i^{(1)}, \ldots, a_i^{(n)}) = 0$, para todo $i \in \mathcal{I}$. Portanto, $f \in \mathrm{Id}\left(\prod_{i\in\mathcal{I}} A_i\right)$, como queríamos demonstrar. □

A partir da proposição acima, vemos que uma variedade $\mathrm{var}(A)$ é fechada ao tomarmos subálgebras, imagens homomórficas e produtos diretos e estas propriedades realmente caracterizam uma variedade como estabelecido pelo Teorema de Birkhoff, que enunciamos abaixo, cuja demonstração pode ser encontrada no livro de Drensky (2000).

Teorema 4.1.11. *Uma classe não vazia de álgebras $\mathcal{V}$ é uma variedade se, e somente se, são válidas as seguintes propriedades:*

1. *Se $A \in \mathcal{V}$ e $f : B \to A$ é um monomorfismo, então $B \in \mathcal{V}$.*
2. *Se $A \in \mathcal{V}$ e $f : A \to B$ é um epimorfismo, então $B \in \mathcal{V}$.*
3. *Se $\{A_i\}_{i\in\mathcal{I}}$ é uma família de álgebras tais que $A_i \in \mathcal{V}$, para todo $i \in \mathcal{I}$, então $\prod_{i\in\mathcal{I}} A_i \in \mathcal{V}$.*

A partir de agora, e até o final do capítulo, F denotará um corpo de característica zero e todas as álgebras serão tomadas sobre corpos de característica zero.

Na Proposição 3.1.34, estabelecemos uma forma de escrever cada polinômio multilinear em $f \in F\langle X\rangle$ e, no Exemplo 3.1.35, reescrevemos o polinômio $f = x_1x_3x_2x_4[x_6, x_5]$ como

$$f = x_1[x_3, x_2, x_4][x_6, x_5] + x_1x_4[x_3, x_2][x_6, x_5] + x_1x_2x_3x_4[x_6, x_5].$$

Para complementar esse exemplo, vamos considerar o T-ideal

$$I = \langle [x_1, x_2][x_3, x_4]\rangle_T .$$

Pelo que vimos acima, podemos escrever f, módulo I, simplesmente como $x_1x_2x_3x_4[x_6, x_5]$, pois os demais termos que compõem f estão em I, ou seja,

$$f \equiv x_1x_2x_3x_4[x_6, x_5] \pmod{I}.$$

Esta será uma estratégia que usaremos na demonstração da próxima proposição, onde determinaremos os geradores do T-ideal da subálgebra $\mathcal{G}_2$ da álgebra de Grassmann $\mathcal{G}$, que é gerada, como álgebra, por $1, e_1$ e e_2, ou seja,

$$\mathcal{G}_2 = \langle 1, e_1, e_2 : e_ie_j = -e_je_i\rangle.$$

Esta subálgebra faz parte de uma família de subálgebras de dimensão finita de $\mathcal{G}$. De fato, para cada $k \geqslant 2$, podemos considerar

$$\mathcal{G}_k = \langle 1, e_1, \ldots, e_k : e_ie_j = -e_je_i\rangle \tag{4.1}$$

uma subálgebra de $\mathcal{G}$ de dimensão 2^k, que possui uma base como espaço vetorial formada por 1 e pelos elementos $\prod_{i_1<\cdots<i_s} e_{i_1}\cdots e_{i_s}$, onde $1 \leqslant s \leqslant k$.

Proposição 4.1.12. $\mathrm{Id}(\mathcal{G}_2) = \langle [x_1, x_2, x_3], [x_1, x_2][x_3, x_4]\rangle_T$.

Demonstração. Como $\mathcal{G}_2$ é uma subálgebra de $\mathcal{G}$ e $[x_1, x_2, x_3] \in \mathrm{Id}(\mathcal{G})$, segue imediatamente que $[x_1, x_2, x_3] \in \mathrm{Id}(\mathcal{G}_2)$. Observamos também que quando avaliamos o polinômio $[x_1, x_2][x_3, x_4]$ em elementos de $\mathcal{G}_2$, se um deles for 1, obtemos zero e se todos forem diferentes de 1, obtemos um elemento que é soma de produtos com pelo menos 4 elementos $e_i's$ e, portanto, o resultado também deve ser o elemento nulo. Assim, $[x_1, x_2][x_3, x_4] \in \mathrm{Id}(\mathcal{G}_2)$.

Considerando $I = \langle [x_1, x_2, x_3], [x_1, x_2][x_3, x_4] \rangle_T$, temos que $I \subset \mathrm{Id}(\mathcal{G}_2)$. Agora seja $f = f(x_1, \ldots, x_n)$ uma identidade de $\mathcal{G}_2$, que podemos assumir multilinear. Desde que $f \in P_n$, podemos usar a Proposição 3.1.34 e escrever f módulo, $P_n \cap I$, como uma combinação linear de elementos da forma

$$x_1 \ldots x_n \text{ e } x_{i_1} \ldots x_{i_{n-2}} [x_i, x_j], \text{ com } i_1 < \cdots < i_{n-2}.$$

Como $[x_i, x_j] = -[x_j, x_i]$, podemos também considerar $i < j$. Assim, existem escalares $\alpha, \beta_{ij} \in F$, com $1 \leqslant i < j \leqslant n$, tais que

$$f \equiv \alpha x_1 \ldots x_n + \sum_{\substack{i,j=1 \\ i<j}}^{n} \beta_{ij} x_{i_1} \ldots x_{i_{n-2}} [x_i, x_j] \pmod{P_n \cap I}. \tag{4.2}$$

Como $f \in \mathrm{Id}(\mathcal{G}_2)$, ao avaliarmos em elementos de $\mathcal{G}_2$, obtemos zero. Fazendo inicialmente $x_k = 1$, para todo $k \in \{1, \ldots, n\}$, usando a Equação (4.2), vamos obter $\alpha = 0$. Em seguida, considerando i e j fixados, fazemos a substituição $x_i = e_1$, $x_j = e_2$ e $x_k = 1$, para todo $k \notin \{i, j\}$. Novamente, voltando na Equação (4.2), obtemos $\beta_{ij} = 0$. Repetindo esse raciocínio, teremos $\beta_{ij} = 0$ para todos $i, j \in \{1, \ldots, n\}$, com $i < j$. Concluímos que $f \in I$ e, portanto, $\mathrm{Id}(\mathcal{G}_2) \subset I$, o que prova o resultado. □

De modo mais geral, temos o seguinte resultado provado por Giambruno, La Mattina e Petrogradsky (2007).

Teorema 4.1.13. *Se $k \geqslant 1$, então*

$$\mathrm{Id}(\mathcal{G}_{2k}) = \langle [x_1, x_2, x_3] \, , [x_1, x_2] \cdots [x_{2k+1}, x_{2k+2}] \rangle_T \, .$$

Para dar exemplos de álgebras que geram a mesma variedade, vamos mostrar que a seguinte subálgebra de UT_3, também definida por Giambruno, La Mattina e Petrogradsky (ibid.), é PI-equivalente à $\mathcal{G}_2$:

$$N_3 = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} : a, b, c, d \in F \right\}.$$

Proposição 4.1.14. $\mathrm{Id}(N_3) = \langle [x_1, x_2, x_3], [x_1, x_2][x_3, x_4] \rangle_T$.

Demonstração. Não é difícil mostrar que $[x_1, x_2, x_3], [x_1, x_2][x_3, x_4] \in \mathrm{Id}(N_3)$. Assim, segue que $I = \langle [x_1, x_2, x_3], [x_1, x_2][x_3, x_4] \rangle_T \subset \mathrm{Id}(N_3)$.

Consideremos agora $f = f(x_1, \ldots, x_n)$ uma identidade multilinear de N_3. Usamos os mesmos argumentos usados na prova da Proposição 4.1.12 e escrevemos f, módulo I, como uma combinação linear de elementos exatamente como na Equação (4.2).

Fazemos inicialmente a avaliação $x_k = e_{11} + e_{22} + e_{33}$, para todo $k \in \{1, \ldots, n\}$, e obtemos $\alpha = 0$. Em seguida, para i e j fixos, fazemos a substituição $x_i = e_{12}$, $x_j = e_{23}$ e $x_k = e_{11} + e_{22} + e_{33}$, para todo $k \notin \{i, j\}$, e obtemos $\beta_{ij} = 0$. Claramente, $\beta_{ij} = 0$ para todos $i, j \in \{1, \ldots, n\}$, com $i < j$ e, assim, $f \in I$, provando que $\mathrm{Id}(N_3) = I$, como queríamos. □

Como consequência das Proposições 4.1.12 e 4.1.14, obtemos que $N_3 \sim_{PI} \mathcal{G}_2$, o que é o mesmo que dizer que $\mathrm{var}(N_3) = \mathrm{var}(\mathcal{G}_2)$.

A álgebra N_3 faz parte de uma família de álgebras que foi introduzida por Giambruno, La Mattina e Petrogradsky (ibid.), com um papel importante na classificação de variedades com propriedades particulares, como veremos futuramente.

Para definir esta família de álgebras, Giambruno, La Mattina e Petrogradsky consideraram, para $k \geqslant 3$, a matriz definida por $H_k = \sum_{i=1}^{k-1} e_{i,i+1}$ da álgebra de matrizes UT_k. Por exemplo, para $k = 4$, temos $H_4 = e_{12} + e_{23} + e_{34}$ e, note que, $H_4^2 = e_{13} + e_{24}$ que explicitamente são as matrizes

$$H_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{e} \quad H_4^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{4.3}$$

Em seguida, os autores definiram a álgebra

$$N_k = \mathrm{span}_F \left\{ I_k, H_k, H_k^2, \ldots, H_k^{k-2}, e_{12}, e_{13}, \ldots, e_{1k} \right\} \tag{4.4}$$

onde I_k denota a matriz identidade $k \times k$. Observe que a definição acima nos indica que as matrizes em N_3 são da forma apresentada e, a partir das Equações (4.3) e (4.4), também vemos que

$$N_4 = \left\{ \begin{pmatrix} a & b & c & d \\ 0 & a & e & f \\ 0 & 0 & a & e \\ 0 & 0 & 0 & a \end{pmatrix} : a, b, c, d, e, f \in F \right\}.$$

A seguir, apresentamos o T-ideal de N_k, conforme provado no artigo de Giambruno, La Mattina e Petrogradsky (2007).

Teorema 4.1.15. *Para $k \geqslant 3$, temos* $\mathrm{Id}(N_k) = \langle [x_1, \ldots, x_k], [x_1, x_2][x_3, x_4] \rangle_T$.

Finalizamos a seção observando que, pela Proposição 4.1.10, para qualquer $n \geqslant 1$, $M_n(F) \in \mathrm{var}(M_{n+1}(F))$, pois $M_{n+1}(F)$ contém uma subálgebra isomorfa a $M_n(F)$. Desta forma, temos $\mathrm{var}(M_n(F)) \subset \mathrm{var}(M_{n+1}(F))$ mas, claramente a inclusão é estrita, pois $M_{n+1}(F) \notin \mathrm{var}(M_n(F))$ de acordo com o Lema 3.4.2 e o Teorema 3.4.13.

Assim, temos uma cadeia ascendente infinita de variedades

$$\mathrm{var}(F) \subsetneq \mathrm{var}(M_2(F)) \subsetneq \mathrm{var}(M_3(F)) \subsetneq \ldots$$

Exercícios V ou F da Seção 4.1: Verifique se cada sentença abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, A e B representam F-álgebras.

(1) $\mathrm{Id}(UT_2) \subset \mathrm{Id}(UT_3)$.

(2) $\mathrm{Id}(M_2(F)) \subset \mathrm{Id}(UT_2)$.

(3) $[x_1, x_2]^2 \in \mathrm{Id}(N_3)$.

(4) $\mathrm{Id}(\mathcal{G}_4) = \mathrm{Id}(N_6)$.

(5) $[x_1, x_2][x_3, x_4][x_5, x_6] \in \mathrm{Id}(\mathcal{G}_4 \oplus N_4)$.

(6) Se J é o radical de Jacobson de A então $J \in \mathrm{var}(A)$.

(7) Se A e B têm radicais de Jacobson $J(A)$ e $J(B)$, respectivamente, então $J(A) \oplus J(B) \in \mathrm{var}(A \oplus B)$.

(8) Se $I = \mathrm{Id}(\mathcal{G}_2)$ e $f = x_3x_1[x_2, x_4] + [x_1, x_2]x_3$ então $f \equiv x_1x_3[x_2, x_4] + x_3[x_1, x_2] (\mathrm{mod}\ I)$.

(9) Se B é uma subálgebra de A e B é uma PI-álgebra, então A é uma PI-álgebra.

4.2 A sequência de codimensões

Para minimizar as dificuldades na descrição de um T-ideal, associamos uma sequência numérica à uma F-álgebra A para, de uma certa maneira, "medir" as identidades polinomiais satisfeitas por essa álgebra. Assim, definiremos a sequência de codimensões de A e passaremos a estudar o T-ideal $\mathrm{Id}(A)$ através do comportamento assintótico desta sequência.

Como vimos na Seção 3.3, o T-ideal das identidades de A é gerado pelo conjunto de seus polinômios multilineares. Desta forma, o F-espaço vetorial dos polinômios multilineares em $x_1, \ldots, x_n$

$$P_n = \mathrm{span}_F\{x_{\sigma(1)} \ldots x_{\sigma(n)} : \sigma \in S_n\}.$$

torna-se particularmente importante.

Observamos que $\mathrm{Id}(A)$ é gerado pelo subespaço

$$(P_1 \cap \mathrm{Id}(A)) \dot{+} (P_2 \cap \mathrm{Id}(A)) \dot{+} (P_3 \cap \mathrm{Id}(A)) \dot{+} \cdots$$

na álgebra associativa livre. Consequentemente, as dimensões dos espaços $P_n \cap \mathrm{Id}(A)$ nos fornecem, de certa forma, o crescimento das identidades da álgebra A. Foi por este motivo que Regev (1972) introduziu a sequência de codimensões de uma álgebra.

Definição 4.2.1. Seja A uma F-álgebra, e consideremos o F-espaço vetorial $P_n(A) = \dfrac{P_n}{P_n \cap \mathrm{Id}(A)}$. Para todo $n \geqslant 1$, definimos a n-ésima codimensão de A por

$$c_n(A) = \dim_F(P_n(A))$$

Além disso, se $\mathcal{V} = \mathrm{var}(A)$ é a variedade gerada por A, então definimos $c_n(\mathcal{V}) = c_n(A)$ e dizemos que esta é a n-ésima codimensão da variedade $\mathcal{V}$.

O conhecimento da sequência $\{c_n(A)\}_{n\geqslant 1}$ de uma F-álgebra A é de bastante interesse em PI-teoria, pois esta fornece uma ideia do crescimento das identidades satisfeitas por A.

A seguir, damos alguns exemplos de álgebras cujas sequências de codimensões são facilmente calculadas, porém esse cálculo não é um trabalho fácil na maioria das situações.

Exemplo 4.2.2. (a) Se A é uma F-álgebra comutativa unitária sabemos que $\mathrm{Id}(A) = \langle [x_1, x_2] \rangle_T$. Qualquer polinômio de P_n pode ser escrito, módulo $P_n \cap \mathrm{Id}(A)$, como um múltiplo escalar do polinômio $x_1 \cdots x_n$, o qual não é uma identidade de A. Logo $\dim_F(P_n(A)) = 1$, ou seja, $c_n(A) = 1$, para todo $n \geqslant 1$.

(b) Seja A uma F-álgebra nilpotente de índice m. Se $f(x_1, \ldots, x_n) \in P_n$, onde $n \geqslant m$, temos que $f(a_1, \ldots, a_n) = 0$ sejam quais forem $a_1, \ldots, a_n \in A$. Dessa forma, $c_n(A) = \dim_F(P_n(A)) = 0$ quando $n \geqslant m$.

O resultado a seguir é importante para que possamos comparar as sequências de codimensões de álgebras A e B em situações específicas.

Proposição 4.2.3.

1. *Se* $B \in \mathrm{var}(A)$*, então* $c_n(B) \leqslant c_n(A)$*, para todo* $n \geqslant 1$.

2. *Se* $\mathrm{Id}(A) \subset \mathrm{Id}(B)$ *e* $c_n(A) = c_n(B)$ *para todo* $n \geqslant 1$*, então* $A \sim_{PI} B$.

Demonstração.

1. Como $B \in \mathrm{var}(A)$, temos que $P_n \cap \mathrm{Id}(A) \subset P_n \cap \mathrm{Id}(B)$. Dessa forma, $\dim_F(P_n \cap \mathrm{Id}(A)) \leqslant \dim_F(P_n \cap \mathrm{Id}(B))$. Assim, temos que $c_n(B) \leqslant c_n(A)$.

2. Por hipótese, temos $c_n(A) = c_n(B)$ e assim,

$$\dim_F(P_n \cap \mathrm{Id}(A)) = \dim_F(P_n \cap \mathrm{Id}(B))$$

para todo $n \geqslant 1$. Como também temos que $P_n \cap \mathrm{Id}(A) \subset P_n \cap \mathrm{Id}(B)$, obtemos $P_n \cap \mathrm{Id}(A) = P_n \cap \mathrm{Id}(B)$ para todo $n \geqslant 1$. Como sobre um corpo de característica zero todo T-ideal é gerado por polinômios multilineares, concluímos que $\mathrm{Id}(A) = \mathrm{Id}(B)$.

□

Com o próximo resultado, vemos que a codimensão da soma direta de duas álgebras A e B é controlada pelas codimensões de A e de B.

Proposição 4.2.4. *Se* A *e* B *são duas* F*-álgebras, então temos que* $c_n(A \oplus B) \leqslant c_n(A) + c_n(B)$.

Demonstração. Pelo Lema 4.1.3, sabemos que $\mathrm{Id}(A \oplus B) = \mathrm{Id}(A) \cap \mathrm{Id}(B)$. Consideremos a aplicação linear entre espaços vetoriais

$$\phi : P_n \to \frac{P_n}{P_n \cap \mathrm{Id}(A)} \dot{+} \frac{P_n}{P_n \cap \mathrm{Id}(B)}$$

dada por $\phi(f) = (f + (P_n \cap \mathrm{Id}(A)), f + (P_n \cap \mathrm{Id}(B)))$, para todo $f \in P_n$. Temos que o núcleo desta aplicação é dado por $\mathrm{Ker}(\phi) = P_n \cap \mathrm{Id}(A) \cap \mathrm{Id}(B) = P_n \cap \mathrm{Id}(A \oplus B)$. Logo temos uma imersão de espaços vetoriais

$$\frac{P_n}{P_n \cap \mathrm{Id}(A \oplus B)} \hookrightarrow \frac{P_n}{P_n \cap \mathrm{Id}(A)} \dot{+} \frac{P_n}{P_n \cap \mathrm{Id}(B)}$$

e segue daí que $c_n(A \oplus B) \leqslant c_n(A) + c_n(B)$. □

Vamos agora definir terminologias em relação à sequência de codimensões de uma dada álgebra A e de variedades.

Definição 4.2.5.

1. A sequência de codimensões $\{c_n(A)\}_{n \geqslant 1}$ de uma álgebra A é limitada exponencialmente se existem constantes $a, \alpha > 0$ tais que $c_n(A) \leqslant a\alpha^n$, para todo $n \geqslant 1$.

2. A sequência de codimensões de A cresce exponencialmente se existe uma constante $\alpha \geqslant 2$ tal que $c_n(A) \geqslant \alpha^n$. Neste caso, dizemos que A tem crescimento exponencial.

3. Uma variedade $\mathcal{V}$ tem crescimento exponencial se $\mathcal{V}$ é gerada por uma álgebra de crescimento exponencial.

Observe que, como $\dim_F(P_n) = n!$, desde que a álgebra livre $F\langle X\rangle$ não é uma PI-álgebra, temos $c_n(F\langle X\rangle) = n!$. Note ainda que podemos verificar se uma F-álgebra é ou não uma PI-álgebra, olhando a sequência de codimensões. De fato, temos $c_n(A) = n! - \dim(P_n \cap \mathrm{Id}(A))$. Além disso, sabemos que se A satisfaz alguma identidade polinomial, então A satisfaz um identidade multilinear. Portanto, A é uma PI-álgebra se, e somente se, $c_n(A) < n!$, para algum $n \geqslant 1$. Por outro lado, é importante informar que Regev (1972) melhorou a cota superior para a sequência de codimensões de uma PI-álgebra provando o teorema a seguir.

Teorema 4.2.6. *Se uma F-álgebra A satisfaz uma identidade polinomial, então $c_n(A)$ é limitada exponencialmente.*

Em seu artigo, o autor usou este fato como uma ferramenta para mostrar que se A e B são PI-álgebras sobre um corpo F, então $A \otimes B$ também satisfaz uma identidade polinomial não nula. De fato, Regev mostrou o seguinte teorema.

Teorema 4.2.7. *Se A e B são PI-álgebras sobre um corpo arbitrário F, então $c_n(A \otimes B) \leqslant c_n(A)c_n(B)$, para todo $n \geqslant 1$.*

Um ano mais tarde, Latyšev (1972) estabeleceu uma cota exponencial para a codimensão em função do grau de uma identidade polinomial satisfeita por A, provando o teorema a seguir.

Teorema 4.2.8. *Se uma álgebra A satisfaz uma identidade polinomial de grau $s \geqslant 1$, então $c_n(A) \leqslant (s-1)^{2n}$.*

Quando temos uma álgebra de dimensão finita, podemos dar uma cota superior para a sua codimensão através do próximo resultado de Bahturin e Drensky (2002).

Proposição 4.2.9. *Se A é uma álgebra tal que $\dim_F(A) = d$, então $c_n(A) \leqslant d^{n+1}$.*

Demonstração. Fixado $n \geqslant 1$, seja $\{m_1(x_1, \ldots, x_n), \ldots, m_N(x_1, \ldots, x_n)\}$ uma base de P_n sobre F.

Seja f uma identidade da álgebra A. Podemos supor, sem perda de generalidade, que f é multilinear de grau n e, portanto, pode ser escrita como

$$f(x_1, \cdots, x_n) = \sum_{j=1}^{N} \alpha_j m_j(x_1, \ldots, x_n), \text{ onde } \alpha_\sigma \in F. \tag{4.5}$$

Se $\Gamma = \{a_1, \ldots, a_d\}$ é uma base de A, consideremos S o conjunto de todas as n-úplas cujas entradas são elementos de Γ. Observamos que S tem d^n elementos e como f é uma identidade polinomial de grau n de A, sabemos que f se anula sob todas as avaliações por elementos de S.

Podemos traduzir o fato acima a partir de um sistema homogêneo contendo $n!$ variáveis, correspondentes aos coeficientes α_j, que aparecem na Equação (4.5), e d^n equações lineares, cada uma delas correspondente a um elemento de S. Escre-

vemos isto abaixo

$$\begin{cases} \sum_{j=1}^{N} \alpha_j m_j(a_1 \dots a_1) & = & 0 \\ \vdots & & \\ \sum_{j=1}^{N} \alpha_j m_j(a_1 a_2 \dots a_n) & = & 0 \\ \vdots & & \\ \sum_{j=1}^{N} \alpha_j m_j(a_d \dots a_d) & = & 0. \end{cases}$$

Agora, reescrevendo o lado esquerdo das equações acima como combinação linear dos elementos de Γ, obtemos um sistema linear homogêneo com d^{n+1} equações e $N = n!$ variáveis.

Notemos que a dimensão do espaço solução do sistema acima é maior ou igual a $n! - d^{n+1}$. Mas a dimensão do espaço solução deste sistema é igual a dimensão de $P_n \cap \mathrm{Id}(A)$. Como $c_n(A) = \dim_F(P_n) - \dim_F(P_n \cap \mathrm{Id}(A))$, segue que $c_n(A) \leqslant d^{n+1}$. □

Veremos que para algumas álgebras podemos melhorar a cota superior dada para a codimensão e estabelecemos a seguinte definição.

Definição 4.2.10.

1. A sequência de codimensões $\{c_n(A)\}_{n\geqslant 1}$ é limitada polinomialmente se existem uma constante a e um número inteiro não negativo k tais que $c_n(A) \leqslant an^k$, para todo n arbitrariamente grande. Neste caso, dizemos que a álgebra A tem crescimento polinomial.

2. Uma variedade $\mathcal{V}$ tem crescimento polinomial se $\mathcal{V}$ é gerada por uma álgebra de crescimento polinomial.

Nas próximas proposições, apresentaremos exemplos de álgebras de crescimento polinomial.

Proposição 4.2.11. *Seja $\mathcal{G}_2$ a álgebra definida na Seção 4.1. Temos $c_n(\mathcal{G}_2) = \frac{n^2-n+2}{2}$, para todo $n \geqslant 1$.*

Demonstração. Temos que mostrar que o espaço quociente $P_n(\mathcal{G}_2) = \frac{P_n}{P_n \cap \mathcal{G}_2}$ possui uma base com $\frac{n^2-n+2}{2}$ elementos. Observamos que, na demonstração da Proposição 4.1.12, já provamos que qualquer polinômio f em P_n módulo $P_n \cap \mathcal{G}_2$ pode ser escrito como uma combinação linear dos polinômios $x_1 \dots x_n$ e $x_{i_1} \dots x_{i_{n-2}}[x_{j_1}, x_{j_2}]$, com $i_1 < \cdots < i_{n-2}$ e $j_1 > j_2$.

Assim, o conjunto de polinômios

$$B = \{x_1 \dots x_n,\ \ x_{i_1} \dots x_{i_{n-2}}[x_{j_1}, x_{j_2}] : i_1 < \cdots < i_{n-2},\ j_1 > j_2\}$$

é um conjunto gerador de $P_n(\mathcal{G}_2)$. Além disso, pela demonstração da Proposição 4.1.12, os polinômios em B são linearmente independentes módulo $P_n \cap \mathcal{G}_2$. Desta forma, B é uma base de $P_n(\mathcal{G}_2)$.

Agora vamos contar quantos elementos temos na base B, começando pelos polinômios do tipo $x_{i_1} \dots x_{i_{n-2}}[x_{j_1}, x_{j_2}]$ nas condições definidas. É claro que é suficiente determinar as variáveis que vão ocupar as entradas do comutador, pois, desta forma, todas as outras já estarão determinadas devido à ordenação. A quantidade destas variáveis é $\binom{n}{2} = \frac{n(n-1)}{2}$. Assim, a quantidade total de elementos na base é $\frac{n(n-1)}{2} + 1$, que é exatamente o que queríamos provar. □

Em geral, no artigo de Giambruno, La Mattina e Petrogradsky (2007), temos o seguinte resultado sobre as álgebras $\mathcal{G}_{2k}$, definidas na Seção 4.1.

Proposição 4.2.12. *Para $k \geqslant 1$, temos $c_n(\mathcal{G}_{2k}) = \sum_{j=0}^{k} \binom{n}{2j}$, para todo $n \geqslant 1$.*

Pela proposição acima, temos que, para $k \geqslant 1$, as álgebras $\mathcal{G}_{2k}$ têm crescimento polinomial. Particularmente, para cada $k \geqslant 1$, as codimensões dadas são expressas por polinômios em n de grau $2k$.

Observemos que a partir das Proposições 4.1.12, 4.1.14 e 4.2.11, temos para todo $n \geqslant 1$,

$$c_n(N_3) = \frac{n^2 - n + 2}{2}. \tag{4.6}$$

Agora vamos enunciar o resultado sobre a sequência de codimensões das álgebras N_k, $k \geqslant 3$, definidas na Seção 4.1.

Proposição 4.2.13. *Para $k \geqslant 3$, temos $c_n(N_k) = 1 + \sum_{j=2}^{k-1} \binom{n}{j}(j-1)$, para todo $n \geqslant 1$.*

A partir da proposição anterior, vemos que, para $k \geqslant 3$, as álgebras N_k têm crescimento polinomial, e as codimensões dadas são expressas por polinômios em n de grau $k-1$. Particularmente, as álgebras N_3 e $\mathcal{G}_2$ têm crescimento quadrático, ou seja, as codimensões são dadas por polinômios de grau 2.

Em geral, se A é uma álgebra de crescimento polinomial, temos que a n-ésima codimensão de A é dada por um polinômio em n com coeficientes racionais como foi provado por Drensky e Regev (1996).

Teorema 4.2.14. *Seja A uma álgebra de crescimento polinomial. Então*

$$c_n(A) = qn^k + \mathcal{O}(n^{k-1})$$

onde $k \geqslant 0$, $q \in \mathbb{Q}$ e $\mathcal{O}(n^{k-1})$ representa um polinômio de grau menor ou igual a $k-1$ com coeficientes racionais.

Motivados pelo teorema acima, a partir de agora, sempre que $\mathcal{V}$ for uma variedade de crescimento polinomial, vamos dizer que $\mathcal{V}$ é uma variedade de crescimento n^k, para algum inteiro $k \geqslant 0$, e para sua sequência de codimensões escreveremos $c_n(\mathcal{V}) \approx qn^k$, para algum $q \in \mathbb{Q}$.

No que segue, estaremos interessados em observar a influência do corpo no cálculo das codimensões de uma álgebra.

Lembremos que, na Proposição 4.1.5, provamos que se A é uma álgebra sobre um corpo F de característica zero, então toda identidade de A é estável. Em particular, se K é uma extensão de F, temos que $\mathrm{Id}(A) \subset \mathrm{Id}(A \otimes K)$, já que K é uma F-álgebra comutativa.

Por outro lado, observemos que também temos $\mathrm{Id}(A \otimes K) \subset \mathrm{Id}(A)$, pois A pode ser vista como uma subálgebra de $A \otimes K$.

Com isso, temos uma igualdade

$$\mathrm{Id}(A \otimes K) = \mathrm{Id}(A) \tag{4.7}$$

onde consideramos apenas as identidades de $A \otimes K$ como F-álgebra. Consequentemente, para $n \geqslant 1$, temos

$$c_n^F(A) = c_n^F(A \otimes K)$$

onde o índice superior na igualdade acima significa que as duas sequências de codimensões são calculadas sobre o corpo F.

No Corolário 1.2.61, já provamos que toda base de A como F-álgebra é uma base para $A \otimes K$ como K-álgebra. Isto permitiu estender os escalares de A de maneira que A pudesse ser considerada como uma K-álgebra.

Uma pergunta natural que surge neste momento é: como se relacionam a sequência de codimensões de A como F-álgebra e a sequência de codimensões de A, considerada como K-álgebra? Ou seja, qual a relação entre $c_n^F(A)$ e $c_n^K(A \otimes K)$?

Na notação acima, estamos considerando

$$c_n^K(A \otimes K) = \dim_K \left(\frac{P_n^K}{P_n^K \cap \mathrm{Id}_K(A \otimes K)} \right)$$

onde $P_n^K = P_n \otimes K$ denota o conjunto dos polinômios multilineares de grau n com coeficientes em K e $\mathrm{Id}_K(A \otimes K)$ as identidades de $A \otimes K$ com coeficientes em K. Vamos responder a questão abaixo.

Proposição 4.2.15. *Sejam A uma PI-álgebra sobre um corpo F de característica zero e K uma extensão de F. Então, para todo $n \geqslant 1$, temos que*

$$c_n^K(A \otimes K) = c_n^F(A).$$

Demonstração. Suponhamos que $c_n^F(A) = m$ e consideremos $\{\bar{f}_1, \ldots, \bar{f}_m\}$ uma base de $P_n^F(A) = \frac{P_n^F}{P_n^F \cap \mathrm{Id}_F(A)}$, onde P_n^F denota o conjunto dos polinômios multilineares de grau n com coeficientes em F e $\mathrm{Id}_F(A)$ as identidades de A com coeficientes em F.

Sejam $\pi\colon P_n^F \to P_n^F(A)$ a projeção canônica, $f_1, \ldots, f_m \in P_n^F$ tais que $\pi(f_i) = \bar{f}_i, i = 1, \ldots, m$, e $\{g_1, \ldots, g_k\}$ uma base de $P_n^F \cap \mathrm{Id}_F(A)$. Assim,

$$\mathcal{B} = \{f_1, \ldots, f_m, g_1 \ldots, g_k\}, \text{ com } m + k = n!$$

é uma base de P_n^F. Pelo Corolário 1.2.61, a partir de $\mathcal{B}$, podemos obter uma base $\mathcal{B}'$ de P_n^K, que por simplicidade continuaremos denotando seus elementos como anteriormente, ou seja, $\mathcal{B}' = \{f_1, \ldots, f_m, g_1 \ldots, g_k\}$.

Com isso, dado um polinômio $f = f(x_1, \ldots, x_n) \in P_n^K$, temos que existem escalares $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_k \in K$ tais que

$$f = \sum_{i=1}^{m} \alpha_i f_i + \sum_{j=1}^{k} \beta_j g_j.$$

Logo,

$$g = g(x_1, \ldots, x_n) = \sum_{j=1}^{k} \beta_j g_j = f - \sum_{i=1}^{m} \alpha_i f_i \in \mathrm{Id}_K(A \otimes K)$$

pois como K é uma extensão de F, temos $\mathrm{Id}_F(A) \subset \mathrm{Id}_F(A \otimes K) \subset \mathrm{Id}_K(A \otimes K)$ e assim, vemos que $g \in P_n^K \cap \mathrm{Id}_K(A \otimes K)$.

Além disso, qualquer combinação linear não nula $\sum_{i=1}^{m} \alpha_i f_i$ não é uma identidade de $A \otimes K$. De fato, consideremos

$$h = \alpha_1 f_1 + \cdots + \alpha_m f_m \in \mathrm{Id}_K(A \otimes K)$$

com $\alpha_1, \ldots, \alpha_m \in K$ e vamos escrever cada um dos escalares α_i em uma base $\mathcal{B}$ de K sobre F

$$\alpha_i = \sum_j \beta_{ij} t_j;\ i \in \{1, \ldots, m\}, t_j \in \mathcal{B}, \beta_{ij} \in F.$$

Sejam $a_1, \ldots, a_n \in A$ e $a_1 \otimes 1, \ldots, a_n \otimes 1 \in A \otimes K$. Assim:

$$\begin{aligned} h(a_1 \otimes 1, \ldots, a_n \otimes 1) &= \sum_{i=1}^{m} \alpha_i f_i(a_1 \otimes 1, \ldots, a_n \otimes 1) \\ &= \sum_j \left(\sum_{i=1}^{m} \beta_{ij} f_i(a_1, \ldots, a_n) \right) \otimes t_j. \end{aligned}$$

Como $h \in \mathrm{Id}_K(A \otimes K)$, temos que:

$$\sum_j \left(\sum_{i=1}^{m} \beta_{ij} f_i(a_1, \ldots, a_n) \right) \otimes t_j = 0.$$

Mas agora, como $\{f_1, \ldots, f_m\}$ é linearmente independente sobre K, então, para qualquer sequência $(b_1, \ldots, b_n)$ de elementos em A, os elementos

$$\left(\sum_{i=1}^{m} \beta_{ij} f_i(b_1, \ldots, b_n) \right) \otimes t_1, \left(\sum_{i=1}^{m} \beta_{ij} f_i(b_1, \ldots, b_n) \right) \otimes t_2, \ldots$$

são linearmente independentes. Daí, segue que $\sum_{i=1}^{m} \beta_{ij} f_i \in \mathrm{Id}_F(A)$, para todo $j \in \{1, 2, \ldots\}$. Como $\bar{f_1}, \ldots, \bar{f_m}$ formam uma base para $P_n^F(A)$, temos que:

$$\beta_{ij} = 0, \text{ para } i \in \{1, \ldots, m\},\ j \in \{1, 2, \ldots\}.$$

Com isso, $\alpha_1 = \cdots = \alpha_m = 0$.

Isso mostra que se $\pi' \colon P_n^K \to P_n^K(A)$ denota a projeção canônica e se continuarmos denotando $\pi'(f_i) = \bar{f_i}$, então $\{\bar{f_1}, \ldots, \bar{f_m}\}$ é linearmente independente sobre K e

$$\pi'(f) = \bar{f} = \sum_{i=1}^{m} \alpha_i \bar{f_i} \in \frac{P_n^K}{P_n^K \cap \mathrm{Id}_K(A \otimes K)}.$$

Portanto, $c_n^K(A \otimes K) = m$ como queríamos mostrar. □

Pela proposição acima, nos resultados sobre a sequência de codimensões de uma F-álgebra A, podemos considerá-la sobre um corpo algebricamente fechado, pois podemos tomar K como o fecho algébrico de F e as codimensões serão mantidas.

Exercícios V ou F da Seção 4.2: Verifique se cada sentença abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, A e B representam F-álgebras.

(1) Se B está isomorficamente imersa em A, então $c_n(A) \leqslant c_n(B)$.

(2) Se J é o radical de Jacobson de A, então $c_n(J) \leqslant c_n(A)$.

(3) Se J é o radical de Jacobson de A e $c_n(J) = c_n(A)$, então A é nilpotente.

(4) Para todo $k \geqslant 3$, temos $c_n(N_k) = c_n(\mathcal{G}_{2k})$.

(5) Para todo $k \geqslant 2$, temos que $c_n(\mathcal{G}_{2k}) \approx q n^{2k}$, para algum $q \in \mathbb{Q}$.

(6) Para todo $k \geqslant 3$, temos que $c_n(N_k) \approx q n^k$, para algum $q \in \mathbb{Q}$.

(7) $c_n(N_4 \oplus \mathcal{G}_4) \approx q n^4$, para algum $q \in \mathbb{Q}$.

4.3 Álgebras de crescimento exponencial

Na seção anterior, exibimos exemplos de álgebras de crescimento polinomial. O objetivo desta seção é apresentar dois exemplos importantes de álgebras de crescimento exponencial: a álgebra UT_2 das matrizes triangulares superiores 2×2 com entradas em um corpo F e a álgebra de Grassmann de dimensão infinita $\mathcal{G}$. Ao longo desta seção, F denota um corpo de característica zero.

Inicialmente, iremos determinar o T-ideal e a sequência de codimensões de UT_2. Como vimos no Exemplo 3.2.6, $[x_1, x_2][x_3, x_4] \in \mathrm{Id}(UT_2)$. Queremos

mostrar que de fato $\mathrm{Id}(UT_2) = \langle [x_1, x_2][x_3, x_4] \rangle_T$, como provado por Malcev (1971). Para isso, denote por $I = \langle [x_1, x_2][x_3, x_4] \rangle_T$. Temos o seguinte lema.

Lema 4.3.1. *Para todo $m \geqslant 2$, temos que*

$$[x_{j_1}, x_{j_2}, \ldots, x_{j_r}, x_{j_{r+1}}, \ldots, x_{j_m}] \equiv [x_{j_1}, x_{j_2}, \ldots, x_{j_{r+1}}, x_{j_r}, \ldots, x_{j_m}] \pmod{I}.$$

Demonstração. Primeiramente, observe que como $[x_1, x_2][x_3, x_4] \in I$, então $[[x_1, x_2], [x_3, x_4]] \in I$. Consequentemente, módulo I, quaisquer dois comutadores comutam. Com isso, se escrevermos $c = [x_{j_1}, x_{j_2}, \ldots, x_{j_{r-1}}]$, temos que

$$[x_{j_1}, x_{j_2}, \ldots, x_{j_r}, x_{j_{r+1}}, \ldots, x_{j_m}] = [c, x_{j_r}, x_{j_{r+1}}, x_{j_{r+2}}, \ldots, x_{j_m}].$$

Pela identidade de Jacobi, obtemos que

$$\begin{aligned} [c, x_{j_r}, x_{j_{r+1}}] &= -[[x_{j_r}, x_{j_{r+1}}], c] - [[x_{j_{r+1}}, c], x_{j_r}] \\ &\equiv [c, x_{j_{r+1}}, x_{j_r}] \pmod{I}. \end{aligned}$$

Portanto,

$$[x_{j_1}, x_{j_2}, \ldots, x_{j_r}, x_{j_{r+1}}, \ldots, x_{j_m}] \equiv [x_{j_1}, x_{j_2}, \ldots, x_{j_{r+1}}, x_{j_r}, \ldots, x_{j_m}] \pmod{I}.$$

□

Teorema 4.3.2. *Seja UT_2 a álgebra das matrizes 2×2 triangulares superiores sobre um corpo F de característica zero. Então:*

1. $\mathrm{Id}(UT_2) = \langle [x_1, x_2][x_3, x_4] \rangle_T$;
2. $c_n(UT_2) = 2^n(n-2) + 2$, *para todo $n \geqslant 1$.*

Demonstração. Para demonstrar o item 1, seja $I = \langle [x_1, x_2][x_3, x_4] \rangle_T$. Já sabemos que $I \subseteq \mathrm{Id}(UT_2)$. Vamos mostrar a inclusão inversa, ou seja, vamos mostrar que se $f \in \mathrm{Id}(UT_2)$, então $f \equiv 0 \pmod{I}$. Para isso, pelo Corolário 3.3.15, podemos supor que f é um polinômio multilinear de grau n. Pela Proposição 3.1.34, temos que f pode ser escrito como combinação linear de polinômios do tipo

$$x_{i_1} \cdots x_{i_r} c_1 \cdots c_s$$

onde $i_1 < \cdots < i_r$ e cada $c_i, i = 1, \ldots, s$, é um comutador de peso arbitrário (eventualmente vazio).

Agora, como $[x_1, x_2][x_3, x_4] \in I$, temos que $[x_{i_1}, \ldots, x_{i_r}][x_{j_1}, \ldots, x_{j_t}] \in I$, para quaisquer $r, t \geqslant 2$. Assim, se $s \geqslant 2$, temos que $c_1 \cdots c_s \in I$, onde cada

$c_i, i = 1, \ldots, s$ é um comutador de peso maior ou igual a 2. Com isso, temos que f pode ser escrito, módulo I, como combinação linear de polinômios do tipo

$$x_{i_1} \cdots x_{i_r}[x_{j_1}, \ldots, x_{j_s}]$$

com $i_1 < \cdots < i_r, n = r + s$.

Agora, pelo Lema 4.3.1, possivelmente renomeando as variáveis, temos que

$$[x_{j_1}, \ldots, x_{j_s}] \equiv [x_k, x_{j_1}, \ldots, x_{j_{n-r-1}}] \pmod{I}$$

onde $k > j_1$ e $j_1 < \cdots < j_{n-r-1}$. Ou seja, dentro de um comutador, módulo I, podemos considerar que a primeira variável possui o maior índice e as outras estão ordenadas.

Portanto concluímos que, módulo I, f pode ser escrito como combinação linear de polinômios do tipo

$$x_{i_1} \cdots x_{i_r}[x_k, x_{j_1}, \ldots, x_{j_{n-r-1}}]$$

onde $i_1 < \cdots < i_r, k > j_1, j_1 < \cdots < j_{n-r-1}$ e $\{i_1, \ldots, i_r, j_1, \ldots, j_{n-r-1}, k\} = \{1, \ldots, n\}$.

Para cada $r \in \{0, \ldots, n\}$, escreva $M = \{i_1, \ldots, i_r\}$, $N = \{j_1, \ldots, j_{n-r-1}\}$, $i_1 < \cdots < i_r$, $j_1 < \cdots < j_{n-r-1}$ e assuma que se $r = 0$ ou $r = n$, então $M = \varnothing$ ou $N = \varnothing$, respectivamente. Escrevendo

$$u^r_{M,N,k} = x_{i_1} \cdots x_{i_r}[x_k, x_{j_1}, \ldots, x_{j_{n-r-1}}]$$

temos que f pode ser escrito, módulo I, como

$$\sum_{r=0}^{n} \sum_{M,N,k} \alpha_{M,N,k} u^r_{M,N,k},\ \alpha_{M,N,k} \in F.$$

Para concluir a demonstração, basta mostrarmos que $\alpha_{M,N,k} = 0$, para cada escolha de M, N como acima. Fixado $r \in \{1, \ldots, n\}$, escolha conjuntos M e N e faça a seguinte avaliação: $x_{i_1} = \cdots = x_{i_r} = 1, x_k = e_{12}, x_{j_1} = \cdots = x_{n-r-1} = e_{12}$. Com isso, $\alpha_{M,N,k} u^r_{M,N,k}$ é avaliado em $\alpha_{M,N,k} e_{12}$. Além disso, para esse mesmo r fixado, se M' e N' são tais que $M \neq M'$ e $N \neq N'$, então $u^r_{M',N',k'}$ é avaliado em 0, já que $k > j_1$. Com isso, $\alpha_{M,N,k} = 0$, e procedendo da mesma maneira maneira para todos os valores de r, obtemos que $f \in I$. Portanto, $\mathrm{Id}(UT_2) = \langle [x_1, x_2][x_3, x_4] \rangle_T$.

Para demonstrar o item 2, observe que o que fizemos acima mostra que os polinômios

$$x_{i_1} \cdots x_{i_r}[x_k, x_{j_1}, \ldots, x_{j_{n-r-1}}]$$

onde, $i_1 < \cdots < i_r, k > j_1, j_1 < \cdots < j_{n-r-1}$ e $n = r + s$, formam uma base de $P_n(UT_2)$. Para determinar $c_n(UT_2)$, basta contarmos quantos elementos possui essa base.

Se $0 \leqslant r \leqslant n-2$, temos

$$\binom{n}{r}(n-r-1) = \binom{n}{n-r}(n-r-1)$$

polinômios. Se $r = n$, temos apenas o monômio $x_1 \cdots x_n$. Portanto,

$$\begin{aligned} c_n(UT_2) &= 1 + \sum_{j=2}^{n} \binom{n}{j}(j-1) \\ &= 1 + \sum_{j=2}^{n} \binom{n}{j} j - \sum_{j=2}^{n} \binom{n}{j} \\ &= 1 + \sum_{j=0}^{n} \binom{n}{j} j - \binom{n}{1} - \sum_{j=0}^{n} \binom{n}{j} + \binom{n}{0} + \binom{n}{1} \\ &= n2^{n-1} - 2^n + 2 \\ &= 2^{n-1}(n-2) + 2. \end{aligned}$$

□

Conforme vimos no Exercício 3.2.7 , temos que UT_n, a álgebra das matrizes triangulares superiores $n \times n$, satisfaz o polinômio $[x_1, x_2] \cdots [x_{2n-1}, x_{2n}] \equiv 0$. De fato, é possível provar o seguinte.

Proposição 4.3.3. *Para todo $n \geqslant 2$, temos*

$$\mathrm{Id}(UT_n) = \langle [x_1, x_2] \cdots [x_{2n-1}, x_{2n}] \rangle_T.$$

Agora, apresentaremos os resultados sobre o T-ideal e a sequência de codimensões da álgebra de Grassmann $\mathcal{G}$, provado por Krakowski e Regev (1973). Vimos no Exemplo 3.2.17 que $[x_1, x_2, x_3] \in \mathrm{Id}(\mathcal{G})$. O nosso objetivo é mostrar que $\mathrm{Id}(\mathcal{G}) = \langle [x_1, x_2, x_3] \rangle_T$.

Para a prova, denotamos por $I = \langle [x_1, x_2, x_3] \rangle_T$ e abaixo, apresentamos um lema técnico que será útil na demonstração do teorema em seguida.

Lema 4.3.4. *Os polinômios* $[x_1, x_2][x_2, x_3]$ *e* $[x_1, x_2][x_3, x_4] + [x_1, x_3][x_2, x_4]$ *pertencem a* I.

Demonstração. Como I é um T-ideal, temos que $[x_1, x_2^2, x_3] \in I$. Com isso, pelo Exercício 3.1.6, temos que

$$\begin{aligned}
[x_1, x_2^2, x_3] &= [[x_1, x_2]x_2 + x_2[x_1, x_2], x_3] \\
&= [[x_1, x_2]x_2, x_3] + [x_2[x_1, x_2], x_3] \\
&= [x_1, x_2][x_2, x_3] + [x_2, x_3][x_1, x_2] + [x_1, x_2, x_3] \circ x_2 \\
&= 2[x_1, x_2][x_2, x_3] + [[x_2, x_3], [x_1, x_2]] + [x_1, x_2, x_3] \circ x_2 \\
&\equiv 2[x_1, x_2][x_2, x_3] \pmod{I}
\end{aligned}$$

já que $[[x_2, x_3], [x_1, x_2]] + [x_1, x_2, x_3] \circ x_2 \in I$. Logo, $[x_1, x_2][x_2, x_3] \in I$ e, linearizando esse polinômio, concluímos que $[x_1, x_2][x_3, x_4] + [x_1, x_3][x_2, x_4] \in I$. □

Teorema 4.3.5. *Seja* $\mathcal{G}$ *a álgebra de Grassmann sobre um corpo* F *de característica zero. Então:*

1. $\mathrm{Id}(\mathcal{G}) = \langle [x_1, x_2, x_3] \rangle_T$;
2. $c_n(\mathcal{G}) = 2^{n-1}$.

Demonstração. Para demonstrar o item 1, seja $I = \langle [x_1, x_2, x_3] \rangle_T$. Já sabemos que $I \subseteq \mathrm{Id}(\mathcal{G})$. Vamos mostrar a inclusão inversa, ou seja, vamos mostrar que se $f \in \mathrm{Id}(\mathcal{G})$, então $f \equiv 0 \pmod{I}$. Para isso, pelo Corolário 3.3.15, podemos supor que f é um polinômio multilinear de grau n. Pela Proposição 3.1.34, temos que f pode ser escrito como combinação linear de polinômios do tipo

$$x_{i_1} \cdots x_{i_r} c_1 \cdots c_s,$$

onde $i_1 < \cdots < i_r$ e cada $c_i, i = 1, \ldots, s$, é um comutador de peso arbitrário (eventualmente vazio).

Agora, como $[x_1, x_2, x_3] \in I$, temos que $[x_1, \ldots, x_s] \in I$, para todo $s \geqslant 3$. Além disso, pelo Lema 4.3.4, temos que $[x_{j_1}, x_{j_2}][x_{j_3}, x_{j_4}] \equiv -[x_{j_1}, x_{j_3}][x_{j_2}, x_{j_4}] \pmod{I}$. Logo, como $[x_{j_1}, x_{j_2}] = -[x_{j_2}, x_{j_1}]$, concluímos que, módulo I, f pode ser escrito como combinação linear de polinômios do tipo

$$x_{i_1} \cdots x_{i_r} [x_{j_1}, x_{j_2}] \cdots [x_{j_{2m-1}}, x_{j_{2m}}],$$

onde $i_1 < \cdots < i_r$, $j_1 < \cdots < j_{2m}$ e $r + 2m = n$.

Para cada $r \in \{0, \ldots, n\}$ tal que $r + 2m = n$, escreva $M = \{i_1, \ldots, i_r\}$, $N = \{j_1, \ldots, j_{2m}\}$, $M \cap N = \varnothing$, $M \cup N = \{1, \ldots, n\}$, $i_1 < \cdots < i_r$, $j_1 < \cdots < j_{2m}$ e assuma que se $r = 0$ ou $r = n$, então $M = \varnothing$ ou $N = \varnothing$, respectivamente. Fixados conjuntos M e N nestas condições, denote por

$$g_{r,M,N} = x_{i_1} \cdots x_{i_r} [x_{j_1}, x_{j_2}] \cdots [x_{j_{2m-1}}, x_{j_{2m}}].$$

Assim, temos que, módulo I, f pode ser escrito como

$$\sum_{\substack{r=0 \\ r+2m=n}}^{n} \sum_{M,N} \alpha_{M,N} g_{r,M,N}, \alpha_{M,N} \in F.$$

Para concluir a demonstração, basta mostrarmos que $\alpha_{M,N} = 0$ para cada escolha de M, N nas condições acima. Para isso, fixado $0 \leqslant r \leqslant n, n = r + 2m$, escolha conjuntos $M = \{i_1, \ldots, i_r\}$ e $N = \{j_1, \ldots, j_{2m}\}$ e faça a seguinte avaliação: $x_{i_1} = \cdots = x_{i_r} = 1$ e $x_{j_k} = e_k, k = 1, \ldots, 2m$. Com isso, $\alpha_{M,N} g_{r,M,N}$ é avaliado em $2^m \alpha_{M,N} e_1 \cdots e_{2m}$. Além disso, para esse mesmo r fixado, se M' e N' são conjuntos tais que $M \neq M'$ e $N \neq N'$, então $g_{r,M',N'}$ é avaliado em 0, já que necessariamente o 1 é avaliado em um comutador. Com isso, $\alpha_{M,N} = 0$. Procedendo da mesma maneira para todos os valores de r, obtemos que $f \in I$. Portanto, $\mathrm{Id}(\mathcal{G}) = \langle [x_1, x_2, x_3] \rangle_T$.

Para demonstrar o item 2, observe que o que fizemos acima mostra que os polinômios

$$\{x_{i_1} \cdots x_{i_r} [x_{j_1}, x_{j_2}] \cdots [x_{j_{2m-1}}, x_{j_{2m}}] : i_1 < \cdots < i_r, j_1 < \cdots < j_{2m}, r + 2m = n\}$$

formam uma base de $P_n(\mathcal{G})$. Para determinar a sua dimensão, vamos contar quantos polinômios possui essa base. Afirmamos que esta quantidade é s_0, onde s_0 denota a soma de todos os binômios

$$\binom{n}{0} + \binom{n}{2} + \cdots + \binom{n}{2q},$$

onde q denota a parte inteira de $\frac{n}{2}$.

De fato, se $m = 0$, então obtemos o polinômio $x_1 \cdots x_n$.

Se $m = 1$, escolhidas as duas variáveis dentro do comutador, as variáveis fora do comutador estão determinadas. Com isso, temos $\binom{n}{2}$ polinômios da forma $x_{i_1} \cdots x_{i_r} [x_{j_1}, x_{j_2}]$, já que $i_1 < \cdots < i_r$. No caso geral, a escolha das variáveis

nos comutadores determinam as variáveis fora dos comutadores. Com isso, escolhidas as variáveis $x_{j_1}, \ldots, x_{j_{2m}}$ para os comutadores, como $j_1 < \cdots < j_{2m}$, temos apenas uma opção para a inserção destas variáveis. Como $i_1 < \cdots < i_r$, obtemos $\binom{n}{2m}$ polinômios da forma $x_{i_1} \cdots x_{i_r}[x_{j_1}, x_{j_2}] \cdots [x_{j_{2m-1}}, x_{j_{2m}}]$. Portanto, a dimensão de $P_n(\mathcal{G})$ é s_0 como afirmamos.

Denote por s_1 a soma de todos os binômios $\binom{n}{i}$, com i ímpar, $i \leqslant n$. Recorde que, para quaisquer a, b, n inteiros positivos, temos que $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$. Com isso, temos que $2^n = (1+1)^n = s_0 + s_1$ e $0 = (1-1)^n = \sum_{i=0}^{n} \binom{n}{i} (-1)^i = s_0 - s_1$. Logo, $2s_0 = 2^n$ e, portanto, $c_n(\mathcal{G}) = 2^{n-1}$. □

As álgebras UT_2 e $\mathcal{G}$ são protagonistas na PI-teoria. Tal protagonismo será evidenciado no Capítulo 5.

A partir dos resultados anteriores, exibiremos mais um exemplo importante de álgebra de crescimento exponencial das codimensões. Para isso, temos o seguinte exercício.

Exercício 4.3.6. Mostre que, para todo $k \geqslant 2$, existe um monomorfismo $\varphi : UT_2 \to M_k(F)$.

Exemplo 4.3.7. Para todo $k \geqslant 2$, $M_k(F)$ tem crescimento exponencial. De fato, pelo Exercício 4.3.6 e Proposição 4.1.10, temos que, para todo $k \geqslant 2$, $UT_2 \in \text{var}(M_k(F))$. Com isso, pela Proposição 4.2.3 e Teorema 4.3.2, temos que $c_n(M_k(F)) \geqslant 2^{n-1}(n-2) + 2$, para todo $k \geqslant 2$. Portanto, $M_k(F)$ tem crescimento exponencial.

Apesar de não ser conhecido o T-ideal de $M_k(F), k \geqslant 3$, Regev (1984) determinou o comportamento assintótico de $c_n(M_k(F))$. Antes de enunciar o próximo resultado, vamos introduzir uma nova notação. Se $f(n)$ e $g(n)$ são duas sequências reais, dizemos que $f(n)$ e $g(n)$ são assintoticamente equivalentes, e escrevemos $f(n) \simeq g(n)$, se $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$.

Teorema 4.3.8. *Se F é um corpo de característica zero, então, para todo $k \geqslant 2$,*

$$c_n(M_k(F)) \simeq \alpha n^g k^{2n}$$

onde $g = -\frac{k^2-1}{2}$ e

$$\alpha = \left(\frac{1}{\sqrt{2\pi}}\right)^{k-1} \left(\frac{1}{2}\right)^{\frac{k^2-1}{2}} 1!2! \cdots (k-1)! k^{\frac{k^2+4}{2}}.$$

Um dos problemas mais importantes em aberto na PI-teoria é a obtenção de uma base finita para $\mathrm{Id}(M_k(F)), k \geqslant 3$. A importância desse problema é evidenciada pelo seguinte teorema cuja demonstração pode ser encontrada no livro de Giambruno e Zaicev (2005).

Teorema 4.3.9. *Seja A uma PI-álgebra finitamente gerada sobre um corpo infinito F. Então $A \in \mathrm{var}(M_k(F))$ para algum $k \geqslant 1$.*

Com esse teorema, concluímos que toda PI-álgebra finitamente gerada sobre um corpo infinito F satisfaz todas as identidades de $M_k(F)$, para algum $k \geqslant 1$.

O próximo exercício mostra que a hipótese de A ser finitamente gerada não pode ser removida do Teorema 4.3.9.

Exercício 4.3.10. Mostre que, para todo $k \geqslant 1$, $\mathcal{G} \notin \mathrm{var}(M_k(F))$.

Exercícios V ou F da Seção 4.3: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente.

(1) $N_3 \in \mathrm{var}(UT_2 \oplus \mathcal{G})$.

(2) Para todo $k \geqslant 2$, temos $N_k \in \mathrm{var}(UT_k \oplus \mathcal{G})$.

(3) Para todo $k \geqslant 2$ e todo $n \geqslant 1$, temos $c_n(UT_2) \geqslant c_n(M_k(F))$.

(4) Para todo $k \geqslant 2$, a álgebra UT_k tem crescimento exponencial.

(5) Para todo $k \geqslant 2$, a álgebra $\mathcal{G}_k$ tem crescimento exponencial

(6) Existe $s \geqslant 2$ tal que $M_s(F) \in \mathrm{var}(\mathcal{G})$.

(7) Existe $s \geqslant 2$ tal que $\mathcal{G} \in \mathrm{var}(M_s(F))$.

4.4 Superálgebras

Em seus principais trabalhos, Kemer estuda a estrutura das álgebras que geram variedades de PI-álgebras. A partir disso, surgiu o particular interesse no estudo de superálgebras na PI-teoria. O objetivo desta seção é apresentar o conceito de superálgebras e estudar a sua estrutura.

No Exemplo 3.2.17, vimos que álgebra de Grassmann $\mathcal{G}$ satisfaz diversas propriedades importantes. Uma delas é que existem subespaços vetoriais

$$\mathcal{G}^{(0)} = \mathrm{span}_F\{e_{i_1} \cdots e_{i_{2k}} : 1 \leqslant i_1 < \cdots < i_{2k}, k \geqslant 0\} \quad \text{e}$$

$$\mathcal{G}^{(1)} = \text{span}_F\{e_{i_1} \cdots e_{i_{2k+1}} : 1 \leqslant i_1 < \cdots < i_{2k+1}, k \geqslant 0\}$$

de $\mathcal{G}$ tais que $\mathcal{G} = \mathcal{G}^{(0)} \dotplus \mathcal{G}^{(1)}$ e que satisfazem as condições

$$\mathcal{G}^{(0)}\mathcal{G}^{(0)} + \mathcal{G}^{(1)}\mathcal{G}^{(1)} \subset \mathcal{G}^{(0)} \text{ e } \mathcal{G}^{(1)}\mathcal{G}^{(0)} + \mathcal{G}^{(0)}\mathcal{G}^{(1)} \subset \mathcal{G}^{(1)}. \tag{4.8}$$

Agora vamos introduzir o conceito mais geral de álgebras com uma decomposição do tipo acima.

Definição 4.4.1. Dizemos que uma álgebra A é uma álgebra $\mathbb{Z}_2$-graduada, ou uma superálgebra, se existem dois subespaços vetoriais $A^{(0)}$ e $A^{(1)}$ de A, tais que $A = A^{(0)} \dotplus A^{(1)}$ e que satisfazem as seguintes propriedades:

1. $A^{(0)}A^{(0)} + A^{(1)}A^{(1)} \subset A^{(0)}$;
2. $A^{(1)}A^{(0)} + A^{(0)}A^{(1)} \subset A^{(1)}$.

Com a definição acima, podemos notar que o subespaço $A^{(0)}$ é uma subálgebra de A, enquanto o mesmo não necessariamente ocorre com $A^{(1)}$. De fato, quando $(A^{(1)})^2 = \{0\}$, temos que $A^{(1)}$ é uma subálgebra de A.

Quando A é uma superálgebra, denotamos $A = (A^{(0)}, A^{(1)})$ e diremos que o par $(A^{(0)}, A^{(1)})$ é uma $\mathbb{Z}_2$-graduação, ou simplesmente uma graduação, de A. É importante ressaltar que se $(A^{(0)}, A^{(1)})$ é uma graduação para uma álgebra A, então, para todo $a \in A$, existem $a_0 \in A^{(0)}$ e $a_1 \in A^{(1)}$ tais que $a = a_0 + a_1$.

Os elementos de $A^{(0)} \cup A^{(1)}$ são chamados de elementos homogêneos. Os elementos de $A^{(0)}$ são chamados de elementos homogêneos de grau 0 (ou elementos pares) e os elementos de $A^{(1)}$ são chamados de elementos homogêneos de grau 1 (ou elementos ímpares). Além disso, denominamos $A^{(0)}$ e $A^{(1)}$ como parte par e parte ímpar de A, respectivamente.

Exemplo 4.4.2. Toda álgebra é uma superálgebra. De fato, basta considerarmos a graduação $A = (A, \{0\})$, chamada de graduação trivial.

Exemplo 4.4.3. A álgebra de Grassmann com a decomposição dada na Equação (4.8) é uma superálgebra, que denotaremos por $\mathcal{G}^{gr}$. Esta graduação é chamada de graduação canônica da álgebra de Grassmann.

Exemplo 4.4.4. Considere a álgebra de Grassmann de dimensão finita $\mathcal{G}_2 = \langle 1, e_1, e_2 : e_1e_2 = -e_2e_1\rangle$. Temos que $(F + Fe_1e_2, Fe_1 + Fe_2)$ é uma graduação para $\mathcal{G}_2$. Observe que $(F + Fe_1, Fe_2 + Fe_1e_2)$ e $(F + Fe_2, Fe_1 + Fe_1e_2)$ também são graduações para $\mathcal{G}_2$.

Exemplo 4.4.5. Considere a álgebra $N_3 = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} : a, b, c, d \in F \right\}$. Temos que $(F(e_{11}+e_{22}+e_{33}) + Fe_{12}, Fe_{13} + Fe_{23})$, $(F(e_{11}+e_{22}+e_{33}) + Fe_{23}, Fe_{12}+Fe_{13})$ e $(F(e_{11}+e_{22}+e_{33})+Fe_{13}, Fe_{12}+Fe_{23})$ são graduações de N_3.

Os exemplos acima mostram que uma álgebra pode ter várias graduações. O próximo teorema nos mostra como construir graduações não triviais em uma dada álgebra.

Teorema 4.4.6. *Uma álgebra A é uma superálgebra com graduação não trivial se, e somente se, existe um automorfismo φ de A de ordem 2.*

Demonstração. Suponhamos inicialmente que A seja uma superálgebra com graduação não trivial $(A^{(0)}, A^{(1)})$ e considere a aplicação $\varphi\colon A \to A$ dada por $\varphi(a_0 + a_1) = a_0 - a_1$.

Temos que $\varphi^2(a_0 + a_1) = \varphi(a_0 - a_1) = a_0 + a_1$. Logo, temos que $\varphi = \varphi^{-1}$ e, consequentemente, $\varphi^2 = 1$. Além disso, como A é uma superálgebra, é facil verificar que φ é de fato um automorfismo. Portanto φ é um automorfismo de A de ordem 2, já que $\varphi \neq 1$, pois a graduação é não trivial.

Reciprocamente, suponhamos que exista um automorfismo φ de ordem 2 de A. Podemos definir os seguintes subespaços de A:

$$A^{(0)} = \{a \in A : \varphi(a) = a\} \text{ e } A^{(1)} = \{a \in A : \varphi(a) = -a\}.$$

Inicialmente, observamos que $A^{(1)} \neq \{0\}$, pois φ tem ordem 2. Agora, se $a \in A^{(0)} \cap A^{(1)}$, então $\varphi(a) = a = -a$. Como $\mathrm{char}(F) = 0$, temos que $a = 0$ e, portanto, $A^{(0)} \cap A^{(1)} = \{0\}$. Além disso, se $a \in A$, temos que

$$a = \frac{a + \varphi(a)}{2} + \frac{a - \varphi(a)}{2}.$$

Como φ tem ordem 2, temos que $\frac{a+\varphi(a)}{2} \in A^{(0)}$ e $\frac{a-\varphi(a)}{2} \in A^{(1)}$. Portanto, $A = A^{(0)} \dotplus A^{(1)}$.

Por fim, como φ é um automorfismo, é fácil ver que

$$A^{(0)}A^{(0)} + A^{(1)}A^{(1)} \subset A^{(0)} \text{ e } A^{(0)}A^{(1)} + A^{(1)}A^{(0)} \subset A^{(1)}.$$

Logo, A é uma superálgebra com graduação não trivial, como queríamos demonstrar. □

Observação 4.4.7. Recorde que se φ é um automorfismo de ordem 2, então seus autovalores são iguais a 1 e -1. Logo, no teorema anterior, temos que $A^{(0)}$ é o autoespaço associado ao autovalor 1, e $A^{(1)}$ é o autoespaço associado ao autovalor -1.

Exercício 4.4.8. Determine os automorfismos induzidos pelas graduações dadas nos Exemplos 4.4.4 e 4.4.5.

Exercício 4.4.9. Seja $A = A^{(0)} \dot{+} A^{(1)}$ uma superálgebra. Mostre que:

(a) Se A é unitária, então $1 \in A^{(0)}$.

(b) Se e é um idempotente homogêneo de A, então $e \in A^{(0)}$.

(c) $A^{(1)}$ é uma subálgebra de A se, e somente se, $(A^{(1)})^2 = \{0\}$.

Exercício 4.4.10. Sejam $A = M_n(F)$ e $g = (g_1, \ldots, g_n) \in \mathbb{Z}_2^n$, onde $\mathbb{Z}_2$ denota o grupo aditivo $\{0, 1\}$. Considere os seguintes subespaços de A:

$$A^{(0)} = \operatorname{span}_F\{e_{ij} : g_i + g_j = 0\} \text{ e } A^{(1)} = \operatorname{span}_F\{e_{ij} : g_i + g_j = 1\}.$$

Mostre que:

(a) $(A^{(0)}, A^{(1)})$ é uma graduação de $M_n(F)$.

(b) Os elementos $g_1 = (g_1, \ldots, g_n)$ e $g_2 = (0, g_2 + g_1 \ldots, g_n + g_1)$ induzem a mesma graduação em $M_n(F)$.

A graduação de $M_n(F)$ definida acima é chamada de graduação elementar induzida pelo elemento $g = (g_1, \ldots, g_n) \in \mathbb{Z}_2^n$. Um bom exercício para o leitor é determinar todas as graduações elementares da álgebra $M_2(F)$.

Exercício 4.4.11. Dados inteiros $k \geqslant l \geqslant 0$ tais que $k + l = n$, considere os seguintes subespaços da álgebra $A = M_n(F)$:

$$A^{(0)} = \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} : A \in M_k(F), D \in M_l(F) \right\}$$

e

$$A^{(1)} = \left\{ \begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix} : B \in M_{k \times l}(F), C \in M_{l \times k}(F) \right\}.$$

Mostre que $(A^{(0)}, A^{(1)})$ é uma graduação elementar de $M_n(F)$.

A álgebra de matrizes $M_n(F)$ munida dessa graduação é denotada por $M_{k,l}(F)$. Observe que se $l = 0$, então a graduação é trivial.

Definição 4.4.12. Seja $A = (A^{(0)}, A^{(1)})$ uma superálgebra e B um subespaço (subálgebra, ideal) de A. Dizemos que B possui graduação induzida de A se $(B \cap A^{(0)}, B \cap A^{(1)})$ é uma graduação de B. Neste caso, dizemos que B é um subespaço (subálgebra, ideal) graduado de A.

Exemplo 4.4.13. A álgebra de Grassmann $\mathcal{G}_2 = \langle 1, e_1, e_2 : e_1e_2 = -e_2e_1 \rangle$ de dimensão finita com graduação $(F + Fe_1e_2, Fe_1 + Fe_2)$ é uma subálgebra graduada de $\mathcal{G}$ com graduação canônica.

Exemplo 4.4.14. A álgebra UT_2 com graduação $(Fe_{11} + Fe_{22}, Fe_{12})$ é uma subálgebra graduada de $M_{1,1}(F)$, que será denotada por UT_2^{gr}.

Como consequência do Teorema 4.4.6, temos uma condição necessária e suficiente para que um subespaço possua graduação induzida de uma superálgebra A.

Corolário 4.4.15. *Sejam A uma superálgebra, φ o automorfismo induzido pela graduação de A e B um subespaço (ideal) de A. Então B é um subespaço (ideal) graduado de A se, e somente se, B é φ-invariante, isto é, $B^{\varphi} \subseteq B$.*

Usando o corolário anterior, temos o seguinte.

Lema 4.4.16. *Se A é uma superálgebra de dimensão finita, então seu radical de Jacobson $J(A)$ é um ideal graduado de A.*

Demonstração. Como A tem dimensão finita, temos que $J(A)$ é o maior ideal nilpotente de A. Logo, como φ é um automorfismo, temos que $J(A)^{\varphi}$ é um ideal nilpotente e, consequentemente, $J(A)^{\varphi} \subseteq J(A)$. □

O seguinte exercício será utilizado implicitamente durante todo o texto.

Exercício 4.4.17. Sejam A uma superálgebra e I um ideal graduado de A. Mostre que:

(a) I^n é um ideal graduado do A, para todo $n \geqslant 1$.

(b) A/I tem estrutura de superálgebra.

A graduação em A/I, como no exercício acima, também será chamada de graduação induzida de A.

Definição 4.4.18. Sejam $A = (A^{(0)}, A^{(1)})$ e $B = (B^{(0)}, B^{(1)})$ superálgebras. Dizemos que A e B são isomorfas como superálgebras se existe um isomorfismo de álgebras $f : A \to B$ tal que $f(A^{(0)}) \subseteq B^{(0)}$ e $f(A^{(1)}) \subseteq B^{(1)}$.

Exemplo 4.4.19. Observamos que, para $P \in M_k(F), Q \in M_{k\times l}(F), R \in M_{l\times k}(F)$ e $S \in M_l(F)$, o homomorfismo $\psi : M_{k,l}(F) \to M_{l,k}(F)$ dado por

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix} \mapsto \begin{pmatrix} S & R \\ Q & P \end{pmatrix}$$

é um isomorfismo de superálgebras. Por este motivo, é natural fixar $k \geqslant l$ como fizemos no Exercício 4.4.11.

Exemplo 4.4.20. Podemos ver que a aplicação $\psi : UT_2 \to M_{k,l}(F)$ dada por

$$e_{11} \mapsto e_{11}, \quad e_{22} \mapsto e_{(k+l),(k+l)} \text{ e } e_{12} \mapsto e_{1,(k+l)}$$

é um homomorfismo injetor de álgebras, que preserva a graduação. Logo é um isomorfismo de UT_2 sobre a imagem de ψ. Assim, a superálgebra $M_{k,l}(F)$ contém uma subálgebra graduada que é isomorfa a álgebra UT_2 com graduação $(Fe_{11} + Fe_{22}, Fe_{12})$.

A seguir, vamos estudar a estrutura de superálgebras de dimensão finita.

Definição 4.4.21. Seja A uma superálgebra. Dizemos que A é uma superálgebra simples se $A^2 \neq \{0\}$ e os únicos ideais graduados de A são $\{0\}$ e A.

Exemplo 4.4.22. Se A é uma álgebra simples, então $A = (A^{(0)}, A^{(1)})$ é uma superálgebra simples. Como consequência disto, a superálgebra $M_{k,l}(F)$ é uma superálgebra simples.

Exemplo 4.4.23. Denote por D^{gr} a álgebra $D = F \oplus F$ com graduação $(F(1,1), F(1,-1))$. Afirmamos que D^{gr} é uma superálgebra simples. De fato, por simplicidade, denotando $1 = (1,1)$ e $c = (1,-1)$, temos que $\left\{\frac{1+c}{2}, \frac{1-c}{2}\right\}$ é uma família completa de idempotentes minimais de D e

$$D = F\frac{1+c}{2} \oplus F\frac{1-c}{2}$$

é uma decomposição de Wedderburn de D.

Com isso, temos que os únicos ideais de D são $\{0\}, D, I_1 = F\frac{1+c}{2}$ e $I_2 = F\frac{1-c}{2}$. Seja φ o automorfismo induzido pela graduação em D, e observe que $\varphi(1) = 1$ e $\varphi(c) = -c$. Assim, temos $I_1^{\varphi} = I_2$ e, pelo Corolário 4.4.15, concluímos que os únicos ideais graduados de D são $\{0\}$ e D. Portanto, D^{gr} é uma superálgebra simples, como afirmamos.

Nosso próximo objetivo é apresentar uma classificação das superálgebras simples de dimensão finita sobre corpos algebricamente fechados de característica diferente de 2.

Primeiramente, vamos apresentar um resultado que será útil na demonstração de uma extensão do Teorema de Wedderburn para superálgebras que faremos em seguida.

Lema 4.4.24. *Se A é uma superálgebra simples de dimensão finita, então A é uma álgebra semissimples.*

Demonstração. De fato, pelo Lema 4.4.16, temos que $J(A)$ é um ideal graduado de A. Logo, $J(A) = \{0\}$ ou $J(A) = A$.

Suponhamos que $J(A) \neq \{0\}$. Como $J(A)$ é nilpotente, existe um inteiro $q \geqslant 1$ tal que $J(A)^q \neq \{0\}$ e $J(A)^{q+1} = \{0\}$. Com isso, $J(A)^q$ é um ideal graduado de A e, como A é uma superálgebra simples e $J(A)^q \neq \{0\}$, temos que $A = J(A)^q$. Mas isso implica que $A^2 = (J(A)^q)^2 = \{0\}$, o que é um absurdo de acordo com a definição de superálgebra simples. Portanto, $J(A) = \{0\}$ e, como A tem dimensão finita, é artiniana e pelo Teorema de Wedderburn–Artin temos que A é semissimples. □

Teorema 4.4.25. *Sejam A uma superálgebra de dimensão finita sobre um corpo F de característica diferente de 2 e φ o automorfismo induzido pela graduação. Então:*

1. *Se A é uma superálgebra simples, então ou A é simples ou $A = B \oplus B^\varphi$, para alguma subálgebra simples B de A;*

2. *Se A é semissimples, então A se escreve como uma soma direta finita de superálgebras simples.*

Demonstração. Para demonstrar o item 1, primeiramente observamos que, pelo Lema 4.4.24, temos que A é semissimples. Supondo que A não é simples, pela Exercício 1.3.53, podemos tomar B um ideal simples próprio de A. Se $B^\varphi = B$, então B é um ideal graduado de A e, como A é uma superálgebra simples, temos $A = B$ o que é absurdo. Logo, $B^\varphi \neq B$ e, então, $C = B \oplus B^\varphi$ é um ideal graduado de A, pois φ tem ordem 2. Novamente, como A é uma superálgebra simples, temos que $A = B \oplus B^\varphi$, o que demonstra o item 1.

Agora, se A é uma álgebra semissimples, então $A = B_1 \oplus \cdots \oplus B_m$, onde cada $B_i, i = 1, \ldots, m$, é uma álgebra simples.

Como φ é um automorfismo, temos que, para todo $i = 1, \ldots, m$, B_i^φ é uma álgebra simples. Logo, $B_i^\varphi = B_j$, para algum $1 \leqslant j \leqslant m$. Renomeando as álgebras $B_1, \ldots, B_m$, temos que

$$A = C_{s_1} \oplus \cdots \oplus C_{s_k}$$

onde ou $C_{s_i} = B_j$, com $B_j^\varphi = B_j$, ou $C_{s_i} = B_j \oplus B_j^\varphi$, com $B_j^\varphi \neq B_j$. Claro que se $C_{s_i} = B_j$, já temos que C_{s_i} é simples e quando $C_{s_i} = B_j \oplus B_j^\varphi$, temos que os únicos ideais bilaterais não triviais de C_{s_i} são B_j e B_j^φ os quais não são φ-invariantes e, portanto, C_{s_i} também é simples neste caso. Isto conclui a demonstração do item 2. □

Estamos prontos para apresentar a classificação das superálgebras simples.

Teorema 4.4.26. *Seja A uma superálgebra simples sobre um corpo algebricamente fechado de característica diferente de 2. Então A é isomorfa ou a $M_n(F)$ com graduação trivial, ou a $M_{k,l}(F), k \geqslant l \geqslant 1, k + l = n$, ou a $M_n(F + cF)$, $c^2 = 1$, com graduação $(M_n(F), cM_n(F))$.*

Demonstração. Pelo Teorema 4.4.25, se φ é o automorfismo induzido pela graduação de A, então ou A é simples, ou $A = B \oplus B^\varphi$, para alguma subálgebra simples B de A. Se A é simples, como F é algebricamente fechado, então $A \cong M_n(F)$, para algum $n \geqslant 1$. Note que se $\varphi = 1$, então A é uma superálgebra simples com graduação trivial, logo isomorfa a $M_n(F)$.

Suponha que φ tem ordem 2. Assim, pelo Corolário 1.4.41, existe uma matriz invertível $Y \in M_n(F)$ tal que $\varphi(X) = YXY^{-1}$, para todo $X \in M_n(F)$. Observe que qualquer múltiplo escalar de Y induz o mesmo automorfismo. Como φ tem ordem 2, temos que $XY^2 = \varphi^2(X)Y^2 = Y^2X(Y^{-1})^2Y^2 = Y^2X$. Logo, Y^2 comuta com toda matriz $X \in M_n(F)$ e, portanto, existe $\alpha \in F$, $\alpha \neq 0$, tal que $Y^2 = \alpha I_n$. Como F é algebricamente fechado, existe $\beta \in F$ tal que $\alpha = \beta^2$ e com isso podemos assumir que $Y^2 = I_n$.

Como $Y^2 = I_n$, temos que os autovalores de Y são iguais a 1 ou -1. Logo, Y é conjugada a uma matriz da forma

$$\begin{pmatrix} I_k & 0 \\ 0 & -I_l \end{pmatrix}.$$

Assim, podemos assumir que $Y = \begin{pmatrix} I_k & 0 \\ 0 & -I_l \end{pmatrix}$. Dado $X \in M_n(F)$, escreva

$$X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

onde $A \in M_k(F)$, $B \in M_{k\times l}(F)$, $C \in M_{l\times k}(F)$ e $D \in M_l(F)$. Como $Y = Y^{-1}$, temos que

$$\varphi(X) = YXY = \begin{pmatrix} I_k & 0 \\ 0 & -I_l \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} I_k & 0 \\ 0 & -I_l \end{pmatrix} = \begin{pmatrix} A & -B \\ -C & D \end{pmatrix}.$$

Pela Observação 4.4.7, sabemos que $A^{(0)}$ é o autoespaço associado ao autovalor 1 e $A^{(1)}$ é o autoespaço associado ao autovalor -1, assim temos que A é isomorfa a $M_{k,l}(F)$.

Agora, suponha que A não é simples, isto é, que $A = B \oplus B^{\varphi}$, para alguma subálgebra simples B de A. Como F é algebricamente fechado, temos que $B \cong M_n(F)$, para algum $n \geqslant 1$. Logo, $A \cong M_n(F) \oplus M_n(F)^{\varphi}$. Escreva

$$A = M_1 \oplus M_{-1}$$

onde

$$M_1 = \{(X, X) : X \in M_n(F)\}$$

é o autoespaço associado ao autovalor 1 e

$$M_{-1} = \{(X, -X) : X \in M_n(F)\}$$

é o autoespaço associado ao autovalor -1. Observe que $M_{-1} = cM_1$, onde $c = (I_n, -I_n)$ e $c^2 = (I_n, I_n)$, e que a aplicação $f : M_1 \to M_n(F)$ dada por $f(X, X) = X$ é um isomorfismo de espaço vetoriais. Logo, $M_1 \cong M_n(F)$ e $M_{-1} \cong cM_1 \cong cM_n(F)$ e, portanto, $A \cong M_n(F + cF)$, $c^2 = 1$. O teorema está provado. □

Mostraremos agora que o Teorema de Wedderburn–Malcev pode ser estendido para a classe de superálgebras.

Teorema 4.4.27. *Seja A uma superálgebra unitária de dimensão finita sobre um corpo F de característica zero e φ o automorfismo induzido pela graduação. Então existe uma subálgebra semissimples maximal B de A que é φ-invariante.*

Demonstração. Se $J = J(A) = \{0\}$, então, pelo Teorema 4.4.25, A é semissimples e não há nada o que provar. Suponhamos, então, que $J \neq \{0\}$ e que $J^2 = \{0\}$. Pelo Teorema de Wedderburn–Malcev (Teorema 1.4.62), considere uma subálgebra semissimples maximal B de A e suponha que B não é φ-invariante. Então,

como φ é um automorfismo, B^φ também é uma subálgebra semissimples maximal de A e, novamente pelo Teorema de Wedderburn–Malcev, existe $x \in J$ tal que

$$B = (1+x)^{-1} B^\varphi (1+x).$$

Observe que, como $J^2 = \{0\}$, $(1+x)^{-1} = 1-x$. Logo, a aplicação $f : B \to B$ definida por $f(b) = (1-x)\varphi(b)(1+x)$ é um automorfismo de B e $\varphi(b) = (1+x)\,f(b)(1-x)$. Como $\varphi^2 = 1$ e $J^2 = \{0\}$, temos que

$$\begin{aligned} b &= \varphi((1+x)\,f(b)(1-x)) \\ &= \varphi(1+x)\varphi(f(b))\varphi(1-x) \\ &= (1+\varphi(x))(1+x)\,f^2(b)(1-x)(1-\varphi(x)) \\ &= (1+(x+\varphi(x)))\,f^2(b)(1-(x+\varphi(x)) \\ &= f^2(b) - f^2(b)(x+\varphi(x)) + (x+\varphi(x))\,f^2(b). \end{aligned}$$

Como $B \cap J = \{0\}$, devemos ter $f^2(b) = b$ e $b(x+\varphi(x)) = (x+\varphi(x))b$, para todo $b \in B$. Escreva $x = x^+ + x^-$, onde $x^+ = \frac{x+\varphi(x)}{2}$ e $x^- = \frac{x-\varphi(x)}{2}$. Observe que, como φ tem ordem 2, $\varphi(x^+) = x^+$ e $\varphi(x^-) = -x^-$. Logo, temos que, para todo $b \in B$, $(1+x)b(1-x) = (1+x^-)b(1+x^-)$.

Considere a subálgebra $B' = \left(1+\frac{x^-}{2}\right) B \left(1-\frac{x^-}{2}\right)$. Dado

$$a = \left(1+\frac{x^-}{2}\right) b \left(1-\frac{x^-}{2}\right) \in B'$$

temos que

$$\begin{aligned} \varphi(a) &= \varphi\left(\left(1+\tfrac{x^-}{2}\right) b \left(1+\tfrac{x^-}{2}\right)\right) \\ &= \left(1-\tfrac{x^-}{2}\right)(1+x^-)\,f(b)(1-x^-)\left(1+\tfrac{x^-}{2}\right) \\ &= \left(1+\tfrac{x^-}{2}\right) f(b) \left(1-\tfrac{x^-}{2}\right) \in B'. \end{aligned}$$

Assim, B' é uma subálgebra φ-invariante. Como $B' \cong B$, temos que B' é uma subálgebra semissimples maximal φ-invariante, o que demonstra o teorema caso $J^2 = \{0\}$.

Agora vamos provar o resultado no caso geral, supondo que q seja o índice de nilpotência de J, usando indução sobre $q \geqslant 2$. Já provamos que o teorema vale quando $q = 2$. Agora vamos admitir que seja válido para qualquer álgebra nas hipóteses do teorema cujo índice de nilpotência do radical de Jacobson seja menor do que q.

Temos $J^{q-1} \neq \{0\}$ e J^{q-1} é um ideal graduado de A. Assim, $\bar{A} = A/J^{q-1}$ possui graduação induzida e $J(\bar{A}) = J/J^{q-1}$ com $J(\bar{A})^{q-1} = \{0\}$. Assim,

usando a hipótese de indução, $\bar{A}$ possui uma subálgebra semissimples maximal φ-invariante $\bar{B}$.

Seja $\pi : A \to \bar{A}$ a projeção canônica e seja B uma subálgebra de A tal que $\pi(B) = \bar{B}$. Nesse caso, $J^{q-1} \subset B$ e $\bar{B} = B/J^{q-1}$. Por outro lado, como $\bar{B}$ é semissimples, temos $J(\bar{B}) = \{0\}$ e, assim, $J(B) = J^{q-1}$. Agora notemos que como $\bar{B}$ e J^{q-1} são φ-invariantes, temos que B é φ-invariante. Por outro lado, notamos que não existe subálgebra semissimples φ-invariante S de $\bar{A}$ tal que $B \subsetneq S$, pois se existisse tal álgebra teríamos $\bar{S} = S/J^{q-1}$ uma subálgebra semissimples φ-invariante de $\bar{A}$ com $\bar{B} \subsetneq \bar{S}$, o que não é possível pela maximalidade de $\bar{B}$.

Assim, se B é semissimples, terminamos a demonstração. Caso contrário, observamos que $J(B)^2 = (J^{q-1})^2 = \{0\}$ e, com isso, podemos usar o caso inicial e considerar B' é uma subálgebra semissimples maximal φ-invariante de B. Por fim, observamos que não existe subálgebra semissimples φ-invariante S' de B tal que $B' \subsetneq S'$ e com isso, B' é uma subálgebra semissimples maximal φ-invariante de A. □

Combinando os Teoremas 4.4.25 a 4.4.27, temos o seguinte teorema.

Teorema 4.4.28. *Seja A uma superálgebra de dimensão finita sobre um corpo F algebricamente fechado de característica zero. Então existe uma subálgebra graduada semissimples maximal B de A tal que*

$$A = B \dotplus J(A).$$

Além disso, B é uma soma direta finita de superálgebras simples isomorfas, ou a $M_n(F)$ com graduação trivial, ou a $M_{k,l}(F), k \geqslant l > 0$, ou a $M_n(F + cF), c^2 = 1$, com graduação $(M_n(F), cM_n(F))$.

O estudo das superálgebras por si só é interessante. Na próxima seção, mostraremos por que as superálgebras são importantes na PI-teoria. Para isso, precisamos da seguinte definição. No que segue, consideramos a álgebra de Grassmann $\mathcal{G}$ com graduação canônica $(\mathcal{G}^{(0)}, \mathcal{G}^{(1)})$ dada na Equação (4.8).

Definição 4.4.29. Dada uma superálgebra $A = (A^{(0)}, A^{(1)})$, definimos a envolvente de Grassmann de A por

$$G(A) = (A^{(0)} \otimes \mathcal{G}^{(0)}) \dotplus (A^{(1)} \otimes \mathcal{G}^{(1)}).$$

Observe que a envolvente de Grassmann $G(A)$ de uma superálgebra $A = (A^{(0)}, A^{(1)})$ é uma superálgebra com graduação $(A^{(0)} \otimes \mathcal{G}^{(0)}, A^{(1)} \otimes \mathcal{G}^{(1)})$. Desta forma, obtemos uma maneira de construir novas superálgebras a partir de uma superálgebra dada.

Exemplo 4.4.30. Se A é uma superálgebra com graduação trivial, então $G(A) = A \otimes \mathcal{G}^{(0)}$.

Exemplo 4.4.31. Observamos que a álgebra UT_2 é uma superálgebra com graduação $(Fe_{11} + Fe_{22}, Fe_{12})$. Com essa graduação, temos que

$$G(UT_2) = \begin{pmatrix} \mathcal{G}^{(0)} & \mathcal{G}^{(1)} \\ 0 & \mathcal{G}^{(0)} \end{pmatrix}.$$

Exercícios V ou F da Seção 4.4: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente.

(1) Se A é uma F-superálgebra de dimensão finita, então qualquer subálgebra de A possui graduação induzida de A.

(2) Se A é uma F-superálgebra, então $A^{(0)}$ é uma subálgebra de A que possui graduação induzida de A.

(3) Não existem superálgebras simples de dimensão infinita.

(4) A álgebra F só pode ser vista como superálgebra por meio da graduação trivial.

(5) $M_n(F \oplus cF)$ com graduação $(M_n(F), cM_n(F))$ contém uma subálgebra isomorfa a $F \oplus F$ munida da graduação $(F(1,1), F(1,-1))$ para todo $n \geqslant 1$.

(6) $M_n(F \oplus cF)$ é uma álgebra simples e, portanto, é uma superálgebra simples.

(7) A álgebra $M_n(F \oplus cF)$ com graduação $(M_n(F), cM_n(F))$ e a álgebra

$$C := \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} : A, B \in M_n(F) \right\}$$

com graduação

$$\left(\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}, \begin{pmatrix} B & 0 \\ 0 & -B \end{pmatrix} \right)$$

são superálgebras isomorfas.

4.5 O PI-expoente de uma álgebra

O objetivo maior da seção é estudar o comportamento assintótico da sequência de codimensões de uma PI-álgebra, com ênfase no cálculo do PI-expoente de uma PI-álgebra. Esta será uma seção expositiva, isto é, as provas dos teoremas enunciados não serão apresentadas, pois fogem do escopo deste livro. As referências para as demonstrações correspondentes estão indicadas durante o texto. Ao longo desta seção, F denotará um corpo de característica zero e todas as álgebras serão tomadas sobre corpos de característica zero.

Na seção anterior definimos a envolvente de Grassmann de uma superálgebra. É importante ressaltar que a envolvente de Grassmann $G(A)$ de uma superálgebra A é uma álgebra. Logo, podemos procurar informações sobre $\mathrm{Id}(G(A))$.

A importância da envolvente de Grassmann é destacada no seguinte teorema que foi demonstrado por Kemer (1991).

Teorema 4.5.1. *Seja $\mathcal{V}$ uma variedade de álgebras não trivial sobre um corpo F de característica zero. Então existe uma superálgebra B de dimensão finita sobre F tal que $\mathcal{V} = \mathrm{var}(G(B))$.*

Este teorema é de grande importância na PI-teoria, que nos mostra que toda variedade de álgebras não trivial é gerada pela envolvente de Grassmann de uma superálgebra de dimensão finita. Observamos que o teorema garante a existência de tal superálgebra, mas, em geral, determiná-la não é uma tarefa fácil.

Exemplo 4.5.2. Seja $\mathcal{V}$ a variedade determinada por $\{[x_1, x_2, x_3]\}$. Sabemos, pelo Teorema 4.3.5, que $\mathrm{Id}(\mathcal{G}) = \langle [x_1, x_2, x_3] \rangle_T$.

Assim, ao considerarmos $\mathcal{G}$ com graduação trivial, temos que $G(\mathcal{G}) = \mathcal{G} \otimes \mathcal{G}^{(0)}$ e, como $\mathcal{G}^{(0)}$ é uma álgebra comutativa, temos, pelo Proposição 4.1.5, que $\mathrm{Id}(G(\mathcal{G})) = \mathrm{Id}(\mathcal{G}) = \mathrm{Id}(\mathcal{V})$. Como sabemos, $\mathcal{G}$ não tem dimensão finita e, assim, não está nas condições do Teorema 4.5.1, ou seja, $\mathcal{G}$ não é a superálgebra procurada na conclusão deste teorema.

Por outro lado, consideremos $B = F \oplus F$ com graduação $(F(1,1), F(1,-1))$. Deste modo, B é superálgebra de dimensão finita tal que

$$G(B) = (F(1,1) \otimes \mathcal{G}^{(0)}) \dot{+} (F(1,-1) \otimes \mathcal{G}^{(1)}) \cong (F \otimes \mathcal{G}^{(0)}) \dot{+} (F \otimes \mathcal{G}^{(1)}) \cong \mathcal{G}$$

ou seja, $\mathcal{V} = \mathrm{var}(G(F \oplus F)) = \mathrm{var}(\mathcal{G})$.

Assim, pelo Teorema 4.5.1, para estudarmos T-ideais e a sequência de codimensões de uma variedade, basta estudarmos os T-ideais e a sequência de codimensões de envolventes de Grassmann de superálgebras de dimensão finita.

Feitas essas considerações, agora estamos interessados em estudar o comportamento assintótico da sequência de codimensões de uma PI-álgebra. Mais especificamente, vamos estudar o chamado PI-expoente, ou simplesmente expoente, de uma PI-álgebra.

Um dos primeiros resultados sobre o comportamento assintótico da sequência de codimensões foi o Teorema 4.2.8, que afirma que se A é uma PI-álgebra, então $c_n(A)$ é limitada exponencialmente. Recorde que se A é uma álgebra nilpotente, então existe $m \geqslant 1$ tal que $c_n(A) = 0$, para todo $n > m$. Portanto, se A é uma PI-álgebra não nilpotente, então existe uma constante $a > 0$ tal que

$$1 \leqslant c_n(A) \leqslant a^n.$$

Com isso, temos que a sequência $\{\sqrt[n]{c_n(A)}\}_{n\geqslant 1}$ é limitada superiormente e inferiormente e assim, podemos considerar $\limsup\{\sqrt[n]{c_n(A)}\}_{n\geqslant 1}$ e também $\liminf\{\sqrt[n]{c_n(A)}\}_{n\geqslant 1}$.

Logo, para uma PI-álgebra A, temos a seguinte definição.

Definição 4.5.3. Se A é uma PI-álgebra, então

$$\overline{\exp}(A) := \limsup_{n\to\infty} \sqrt[n]{c_n(A)} \quad \text{e} \quad \underline{\exp}(A) := \liminf_{n\to\infty} \sqrt[n]{c_n(A)}$$

são chamados de PI-expoente superior e PI-expoente inferior de A, respectivamente. Caso $\overline{\exp}(A) = \underline{\exp}(A)$, temos que $\{\sqrt[n]{c_n(A)}\}_{n\geqslant 1}$ possui limite e definimos o PI-expoente de A, ou simplesmente o expoente de A, por:

$$\exp(A) = \lim_{n\to\infty} \sqrt[n]{c_n(A)}.$$

No caso em que $\mathcal{V} = \operatorname{var}(A)$, definimos

$$\exp(\mathcal{V}) := \exp(A).$$

Destacaremos três exemplos para fixar as ideias.

Exemplo 4.5.4. Se A é uma álgebra nilpotente, então $\exp(A) = 0$.

Exemplo 4.5.5. Se A é uma álgebra comutativa não nilpotente, então $\exp(A) = 1$.

Exemplo 4.5.6. Considere as álgebras $\mathcal{G}$ e $UT_2(F)$. Pelos Teoremas 4.3.2 e 4.3.5, temos que

$$c_n(UT_2(F)) = 2^{n-1}(n-2) + 2 \text{ e } c_n(\mathcal{G}) = 2^{n-1}.$$

Portanto,

$$\exp(UT_2(F)) = \lim_{n\to\infty} \sqrt[n]{2^{n-1}(n-2)+2} = 2$$

e

$$\exp(\mathcal{G}) = \lim_{n\to\infty} \sqrt[n]{2^{n-1}} = 2.$$

Com esses três exemplos em mente, na década de 1980, Amitsur fez a seguinte conjectura.

Conjectura 4.5.7 (Amitsur)**.** *Para toda PI-álgebra A,* $\exp(A)$ *existe e é um inteiro não negativo.*

Um pouco mais tarde, motivado pelo Teorema 4.3.8, Regev conjecturou o seguinte.

Conjectura 4.5.8 (Regev)**.** *Para toda PI-álgebra A,*

$$c_n(A) \simeq Cn^t q^n$$

onde q é um inteiro não negativo, $C \in \frac{1}{2}\mathbb{Z} = \left\{\frac{k}{2} : k \in \mathbb{Z}\right\} \subseteq \mathbb{Q}$ e $t \in \mathbb{Q}[\sqrt{2\pi}, \sqrt{b}]$, para algum $0 < b \in \mathbb{Z}$.

Se $c_n(A) \simeq Cn^t q^n$, então Cn^t é chamada de parte racional de $c_n(A)$ e q^n é chamada de parte exponencial de $c_n(A)$.

Após feitas estas conjecturas, vários matemáticos se empenharam para demonstrá-las. Giambruno e Zaicev (1999) provaram a conjectura de Amitsur, para o caso em que F é um corpo de característica zero, e obtiveram avanços sobre a conjectura de Regev.

Primeiramente, eles provaram o seguinte resultado a respeito da envolvente de Grassmann de uma superálgebra de dimensão finita sobre um corpo algebricamente fechado de característica zero.

Teorema 4.5.9. *Seja B uma superálgebra de dimensão finita sobre um corpo algebricamente fechado de característica zero. Então existe um inteiro não negativo q e constantes C_1, C_2, r_1, r_2 tais que $C_1 > 0$ e*

$$C_1 n^{r_1} q^n \leqslant c_n(G(B)) \leqslant C_2 n^{r_2} q^n. \tag{4.9}$$

Em particular, temos

$$\exp(G(B)) = q.$$

Pela demonstração desse teorema, os autores mostraram que $C_1 n^{r_1}$ e $C_2 n^{r_2}$ são polinômios de Laurent, não necessariamente do mesmo grau.

Como corolário do Teorema 4.5.9, os autores provaram a conjectura de Amitsur. Veremos que a hipótese de F ser algebricamente fechado pode ser retirada no enunciado do teorema.

Corolário 4.5.10. *Seja A uma PI-álgebra. Então existe um inteiro não negativo q e constantes C_1, C_2, r_1, r_2 tais que $C_1 > 0$ e*

$$C_1 n^{r_1} q^n \leqslant c_n(A) \leqslant C_2 n^{r_2} q^n,$$

Consequentemente $\exp(A)$ *existe e é um inteiro não negativo.*

Demonstração. Pela Proposição 4.2.15, sabemos que $c_n^F(A) = c_n^{\overline{F}}(A \otimes \overline{F})$ para todo $n \geqslant 1$, onde $\overline{F}$ é o fecho algébrico de F. Desta forma, podemos supor sem perda de generalidade que F é um corpo algebricamente fechado. Considere $\mathcal{V} = \text{var}(A)$. Pelo Teorema 4.5.1, sabemos que existe uma superálgebra de dimensão finita B tal que $\text{var}(A) = \text{var}(G(B))$, ou seja, $c_n(G(B)) = c_n(A)$ para todo $n \geqslant 1$. Assim, pelo Teorema 4.5.9, o resultado está provado. □

Berele e Regev (2008) demonstraram um caso particular da Conjectura 4.5.8.

Teorema 4.5.11. *Seja A uma PI-álgebra unitária que satisfaz uma identidade de Capelli. Então existe uma constante $C \geqslant 0$ tal que*

$$c_n(A) \simeq C n^t q^n$$

onde q é um inteiro não negativo e $t \in \frac{1}{2}\mathbb{Z}$. Além disso, se $c_n(A)$ é eventualmente não decrescente, isto é, é não decrescente para n suficientemente grande, então existem constantes C_1, C_2 tais que $C_1 > 0$ e

$$C_1 n^t q^n \leqslant c_n(A) \leqslant C_2 n^t q^n.$$

Giambruno e Zaicev (2014) estabeleceram o seguinte teorema.

Teorema 4.5.12. *Para toda PI-álgebra A, temos que a sequência de codimensões $\{c_n(A)\}_{n \geqslant 1}$ é eventualmente não decrescente, isto é, $c_{n+1}(A) \geqslant c_n(A)$, para todo n suficientemente grande.*

Como consequência desse teorema, os autores estenderam o Teorema 4.5.11 e concluíram o seguinte.

Teorema 4.5.13. *Para toda PI-álgebra, existem* $t \in \frac{1}{2}\mathbb{Z}$, $C_1, C_2 > 0$ *tais que*

$$C_1 n^t (\exp(A))^n \leqslant c_n(A) \leqslant C_2 n^t (\exp(A))^n$$

para todo $n \geqslant 1$. *Assim,*

$$\lim_{n\to\infty} \log_n \frac{c_n(A)}{(\exp(A))^n}$$

existe e pertence a $\frac{1}{2}\mathbb{Z}$.

Esse teorema nos permite atribuir a cada T-ideal da álgebra livre dois parâmetros: o expoente e o limite acima, que nos permite distinguir T-ideais com o mesmo expoente.

Exercício 4.5.14. Mostre que se $A_1, \ldots, A_m$ são PI-álgebras, então

$$\exp(A_1 \oplus \cdots \oplus A_m) = \max_{1\leqslant i\leqslant m} \{\exp(A_i)\}.$$

Giambruno e Zaicev (1999) exibiram uma maneira de calcular o expoente de uma álgebra, como veremos a seguir.

Sejam $\mathcal{V}$ uma variedade de PI-álgebras e B uma F-superálgebra de dimensão finita tal que $\mathcal{V} = G(B)$. Como estamos estudando questões relativas à sequência de codimensões de $\mathcal{V}$, podemos supor que F é algebricamente fechado.

Considere $B = B_1 \oplus \cdots \oplus B_n \dotplus J$ uma decomposição de Wedderburn–Malcev de B, onde cada B_i é uma superálgebra simples de dimensão finita e $J = J(B)$ é o radical de Jacobson de B. Considere todos os produtos da forma

$$B'_1 J B'_2 J \cdots J B'_r \neq \{0\} \tag{4.10}$$

onde, para $r = 1, \ldots, n$, $B'_1, \ldots, B'_r$ são superálgebras simples distintas tomadas no conjunto $\{B_1, \ldots, B_n\}$. Se $r = 1$, então $B'_1 = B_i$, para algum $i = 1, \ldots, n$. Defina

$$q = \max \dim_F (B'_1 \oplus \cdots \oplus B'_r)$$

onde as superálgebras $B'_1, \ldots, B'_r$ satisfazem Equação (4.10).

Giambruno e Zaicev mostraram o seguinte.

Teorema 4.5.15. $\exp(G(B)) = q$.

Exemplo 4.5.16. Pelo Exemplo 4.5.2, sabemos que $\text{var}(\mathcal{G}) = \text{var}(G(F \oplus F))$ e que $F \oplus F$ é uma superálgebra simples. Portanto, $\exp(\mathcal{G}) = \dim_F(F \oplus F) = 2$.

Agora, se A é uma álgebra, então A pode ser vista como uma superálgebra com graduação trivial $(A, \{0\})$ e $G(A) = \mathcal{G}^{(0)} \otimes A \sim_{PI} A$, já que $\mathcal{G}^{(0)}$ é uma álgebra comutativa e pela Proposição 4.1.5 toda identidade de A é estável.

Seja A uma álgebra de dimensão finita sobre um corpo algebricamente fechado F e considere uma decomposição de Wedderburn–Malcev de A

$$A = A_1 \oplus \cdots \oplus A_m \dot{+} J(A)$$

onde $A_i \cong M_{n_i}(F)$, para todo $i = 1, \ldots, m$, é uma álgebra simples. Considere todos os produtos possíveis da forma

$$B_1 J B_2 J \cdots J B_r \neq \{0\} \tag{4.11}$$

onde $B_1, \ldots, B_r$ são subálgebras distintas tomadas em $\{A_1, \ldots, A_m\}, r = 1, \ldots, n$ e $J = J(A)$. Se $r = 1$, então $B_1 = A_i$, para algum $1 \leqslant i \leqslant m$. Defina

$$q = \max\{\dim_F(B_1 \oplus \cdots \oplus B_r) : B_1 J B_2 \ldots J B_r \neq 0\}.$$

Como corolário do Teorema 4.5.15, temos o seguinte teorema.

Teorema 4.5.17. *Se A é uma álgebra de dimensão finita sobre um corpo algebricamente fechado de característica zero, então* $\exp(A) = q$. *Consequentemente,* $\exp(A) \leqslant \dim_F(A)$.

Nos exemplos a seguir, F é um corpo algebricamente fechado de característica zero.

Exemplo 4.5.18. Toda álgebra de dimensão finita do tipo $A = F \dot{+} J(A)$ tem expoente igual a 1.

Exemplo 4.5.19. Considere a seguinte decomposição de Wedderburn–Malcev da álgebra UT_2:

$$UT_2 = (Fe_{11} \oplus Fe_{22}) \dot{+} Fe_{12}.$$

Nessa decomposição, temos que $A_1 = Fe_{11} \cong F$, $A_2 = Fe_{22} \cong F$ e $J = J(UT_2) = Fe_{12}$. Dessa forma, obtemos que $A_1 J A_2 \neq \{0\}$. Portanto, $\exp(UT_2) = \dim_F(A_1 \oplus A_2) = 2$.

Exemplo 4.5.20. Considere a seguinte subálgebra de UT_4:

$$M = \left\{ \begin{pmatrix} a & d & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & b & e \\ 0 & 0 & 0 & c \end{pmatrix} : a, b, c, d, e \in F \right\}.$$

Temos que a decomposição de Wedderburn–Malcev de M é $M = A_1 \oplus A_2 \oplus A_3 + J(M)$, onde $A_1 = Fe_{11}$, $A_2 = F(e_{22} + e_{33})$, $A_3 = Fe_{44}$ e $J = J(M) = Fe_{12} \oplus Fe_{34}$. Observe que $A_{i_1} J A_{i_2} J A_{i_3} = \{0\}$, mas $A_1 J A_2 \neq \{0\}$. Portanto $\exp(M) = \dim_F(A_1 \oplus A_2) = 2$.

Uma importante classe de álgebras de dimensão finita é dada pela álgebra das matrizes bloco triangulares superiores

$$UT(d_1, \ldots, d_n) = \begin{pmatrix} M_{d_1}(F) & B_{12} & \cdots & B_{1m} \\ 0 & M_{d_2}(F) & \cdots & B_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M_{d_n}(F) \end{pmatrix}$$

onde todas as B_{ij}'s são matrizes retangulares sobre F de tamanhos apropriados. É claro que se $d_1 = \cdots = d_n = 1$, então $UT(1, \ldots, 1) = UT_n$.

Exercício 4.5.21. Mostre que $\exp(UT(d_1, \ldots, d_n)) = d_1^2 + \cdots + d_n^2$. Conclua que para cada inteiro $k \geqslant 1$, existe uma álgebra A tal que $\exp(A) = k$.

No Teorema 4.5.17, vimos que se A é uma álgebra de dimensão finita, então $\exp(A) \leqslant \dim_F(A)$. O teorema a seguir nos mostra quando temos a igualdade.

Teorema 4.5.22. *Seja A uma F-álgebra de dimensão finita. Então:*

1. *Se A é semissimples, então $\exp(A) = \dim_{Z(B)}(B)$, onde B é uma subálgebra simples de A de maior dimensão sobre seu centro $Z(B)$. Em particular, se A é simples, então $\exp(A) = \dim_{Z(A)}(A)$.*

2. *A é uma álgebra central simples sobre F se, e somente se, $\exp(A) = \dim_F(A)$.*

Exercícios V ou F da Seção 4.5: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, A e B representam F-álgebras.

(1) Se $B \in \text{var}(A)$, então $\exp(B) \geqslant \exp(A)$.

(2) $\exp(A \oplus B) \leqslant \exp(A) + \exp(B)$.

(3) Se $\exp(A) \leqslant 0$, então A é nilpotente.

(4) Se A é nilpotente e B é comutativa, então $\exp(A) \leqslant \exp(B)$.

(5) É verdade que $\exp(M_n(F)) = n^2$.

(6) É falso que $\exp(UT_n) = n$.

5 Variedades de crescimento polinomial

Neste capítulo, apresentaremos resultados que caracterizam variedades de crescimento polinomial das codimensões. O primeiro deles foi demonstrado por Kemer, sendo considerado um dos principais teoremas da PI-teoria, e evidencia a importância da álgebra de Grassmann de dimensão infinita $\mathcal{G}$ e da álgebra de matrizes 2×2 triangulares superiores UT_2.

Para apresentar uma segunda caracterização, introduziremos a noção de S_n-cocaracter de uma variedade $\mathcal{V}$ e as propriedades de sua decomposição em S_n-caracteres irredutíveis. Esta segunda caracterização mostra uma restrição no tipo de diagramas de Young correspondentes aos S_n-caracteres irredutíveis que aparecem com multiplicidade não nula na decomposição do cocaracter de $\mathcal{V}$, quando esta variedade tem crescimento polinomial.

Por fim, outras caracterizações serão apresentadas, dando-nos uma série de alternativas de comprovação de crescimento polinomial, dependendo da situação trabalhada.

5.1 A álgebra de Grassmann e polinômios standard

Nesta seção, estaremos interessados em determinar condições necessárias e suficientes para que uma variedade seja gerada por uma álgebra de dimensão finita.

Quando todas as álgebras em uma variedade $\mathcal{V}$ satisfazem um polinômio f, dizemos que a variedade satisfaz f. Observamos que se uma variedade é gerada por uma álgebra de dimensão finita, então, de acordo com o Corolário 3.2.11, esta satisfaz um polinômio standard.

Por outro lado, se uma variedade satisfaz um polinômio standard, então a álgebra de Grassmann $\mathcal{G}$ não pertence a esta variedade, pois não satisfaz polinômios deste tipo, conforme visto no Exercício 3.2.18.

Para obter uma caracterização de variedades geradas por álgebras de dimensão finita, vamos trabalhar com a relação entre as afirmações descritas acima. Mais especificamente, nesta seção, vamos provar o seguinte teorema.

Teorema 5.1.1. *Seja $\mathcal{V}$ uma variedade de álgebras sobre um corpo F de característica zero. As seguintes afirmações são equivalentes:*

1. *$\mathcal{V}$ é gerada por uma F-álgebra de dimensão finita.*
2. *$\mathcal{V}$ satisfaz um polinômio standard.*
3. *$\mathcal{G} \notin \mathcal{V}$.*

A demonstração será feita por etapas, e inicialmente vamos provar as equivalências entre os itens 1 e 2. Para isto, vamos usar o conceito de envolvente de Grassmann, dado na Definição 4.4.29, e suas propriedades, como a que segue no próximo lema.

Lema 5.1.2. *Seja $B = B^{(0)} \dot{+} B^{(1)}$ uma F-superálgebra e consideremos $\overline{F}$ o fecho algébrico de F. Definindo $\overline{B} = B \otimes \overline{F}$ e $\overline{\mathcal{G}} = \mathcal{G} \otimes \overline{F}$, temos que valem os seguintes itens.*

1. *$B^{(1)}$ gera um ideal nilpotente em B se, e somente se, $B^{(1)} \otimes \overline{F}$ gera um ideal nilpotente em $\overline{B}$.*
2. *A envolvente de Grassmann $G(B)$ satisfaz uma identidade standard se, e somente se, a envolvente de Grassmann $\overline{G}(\overline{B})$ satisfaz uma identidade standard.*

Demonstração. Os itens são facilmente provados, bastando observar que $\overline{B}$ é uma superálgebra com graduação $(B^{(0)} \otimes \overline{F}, B^{(1)} \otimes \overline{F})$, e

$$\overline{G}(\overline{B}) = ((B^{(0)} \otimes \overline{F}) \otimes (\mathcal{G}^{(0)} \otimes \overline{F})) \oplus ((B^{(1)} \otimes \overline{F}) \otimes (\mathcal{G}^{(1)} \otimes \overline{F})).$$

□

Observação 5.1.3. Se $B = B^{(0)} \dotplus B^{(1)}$ é uma F-superálgebra tal que $G(B)$ satisfaz uma identidade standard, e I é um ideal graduado de B, então $G(B/I)$ também satisfaz uma identidade standard.

Com o próximo resultado, vemos que a existência de uma identidade polinomial da envolvente de Grassmann $G(B)$ de uma superálgebra de dimensão finita $B = B^{(0)} \dotplus B^{(1)}$ implica em propriedades para o ideal gerado por $B^{(1)}$.

Proposição 5.1.4. *Seja $B = B^{(0)} \dotplus B^{(1)}$ uma F-superálgebra de dimensão finita, e suponha que sua envolvente de Grassmann $G(B)$ satisfaz um polinômio standard. Então o ideal gerado por $B^{(1)}$ é nilpotente.*

Demonstração. Sob as hipóteses desta proposição, de acordo com o Lema 5.1.2, podemos supor que F é um corpo algebricamente fechado. Denotando por J o radical de Jacobson de B, notamos que se $B^{(1)} \subset J$ não há nada para fazer, pois já sabemos que J é nilpotente. Assim, vamos supor que $B^{(1)}$ não está contido em J.

Pelo Teorema 4.4.25, o radical de Jacobson J é um ideal graduado de B e, assim, B/J tem graduação induzida de B. Além disso, $(B/J)^{(1)} \neq \{0\}$, já que $B^{(1)} \not\subset J$. Pela Observação 5.1.3, temos que $G(B/J)$ satisfaz uma identidade standard. Dessa forma, B/J e B obedecem as mesmas hipóteses do lema e assim podemos supor, sem perda de generalidade, que $J = \{0\}$ e $B^{(1)} \neq \{0\}$. Agora, usando o Teorema 4.4.25, podemos escrever B como soma direta de F-superálgebras simples A_i cada uma com graduação induzida de B:

$$B = A_1 \oplus \cdots \oplus A_s. \tag{5.1}$$

Pelo Teorema 4.4.26, temos que cada superálgebra simples A_i é isomorfa a uma das seguintes F-superálgebras:

$$M_n(F) \text{ ou } M_{k,l}(F) \text{ ou } M_n(F \oplus cF), \text{ onde } c^2 = 1.$$

Como $B^{(1)} \neq 0$, alguma F-superálgebra simples A_j na Equação (5.1) é necessariamente isomorfa a $M_{k,l}(F)$ ou $M_n(F \oplus cF)$. No primeiro caso, A_j contém uma subálgebra isomorfa a:

$$F(e_{11} + e_{22}) \dotplus F(e_{12} + e_{21}).$$

Assim, $G(B)$ contém uma subálgebra isomorfa a:

$$(F(e_{11} + e_{22}) \otimes \mathcal{G}^{(0)}) \dotplus (F(e_{12} + e_{21}) \otimes \mathcal{G}^{(1)}). \tag{5.2}$$

A F-álgebra na Equação (5.2) é isomorfa a $\mathcal{G}$, pois a aplicação abaixo é um isomorfismo de F-álgebras:

$$\begin{array}{rccc} \varphi: & \mathcal{G} & \to & (F(e_{11}+e_{22})\otimes\mathcal{G}^{(0)}) \dot{+} (F(e_{12}+e_{21})\otimes\mathcal{G}^{(1)}) \\ & g^{(0)}+g^{(1)} & \mapsto & (e_{11}+e_{22})\otimes g^{(0)} + (e_{12}+e_{21})\otimes g^{(1)}. \end{array}$$

No segundo caso, sabemos que A_j tem uma subálgebra isomorfa a $F \oplus cF$ e, assim, $G(B)$ contém uma subálgebra isomorfa a:

$$(F \otimes \mathcal{G}^{(0)}) \dot{+} (cF \otimes \mathcal{G}^{(1)}). \tag{5.3}$$

Notemos que a F-álgebra na Equação (5.3) é isomorfa a $\mathcal{G}$, pois a aplicação abaixo é um isomorfismo de álgebras:

$$\begin{array}{rccc} \beta: & \mathcal{G} & \to & (F \otimes \mathcal{G}^{(0)}) \dot{+} (cF \otimes \mathcal{G}^{(1)}) \\ & g^{(0)}+g^{(1)} & \mapsto & 1 \otimes g^{(0)} + c \otimes g^{(1)}. \end{array}$$

Em qualquer um dos casos, mostramos que $G(B)$ contém uma F-subálgebra isomorfa a $\mathcal{G}$. Como $\mathcal{G}$ não satisfaz uma identidade standard, segue que $G(B)$ também não satisfaz. Essa contradição mostra que é um absurdo supor que $B^{(1)}$ não está contido em J e, assim, o ideal gerado por $B^{(1)}$ é nilpotente. □

O resultado a seguir mostra que, sob certas condições, particulares propriedades de uma superálgebra $B = B^{(0)} \dot{+} B^{(1)}$ podem ser transferidas para sua envolvente de Grassmann $G(B)$.

Lema 5.1.5. *Seja $B = B^{(0)} \dot{+} B^{(1)}$ uma F-superálgebra de dimensão finita tal que o ideal I_B gerado por $B^{(1)}$ em B é nilpotente. Então $B^{(1)} \otimes \mathcal{G}^{(1)}$ gera um ideal nilpotente em $G(B)$.*

Demonstração. Suponhamos que o índice de nilpotência de I_B seja r. Para provar o lema, tomamos $b_1, \ldots, b_r \in I_B$ e observamos que

$$(b_1 \otimes e_{i_1}) \cdots (b_r \otimes e_{i_r}) = b_1 \cdots b_r \otimes e_{i_1} \cdots e_{i_r} = 0 \otimes e_{i_1} \cdots e_{i_r}$$

para quaisquer $e_{i_1}, \ldots, e_{i_r} \in \mathcal{G}^{(1)}$. Desde que $0 \otimes e_{i_1} \cdots e_{i_1} = 0$, teremos

$$(b_1 \otimes e_{i_1}) \cdots (b_r \otimes e_{i_r}) = 0$$

e isto implica que o ideal gerado por $B^{(1)} \otimes \mathcal{G}^{(1)}$ é nilpotente de índice $m \leqslant r$. □

Antes de provar o próximo teorema, vamos fazer, através de um exemplo, uma observação que será usada na demonstração. Consideremos o polinômio multilinear

$$f(x_1, x_2, x_3) = x_2x_1x_3 + x_1x_3x_2 \in F\langle X\rangle$$

e tomemos elementos $a_1 = b_1 \otimes g_1$, $a_2 = b_2 \otimes g_2$ e $a_3 = b_3 \otimes g_3$ na envolvente de Grassmann $G(B)$ de uma superálgebra B, onde $b_1, b_2, b_3 \in B$ e $g_1 \in \mathcal{G}^{(0)}$ e $g_2, g_3 \in \mathcal{G}^{(1)}$. Ao fazer a avaliação $f(a_1, a_2, a_3)$, obtemos:

$$b_2b_1b_3 \otimes g_2g_1g_3 + b_1b_3b_2 \otimes g_1g_3g_2 = b_2b_1b_3 \otimes g_1g_2g_3 - b_1b_3b_2 \otimes g_1g_2g_3$$

ou seja, $f(a_1, a_2, a_3) = (b_2b_1b_3 - b_1b_3b_2) \otimes g_1g_2g_3$.

Com isso, podemos dizer que $f(a_1, a_2, a_3) = f'(b_1, b_2, b_3) \otimes g_1g_2g_3$, onde f' é um polinômio multilinear.

Agora estamos aptos a provar as equivalências entre os itens 1 e 2 do Teorema 5.1.1.

Teorema 5.1.6. *Uma variedade de álgebras $\mathcal{V}$ é gerada por uma F-álgebra de dimensão finita A se, e somente se, $\mathcal{V}$ satisfaz uma identidade standard.*

Demonstração. Obviamente nada precisa ser feito no caso em que $\mathcal{V} = \text{var}(0)$. Desta forma, consideramos $\mathcal{V}$ uma variedade não trivial e suponhamos que $\mathcal{V} = \text{var}(A)$ para alguma F-álgebra arbitrária de dimensão finita A, digamos $\dim_F(A) = d$.

Deste modo, St_{d+1} é uma identidade de A e, portanto, qualquer F-álgebra em $\mathcal{V}$ satisfaz este polinômio standard. Com isso, $\mathcal{V}$ satisfaz uma identidade standard, como queríamos.

Para a recíproca, vamos supor que $\mathcal{V}$ satisfaça uma identidade standard. Pelo Teorema 4.5.1, sabemos que existe uma F-superálgebra de dimensão finita $B = B^{(0)} \dotplus B^{(1)}$ tal que $\mathcal{V} = \text{var}(G(B))$. Como B tem dimensão finita e $G(B)$ satisfaz uma identidade standard, pela Proposição 5.1.4 temos que o ideal gerado por $B^{(1)}$ em B é nilpotente. Portanto, pelo Lema 5.1.5 o ideal gerado por $B^{(1)} \otimes \mathcal{G}^{(1)}$ em $G(B)$ também é nilpotente, digamos de índice m.

Sejam $\mathcal{B} = \{b_1, \cdots, b_k\}$ uma base de $B^{(1)}$ e $t = \max\{k, m\}$. Considere A a subálgebra de $G(B)$ gerada por:

$$B^{(0)} \otimes 1 \text{ e } \{b_i \otimes e_j : 1 \leqslant i \leqslant k \text{ e } 1 \leqslant j \leqslant t\}$$

onde $e_1, e_2, \ldots$ denotam os elementos básicos de $\mathcal{G}^{(1)}$. Observamos que A é uma subálgebra graduada de $G(B)$, onde

$$A^{(0)} = B^{(0)} \otimes 1 \text{ e } A^{(1)} = \text{span}\{b_i \otimes e_j : 1 \leqslant i \leqslant k \text{ e } 1 \leqslant j \leqslant t\}$$

Assim, obtemos $\mathrm{Id}(G(B)) \subset \mathrm{Id}(A)$. Note ainda que A tem dimensão finita, portanto se provarmos que $\mathrm{Id}(A) = \mathrm{Id}(G(B))$, teremos que $\mathcal{V} = \mathrm{var}(A)$ o que prova a segunda parte do teorema.

Para provarmos a inclusão contrária entre os T-ideais, vamos considerar um polinômio $f = f(x_1, \ldots, x_n)$ de grau n tal que $f \notin \mathrm{Id}(G(B))$, o qual podemos assumir ser multilinear. Assim, a fim de simplificar a notação, podemos dizer que existem $\widetilde{b}_1, \ldots, \widetilde{b}_s \in B^{(0)}$, $g_1, \ldots, g_s \in \mathcal{G}^{(0)}$, $b_{i_1}, \ldots, b_{i_{n-s}} \in \mathcal{B}$ e $h_1, \ldots, h_{n-s} \in \mathcal{G}^{(1)}$ tais que:

$$f(\widetilde{b}_1 \otimes g_1, \ldots, \widetilde{b}_s \otimes g_s, b_{i_1} \otimes h_1, \ldots, b_{i_{n-s}} \otimes h_{n-s}) \neq 0 \text{ em } G(B).$$

Observe que é necessário ter $n-s < m \leqslant t$, pois o ideal gerado por $B^{(1)} \otimes \mathcal{G}^{(1)}$ tem índice de nilpotência m em $G(B)$. Por outro lado, como $g_1, \ldots, g_s \in \mathcal{G}^{(0)}$ e $h_1, \ldots, h_{n-s} \in \mathcal{G}^{(1)}$, usando a observação feita no exemplo antes do enunciado deste teorema, podemos reescrever

$$f(\widetilde{b}_1 \otimes g_1, \ldots, \widetilde{b}_s \otimes g_s, b_{i_1} \otimes h_1, \ldots, b_{i_{n-s}} \otimes h_{n-s}) =$$

$$f'(\widetilde{b}_1, \ldots, \widetilde{b}_s, b_{i_1}, \ldots, b_{i_{n-s}}) \otimes g_1 \cdots g_s h_1 \cdots h_{n-s} \neq 0$$

onde f' é um polinômio multilinear, $0 \neq f'(\widetilde{b}_1, \ldots, \widetilde{b}_s, b_{i_1}, \ldots, b_{i_{n-s}}) \in B$ e o elemento $g_1 \cdots g_s h_1 \cdots h_{n-s} \in \mathcal{G}$ é não nulo.

Dessa forma, podemos avaliar f nos elementos de A dados por $\widetilde{b}_1 \otimes 1, \ldots, \widetilde{b}_s \otimes 1 \in A^{(0)}$ e $b_{i_1} \otimes e_1, \ldots, b_{i_{n-s}} \otimes e_{n-s} \in A^{(1)}$ e obtemos

$$f(\widetilde{b}_1 \otimes 1, \ldots, \widetilde{b}_s \otimes 1, b_{i_1} \otimes e_1, \ldots, b_{i_{n-s}} \otimes e_{n-s}) \neq 0$$

Isto mostra que $f \notin \mathrm{Id}(A)$, garantindo o resultado. □

Para provar a equivalência entre os itens 2 e 3 do Teorema 5.1.1, utilizaremos a teoria desenvolvida na Seção 2.4.

No Exemplo 3.3.4, definimos uma ação à esquerda do grupo simétrico S_n sobre os elementos da álgebra $F\langle x_1, \ldots, x_n\rangle$ e podemos observar que esta ação pode ser restrita ao espaço dos polinômios multilineares P_n. De fato, não é difícil ver que se $f = f(x_1, \ldots, x_n) \in P_n$ e $\sigma \in S_n$, temos

$$\sigma \cdot f = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in P_n. \tag{5.4}$$

A ação definida acima pode ser estendida linearmente para FS_n, ou seja, se $\omega = \alpha_1\sigma_1 + \cdots + \alpha_s\sigma_s \in FS_n$ e $f = f(x_1, \ldots, x_n) \in P_n$, então

$$\omega \cdot f := \alpha_1 f(x_{\sigma_1(1)}, \ldots, x_{\sigma_1(n)}) + \cdots + \alpha_s f(x_{\sigma_s(1)}, \ldots, x_{\sigma_s(n)}).$$

Neste momento, a ação de um idempotente essencial de FS_n sobre o espaço P_n será importante. Vamos ver um exemplo.

Exemplo 5.1.7. Consideremos as tabelas de Young dos tipos $\lambda = (n-1,1) \vdash n$ e $\mu = (n-2,1,1) \vdash n$ e os idempotentes essenciais correspondentes dados nos Exemplos 2.4.10 e 2.4.11, respectivamente. Para $f = f(x_1, \ldots, x_n) = x_1 \cdots x_n$, vamos ter

$$e_{T_\lambda} f = \sum_{\rho \in S_{n-1}} \rho(x_1 \cdots x_n) - \sum_{\rho \in S_{n-1}} \rho(1\ n)(x_1 \cdots x_n)$$

e assim, $e_{T_\lambda} f$ é igual a

$$\sum_{\rho \in S_{n-1}} (x_{\rho(1)} \cdots x_{\rho(n-1)} x_n) - \sum_{\rho \in S_{n-1}} (x_n x_{\rho(2)} \cdots x_{\rho(n-1)} x_{\rho(1)}). \tag{5.5}$$

Além disso, temos que e_{T_μ} é igual a

$$\sum_{\rho \in S_{n-2}} (\rho - \rho(1\ n) - \rho(1\ n-1) - \rho(n-1\ n) + \rho(1\ n-1\ n) + \rho(1\ n\ n-1))$$

e observamos que

$$\begin{aligned}
f_1(x_1, \ldots, x_n) &= \sum_{\rho \in S_{n-2}} \rho f = \sum_{\rho \in S_{n-2}} (x_{\rho(1)} \cdots x_{\rho(n-2)} x_{n-1} x_n) \\
f_2(x_1, \ldots, x_n) &= \sum_{\rho \in S_{n-2}} \rho(1\ n) f = \sum_{\rho \in S_{n-2}} (x_n x_{\rho(2)} \cdots x_{\rho(n-2)} x_{n-1} x_{\rho(1)}) \\
f_3(x_1, \ldots, x_n) &= \sum_{\rho \in S_{n-2}} \rho(1\ n-1) f = \sum_{\rho \in S_{n-2}} (x_{n-1} x_{\rho(2)} \cdots x_{\rho(n-2)} x_{\rho(1)} x_n) \\
f_4(x_1, \ldots, x_n) &= \sum_{\rho \in S_{n-2}} \rho(n-1\ n) f = \sum_{\rho \in S_{n-2}} (x_{\rho(1)} \cdots x_{\rho(n-2)} x_n x_{n-1}) \\
f_5(x_1, \ldots, x_n) &= \sum_{\rho \in S_{n-2}} \rho(1\ n-1\ n) f = \sum_{\rho \in S_{n-2}} (x_n x_{\rho(2)} \cdots x_{\rho(n-2)} x_{\rho(1)} x_{n-1}) \\
f_6(x_1, \ldots, x_n) &= \sum_{\rho \in S_{n-2}} \rho(1\ n\ n-1) f = \sum_{\rho \in S_{n-2}} (x_{n-1} x_{\rho(2)} \cdots x_n x_{\rho(1)}).
\end{aligned}$$

Assim,

$$e_{T_\lambda} f = f_1 - f_2 - f_3 - f_4 + f_5 + f_6. \tag{5.6}$$

Estaremos particularmente interessados na ação do idempotente essencial dado na Equação (2.18) sobre alguns polinômios multilineares.

Observação 5.1.8. Notamos que a ação de $e_{(1^n)}$ sobre um polinômio multilinear $f = f(x_1, \ldots, x_n)$ corresponde a um operador de alternância sobre f de acordo com a Definição 3.1.27, pois

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

Ou seja, a ação apenas modifica os coeficientes dos monômios, e o polinômio resultante $e_{(1^n)} f$ é multilinear e alternado.

Exercício 5.1.9. Mostre que $e_{(1^3)}[x_1, x_2, x_3] = \sum_{\sigma \in S_3} \operatorname{sgn}(\sigma)\sigma[x_1, x_2, x_3]$ é o polinômio nulo.

O próximo lema generaliza o exercício anterior.

Lema 5.1.10. *Sejam $r + s + 1 = n$ e $\{i_1, \ldots, i_r, j_1, \ldots, j_s, t\} = \{1, 2, \ldots, n\}$. Então*

$$e_{(1^n)}[[x_{i_1} \cdots x_{i_r}, x_{j_1} \cdots x_{j_s}], x_t] = 0 \tag{5.7}$$

em $F\langle X\rangle$.

Demonstração. Pela Observação 5.1.8, é suficiente demonstrar esse teorema para o caso em que $i_1 = 1, \ldots, i_r = r$, $j_1 = r + 1, \ldots, j_s = n - 1$ e $t = n$. Temos que $[[x_1 \cdots x_r, x_{r+1} \cdots x_{n-1}], x_n]$ é igual a

$$x_1 \cdots x_n - x_{r+1} \cdots x_{n-1} x_1 \cdots x_r x_n - x_n x_1 \cdots x_{n-1} + x_n x_{r+1} \cdots x_{n-1} x_1 \cdots x_r.$$

Para simplificar, vamos denotar

$$A := x_1 \cdots x_n, \quad B := -x_{r+1} \cdots x_{n-1} x_1 \ldots x_r x_n$$

$$C := -x_n x_1 \cdots x_{n-1} \text{ e } D := x_n x_{r+1} \cdots x_{n-1} x_1 \ldots x_r.$$

Usando a Observação 5.1.8 e o Corolário 3.1.26, temos que

$$e_{(1^n)}[[x_1 \cdots x_r, x_{r+1} \cdots x_{n-1}], x_n] = \alpha St_n, \text{ para algum } \alpha \in F.$$

Dessa forma, o problema se reduz a mostrar que $\alpha = 0$. Escrevemos:

$$e_{(1^n)}[[x_1 \cdots x_r, x_{r+1} \cdots x_{n-1}], x_n] = e_{(1^n)}A + e_{(1^n)}B + e_{(1^n)}C + e_{(1^n)}D$$

e denotando por $\alpha_A, \alpha_B, \alpha_C$ e α_D os coeficientes do monômio $x_1 \dots x_n$ em

$$e_{(1^n)}A,\ e_{(1^n)}B,\ e_{(1^n)}C \ \text{ e } \ e_{(1^n)}D, \text{ respectivamente} \tag{5.8}$$

temos $\alpha = \alpha_A + \alpha_B + \alpha_C + \alpha_D$. O nosso objetivo é provar que $\alpha = 0$, e para isto vamos considerar $p = n - 1 - r$ e calcular cada um dos coeficientes α_A, α_B, α_C e α_D.

O coeficiente α_A é 1. Para computar os demais coeficientes, usamos a decomposição de cada permutação como um produto de transposições e observamos o sinal resultante após a permutação das variáveis até obter o coeficiente do monômio $x_1 \dots x_n$ nos polinômios na Equação (5.8). Por exemplo, para obter α_B, transpomos x_{n-1} sucessivamente até que este fique entre x_r e x_n. Repetimos o mesmo processo para x_{n-2} com o objetivo de ter esta variável entre x_r e x_{n-1}. Em seguida, transpomos todos os termos de x_{n-3} a x_{r+1}, respeitando a mesma linha de raciocínio. No total, serão rp transposições. Fazendo o mesmo tipo de análise para α_C e α_D, vamos obter:

$$\alpha_B = -(-1)^{rp},\ \alpha_C = -(-1)^{n-1},\ \alpha_D = (-1)^{rp}(-1)^{n-1}.$$

Desta forma, lembrando que $n - 1 = r + p$ temos

$$\alpha = 1 - (-1)^{rp} - (-1)^{r+p} + (-1)^{rp}(-1)^{r+p} = (1 - (-1)^{rp})(1 - (-1)^{r+p}).$$

Se r for par ou p for par, então $1-(-1)^{rp} = 0$. Se r e p forem ambos ímpares, temos que $1 - (-1)^{r+p} = 0$. Com isso, $\alpha = 0$ e o lema está provado. □

O próximo resultado é um lema técnico sobre identidades da álgebra de Grassmann, que será necessário para a prova do teorema final, que demonstra as equivalências entre os itens 2 e 3 do Teorema 5.1.1.

Lema 5.1.11. *Qualquer elemento de* $\mathrm{Id}(\mathcal{G})$ *pode ser escrito como uma combinação linear de produtos do tipo*

$$u[[x_{i_1} \cdots x_{i_k}, x_{j_1} \cdots x_{j_l}], x_r]v. \tag{5.9}$$

onde u e v são monômios, eventualmente de grau 0, em $F\langle X\rangle$.

Demonstração. Pelo Teorema 4.3.5 sabemos que o T-ideal de $\mathcal{G}$ é gerado por $[x_1, x_2, x_3]$ e, portanto, qualquer polinômio em $\mathrm{Id}(\mathcal{G})$ é consequência de polinômios do tipo:

$$u[[f, g], h]v \tag{5.10}$$

onde $u, v, f, g, h \in F\langle X\rangle$ e obviamente, u e v podem ser considerados como monômios de grau eventualmente nulo.

Agora, usando a linearidade do comutador, para $f_1, f_2, g_1, g_2 \in F\langle X\rangle$, sabemos que

$$[f_1 + f_2, g] = [f_1, g] + [f_2, g] \text{ e } [f, g_1 + g_2] = [f, g_1] + [f, g_2]$$

e portanto na Equação (5.10), f e g podem ser considerados como monômios. Além disso, pelo Exercício 3.1.6, para $h_1, h_2 \in F\langle X\rangle$, temos que

$$[[f, g], h_1h_2] = [[f, g], h_1]h_2 + h_1[[f, g], h_2]$$

e, assim, o polinômio h na Equação (5.10) pode ser considerado como um monômio de grau 1. Concluímos, assim, que qualquer polinômio em $\mathrm{Id}(\mathcal{G})$ pode ser escrito como uma combinação linear de produtos como dados na Equação (5.9). □

Finalmente, podemos provar a equivalência desejada.

Teorema 5.1.12. *Seja $\mathcal{V}$ uma variedade de álgebras sobre um corpo F de característica zero. Então $\mathcal{V}$ satisfaz um polinômio standard se, e somente se, $\mathcal{G} \notin \mathcal{V}$.*

Demonstração. Obviamente se $\mathcal{V}$ satisfaz uma identidade standard, pelo Exercício 3.2.18, temos que $\mathcal{G} \notin \mathcal{V}$. Assim, vamos provar a recíproca supondo que $\mathcal{G} \notin \mathcal{V}$. Logo, existe um polinômio $f = f(x_1, \ldots, x_n) \in F\langle X\rangle$, que podemos assumir ser multilinear, tal que $f \in \mathrm{Id}(\mathcal{V})$ e $f \notin \mathrm{Id}(\mathcal{G})$.

Recordemos que a demonstração do Teorema 4.3.5 nos mostra que os polinômios em P_n, módulo $P_n \cap \mathrm{Id}(\mathcal{G})$, podem ser escritos como combinação linear de elementos do tipo

$$x_{i_1} \cdots x_{i_k}[x_{j_1}, x_{j_2}] \cdots [x_{j_{2m-1}}, x_{j_{2m}}] \tag{5.11}$$

onde $i_1 < \cdots < i_k$, $j_1 < \cdots < j_{2m}$ e $k + 2m = n$.

Desde que $f \in (P_n \cap \mathrm{Id}(\mathcal{V})) - \mathrm{Id}(\mathcal{G})$, podemos escrever f como uma combinação linear de polinômios dos tipos dados nas Equações (5.9) e (5.11), onde pelo menos um dos polinômios na Equação (5.11) tem coeficiente não nulo. Podemos supor sem perda de generalidade que este polinômio com coeficiente não nulo seja do tipo:

$$x_1 \cdots x_k[x_{k+1}, x_{k+2}] \cdots [x_{n-1}, x_n]$$

e consideramos que este polinômio aparece em f com coeficiente igual a 1.

Consideramos a seguinte aplicação:

$$\begin{aligned}\phi: \quad & F\langle X\rangle \to F\langle X\rangle \\ & x_i \mapsto [x_i, y_i], \text{ se } 1 \leqslant i \leqslant k \\ & x_j \mapsto x_j, \text{ se } k+1 \leqslant j \leqslant n.\end{aligned}$$

e vemos que ϕ é um endomorfismo de $F\langle X\rangle$. Isto significa que ao considerarmos $\phi(f)$, obtemos uma nova identidade $g = g(x_1, \ldots, x_n, y_1, \ldots, y_k)$ de $\mathcal{V}$.

Observemos que, em relação aos elementos que são do tipo dado na Equação (5.11), com exceção daquele em que $i_1 = 1, \ldots, i_k = k$ e $j_1 = k+1, \ldots, j_{2m} = n$, todos são enviados em $\mathrm{Id}(\mathcal{G})$ pelo endomorfismo ϕ. Assim, podemos escrever

$$g = [x_1, y_1] \cdots [x_k, y_k][x_{k+1}, x_{k+2}] \cdots [x_{n-1}, x_n] + h,$$

onde h é um polinômio multilinear que é combinação linear de elementos de $P_n \cap \mathrm{Id}(\mathcal{G})$.

Renomeando as variáveis o polinômio g, temos:

$$g = [x_1, x_2] \cdots [x_{2q-1}, x_{2q}] + h,$$

onde h é um polinômio multilinear de grau $2q$ em $\mathrm{Id}(\mathcal{G})$, que é combinação linear de polinômios como na Equação (5.9).

Consideremos $\Gamma = \{i_1, \ldots, i_k, j_1, \ldots, j_l, r\} \subset \{1, \ldots, 2q\}$ e S_Γ o subgrupo do grupo simétrico S_{2q} formado por todas as permutações que fixam os elementos de $\widehat{2q}\backslash\Gamma$. Pelo Lema 2.4.13, ao tomar $e = \sum_{\sigma \in S_\Gamma} \mathrm{sgn}(\sigma)\sigma$, existe $\omega \in FS_{2q}$ tal que $\omega e = e_{(1^{2q})}$.

Agora, notemos que se h' é um polinômio do tipo dado na Equação (5.9), então, pelo Lema 5.1.10, temos $\omega e h' = e_{(1^{2q})}h' = 0$, o que implica em

$$e_{(1^{2q})}h = 0. \tag{5.12}$$

Observemos que $e_{(1^{2q})}g \in \mathrm{Id}(\mathcal{V})$, e como a ação de $e_{(1^{2q})}$ corresponde a um operador de alternância nas primeiras $2q$ variáveis, pelo item (c) do Exercício 3.1.29, temos

$$e_{(1^{2q})}[x_1, x_2] \cdots [x_{2q-1}, x_{2q}] = 2^q St_{2q}. \tag{5.13}$$

Desta forma, a partir das Equações (5.12) e (5.13), obtemos

$$e_{(1^{2q})}g = e_{(1^{2q})}[x_1, x_2] \cdots [x_{2q-1}, x_{2q}] + e_{(1^{2q})}h = 2^q St_{2q}$$

ou seja, $\frac{1}{2^q}e_{(1^{2q})}g = St_{2q}$ é uma identidade de $\mathcal{V}$, como desejávamos. □

Com os Teoremas 5.1.6 e 5.1.12, temos provado o Teorema 5.1.1. Agora, vamos ver uma consequência importante, provada por Kemer (1991).

Corolário 5.1.13. *Seja A uma F-álgebra de crescimento polinomial. Então existe uma F-álgebra de dimensão finita B tal que* $\text{var}(A) = \text{var}(B)$.

Demonstração. Sendo A uma álgebra de crescimento polinomial, já sabemos que $\mathcal{G} \notin \mathcal{V} = \text{var}(A)$, pois a codimensão de $\mathcal{G}$ é exponencial. Assim, pelo Teorema 5.1.1, temos que $\mathcal{V}$ é gerada por uma álgebra B de dimensão finita, ou seja, $\mathcal{V} = \text{var}(B)$, como queríamos mostrar. □

Exercícios V ou F da Seção 5.1: Verifique se cada sentença abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, A e B representam F-superálgebras.

(1) Uma álgebra de dimensão infinita não satisfaz um polinômio standard.

(2) Se A é isomorfa a B como superálgebra, então $G(A)$ é isomorfa a $G(B)$ como superálgebra.

(3) Se $G(A)$ satisfaz uma identidade standard e J é o radical de Jacobson de A, então $G(A/J)$ satisfaz uma identidade standard .

(4) Se $e_{(1^n)} = \sum_{\sigma \in S_n} \text{sgn}(\sigma)\sigma$ é o idempotente essencial de FS_n definido na Equação (2.18), então $e_{(1^n)}x_1 \dots x_n = St_n$.

(5) Se $\mathcal{V}$ é uma variedade que satisfaz um polinômio standard, então $\mathcal{G} \in \mathcal{V}$.

(6) Existe uma álgebra de dimensão finita $\mathcal{A}$ tal que $\text{var}(\mathcal{A}) = \text{var}(\mathcal{G})$

5.2 O Teorema de Kemer

Esta seção é devotada para a demonstração do teorema que caracteriza variedades de crescimento polinomial das codimensões via exclusão de álgebras da variedade. Esta foi a primeira caracterização para variedades deste tipo e foi dada por Kemer (1979), que mostrou que uma variedade $\mathcal{V}$ tem crescimento polinomial se, e somente se, as álgebras $\mathcal{G}$ e UT_2 não pertencem a $\mathcal{V}$.

Para apresentar a demonstração aqui, vamos inicialmente fazer algumas considerações a respeito do expoente de uma álgebra de dimensão finita, lembrando o

que já foi dito na Seção 4.5. Giambruno e Zaicev provaram que, sobre um corpo de característica zero, o PI-expoente de uma PI-álgebra associativa existe e é um inteiro não negativo. Além disso, os autores exibiram uma forma de determinar tal inteiro no caso em que a álgebra A tem dimensão finita.

Para isso, usaram uma decomposição de Wedderburn–Malcev de A, digamos, $A_1 \oplus \cdots \oplus A_m \dotplus J$, com $J = J(A)$, e consideraram todos os produtos

$$B_1 J B_2 J \cdots J B_r \neq \{0\}$$

onde B_s, $s = 1, \ldots, r$, são álgebras distintas do conjunto $\{A_1, \ldots, A_m\}$ e $r = 1, 2, \ldots$. Tomando álgebras satisfazendo esta condição, os autores definiram

$$q = \max \dim_F (B_1 \oplus \cdots \oplus B_r)$$

e mostraram que, nas condições do Teorema 4.5.17, temos $\exp(A) = q$.

Observação 5.2.1. Notemos que se uma PI-álgebra A tem crescimento polinomial, então existe uma constante C e um inteiro não negativo r tais que $c_n(A) \leqslant Cn^r$. Isto implica $\exp(A) \leqslant \lim\limits_{n\to\infty} \sqrt[n]{Cn^r} = 1$, ou seja, $\exp(A) \leqslant 1$.

Mais do que foi dito na Observação 5.2.1, a recíproca também é válida. De fato, suponhamos que $\exp(A) = q \leqslant 1$. Desta forma, q satisfaz as desigualdades no Corolário 4.5.10 e, assim, $c_n(A) \leqslant C_2 n^{r_2}$.

Agora, tomamos k um número natural tal que $r_2 \leqslant k$ e teremos $c_n(A) \leqslant C_2 n^k$, ou seja, A tem crescimento polinomial.

Portanto, temos o seguinte resultado que dá uma primeira caracterização de variedades de crescimento polinomial a partir do PI-expoente.

Teorema 5.2.2. *Seja A uma PI-álgebra. Então a sequência de codimensões $\{c_n(A)\}_{n\geqslant 1}$ é polinomialmente limitada se, e somente se,* $\exp(A) \leqslant 1$.

A seguir daremos uma caracterização de álgebras de dimensão finita de crescimento polinomial a partir da decomposição de Wedderburn–Malcev.

Teorema 5.2.3. *Seja $A = A_1 \oplus \cdots \oplus A_m \dotplus J$ uma decomposição de Wedderburn–Malcev de uma álgebra de dimensão finita sobre um corpo algebricamente fechado de característica zero, onde $J = J(A)$. A álgebra A tem crescimento polinomial se, e somente se, para todo $i = 1, \ldots, m$, temos $A_i \cong F$ e $A_i J A_j = \{0\}$, para todo $j \neq i$.*

Demonstração. Suponhamos que A tem crescimento polinomial. Assim pelo Teorema 1.4.62, podemos tomar

$$A = A_1 \oplus \cdots \oplus A_m \dotplus J$$

uma decomposição de Wedderburn–Malcev de A, onde $J = J(A)$ e para cada $i = 1, \ldots, m$, temos $A_i \cong M_{k_i}(F)$, para algum $k_i \in \mathbb{N}$. Como $M_{k_i}(F) \in \text{var}(A)$, para todo $i = 1, \ldots, m$, se algum k_i é maior do que 1, então A teria crescimento exponencial, o que contraria a hipótese que A tem crescimento polinomial. Logo, $k_i = 1$ e, assim, $\dim_F(A_i) = 1$, ou seja, $A_i \cong F$ para todo $i = 1, \ldots, m$. Além disso, pela Observação 5.2.1, temos $A_i J A_j = \{0\}$, para todo $j \neq i$.

Reciprocamente, se para todo $i = 1, \ldots, m$, temos $A_i \cong F$ e $A_i J A_j = \{0\}$, para todo $j \neq i$, então $\exp(A) \leqslant 1$. Pelo Teorema 5.2.2, A tem crescimento polinomial. □

Desde que as álgebras UT_2 e $\mathcal{G}$ têm crescimento exponencial, ao considerar $\mathcal{V}$ uma variedade de crescimento polinomial, temos que $UT_2, \mathcal{G} \notin \mathcal{V}$. O próximo lema será fundamental para garantirmos que a recíproca é verdadeira e assim estaremos aptos a provar o célebre Teorema de Kemer.

Lema 5.2.4. *Considere A uma álgebra de dimensão finita sobre um corpo algebricamente fechado de característica zero e $A_1 \oplus \cdots \oplus A_m \dotplus J$ uma decomposição de Wedderburn–Malcev de A. Se existem $i, j \in \{1, \ldots, m\}$, $i \neq j$, com $A_i J A_j \neq \{0\}$, então $UT_2 \in \text{var}(A)$.*

Demonstração. Tomamos A_i e A_j, com $i \neq j$, tais que $A_i J A_j \neq \{0\}$. Dessa forma, existem $a_1 \in A_i$, $a_2 \in A_j$ e $a \in J$ tais que $a_1 a a_2 \neq 0$. Considerando u_1 e u_2 as unidades de A_i e A_j, respectivamente, teremos $u_1 a u_2 \neq 0$.

Afirmamos que u_1, u_2 e $u_1 a u_2$ são elementos linearmente independentes em A. De fato, considerando uma combinação linear

$$\alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_1 a u_2 = 0, \text{ com } \alpha_i \in F$$

usando o fato que $u_1 u_2 = u_2 u_1 = 0$, obtemos $\alpha_i = 0$, para $i = 1, 2, 3$.

Consideramos, então, $B = \text{span}_F\{u_1, u_2, u_1 a u_2\}$. Desde que $u_r^2 = u_r$ e também $u_r u_s = 0$, para $r \neq s$, temos que B é uma F-subálgebra de A. Seja $\phi : B \to UT_2$ o homomorfismo de F-álgebras definido por:

$$u_1 \mapsto e_{11}, \qquad u_2 \mapsto e_{22}, \qquad u_1 a u_2 \mapsto e_{12}$$

onde e_{ij} denotam as matrizes elementares. Observamos que ϕ é, na verdade, um isomorfismo de álgebras. Portanto, $UT_2 \in \text{var}(A)$, como gostaríamos. □

Agora temos todos os pré-requisitos necessários para provar abaixo o principal resultado deste capítulo.

Teorema 5.2.5. *Seja $\mathcal{V}$ uma variedade de álgebras sobre um corpo F de característica zero. Então $\mathcal{V}$ tem crescimento polinomial se, e somente se, $UT_2,\ \mathcal{G} \notin \mathcal{V}$.*

Demonstração. Inicialmente, notemos que se $\mathcal{V} = \text{var}(0)$, o resultado é imediato. Consideramos então que $\mathcal{V}$ é não trivial. Como já comentado, sendo $\mathcal{V}$ variedade de crescimento polinomial, temos $UT_2,\ \mathcal{G} \notin \mathcal{V}$.

Reciprocamente, desde que $\mathcal{G} \notin \mathcal{V}$, pelo Teorema 5.1.1, temos que $\mathcal{V} = \text{var}(A)$ para alguma F-álgebra de dimensão finita A. Desse modo, podemos considerar

$$A = B_1 \oplus \cdots \oplus B_m \dotplus J$$

uma decomposição de Wedderburn–Malcev de A, onde $J = J(A)$ é seu radical de Jacobson. Pela Proposição 4.2.15, podemos supor que F é algebricamente fechado e, assim, para cada $1 \leqslant i \leqslant m$, temos $B_i \cong M_{n_i}(F)$, para algum $n_i \in \mathbb{N}$.

Observemos agora que, se $n_i > 1$ para algum $1 \leqslant i \leqslant m$, segue que A contém uma F-subálgebra isomorfa a UT_2, uma contradição à hipótese inicial. Logo, temos que $B_i \cong F$, para todo $i = 1, \ldots, m$. Desde que $UT_2 \notin \mathcal{V}$, pelo Lema 5.2.4, obtemos que $B_i J B_j = \{0\}$, para todos $i, j \in \{1, \ldots, m\}$, com $i \neq j$. Logo, a partir do Teorema 5.2.3, concluímos que $\mathcal{V}$ tem crescimento polinomial. □

Como uma consequência imediata do Teorema de Kemer, todas as subvariedades próprias da variedade gerada por $\mathcal{G}$ e da variedade gerada por UT_2 têm crescimento polinomial das codimensões, conforme provamos abaixo.

Corolário 5.2.6. *Se $\mathcal{U}$ é uma subvariedade própria de* $\text{var}(\mathcal{G})$ *ou de* $\text{var}(UT_2)$*, então $\mathcal{U}$ tem crescimento polinomial.*

Demonstração. Suponhamos que $\mathcal{U} \subsetneq \text{var}(UT_2)$. Note que assim, $UT_2 \notin \mathcal{U}$ e desde que $\mathcal{G} \notin \text{var}(UT_2)$, segue que $\mathcal{G} \notin \mathcal{U}$. Logo, pelo Teorema de Kemer, isso implica que $\mathcal{U}$ tem crescimento polinomial. Obviamente, a demonstração para subvariedades próprias de $\text{var}(\mathcal{G})$ é análoga. □

Como as álgebras $\mathcal{G}$ e UT_2 têm crescimento exponencial, estabelecemos uma nova definição.

Definição 5.2.7. Dizemos que uma variedade $\mathcal{V}$ tem crescimento quase polinomial se $\mathcal{V}$ tem crescimento exponencial, mas qualquer subvariedade própria de $\mathcal{V}$ tem crescimento polinomial.

Corolário 5.2.8. $\mathrm{var}(UT_2)$ *e* $\mathrm{var}(\mathcal{G})$ *são as únicas variedades de crescimento quase polinomial.*

Demonstração. De fato, já vimos que as álgebras UT_2 e $\mathcal{G}$ geram variedades de crescimento exponencial. Agora, consideremos $\mathcal{V}$ uma variedade de crescimento quase polinomial.

Como $\mathcal{V}$ tem crescimento exponencial, pela caracterização apresentada por Kemer, não podemos ter ambas UT_2 e $\mathcal{G}$ excluídas da variedade $\mathcal{V}$. Suponhamos, sem perda de generalidade, que $UT_2 \in \mathcal{V}$. Desse modo, $\mathrm{var}(UT_2) \subseteq \mathcal{V}$. Uma vez que $\mathcal{V}$ tem crescimento quase polinomial e $\mathrm{var}(UT_2)$ tem crescimento exponencial da sequência de codimensões, essa inclusão não pode ser própria e, portanto, $\mathcal{V} = \mathrm{var}(UT_2)$. Na segunda situação, ou seja, quando $\mathcal{G} \in \mathcal{V}$, temos $\mathcal{V} = \mathrm{var}(\mathcal{G})$.

Assim, concluímos que $\mathcal{V} = \mathrm{var}(UT_2)$ ou $\mathcal{V} = \mathrm{var}(\mathcal{G})$, como queríamos mostrar. □

Podemos dar uma descrição de variedades de crescimento quase polinomial em termos de identidades. Pelo corolário anterior, $\mathrm{var}(UT_2)$ e $\mathrm{var}(\mathcal{G})$ são as únicas variedades de crescimento quase polinomial. Tome, por exemplo, $\mathrm{var}(UT_2)$. Sabemos que $\mathrm{Id}(UT_2) = \langle [x_1, x_2][x_3, x_4] \rangle_T$. Com isso, se $f \in P_n$ é um polinômio que não é consequência de $[x_1, x_2][x_3, x_4]$, então a álgebra A determinada por $\langle [x_1, x_2][x_3, x_4], f \rangle_T$ pertence a $\mathrm{var}(UT_2)$ e, consequentemente, tem crescimento polinomial.

Logo, temos uma certa minimalidade nos geradores de $\mathrm{Id}(UT_2)$, no sentido que ao acrescentarmos qualquer polinômio a $\mathrm{Id}(UT_2)$, que não é consequência de $[x_1, x_2][x_3, x_4]$, obtemos uma variedade de crescimento polinomial. O mesmo ocorre com a álgebra de Grassmann $\mathcal{G}$.

Essa minimalidade pode ser descrita em termos do expoente. De fato, o que o corolário anterior nos diz é que $\exp(UT_2) = \exp(\mathcal{G}) = 2$, mas qualquer subvariedade própria destas variedades possui expoente menor ou igual a 1. Neste caso, dizemos que $\mathrm{var}(UT_2)$ e $\mathrm{var}(\mathcal{G})$ são variedade minimais de expoente 2 e, consequentemente, UT_2 e $\mathcal{G}$ geram as únicas variedades minimais de expoente 2.

Observe que se $\mathcal{V}$ é uma variedade de expoente maior ou igual a 2, então necessariamente ou UT_2 ou $\mathcal{G}$ pertencem a $\mathcal{V}$. Com isso, temos o seguinte corolário.

Corolário 5.2.9. *Uma variedade de álgebras associativas tem crescimento exponencial ou tem crescimento polinomial.*

Demonstração. Seja $\mathcal{V}$ uma variedade de álgebras associativas. Temos duas opções: ou $\mathcal{G}, UT_2 \notin \mathcal{V}$, ou uma das duas álgebras, $\mathcal{G}$ ou UT_2, pertence a $\mathcal{V}$. Na

primeira situação, $\mathcal{V}$ tem crescimento polinomial e, na segunda situação, a variedade tem crescimento exponencial. □

Variedades de crescimento intermediário das codimensões são variedades que não têm crescimento exponencial e cuja sequência das codimensões não é polinomialmente limitada. Pelo corolário anterior, esse tipo de variedade não existe na classe das álgebras associativas, mas é possível dar exemplos de álgebras não associativas com crescimento intermediário das codimensões.

Exercícios V ou F da Seção 5.2: Verifique se cada sentença abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, A representa uma F-álgebra.

(1) Se $\exp(A) \leqslant 2$, então A tem crescimento polinomial.

(2) Se A tem crescimento exponencial e $B \in \text{var}(A)$, então B tem crescimento polinomial.

(3) Se $\mathcal{U}$ é uma subvariedade própria de $\text{var}(\mathcal{G})$, então $\exp(A) \leqslant 1$.

(4) Se A é uma álgebra de dimensão finita tal que $A \cong F + J(A)$, então A tem crescimento polinomial.

(5) Se uma variedade $\mathcal{V}$ não tem crescimento polinomial, então $\mathcal{G} \in \mathcal{V}$.

(6) Se $\mathcal{V}$ é uma variedade de crescimento quase polinomial, então $UT_2 \in \mathcal{V}$.

(7) A álgebra de Grassmann $\mathcal{G}$ é um exemplo de álgebra de crescimento intermediário.

5.3 A sequência de cocaracteres

Nosso objetivo agora é definir a sequência de cocaracteres de uma F-álgebra A, a qual corresponde à sequência de S_n-caracteres de S_n-módulos associados à álgebra A. Esta sequência tem sido extensivamente estudada devido à sua relação com a sequência de codimensões de A. Assim, temos o propósito de provar o teorema de Giambruno e Zaicev (2001) que garante que uma álgebra A tem crescimento polinomial se, e somente se, na decomposição da sequência de cocaracteres de A, temos específicos S_n-caracteres irredutíveis com multiplicidade nula.

A ação à esquerda do grupo simétrico S_n sobre o espaço dos polinômios multilineares P_n, definida na Equação (5.4), corresponde a permutação das variáveis

em cada um dos monômios de f de acordo com a permutação σ e, assim, P_n tem estrutura de S_n-módulo sob esta ação. Como já observamos no Exemplo 3.3.4, o T-ideal $\mathrm{Id}(A)$ também é invariante sob esta ação. Assim, o espaço quociente

$$P_n(A) = \frac{P_n}{P_n \cap \mathrm{Id}(A)}$$

tem estrutura de FS_n-módulo. Com isso, podemos considerar seu S_n-caracter como na próxima definição.

Definição 5.3.1. O S_n-caracter de $P_n(A)$, denotado por $\chi_n(A)$, é o chamado n-ésimo cocaracter de A. Para $\mathcal{V} = \mathrm{var}(A)$, definimos $\chi_n(\mathcal{V}) = \chi_n(A)$, para todo $n \geqslant 1$. Assim, formamos uma sequência $\{\chi_n(A)\}_{n\geqslant 1}$ (resp. $\{\chi_n(\mathcal{V})\}_{n\geqslant 1}$) dita sequência de cocaracteres de A (resp. de $\mathcal{V}$).

Sabemos que, em característica zero, existe uma correspondência biunívoca entre S_n-caracteres irredutíveis e partições $\lambda \vdash n$, conforme vimos no Capítulo 2. Assim, de acordo com a Teorema 2.3.15, podemos decompor $\chi_n(A)$ em S_n-caracteres irredutíveis

$$\chi_n(A) = \sum_{\lambda\vdash n} m_\lambda \chi_\lambda \tag{5.14}$$

onde χ_λ representa o caracter irredutível associado à partição $\lambda \vdash n$ e m_λ é sua multiplicidade.

Podemos, inicialmente, observar o seguinte fato sobre o cocaracter de uma álgebra A.

Observação 5.3.2. Pela Observação 2.3.17, se considerarmos A uma F-álgebra e $\overline{A} = A \otimes_F \overline{F}$, vemos que o cocaracter $\chi_n(\overline{A})$ tem a mesma decomposição que o cocaracter $\chi_n(A)$. Portanto, em resultados sobre a decomposição de cocaracteres de F-álgebras, podemos considerar que o corpo F é algebricamente fechado.

A decomposição do cocaracter de uma álgebra A nos dá informações sobre a codimensão desta álgebra desde que

$$\chi_n(A)(1) = \sum_{\lambda\vdash n} m_\lambda \chi_\lambda(1), \text{ ou seja, } c_n(A) = \sum_{\lambda\vdash n} m_\lambda d_\lambda \tag{5.15}$$

onde d_λ é o grau do caracter irredutível χ_λ dado pela fórmula do gancho na Equação (2.14).

Desta forma, é importante saber informações sobre as multiplicidades m_λ dos caracteres irredutíveis χ_λ na decomposição dada na Equação (5.14). Primeiramente, temos a seguinte observação a fazer.

Observação 5.3.3. Berele e Regev (1983) provaram que as multiplicidades m_λ, dadas na Equação (5.14), são polinomialmente limitadas, isto é, para todo $n \geqslant 1$ e toda $\lambda \vdash n$, temos $m_\lambda \leqslant Cn^t$, onde C e $t > 0$ são constantes que não dependem de n.

Agora, apresentamos um resultado que garante uma maneira de verificar quando a multiplicidade m_λ é não nula. Para enunciá-lo, faremos uso de idempotentes essenciais e a sua demonstração pode ser consultada no livro de Giambruno e Zaicev (2005).

Teorema 5.3.4. *Seja A uma PI-álgebra cujo n-ésimo cocaracter $\chi_n(A)$ tem uma decomposição como na Equação (5.14). Para uma partição $\lambda \vdash n$, temos que $m_\lambda \neq 0$ se, e somente se, existe uma tabela de Young T_λ do tipo λ e um polinômio $f = f(x_1, \ldots, x_n) \in P_n$ tal que $e_{T_\lambda} f \notin \mathrm{Id}(A)$.*

Faremos mais uma observação abaixo.

Observação 5.3.5. Dada uma tabela de Young do tipo $\lambda = (\lambda_1, \ldots, \lambda_t) \vdash n$ e um polinômio $f = f(x_1, \ldots, x_n) \in P_n$, temos que o polinômio $e_{T_\lambda} f$ é uma combinação linear de polinômios alternados em λ_1 conjuntos disjuntos de variáveis.

Faremos um exemplo do que foi dito na observação anterior, considerando $\lambda = (2, 2) \vdash 4$ e $f = f(x_1, \ldots, x_4) = x_1x_2x_3x_4$. Para o idempotente essencial, calculado no Exercício 2.4.12, temos que $e_{T_\lambda} f$ é uma combinação linear de polinômios alternados em $\lambda_1 = 2$ conjuntos disjuntos de variáveis, que estão dispostos na tabela abaixo.

Polinômio na combinação linear de $e_{T_\lambda} f$	alternado nos conjuntos disjuntos
$x_1x_2x_3x_4 - x_1x_3x_2x_4 - x_4x_2x_3x_1 + x_4x_3x_2x_1 +$ $x_2x_1x_4x_3 - x_2x_4x_1x_3 - x_3x_1x_4x_2 + x_3x_4x_1x_2$	$\{x_1, x_4\}$ e $\{x_2, x_3\}$
$x_2x_1x_3x_4 - x_2x_3x_1x_4 - x_4x_1x_3x_2 + x_4x_3x_1x_2 +$ $x_1x_2x_4x_3 - x_1x_4x_2x_3 - x_3x_2x_4x_1 + x_3x_4x_2x_1$	$\{x_1, x_3\}$ e $\{x_2, x_4\}$

A seguir, para exemplificar o uso do Teorema 5.3.4, vamos determinar a decomposição de $\chi_n(A)$ onde A é uma álgebra comutativa unitária, e também a decomposição de $\chi_n(\mathcal{G})$.

Exemplo 5.3.6. Seja A uma álgebra comutativa unitária. Pelo Exemplo 4.2.2, sabemos que $c_n(A) = 1$ e agora vamos mostrar que $\chi_n(A) = \chi_{(n)}$. Para isto, consideramos a tabela de Young do tipo $(n) \vdash n$ abaixo, e o idempotente essencial

correspondente

$$T_{(n)} = \boxed{1}\boxed{2}\boxed{\cdots}\boxed{n}\ , \quad e_{T_{(n)}} = \sum_{\sigma \in S_n} \sigma. \tag{5.16}$$

Assim, se f é o polinômio $x_1 \cdots x_n$, temos

$$e_{T_{(n)}} f = \sum_{\sigma \in S_n} x_{\sigma(1)} \cdots x_{\sigma(n)}$$

e este não é uma identidade de A, pois fazendo a avaliação $x_i = 1$ para todo $i = 1, \ldots, n$ temos $e_{T_{(n)}} f(1, \ldots, 1) = n! \neq 0$. Pelo Teorema 5.3.4, temos que $m_{(n)} \neq 0$. Além disso, a partir da Equação (2.14), sabemos que $d_{(n)} = 1$, e usando a Equação (5.15), teremos

$$1 = c_n(A) = \sum_{\lambda \vdash n} m_\lambda d_\lambda \geqslant m_{(n)} d_{(n)} = m_{(n)} \geqslant 1.$$

Portanto, $m_{(n)} = 1$ e concluímos que $\chi_n(A) = \chi_{(n)}$, como queríamos mostrar.

Proposição 5.3.7. *$\chi_n(\mathcal{G}) = \sum_{k=1}^{n} \chi_{\lambda^{(k)}}$, onde $\lambda^{(k)} = (k, 1^{n-k}) \vdash n$.*

Demonstração. Vamos mostrar inicialmente que, para todo $k = 1, \ldots, n$, a multiplicidade $m_{\lambda^{(k)}}$ da partição $\lambda^{(k)} = (k, 1^{n-k})$ é não nula e para isso usaremos o Teorema 5.3.4. Consideremos a seguinte tabela de Young do tipo $\lambda^{(k)}$:

$$T_{\lambda^{(k)}} = \begin{array}{|c|c|c|c|} \hline 1 & 2 & \cdots & k \\ \hline k+1 \\ \cline{1-1} \vdots \\ \cline{1-1} n-1 \\ \cline{1-1} n \\ \cline{1-1} \end{array}$$

e observemos que $C = C_{T_{\lambda^{(k)}}} = S_{n-k+1}(1, k+1, \ldots, n-1, n)$ e $R = R_{T_{\lambda^{(k)}}} = S_k$.

Considerando o idempotente essencial $e = e_{T_{\lambda^{(k)}}}$ e $f = f(x_1, \ldots, x_n) = x_1 \cdots x_n$, vamos ter

$$ef = \left(\sum_{\substack{\rho \in R \\ \sigma \in C}} (\operatorname{sgn} \sigma) \rho\sigma \right) x_1 \cdots x_n$$

ou seja,

$$ef = \left(\sum_{\rho\in S_k}\rho\right)\left(\sum_{\sigma\in S_{n-k+1}}\operatorname{sgn}(\sigma)x_{\sigma(1)}x_2\cdots x_k x_{\sigma(k+1)}\cdots x_{\sigma(n)}\right)$$

onde S_{n-k+1} denota o grupo de permutações das variáveis $1, k+1, \ldots, n$.

Afirmamos que $ef \neq 0$ e, para provar isto, vamos considerar uma substituição por elementos da álgebra de Grassmann $\mathcal{G}$, que não anula esse polinômio. De fato, escolhemos a substituição onde tomamos:

$$\overline{x}_1 = e_1,\ \overline{x}_{k+1} = e_2, \ldots,\ \overline{x}_n = e_{n-k+1}$$

e

$$\overline{x}_2 = e_{n-k+2}e_{n-k+3},\ \overline{x}_3 = e_{n-k+4}e_{n-k+5}, \ldots,\ \overline{x}_k = e_{n+k-2}e_{n+k-1}$$

e observamos que $\overline{x}_2, \overline{x}_3, \ldots, \overline{x}_k \in \mathcal{G}^{(0)}$ e $\overline{x}_1, \overline{x}_{k+1}, \ldots, \overline{x}_n \in \mathcal{G}^{(1)}$.

Considerando o resultado da substituição $\omega = ef(\overline{x}_1, \ldots, \overline{x}_n)$, usando que os elementos $\overline{x}_2 = e_{n-k+2}e_{n-k+3}, \ldots, \overline{x}_k = e_{n+k-2}e_{n+k-1}$ são centrais, vamos ter

$$\begin{aligned}\omega &= \left(\sum_{\rho\in S_k}\rho\right)(\overline{x}_2\cdots\overline{x}_k)\left(\sum_{\sigma\in S_{n-k+1}}\operatorname{sgn}(\sigma)\overline{x}_{\sigma(1)}\overline{x}_{\sigma(k+1)}\cdots\overline{x}_{\sigma(n)}\right)\\ &= \left(\sum_{\rho\in S_k}\rho\right)(\overline{x}_2\cdots\overline{x}_k)St_{n-k+1}(\overline{x}_1, \overline{x}_{k+1}, \ldots, \overline{x}_n).\end{aligned} \tag{5.17}$$

Agora observe que

$$\left(\sum_{\rho\in S_k}\rho\right)(\overline{x}_2\cdots\overline{x}_k) = k!e_{n-k+2}e_{n-k+3}\cdots e_{n+k-2}e_{n+k-1}$$

e

$$St_{n-k+1}(\overline{x}_1, \overline{x}_{k+1}, \ldots, \overline{x}_n) = (n-k+1)!e_1\cdots e_{n-k+1}.$$

Portanto, ao fazer o produto final na Equação (5.17), vamos obter

$$w = k!(n-k+1)!e_1\cdots e_{n-k+1}e_{n-k+2}e_{n-k+3}\cdots e_{n+k-2}e_{n+k-1} \neq 0.$$

Desta forma, garantimos que $m_{\lambda^{(k)}} \geqslant 1$, para todo $k = 1, \ldots, n$ e usando a fórmula do gancho dada na Equação (2.14), temos que $d_{\lambda^{(k)}} = \binom{n-1}{k-1}$. Agora, pelo Teorema 4.3.5, lembramos que $c_n(\mathcal{G}) = 2^{n-1}$ e assim:

$$2^{n-1} = c_n(\mathcal{G}) = \sum_{\lambda \vdash n} m_\lambda d_\lambda \geqslant \sum_{\lambda^{(k)} \vdash n} d_{\lambda^{(k)}} = \sum_{k=1}^{n} \binom{n-1}{k-1} = 2^{n-1}.$$

Isto nos leva a concluir que $m_{\lambda^{(k)}} = 1$ para $k = 1, 2, \ldots, n$ e $m_\lambda = 0$, para qualquer outra partição λ de n. Portanto, temos a decomposição $\chi_n(\mathcal{G}) = \sum_{k=1}^{n} \chi_{\lambda^{(k)}}$. □

Notemos que a decomposição do cocaracter da álgebra de Grassmann $\mathcal{G}$ mostra que as partições que correspondem a caracteres irredutíveis com multiplicidades não nulas são todas do tipo $\lambda^{(k)} = (k, 1^{n-k}) \vdash n$, com $1 \leqslant k \leqslant n$. Notamos ainda que, para tais partições, temos $\lambda_2^{(k)} \leqslant 1$ e, portanto, os diagramas de Young correspondentes a essas partições têm um formato especial, ou seja, todas as linhas a partir da segunda têm no máximo um box.

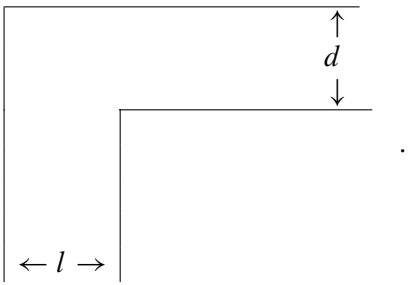
A observação feita pode ser estendida a PI-álgebras em geral, conforme dado por um importante teorema provado por Amitsur (1953). Para enunciar esse teorema, vamos precisar da seguinte definição.

Definição 5.3.8. Dados inteiros $d, l \geqslant 0$ definimos o gancho infinito $H(d, l)$ como sendo $H(d, l) = \bigcup_{n \geqslant 1} \{\lambda = (\lambda_1, \lambda_2, \ldots) \vdash n : \lambda_{d+1} \leqslant l\}$.

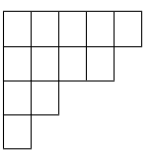
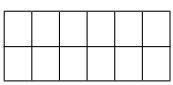
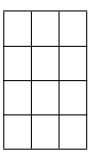
De acordo com a definição anterior, os diagramas correspondentes a partições pertencentes ao gancho infinito $H(d, l)$ têm no máximo l boxes nas linhas a partir da $(d+1)$-ésima linha e, vemos que, para as partições $\lambda^{(k)} = (k, 1^{n-k}) \vdash n$, com $1 \leqslant k \leqslant n$, temos $\lambda^{(k)} \in H(1, 1)$. Desta forma, podemos reescrever a Proposição 5.3.7 como $\chi_n(\mathcal{G}) = \sum_{\substack{\lambda \vdash n \\ \lambda \in H(1,1)}} \chi_\lambda$.

Notamos que para uma partição $\lambda \in H(d, l)$, o diagrama de Young do tipo λ

terá uma representação gráfica como a seguinte:



Exemplo 5.3.9. Vamos considerar $n = 12$ e as partições com seus diagramas de Young associados a seguir.

$D_{(5,4,2,1)} =$  $D_{(6,6)} =$  $D_{(3,3,3,3)} =$ 

Então, $(5,4,2,1), (6,6) \in H(3,2)$, enquanto que $(3,3,3,3) \notin H(3,2)$.

O próximo resultado mostra que as partições, que eventualmente contribuem com multiplicidades não nulas na decomposição do cocaracter de uma PI-álgebra, estão em algum gancho infinito. Este teorema foi demonstrado por Regev e Amitsur (1982).

Teorema 5.3.10. *Seja A uma PI-álgebra sobre um corpo de característica zero. Então existem inteiros $d, l \geqslant 0$, tais que*

$$\chi_n(A) = \sum_{\substack{\lambda \vdash n \\ \lambda \in H(d,l)}} m_\lambda \chi_\lambda, \text{ para todo } n \geqslant 1.$$

Já sabemos que a álgebra de Grassmann $\mathcal{G}$ não satisfaz uma identidade standard, mas observamos que

$$[x_1, x_2]^2 = [x_1, x_2, x_1]x_2 - [x_1 x_2, x_2, x_1]$$

e assim, $[x_1, x_2, x_3] \rightsquigarrow [x_1, x_2]^2$. Desta forma, concluímos que $\mathcal{G}$ satisfaz o polinômio $St_2(x_1, x_2)^2$. Vamos provar que este não é um privilégio da álgebra de Grassmann, pois, na verdade, qualquer PI-álgebra satisfaz uma potência de algum polinômio standard, sendo esse mais um resultado demonstrado por Regev e Amitsur (ibid.) . Para prová-lo aqui, usaremos o Teorema 5.3.10.

Teorema 5.3.11. *Seja A uma PI-álgebra sobre um corpo de característica zero. Então existem inteiros r e m tais que $(St_r(x_1,\dots,x_r))^m \in \mathrm{Id}(A)$.*

Demonstração. Pelo Teorema 5.3.10, sabemos que existem k e l inteiros não negativos tais que, para qualquer $n \geqslant 1$, temos que o n-ésimo cocaracter tem uma decomposição $\chi_n(A) = \sum_{\substack{\lambda\vdash n \\ \lambda\in H(k,l)}} m_\lambda \chi_\lambda$. Isto significa que $m_\lambda = 0$ sempre que $\lambda \notin H(k,l)$.

Vamos considerar $n = (l+1)(k+1)$ e a seguinte partição

$$\lambda = (\underbrace{l+1,\dots,l+1}_{k+1 \text{ vezes}}) \vdash n.$$

Como $\lambda \notin H(k,l)$, temos $m_\lambda = 0$. Agora, consideremos a seguinte tabela de Young associada a λ.

$$T_\lambda = \begin{array}{|c|c|c|c|}\hline 1 & k+2 & \cdots & (k+1)l+1 \\ \hline 2 & k+3 & \cdots & (k+1)l+2 \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline k+1 & 2k+2 & \cdots & (k+1)(l+1) \\ \hline \end{array}$$

Para esta tabela, temos

$$R_{T_\lambda} = X_1 \times X_2 \times \cdots \times X_{k+1} \text{ e } C_{T_\lambda} = Y_1 \times Y_2 \times \cdots \times Y_{l+1}$$

onde

$$\begin{aligned} X_1 &= S_{l+1}(1, k+2, \dots, (k+1)l+1), \\ X_2 &= S_{l+1}(2, k+3, \dots, (k+1)l+2), \\ &\vdots \\ X_{k+1} &= S_{l+1}(k+1, 2k+2, \dots, (k+1)(l+1) \\ Y_1 &= S_{k+1}(1, 2, \dots, k+1), \\ Y_2 &= S_{k+1}(k+2, k+3, \dots, 2k+2), \\ &\vdots \\ Y_{l+1} &= S_{k+1}((k+1)l+1, (k+1)l+2, \dots, (k+1)(l+1)). \end{aligned}$$

Assim, para $\tau \in C_{T_\lambda}$, podemos escrever

$$\tau = \tau_1 \cdots \tau_{l+1}, \text{ com } \tau_j \in Y_j,\ 1 \leqslant j \leqslant l+1.$$

Portanto, por definição, o idempotente essencial associado a T_λ é dado por

$$e_{T_\lambda} = \sum_{\substack{\sigma \in X_1 X_2 \cdots X_{k+1} \\ \tau_j \in Y_j}} \operatorname{sgn}(\tau_1) \cdots \operatorname{sgn}(\tau_{l+1}) \sigma \tau_1 \cdots \tau_{l+1}.$$

Agora considerando $f = f(x_1, \ldots, x_n) = x_1 \cdots x_n$ e lembrando que tomamos $n = (l+1)(k+1)$, obtemos que $e_{T_\lambda} f$ é igual a

$$\sum_{\sigma \in X_1 X_2 \cdots X_{k+1}} \sigma \Bigg(\sum_{\tau_j \in Y_j} \operatorname{sgn}(\tau_1) \cdots \operatorname{sgn}(\tau_l)\ \tau_1 \cdots \tau_l (x_1 \cdots x_{(k+1)l}) St_{l+1} \Bigg)$$

onde $St_{l+1} = St_{l+1}(x_{(k+1)l+1}, \ldots, x_{(k+1)(l+1)})$. Assim, repetindo esta ideia vamos obter que $e_{T_\lambda} f$ é dado por

$$\sum_{\sigma \in X_1 X_2 \cdots X_{k+1}} \sigma \Big(St_{k+1}(x_1, \ldots, x_{k+1}) \cdots S_{k+1}(x_{(k+1)l+1}, \ldots, x_{(k+1)(l+1)}) \Big)$$

e por fim, vamos obter $e_{T_\lambda} f$ como

$$\sum_{\sigma \in X_1 \cdots X_{k+1}} \Big(St_{k+1}(x_{\sigma(1)}, \ldots, x_{\sigma(k+1)}) \cdots S_{k+1}(x_{\sigma((k+1)l+1)}, \ldots, x_{\sigma((k+1)(l+1))}) \Big).$$

Agora, desde que $m_\lambda = 0$, pelo Teorema 5.3.4, temos $e_{T_\lambda} f \in \mathrm{Id}(A)$. Portanto, renomeando as variáveis de modo que $x_{(k+1)+i}, x_{(2k+2)+i}, \ldots, x_{(k+1)l+i}$ sejam trocadas por y_i, para $i = 1, 2, \ldots, k+1$ e $x_{(2k+2)}, \ldots, x_{(k+1)l}$ sejam trocadas por y_{k+1}, temos a seguinte identidade de A

$$e_{T_\lambda} f(y_1, \ldots, y_{k+1}) = \sum_{\sigma \in X_1 X_2 \cdots X_{k+1}} \Big(St_{k+1}(y_{\sigma(1)}, \ldots, y_{\sigma(k+1)}) \Big)^{(l+1)}$$

e isto é o mesmo que dizer que

$$((k+1)!)^{l+1} (St_{k+1}(y_1, \ldots, y_{k+1}))^{(l+1)} \in \mathrm{Id}(A).$$

Como estamos trabalhando em característica zero, vamos obter

$$(St_{k+1}(y_1, \ldots, y_{k+1}))^{(l+1)} \in \mathrm{Id}(A)$$

como queríamos mostrar. □

O próximo resultado, provado por Giambruno e Zaicev (2001), apresenta uma caracterização de álgebras de dimensão finita de crescimento polinomial. Neste resultado, para a álgebra A cujo índice de nilpotência do radical de Jacobson é igual a q, escreveremos simplesmente $J(A)^q = \{0\}$.

Teorema 5.3.12. *Seja A uma álgebra de dimensão finita sobre um corpo F de característica zero tal que $J(A)^q = \{0\}$. Então A tem crescimento polinomial se, e somente se,*

$$\chi_n(A) = \sum_{\substack{\lambda \vdash n \\ n-\lambda_1 < q}} m_\lambda \chi_\lambda.$$

Demonstração. Inicialmente, recordemos que de acordo com a Teorema 1.4.48 e a Observação 5.3.2, podemos assumir que F é um corpo algebricamente fechado. Suponhamos que A tem crescimento polinomial e que exista uma partição $\lambda \vdash n$ com $n - \lambda_1 \geqslant q$ tal que $m_\lambda \neq 0$.

Pelo Teorema 5.3.4, existe uma tabela de Young T_λ do tipo λ e um polinômio $f = f(x_1, \ldots, x_n) \in P_n$ tal que $e_{T_\lambda} f \notin \mathrm{Id}(A)$. Pela Observação 5.3.5, vemos que $e_{T_\lambda} f$ é uma combinação linear de polinômios que são, cada um deles, alternados em $\lambda_1 = t$ conjuntos disjuntos de variáveis.

Nosso próximo passo será mostrar que cada um dos polinômios alternados de $e_{T_\lambda} f$ descritos acima é uma identidade de A e, com isso, chegarmos ao absurdo que $e_{T_\lambda} f \in \mathrm{Id}(A)$.

Vamos considerar $A = A_1 \oplus \cdots \oplus A_m \dotplus J$ uma decomposição de Wedderburn–Malcev de A, onde $J = J(A)$ é seu radical de Jacobson. Como A tem crescimento polinomial, pelo Teorema 5.2.3, para todo $i = 1, \ldots, m$, temos que $A_i \cong F$ e $A_i J A_j = \{0\}$, para todo $j \neq i$.

Vamos fixar uma base $\mathcal{B}$ de A formada pela união de bases de $A_1, \ldots, A_m$ e J, respectivamente, e vamos considerar h um polinômio alternado de $e_{T_\lambda} f$. Nosso objetivo é mostrar que $h \in \mathrm{Id}(A)$.

Observamos que como $A_i A_j = A_i J A_j = \{0\}$, para todo $j \neq i$, para que h não seja uma identidade de A, ao fazer uma avaliação devemos substituir as suas variáveis por elementos de J e por elementos de no máximo uma única componente simples, digamos A_i. Por outro lado, temos que $\dim_F(A_i) = 1$ e portanto, usando o Exercício 3.2.10, podemos substituir em cada conjunto alternado no máximo um elemento de A_i, ou seja, podemos usar no máximo $\lambda_1 = t$ elementos de A_i na substituição.

Assim, ao considerar uma substituição não nula devemos tomar pelo menos $n - \lambda_1 \geqslant q$ elementos de J. Mas como $J^q = \{0\}$, essa avaliação é nula, ou seja,

$h \in \mathrm{Id}(A)$, o que é uma contradição já que $e_{T_\lambda} f \notin \mathrm{Id}(A)$. Isto nos faz concluir que $m_\lambda = 0$ sempre que $n - \lambda_1 \geqslant q$, tendo a decomposição desejada para $\chi_n(A)$.

Para provar a recíproca, vamos supor que $\chi_n(A) = \sum_{\substack{\lambda \vdash n \\ n-\lambda_1 < q}} m_\lambda \chi_\lambda$. Com isso, para qualquer partição $\lambda \vdash n$ tal que $n - \lambda_1 \geqslant q$ temos $m_\lambda = 0$. Mas quando $n - \lambda_1 < q$, ou seja, quando $\lambda_1 > n - q$, usando a fórmula do gancho dada na Equação (2.14), temos:

$$d_\lambda \leqslant \frac{n!}{\lambda_1!} < \frac{n!}{(n-q)!} = n(n-1)\cdots(n-q+1) \leqslant an^q$$

para alguma constante $a > 0$. Agora, lembre que, pela Observação 5.3.3, as multiplicidades m_λ são polinomialmente limitadas. Usando essa informação e o fato acima, da Equação (5.15), obtemos

$$c_n(A) = \sum_{\substack{\lambda \vdash n \\ n-\lambda_1 < q}} m_\lambda d_\lambda \leqslant Cn^t \sum_{\substack{\lambda \vdash n \\ n-\lambda_1 < q}} d_\lambda \leqslant \alpha n^{t+q}$$

para alguma constante α, completando a prova do teorema. □

O teorema acima nos diz que, para uma álgebra A de dimensão finita de crescimento polinomial, com $J(A)^q = \{0\}$, na decomposição do cocaracter $\chi_n(A)$, apenas as partições $\lambda = (\lambda_1, \ldots, \lambda_s) \vdash n$ cujos diagramas de Young associados contêm menos de q boxes abaixo da primeira linha podem contribuir com multiplicidades não nulas.

Vamos fazer um exemplo, utilizando a informação dada no Teorema 5.3.12 e, para isto, vamos usar a álgebra

$$N_3 = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} : a, b, c, d \in F \right\}.$$

Na Proposição 4.1.14, provamos que $\mathrm{Id}(N_3) = \langle [x_1, x_2, x_3], [x_1, x_2][x_3, x_4] \rangle_T$ e notamos que

$$J(N_3) = \left\{ \begin{pmatrix} 0 & b & c \\ 0 & 0 & d \\ 0 & 0 & 0 \end{pmatrix} : b, c, d \in F \right\}. \tag{5.18}$$

Exemplo 5.3.13. A partir da Equação (5.18), vemos que o índice de nilpotência de $J = J(N_3)$ é $q = 3$. Portanto, partições de n que podem contribuir com multiplicidade não nula na decomposição de $\chi_n(N_3)$ são aquelas cujo diagrama associado tem no máximo 2 boxes abaixo da primeira linha. Exemplos de partições deste tipo são (n), $(n-1,1)$ e $(n-2,1,1)$.

Além disso, usando a fórmula do gancho dada na Equação (2.14), temos

$$d_{(n)} = 1, \quad d_{(n-1,1)} = n-1 \quad \text{e} \quad d_{(n-2,1,1)} = \frac{(n-1)(n-2)}{2}$$

e a partir da Equação (4.6), observamos que

$$c_n(N_3) = \frac{n^2-n+2}{2} = 1 + (n-1) + \frac{(n-1)(n-2)}{2}.$$

Desta forma, basta provar que as multiplicidades correspondentes às partições (n), $(n-1,1)$ e $(n-2,1,1)$ são não nulas e, de acordo com Equação (5.15), teremos a decomposição

$$\chi_n(N_3) = \chi_{(n)} + \chi_{(n-1,1)} + \chi_{(n-2,1,1)}. \tag{5.19}$$

Para ver isto, vamos usar o Teorema 5.3.4 e, para qualquer uma das partições consideradas, vamos tomar f como o polinômio $f(x_1,\ldots,x_n) = x_1\cdots x_n$.

Obviamente usando a tabela de Young do tipo $(n) \vdash n$ e o idempotente essencial dado na Equação (5.16), temos $e_{T_{(n)}} f \notin \mathrm{Id}(N_3)$. Para ver isto, basta fazer a avaliação $\bar{x}_i = I_3$ para todo $i = 1,\ldots,n$ e temos $e_{T_{(n)}} f(\bar{x}_1,\ldots,\bar{x}_n) = n! I_3 \neq 0$, onde I_3 é a matriz identidade 3×3.

Agora, para a partição $\lambda = (n-1,1) \vdash n$, vamos usar o que vimos no Exemplo 5.1.7 e fazer a substituição $\bar{x}_i = I_3 + e_{12}$ para todo $i = 1,\ldots,n-1$ e $\bar{x}_n = e_{23}$. Pela Equação (5.5), vamos ter que $e_{T_{(n)}} f(\bar{x}_1,\ldots,\bar{x}_n)$ é igual a

$$\left(\sum_{\rho\in S_{n-1}} \bar{x}_{\rho(1)}\cdots\bar{x}_{\rho(n-1)}\right)\bar{x}_n - \bar{x}_n\left(\sum_{\rho\in S_{n-1}} \bar{x}_{\rho(2)}\cdots\bar{x}_{\rho(n-1)}\bar{x}_{\rho(1)}\right)$$

que é o mesmo que

$$(n-1)!(I_3+(n-1)e_{12})e_{23} - (n-1)!e_{23}(I_3+(n-1)e_{12}) = (n-1)(n-1)!e_{13} \neq 0.$$

Finalmente, também vamos usar o Exemplo 5.1.7 e faremos a substituição $\bar{x}_i = I_3$ para todo $i = 1,\ldots,n-2$, $\bar{x}_{n-1} = e_{12}$ e $\bar{x}_n = e_{23}$ em cada um dos

polinômios, $f_1, \ldots, f_6$ para obter a avaliação final. Temos

$$\begin{aligned} f_1(\bar{x}_1, \ldots, \bar{x}_n) &= (n-2)!e_{13} \\ f_2(\bar{x}_1, \ldots, \bar{x}_n) &= 0 \\ f_3(\bar{x}_1, \ldots, \bar{x}_n) &= (n-2)!e_{13} \\ f_4(\bar{x}_1, \ldots, \bar{x}_n) &= 0 \\ f_5(\bar{x}_1, \ldots, \bar{x}_n) &= 0 \\ f_6(\bar{x}_1, \ldots, \bar{x}_n) &= (n-2)!e_{13}. \end{aligned}$$

Pela Equação (5.6), vamos obter que o valor de $e_{T_{(n-2,1,1)}} f(\bar{x}_1, \ldots, \bar{x}_n)$ é $(n-2)!e_{13} \neq 0$ e isto mostra que a decomposição de $\chi_n(N_3)$ é como dada na Equação (5.19).

Assim, como fizemos com a sequência de codimensões, quando $\mathcal{V} = \text{var}(A)$ usaremos a notação $\chi_n(\mathcal{V})$, significando o cocaracter de uma álgebra geradora de $\mathcal{V}$, ou seja, é o mesmo que $\chi_n(A)$.

Podemos nos perguntar se o Teorema 5.3.12 pode ser generalizado para álgebras de dimensões quaisquer, ou seja, se temos um resultado geral que caracteriza PI-álgebras de crescimento polinomial de acordo com a decomposição da sequência de cocaracteres. Para responder essa questão, vamos usar o Corolário 5.1.13.

Teorema 5.3.14. *Seja $\mathcal{V}$ uma variedade de álgebras sobre um corpo F de característica zero. Então $\mathcal{V}$ tem crescimento polinomial se, e somente se, existe um inteiro não negativo q tal que*

$$\chi_n(\mathcal{V}) = \sum_{\substack{\lambda \vdash n \\ n - \lambda_1 < q}} m_\lambda \chi_\lambda.$$

Demonstração. Observe que, ao assumir que $\mathcal{V}$ tem crescimento polinomial, pelo Corolário 5.1.13, já sabemos que temos uma F-álgebra de dimensão finita A tal que $\mathcal{V} = \text{var}(A)$. Consequentemente, basta usar o teorema anterior para garantir a existência do inteiro não negativo q nas condições que exigimos. Para a recíproca, basta observar que a demonstração feita para a recíproca do Teorema 5.3.12 também pode se usada aqui e, então, a demonstração está concluída. □

Observamos que a decomposição do cocaracter de uma álgebra A nos informa sobre as multiplicidades dos FS_n-módulos simples, que aparecem na decomposição do FS_n-módulo $P_n(A)$. Isto nos leva a seguinte definição.

Definição 5.3.15. Dada a decomposição $\chi_n(A) = \sum_{\lambda \vdash n} m_\lambda \chi_\lambda$, para cada $n \geqslant 1$ definimos

$$l_n(A) := \sum_{\lambda \vdash n} m_\lambda$$

que é chamado n-ésimo cocomprimento de A.

Desta forma, temos uma sequência numérica $\{l_n(A)\}_{n \geqslant 1}$ associada a A, dita sequência de cocomprimentos de A. Observe que, para cada $n \geqslant 1$, o n-ésimo cocomprimento $l_n(A)$ conta o número de FS_n-módulos simples, que aparecem na decomposição de $P_n(A)$. Assim como foi feito no caso de codimensões, para $\mathcal{V} = \text{var}(A)$ uma variedade de álgebras gerada por uma F-álgebra A, definimos $l_n(\mathcal{V}) = l_n(A)$, para todo $n \geqslant 1$.

Exemplo 5.3.16. De acordo com a Equação (5.19), temos $l_n(N_3) = 3$.

Exercício 5.3.17. Mostre que se $B \in \text{var}(A)$, então $l_n(B) \leqslant l_n(A)$.

Proposição 5.3.18. *Sejam A e B duas F-álgebras. Se $\chi_n(A) = \sum_{\lambda \vdash n} m_\lambda \chi_\lambda$, $\chi_n(B) = \sum_{\lambda \vdash n} m'_\lambda \chi_\lambda$ e $\chi_n(A \oplus B) = \sum_{\lambda \vdash n} m''_\lambda \chi_\lambda$ são os n-ésimos cocaracteres de A, B e da soma direta $A \oplus B$, respectivamente, então*

$$m''_\lambda \leqslant m_\lambda + m'_\lambda \quad e \quad l_n(A \oplus B) \leqslant l_n(A) + l_n(B).$$

Demonstração. Para provar, basta usar a imersão de FS_n-módulos abaixo, dada na demonstração da Proposição 4.2.4

$$\frac{P_n}{P_n \cap Id(A \oplus B)} \hookrightarrow \frac{P_n}{P_n \cap Id(A)} \oplus \frac{P_n}{P_n \cap Id(B)}.$$

□

Definição 5.3.19. Dizemos que uma variedade $\mathcal{V}$ tem cocomprimento finito se existe uma constante C tal que $l_n(\mathcal{V}) \leqslant C$, para todo $n \geqslant 1$.

A partir da decomposição do cocaracter da álgebra de Grassmann $\mathcal{G}$ dada na Proposição 5.3.7, podemos observar que $l_n(\mathcal{G}) = n$. Assim, percebe-se uma diferença entre as variedades $\text{var}(N_3)$ e $\text{var}(\mathcal{G})$: enquanto o cocomprimento da primeira é finito, para todo $n \geqslant 1$, a sequência de cocomprimentos de $\text{var}(\mathcal{G})$ não é limitada por uma constante.

De fato, uma diferença marcante entre as álgebras N_3 e $\mathcal{G}$ é que a primeira tem crescimento polinomial enquanto que a segunda tem crescimento exponencial. Essas informações foram consideradas por Mishchenko, Regev e Zaicev (1999) e levaram à demonstração da seguinte caracterização de variedades de crescimento polinomial a partir do comportamento da sua sequência de cocomprimentos.

Teorema 5.3.20. *Uma variedade $\mathcal{V}$ tem cocomprimento finito se, se somente se, $\mathcal{V}$ tem crescimento polinomial.*

Exercícios V ou F da Seção 5.3: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, A representa uma F-álgebra.

(1) O n-ésimo cocaracter de A é o S_n-caracter da álgebra A como S_n-módulo.

(2) Se existe uma tabela de Young T_λ do tipo $\lambda \vdash n$ e um polinômio $f = f(x_1, \ldots, x_n) \in P_n$ tal que $e_{T_\lambda} f \in \mathrm{Id}(A)$, então a multiplicidade do caracter irredutível χ_λ é não nula em $\chi_n(A)$.

(3) A partição $(n-2, 2)$ tem multiplicidade não nula em $\chi_n(\mathcal{G})$.

(4) Se A é uma álgebra comutativa unitária, então $\chi_n(A) = \chi_{(n)} + \chi_{(n-1,1)}$.

(5) A partição $(3, 3, 3, 2) \vdash 11$ não pertence ao gancho infinito $H(2, 2)$.

(6) Se $J(A)$ tem índice de nilpotência 3, então a partição $(n-1, 1)$ aparece com multiplicidade não nula em $\chi_n(A)$.

(7) Se I é um ideal de A, então $l_n(A/I) \leqslant l_n(A)$.

(8) UT_2 é uma álgebra de cocomprimento finito.

5.4 Estrutura de álgebras de crescimento polinomial

Nesta seção, vamos estabelecer mais uma caracterização de variedades de crescimento polinomial. Para isto, consideraremos $\mathcal{V}$ uma variedade gerada por uma álgebra A e daremos uma condição necessária e suficiente sobre a estrutura de uma álgebra PI-equivalente à álgebra A, para garantir que $\mathcal{V}$ tenha crescimento polinomial.

Mais especificamente, mostraremos que uma álgebra A tem crescimento polinomial se, e somente se, $\mathrm{var}(A) = \mathrm{var}(B)$, onde B é uma álgebra de dimensão

finita, que é uma soma direta de subálgebras com propriedades particulares. Tais propriedades são referentes ao quociente de uma álgebra sobre seu radical de Jacobson. Para provar o resultado, começaremos com dois lemas que serão essenciais.

Lema 5.4.1. *Sejam $\bar{F}$ o fecho algébrico de um corpo de característica zero F e A uma álgebra de dimensão finita sobre $\bar{F}$. Então* $\mathrm{var}(A) = \mathrm{var}(B)$*, onde B é uma álgebra de dimensão finita sobre F tal que* $\dim_{\bar{F}}(A/J(A)) = \dim_F(B/J(B))$.

Demonstração. Consideremos uma decomposição de Wedderburn–Malcev $A = A_1 \oplus \cdots \oplus A_m \dotplus J$, onde cada A_i é uma $\bar{F}$-álgebra simples, $i = 1, \ldots, m$ e $J = J(A)$ é o radical de Jacobson de A. Pelo Teorema de Wedderburn–Artin, as constantes estruturais de cada A_i são racionais.

Para cada $i = 1, \ldots, m$, vamos tomar $\mathcal{B}_i$ uma base de A_i sobre $\bar{F}$ e considerar B_i a álgebra gerada por $\mathcal{B}_i$ sobre F. Como $\mathrm{char}(F) = 0$, temos que $\mathbb{Q} \subset F$ e, assim, cada B_i tem dimensão finita sobre F. Agora consideremos Γ uma base de J sobre $\bar{F}$, e B a álgebra gerada por $\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_m \cup \Gamma$ sobre F. Notemos que, como J é nilpotente, temos que B tem dimensão finita sobre F.

Por fim, temos

$$\dim_{\bar{F}}(A/J(A)) = \dim_{\bar{F}}(A_1 \oplus \cdots \oplus A_m) = \dim_F(B_1 \oplus \cdots \oplus B_m) = \dim_F(B/J(B))$$

e claramente temos $\mathrm{Id}(A) \subset \mathrm{Id}(B)$. Para ver a inclusão contrária, tomamos $f \in \mathrm{Id}(B)$, que podemos assumir ser multilinear, e vemos f se anula sob avaliação de elementos no conjunto $\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_m \cup \Gamma$. Como este último conjunto é uma base de A sobre $\bar{F}$, temos $f \in \mathrm{Id}(A)$. Concluímos que $\mathrm{var}(A) = \mathrm{var}(B)$, onde B é uma álgebra nas condições requeridas no teorema. □

Lema 5.4.2. *Sejam F um corpo algebricamente fechado de característica zero e A uma F-álgebra de dimensão finita de crescimento polinomial. Se $A = A_1 \oplus \cdots \oplus A_m \dotplus J(A)$ é uma decomposição de Wedderburn–Malcev de A e para cada $i = 1, \ldots, m$, definimos $E_i = A_i \dotplus J(A)$, então*

$$\mathrm{Id}(A) = \mathrm{Id}(E_1) \cap \cdots \cap \mathrm{Id}(E_m) \cap \mathrm{Id}(J(A)).$$

Demonstração. Inicialmente observamos que, como $A = A_1 \oplus \cdots \oplus A_m \dotplus J(A)$, considerando $E_i = A_i \dotplus J(A)$, temos $A = E_1 \dotplus \cdots \dotplus E_m$. Além disso, se para cada $i = 1, \ldots, m$, denotamos por J_i o radical de Jacobson de E_i, então $J_i = J(A) \subset E_i$.

É claro que

$$\mathrm{Id}(A) \subset \mathrm{Id}(E_1) \cap \cdots \cap \mathrm{Id}(E_m) \cap \mathrm{Id}(J(A)).$$

Para provar a inclusão contrária, suponhamos, por absurdo, que existe $f = f(x_1, \ldots, x_n)$ uma identidade multilinear de $\mathrm{Id}(E_1) \cap \cdots \cap \mathrm{Id}(E_m) \cap \mathrm{Id}(J(A))$ tal que $f \notin \mathrm{Id}(A)$.

Considerando $\mathcal{B}$ uma base de $A_1 \oplus \cdots \oplus A_m$ formada pela união das bases dos A_i's e Γ uma base de $J = J(A)$, temos que $\mathcal{A} = \mathcal{B} \cup \Gamma$ é uma base de A. Desde que $f \notin \mathrm{Id}(A)$, existem elementos $a_1, \ldots, a_n \in \mathcal{A}$ tais que $f(a_1, \ldots, a_n) \neq 0$. Por outro lado, como $f \in \mathrm{Id}(J)$, um destes elementos escolhidos não está em Γ, digamos que $a_k \notin \Gamma$. Assim, $a_k \in A_s$, para algum $s \in \{1, \ldots, m\}$.

Agora, como A tem crescimento polinomial, pelo Teorema 5.2.3, $A_i J A_j = \{0\}$, para todo $j \neq i$. Desde que $A_i A_j = \{0\}$ para $j \neq i$, a fim de que f não seja uma identidade de A, devemos ter $a_1, \ldots, a_n \in A_s \cup \Gamma$. Assim, obtemos que $a_1, \ldots, a_n \in A_s \dotplus J = E_s$ e isto é uma contradição, pois $f \in \mathrm{Id}(E_s)$. □

Agora, vamos apresentar o teorema que caracteriza variedades de álgebras de crescimento polinomial, estabelecendo uma condição necessária e suficiente sobre a estrutura de uma álgebra geradora para a variedade. Esse resultado foi provado por Giambruno e Zaicev (2001).

Teorema 5.4.3. *Seja A uma álgebra sobre um corpo F de característica zero. Então A tem crescimento polinomial se, e somente se,*

$$\mathrm{var}(A) = \mathrm{var}(B_1 \oplus \cdots \oplus B_k)$$

onde B_i é uma álgebra de dimensão finita sobre F tal que $\dim_F (B_i / J(B_i)) \leqslant 1$, *para todo $i = 1, \ldots, k$.*

Demonstração. Suponhamos que $\mathcal{V} = \mathrm{var}(A)$ tem crescimento polinomial. Pelo Corolário 5.1.13, sem perda de generalidade, podemos considerar que A é de dimensão finita sobre F. Inicialmente suponhamos que F é algebricamente fechado. Consideramos uma decomposição de Wedderburn–Malcev

$$A = A_1 \oplus \cdots \oplus A_m \dotplus J$$

onde $J = J(A)$ é o radical de Jacobson de A, e denotamos $E_i = A_i \dotplus J$. Pelo Lema 5.4.2, temos

$$\mathrm{Id}(A) = \mathrm{Id}(E_1) \cap \cdots \cap \mathrm{Id}(E_m) \cap \mathrm{Id}(J).$$

Pelo Lema 4.1.3, isto quer dizer que $\mathrm{Id}(A) = \mathrm{Id}(E_1 \oplus \cdots \oplus E_m \oplus J)$. Com isso, obtemos $\mathrm{var}(A) = \mathrm{var}(E_1 \oplus \cdots \oplus E_m \oplus J)$ e, como A tem crescimento polinomial, pelo Teorema 5.2.3, temos $\dim_F(A_i) = 1$.

Observando que o radical de Jacobson J_i de E_i é igual a J, isto nos leva a concluir que $\dim_F(E_i/J_i) = 1$ e $\dim_F(J/J) = 0$, ou seja, temos que as componentes da soma direta estão nas condições requeridas.

Para provar o caso geral, vamos assumir que F é um corpo arbitrário, não necessariamente algebricamente fechado.

Nessa situação, consideramos $\bar{F}$ o fecho algébrico de F e $\bar{A} = A \otimes \bar{F}$. Pela Equação (4.7), temos $\mathrm{Id}(\bar{A}) = \mathrm{Id}(A)$ e como $\dim_F(A) = \dim_{\bar{F}}(\bar{A})$, usando a primeira parte da demonstração temos $\mathrm{var}(\bar{A}) = \mathrm{var}(C_1 \oplus \cdots \oplus C_k)$, onde cada C_i é uma álgebra de dimensão finita sobre $\bar{F}$ com $\dim_{\bar{F}}(C_i/J(C_i)) \leqslant 1$.

Agora, usamos o Lema 5.4.1 para cada $i = 1, \ldots, k$ e obtemos que $\mathrm{var}(C_i) = \mathrm{var}(B_i)$, onde B_i é uma álgebra de dimensão finita sobre F tal que

$$\dim_F(B_i/J(B_i)) = \dim_{\bar{F}}(C_i/J(C_i)) \leqslant 1.$$

Por fim, obtemos

$$\begin{aligned} \mathrm{Id}(A) &= \mathrm{Id}(C_1 \oplus \cdots \oplus C_k) \\ &= \mathrm{Id}(C_1) \cap \cdots \cap \mathrm{Id}(C_k) \\ &= \mathrm{Id}(B_1) \cap \cdots \cap \mathrm{Id}(B_k) \\ &= \mathrm{Id}(B_1 \oplus \cdots \oplus B_k) \end{aligned}$$

e, assim, $\mathrm{var}(A) = \mathrm{var}(B_1 \oplus \cdots \oplus B_k)$, de acordo com o que queríamos.

Para provar a recíproca, suponhamos que $\mathrm{var}(A) = \mathrm{var}(B_1 \oplus \cdots \oplus B_k)$, onde cada B_i é uma álgebra de dimensão finita sobre F e $\dim_F(B_i/J(B_i)) \leqslant 1$, com $1 \leqslant i \leqslant k$. Usando a Proposição 4.2.15, vamos assumir que F é algebricamente fechado.

Como $\mathrm{var}(A) = \mathrm{var}(B_1 \oplus \cdots \oplus B_k)$ temos, para todo $n \geqslant 1$,

$$c_n(A) = c_n(B_1 \oplus \cdots \oplus B_k) \leqslant c_n(B_1) + \cdots + c_n(B_k). \tag{5.20}$$

Como $\dim_F(B_i/J(B_i)) \leqslant 1$, com $1 \leqslant i \leqslant k$, temos, para cada i, que ou $B_i = J(B_i)$ ou $B_i \cong F \dotplus J(B_i)$. Se $B_i = J(B_i)$, como B_i tem dimensão finita, então B_i é nilpotente e, com isso, $c_n(B_i) = 0$, para todo n suficientemente grande. Se $B_i \cong F \dotplus J(B_i)$, então, pelo Exemplo 4.5.18, $\exp(B_i) = 1$ e, pelo Teorema 5.2.2, B_i tem crescimento polinomial. Portanto, pela Equação (5.20), temos que A tem crescimento polinomial. □

No que segue, vamos concentrar em um mesmo resultado as principais caracterizações de variedades de crescimento polinomial, que demonstramos nas Seções 5.2 e 5.3 e também aqui nesta seção.

Teorema 5.4.4. *Seja $\mathcal{V}$ uma variedade de álgebras sobre um corpo F de característica zero. Então, as seguintes condições são equivalentes:*

1. *$\mathcal{V}$ tem crescimento polinomial;*
2. *$UT_2, \mathcal{G} \notin \mathcal{V}$;*
3. *$\mathcal{V} = \mathrm{var}(B_1 \oplus \cdots \oplus B_m)$, onde B_i é uma álgebra de dimensão finita sobre F tal que $\dim_F(B_i/J(B_i)) \leqslant 1$, para todo $i = 1, \ldots, m$;*
4. *existe um inteiro não negativo q tal que*

$$\chi_n(\mathcal{V}) = \sum_{\substack{\lambda \vdash n \\ n - \lambda_1 < q}} m_\lambda \chi_\lambda;$$

5. $\exp(\mathcal{V}) \leqslant 1$.

Exercícios V ou F da Seção 5.4: Verifique se cada afirmativa abaixo é verdadeira ou falsa, justificando convenientemente. Nas afirmações, A e B representam F-álgebras, onde F é um corpo de característica zero.

(1) Se $\mathrm{var}(A) = \mathrm{var}(B)$, então $\dim_F(A/J(A)) = \dim_F(B/J(B))$.

(2) Se $\dim_F(A)$ é finita, então $A \sim_{PI} B_1 \oplus \cdots \oplus B_m$, onde $\dim(B_i)$ é finita e $\dim(B_i/J(B_i)) \leqslant 1$, para todo $i = 1, \ldots, m$.

(3) $\mathrm{var}(M_2(\mathbb{C})) = \mathrm{var}(\mathcal{A})$, onde $\mathcal{A}$ é uma álgebra de dimensão finita sobre $\mathbb{R}$ tal que $\dim_{\mathbb{R}}(\mathcal{A}/J(\mathcal{A})) = 4$.

(4) Se A é uma álgebra comutativa unitária, então $\dim_F(A/J(A)) \leqslant 1$.

(5) Se A é uma álgebra comutativa unitária, então $\dim_F(A/J(A)) \geqslant 1$ e portanto, A não pode ter crescimento polinomial.

(6) Se $A \sim_{PI} B_1 \oplus \cdots \oplus B_m$, onde $B_i \cong F$, para todo $i = 1, \ldots, m$, então A tem crescimento polinomial.

6 Para onde seguir?

Neste capítulo, nos dedicamos a apresentar resultados mais recentes no desenvolvimento da PI-teoria. Vamos introduzir novos exemplos de álgebras com estruturas adicionais, complementando o que já foi estudado no Capítulo 4 a respeito de superálgebras, de forma que teremos uma situação paralela a tratar. A partir de agora, sempre que trabalharmos com álgebras sobre as quais não consideramos estruturas adicionais, ou seja, no contexto de PI-álgebras simplesmente, vamos nos referir ao caso ordinário. Assim, vamos discutir diversos resultados de classificação de variedades de crescimento polinomial, tanto no contexto ordinário quanto no contexto de álgebras munidas de novas estruturas.

Os resultados apresentados terão as correspondentes referências listadas para consulta e não serão demonstrados aqui, pois o objetivo principal do capítulo é conduzir o leitor interessado aos limites da pesquisa recentemente realizada na área, no que diz respeito à sequência de codimensões em suas diversas formas de apresentação.

Para nossos propósitos, lembremos que sempre que $\mathcal{V}$ for uma variedade de crescimento polinomial, vamos dizer que $\mathcal{V}$ é uma variedade de crescimento n^k, para algum inteiro $k \geqslant 0$ e para sua sequência de codimensões, escreveremos $c_n(\mathcal{V}) \approx q\, n^k$, para algum $q \in \mathbb{Q}$.

6.1 PI-álgebras com estruturas adicionais

Noções similares de T-ideais, variedades de álgebras, polinômios multilineares e codimensões, tratados no contexto ordinário da PI-teoria, têm sido naturalmente estendidas para o caso de álgebras munidas de alguma estrutura adicional. Como exemplo de tais estruturas adicionais, destacamos as superálgebras e as álgebras munidas de uma involução $*$. Alguns resultados sobre superálgebras já foram tratados anteriormente. Agora vamos definir as $*$-álgebras.

O estudo de álgebras com estruturas adicionais passou a ser um foco de investigação nos últimos anos e, consequentemente, caracterizações de variedades de crescimento polinomial, análogas a que foi dada por Kemer, também têm sido fornecidas nesses contextos. A fim de apresentar tais caracterizações, nesta seção, faremos uma breve descrição dessas estruturas.

Na Seção 4.4, definimos o conceito de superálgebras e estudamos diversas propriedades dessa classe de álgebras. Agora, vamos introduzir o conceito de $*$-álgebra, iniciando com o conceito de involução.

Definição 6.1.1. Uma aplicação F-linear $* : A \to A$ definida sobre uma F-álgebra A é chamada involução se, para todos $a, b \in A$, temos

1. $(ab)^* = b^*a^*$;
2. $(a^*)^* = a$.

Observação 6.1.2. A definição de involução dada acima é chamada por alguns autores de involução do primeiro tipo.

Um exemplo importante é a involução ρ definida sobre a álgebra UT_n por

$$(e_{ij})^\rho = e_{n-j+1,n-i+1}, \text{ para } 1 \leqslant i \leqslant j \leqslant n.$$

Essa involução é chamada involução reflexão e ela é definida pela reflexão de uma matriz triangular superior ao longo de sua diagonal secundária.

Dizemos que A é uma álgebra com involução, ou simplesmente que A é uma $*$-álgebra, se esta possui uma involução. Vamos dar alguns exemplos de involuções e $*$-álgebras que serão importantes para estabelecer os resultados desta seção.

Exemplo 6.1.3. Se A é uma álgebra comutativa, então a aplicação identidade é uma involução sobre A, dita involução trivial.

Observamos que se a aplicação identidade é uma involução sobre uma álgebra A, então A é necessariamente uma álgebra comutativa.

Exemplo 6.1.4. Consideremos a álgebra comutativa $D = F \oplus F$ e $* : D \to D$ a aplicação dada por $(a, b)^* = (b, a)$. Temos que $*$ é uma involução não trivial sobre D denominada involução troca. Denotamos por D_* a $*$-álgebra D munida dessa involução.

Observação 6.1.5. Observe que se A é uma $*$-álgebra unitária, então

$$1 = (1^*)^* = (1^* \cdot 1)^* = 1^* \cdot 1 = 1^*.$$

Em particular, a álgebra F admite apenas a involução trivial.

Sobre a álgebra de matrizes $M_n(F)$, temos duas involuções bastante conhecidas como apresentadas nos próximos exemplos.

Exemplo 6.1.6. Em $M_n(F)$, temos definida a involução

$$\begin{aligned} t : M_n(F) &\to M_n(F) \\ (a_{ij}) &\mapsto (a_{ji}) \end{aligned}$$

chamada de involução transposta.

Exemplo 6.1.7. Quando n é par, ou seja, $n = 2k$, para algum $k \geqslant 1$, podemos considerar a aplicação $s : M_{2k}(F) \to M_{2k}(F)$ dada por

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}^s = \begin{pmatrix} D^t & -B^t \\ -C^t & A^t \end{pmatrix}$$

onde $A, B, C, D \in M_k(F)$ e t é a aplicação transposta. A aplicação s é uma involução, denominada involução simplética, que está definida apenas sobre matrizes de ordem par.

Exemplo 6.1.8. Consideremos a subálgebra de UT_4 definida, no Exemplo 4.5.20, por

$$M = F(e_{11} + e_{44}) + Fe_{12} + F(e_{22} + e_{33}) + Fe_{34}.$$

Vamos considerar a involução reflexão ρ sobre M, isto é,

$$\begin{pmatrix} a & b & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & c & d \\ 0 & 0 & 0 & a \end{pmatrix}^\rho = \begin{pmatrix} a & d & 0 & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & c & b \\ 0 & 0 & 0 & a \end{pmatrix}.$$

Denotaremos a álgebra M com involução reflexão por M_*.

Se A é uma $*$-álgebra, então podemos considerar os seguintes subespaços vetoriais

$$A^+ = \{a \in A \,:\, a^* = a\} \quad \text{e} \quad A^- = \{a \in A \,:\, a^* = -a\}$$

ditos subespaço dos elementos simétricos e subespaço dos elementos antissimétricos de A, respectivamente. De imediato, é fácil ver que $A^+ \cap A^- = \{0\}$ e, considerando $\text{char}(F) \neq 2$, temos que todo $a \in A$ pode ser escrito como

$$a = \frac{a + a^*}{2} + \frac{a - a^*}{2}, \quad \text{com} \quad \frac{a + a^*}{2} \in A^+ \quad \text{e} \quad \frac{a - a^*}{2} \in A^-.$$

Consequentemente, podemos escrever $A = A^+ \dot{+} A^-$.

Exemplo 6.1.9. Para a $*$-álgebra D_*, temos $D_*^+ = F(1,1)$ e $D_*^- = F(1,-1)$.

Exemplo 6.1.10. Para a $*$-álgebra M_*, observamos que $M_*^+ = F(e_{11} + e_{44}) + F(e_{22} + e_{33}) + F(e_{12} + e_{34})$ e $M_*^- = F(e_{12} - e_{34})$.

Exercício 6.1.11. Considere $a_1, a_2 \in A^+$ e $b_1, b_2 \in A^-$. Mostre que

(*a*) $[a_1, a_2] \in A^-$, $[b_1, b_2] \in A^-$ e $[a_1, b_1] \in A^+$;

(*b*) $a_1 \circ a_2 \in A^+$, $b_1 \circ b_2 \in A^+$ e $a_1 \circ b_1 \in A^-$.

Se A é uma $*$-álgebra e B é uma subálgebra de A, dizemos que B possui involução induzida se $*$ é uma involução de B pela restrição, ou seja, $B^* = B$. Nesse caso, dizemos que B é uma $*$-subálgebra de A.

Como exemplo, para cada $k \geqslant 2$ vamos definir a seguir, $*$-subálgebras de UT_{2k}, onde $* = \rho$ é a involução reflexão. Para isso, vamos considerar

$$P_k, \; Q_k \;\text{ e }\; R_k \tag{6.1}$$

as seguintes subálgebras de UT_{2k}:

$$P_k = \text{span}_F\{I_{2k}, E, \ldots, E^{k-2}; e_{12} - e_{2k-1,2k}, e_{13}, \ldots, e_{1k}, e_{k+1,2k}, \ldots, e_{2k-2,2k}\}$$

$$Q_k = \text{span}_F\{I_{2k}, E, \ldots, E^{k-2}; e_{12} + e_{2k-1,2k}, e_{13}, \ldots, e_{1k}, e_{k+1,2k}, \ldots, e_{2k-2,2k}\}$$

$$R_k = \text{span}_F\{e_{11} + e_{2k,2k}, E, \ldots, E^{k-2}; e_{12}, e_{13}, \ldots, e_{1k}, e_{k+1,2k}, \ldots, e_{2k-1,2k}\} \text{ onde}$$

I_{2k} é a matriz identidade $2k \times 2k$ e $E = \displaystyle\sum_{i=2}^{k-1} e_{i,i+1} + e_{2k-i,2k-i+1} \in UT_{2k}$.

Para cada $k \geqslant 2$, essas álgebras com involução reflexão ρ são $*$-subálgebras de UT_{2k} com involução induzida, sendo denotadas, respectivamente, por

$$P_{k,\rho}, \quad Q_{k,\rho} \text{ e } \quad R_{k,\rho}.$$

Note que as $*$-álgebras $P_{k,\rho}$ e $Q_{k,\rho}$ são unitárias, enquanto $R_{k,\rho}$ não é.

Exemplo 6.1.12. Considerando $k = 4$, temos

$$\text{(a) } P_{4,\rho} = \left\{ \begin{pmatrix} a & b & c & d & 0 & 0 & 0 & 0 \\ 0 & a & e & f & 0 & 0 & 0 & 0 \\ 0 & 0 & a & e & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & e & f & g \\ 0 & 0 & 0 & 0 & 0 & a & e & h \\ 0 & 0 & 0 & 0 & 0 & 0 & a & -b \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a \end{pmatrix} : a,b,c,d,e,f,g,h \in F \right\};$$

$$\text{(b) } Q_{4,\rho} = \left\{ \begin{pmatrix} a & b & c & d & 0 & 0 & 0 & 0 \\ 0 & a & e & f & 0 & 0 & 0 & 0 \\ 0 & 0 & a & e & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & e & f & g \\ 0 & 0 & 0 & 0 & 0 & a & e & h \\ 0 & 0 & 0 & 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a \end{pmatrix} : a,b,c,d,e,f,g,h \in F \right\};$$

$$\text{(c) } R_{4,\rho} = \left\{ \begin{pmatrix} a & b & c & d & 0 & 0 & 0 & 0 \\ 0 & 0 & e & f & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & e & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & e & f & g \\ 0 & 0 & 0 & 0 & 0 & 0 & e & h \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & i \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a \end{pmatrix} : a,b,c,d,e,f,g,h,i \in F \right\}.$$

Exercício 6.1.13. Para cada $*$-álgebra $A \in \{P_{4,\rho}, \ Q_{4,\rho}, \ R_{4,\rho}\}$, determine os subespaços A^+ e A^-.

Na Seção 4.4, vimos que à uma superálgebra A, podemos associar o automorfismo de ordem no máximo 2 induzido pela graduação. No caso de uma $*$-álgebra,

temos que a involução $*$ é um antiautomorfismo de A. Vamos recordar este conceito abaixo.

Definição 6.1.14. Uma aplicação F-linear $\psi : A \to A$ é um antiautomorfismo de uma álgebra A se $\psi(ab) = \psi(b)\psi(a)$, para todos $a, b \in A$.

De fato, quando A é uma álgebra munida de uma involução $*$, podemos observar que $*$ satisfaz essa definição e, portanto, é um antiautomorfismo de ordem no máximo 2 de A. Observamos que uma $*$-álgebra com um antiautomorfismo de ordem 1 é uma álgebra comutativa.

Para estabelecer uma nomenclatura comum entre superálgebras e $*$-álgebras, introduzimos o conceito de φ-álgebras.

Definição 6.1.15. Uma álgebra A munida de um automorfismo ou um antiautomorfismo φ de ordem no máximo 2 será chamada de φ-álgebra. Assim, qualquer superálgebra ou qualquer álgebra com involução, será uma φ-álgebra.

Observamos que qualquer álgebra com graduação trivial e qualquer álgebra comutativa com involução trivial são exemplos de φ-álgebras com automorfismo e antiautomorfismo de ordem 1, respectivamente.

Notemos que, se A é uma φ-álgebra, podemos escrever $A = A_\varphi^+ \dot{+} A_\varphi^-$, onde

$$A_\varphi^+ = \{a \in A : a^\varphi = a\} \quad \text{e} \quad A_\varphi^- = \{a \in A : a^\varphi = -a\}.$$

De fato, quando φ é um automorfismo de ordem no máximo 2, ou seja, se A é uma superálgebra, temos $A_\varphi^+ = A^{(0)}$ e $A_\varphi^- = A^{(1)}$. Por outro lado, se φ é um antiautomorfismo de ordem no máximo 2, ou seja, se A é uma $*$-álgebra, temos que $A_\varphi^+ = A^+$ e $A_\varphi^- = A^-$.

A seguir, vamos estender a linguagem utilizada no contexto ordinário de PI-álgebras para φ-álgebras, definindo primeiramente os conceitos de φ-identidades polinomiais e φ-codimensões.

Para fazer isto, vamos considerar $X = \{x_1, x_2, \ldots\}$ um conjunto enumerável de variáveis não comutativas e $F\langle X, \varphi\rangle = \langle x_1, x_1^\varphi, x_2, x_2^\varphi, \ldots\rangle$ a álgebra associativa livre munida de um automorfismo ou um antiautomorfismo φ de ordem no máximo 2. Observamos que, ao considerar $y_i = x_i + x_i^\varphi$ e $z_i = x_i - x_i^\varphi$, temos que $F\langle X, \varphi\rangle = F\langle y_1, z_1, y_2, z_2, \ldots\rangle$ e definindo $Y = \{y_i : i \geqslant 1\}$ e $Z = \{z_i : i \geqslant 1\}$, os elementos da φ-álgebra livre $F\langle X, \varphi\rangle = F\langle Y \cup Z\rangle$ são combinações lineares de palavras nas variáveis em Y e em Z chamados de φ-polinômios.

Exemplo 6.1.16. $f(y_1, z_1, z_2) = z_2^4 - 2z_1[y_1, z_1] + 3y_1z_2$ e $g(y_1, y_2, z_1, z_2, z_3) = y_2z_1y_2z_3^2 + z_3[y_1, z_3]y_2z_2$ são φ-polinômios.

Chamamos atenção para o fato que, se φ é um automorfismo de ordem no máximo 2, $F\langle Y \cup Z\rangle$ admite uma estrutura de superálgebra, definindo $F\langle Y \cup Z\rangle^{(0)}$ o subespaço gerado por todos monômios nas variáveis $Y \cup Z$ que possuem um número par de variáveis em Z, e $F\langle Y \cup Z\rangle^{(1)}$ será o subespaço gerado por todos monômios nas variáveis $Y \cup Z$ que possuem um número ímpar de variáveis em Z. Por outro lado, um antiautomorfismo $\varphi = *$ de ordem no máximo 2 induz uma estrutura de $*$-álgebra em $F\langle Y \cup Z\rangle$, onde as variáveis de Y são simétricas $y_i^* = y_i$, e as variáveis de Z são antissimétricas $z_i^* = -z_i$.

Definição 6.1.17. Seja A uma φ-álgebra. Dizemos que um φ-polinômio $f = f(y_1, \ldots, y_n, z_1, \ldots, z_m) \in F\langle Y \cup Z\rangle$ é uma φ-identidade polinomial de A se $f(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0$ para quaisquer $a_1, \ldots, a_n \in A_\varphi^+$ e $b_1, \ldots, b_m \in A_\varphi^-$.

Na definição anterior, se A é uma superálgebra, dizemos que f é uma identidade graduada de A e, quando A é uma $*$-álgebra, dizemos que f é uma $*$-identidade de A. Notemos que, para uma superálgebra A com graduação trivial, temos que z é uma identidade graduada de A enquanto que, para uma $*$-álgebra comutativa com involução trivial, z é uma $*$-identidade.

Exemplo 6.1.18. Lembremos, pelo Exemplo 4.4.23, que D^{gr} é a álgebra $D = F \oplus F$ com graduação $(F(1, 1), F(1, -1))$. Temos que $[y_1, y_2]$, $[z_1, z_2]$, $[y_1, z_2]$ e $[z_1, y_2]$ são identidades graduadas de D^{gr}. Podemos notar que esses mesmos polinômios são $*$-identidades da $*$-álgebra D_* definida no Exemplo 6.1.4.

Exemplo 6.1.19. A partir do Exemplo 6.1.10, vemos que z_1z_2 é uma $*$-identidade de M_*.

Exercício 6.1.20. Mostre que

(*a*) $[y_1, y_2]$ e $[y, z]$ são identidades graduadas da superálgebra $\mathcal{G}^{gr}$ como definida no Exemplo 4.4.3;

(*b*) $[y_1, y_2]$ e z_1z_2 são identidades graduadas da superálgebra UT_2^{gr} como definida no Exemplo 4.4.14.

Definimos o T_φ-ideal de A de uma φ-álgebra A como o ideal $\mathrm{Id}^\varphi(A)$ de $F\langle Y \cup Z\rangle$ formado por todas as φ-identidades polinomiais de A.

No caso em que A é uma $*$-álgebra, denotamos por $\mathrm{Id}^*(A)$ o T_*-ideal de A e quando A é uma superálgebra, escrevemos $\mathrm{Id}^{gr}(A)$ para denotar o T_2-ideal de A.

Assim como no caso ordinário, sobre um corpo de característica zero, todo T_φ-ideal é finitamente gerado, e usamos a notação $\langle f_1, \ldots, f_m \rangle_{T_\varphi}$ para indicar que $\mathrm{Id}^\varphi(A)$ é gerado por $f_1, \ldots, f_m$.

Observamos que, quando uma superálgebra tem graduação trivial, seu T_2-ideal pode ser obtido diretamente do seu T-ideal. Para as álgebras UT_2 e $\mathcal{G}$ com graduação trivial, continuaremos usando a mesma notação para nos referirmos como superálgebras. Lembrando dos T-ideais determinados nos Teoremas 4.3.2 e 4.3.5, colocamos dois exemplos a seguir.

Exemplo 6.1.21. Para as superálgebras UT_2 e $\mathcal{G}$, temos o seguinte:

1. $\mathrm{Id}^{gr}(UT_2) = \langle [y_1, y_2][y_3, y_4], z \rangle_{T_2}$;
2. $\mathrm{Id}^{gr}(\mathcal{G}) = \langle [y_1, y_2, y_3], z \rangle_{T_2}$.

No próximo resultado, coletamos os T_φ-ideais das principais φ-álgebras desta seção com as referências para as respectivas demonstrações.

Lema 6.1.22. *Temos os seguintes* T_φ*-ideais:*

1. $\mathrm{Id}^{gr}(D^{gr}) = \langle [y_1, y_2], [y, z], [z_1, z_2] \rangle_{T_2}$, *Giambruno e Mishchenko (2001);*
2. $\mathrm{Id}^{gr}(UT_2^{gr}) = \langle [y_1, y_2], z_1 z_2 \rangle_{T_2}$, *Valenti (2002);*
3. $\mathrm{Id}^{gr}(\mathcal{G}^{gr}) = \langle [y_1, y_2], [y, z], z_1 \circ z_2 \rangle_{T_2}$, *Giambruno, Mishchenko e Zaicev (2001);*
4. $\mathrm{Id}^*(D_*) = \langle [y_1, y_2], [y, z], [z_1, z_2] \rangle_{T_*}$, *Giambruno e Mishchenko (2001);*
5. $\mathrm{Id}^*(M_*) = \langle z_1 z_2 \rangle_{T_*}$, *Mishchenko e Valenti (2000).*

Também é conhecido que qualquer φ-identidade é consequência de uma φ-identidade multilinear. Por este motivo, para $n \geqslant 1$, consideramos

$$P_n^\varphi = \mathrm{span}_F \{ w_{\sigma(1)} \cdots w_{\sigma(n)} : \sigma \in S_n, w_i = y_i \text{ ou } w_i = z_i, \, i \in \mathbb{N} \}$$

o espaço dos φ-polinômios multilineares de grau n nas variáveis $y_1, z_1, \ldots, y_n, z_n$ e estudamos o comportamento das φ-identidades de uma φ-álgebra, considerando o espaço quociente

$$P_n^\varphi(A) := \frac{P_n^\varphi}{P_n^\varphi \cap \mathrm{Id}^\varphi(A)}.$$

Desta forma, temos interesse na seguinte definição.

Definição 6.1.23. Definimos a n-ésima φ-codimensão de uma φ-álgebra A como a dimensão de $P_n^{\varphi}(A)$ sobre F e a denotamos por $c_n^{\varphi}(A)$.

Se A é uma álgebra com involução, escrevemos $c_n^*(A)$ como a n-ésima $*$-codimensão de A. Por outro lado, se A é uma superálgebra, denotamos por $c_n^{gr}(A)$ a sua n-ésima codimensão graduada.

Quando A é uma PI-álgebra com um automorfismo ou um antiautomorfismo φ de ordem no máximo 2, a relação abaixo entre sua codimensão no caso ordinário e a sua φ-codimensão foi dada por Giambruno e Regev (1985)

$$c_n(A) \leqslant c_n^{\varphi}(A) \leqslant 2^n c_n(A). \tag{6.2}$$

Paralelamente ao caso ordinário, também estamos interessados em φ-álgebras cuja sequência de φ-codimensões é polinomialmente limitada, ou seja, aquelas para as quais existem constantes k e $a \geqslant 0$ tais que $c_n^{\varphi}(A) \leqslant an^k$. Nesse caso, dizemos que A tem crescimento polinomial da sequência de φ-codimensões.

É importante destacar que La Mattina, Mauceri e Misso (2009) provaram que se A é uma φ-álgebra unitária de crescimento polinomial das φ-codimensões, então a sequência $\{c_n^{\varphi}(A)\}_{n\geqslant 1}$ é descrita por um polinômio com coeficientes racionais, ou seja, $c_n^{\varphi}(A) \approx qn^s$, para algum $s \geqslant 0$ e $q \in \mathbb{Q}$.

Por outro lado, dizemos que a sequência de φ-codimensões de uma φ-álgebra cresce exponencialmente se existe um inteiro $\alpha \geqslant 2$ tal que $c_n^{\varphi}(A) \geqslant \alpha^n$, para todo $n \geqslant 1$. Através da Equação (6.2), notamos que se A é uma álgebra de crescimento exponencial, então a sequência de φ-codimensões de A cresce exponencialmente, ou seja, A tem crescimento exponencial como φ-álgebra. Desta forma, claramente as superálgebras $\mathcal{G}^{gr}$ e UT_2^{gr} têm crescimento exponencial.

Também é conhecido que a álgebra M definida no Exemplo 4.5.20 é PI-equivalente à álgebra UT_2 e, portanto,

$$c_n(UT_2) = c_n(M) \leqslant c_n^{\varphi}(M) \tag{6.3}$$

o que implica que $c_n^*(M_*)$ cresce exponencialmente.

Denotamos por $\mathrm{var}^{\varphi}(A)$ a classe de todas as φ-álgebras que satisfazem as φ-identidades satisfeitas por A, dita a φ-variedade gerada por A. No caso em que A é uma $*$-álgebra, denotaremos por $\mathrm{var}^*(A)$ a $*$-variedade gerada por A e caso A seja uma superálgebra, denotaremos por $\mathrm{var}^{gr}(A)$ a supervariedade gerada por A. Além disso, diremos que a φ-variedade $\mathcal{V}$ tem crescimento polinomial se $\mathcal{V} = \mathrm{var}^{\varphi}(A)$, para uma φ-álgebra A de crescimento polinomial da sequência de φ-codimensões.

Com todos esses conceitos estabelecidos, podemos apresentar os teoremas que caracterizam φ-variedades de crescimento polinomial através da exclusão de φ-álgebras da variedade. Nos referimos a esses teoremas como sendo do tipo Kemer. No caso de supervariedades, o resultado foi provado por Giambruno, Mishchenko e Zaicev (2001) e, no caso de $*$-variedades, a demonstração foi feita por Giambruno e Mishchenko (2001).

Teorema 6.1.24. *A sequência $c_n^{gr}(\mathcal{V})$ é limitada polinomialmente se, e somente se, $\mathcal{G}, UT_2, \mathcal{G}^{gr}, UT_2^{gr}, D^{gr} \notin \mathcal{V}$.*

Teorema 6.1.25. *A sequência $c_n^*(\mathcal{V})$ é limitada polinomialmente se, e somente se, $D_*, M_* \notin \mathcal{V}$.*

Pelas observações que fizemos anteriormente, a presença das φ-álgebras $\mathcal{G}$, $UT_2, \mathcal{G}^{gr}, UT_2^{gr}$ e M_* nos dois últimos teoremas não nos causa estranheza, mas como D é uma álgebra comutativa, temos $c_n(D) = 1$, para todo $n \geqslant 1$, e então devemos explicar porque D^{gr} e D_* aparecem nestes teoremas. A Equação (6.2) não nos indica que D^{gr} e D_* têm crescimento exponencial, mas tal fato foi provado por Giambruno e Mishchenko (ibid.).

Proposição 6.1.26. *Considere D_φ como uma das φ-álgebras: D_* ou D^{gr}. Então $c_n^\varphi(D_\varphi) = 2^n$, para todo $n \geqslant 1$.*

Como no caso ordinário, temos que as subvariedades próprias das variedades geradas pelas superálgebras $\mathcal{G}, UT_2, \mathcal{G}^{gr}, UT_2^{gr}$ e D^{gr} são de crescimento polinomial das codimensões graduadas. O mesmo ocorre com as variedades geradas por D_* e M_*, ou seja, todas as subvariedades próprias de $\mathrm{var}^*(D_*)$ e $\mathrm{var}^*(M_*)$ têm crescimento polinomial das $*$-codimensões.

Usando as mesmas ideias utilizadas no contexto ordinário, que foram apresentadas na Seção 5.2, também podemos concluir que $\mathrm{var}^{gr}(\mathcal{G})$, $\mathrm{var}^{gr}(UT_2)$, $\mathrm{var}^{gr}(\mathcal{G}^{gr})$, $\mathrm{var}^{gr}(UT_2^{gr})$ e $\mathrm{var}^{gr}(D^{gr})$ são as únicas variedades de crescimento quase polinomial das codimensões graduadas e que $\mathrm{var}^*(D_*)$ e $\mathrm{var}^*(M_*)$ são as únicas variedades de crescimento quase polinomial das $*$-codimensões.

Na próxima seção, vamos apresentar os resultados que classificam as subvariedades de variedades de crescimento quase polinomial, tanto no contexto ordinário, quanto no contexto de álgebras com estrutura adicional.

6.2 Variedades minimais de crescimento polinomial

Pelos resultados apresentados na Seção 5.2, sabemos que todas as subvariedades próprias de cada uma das variedades $\mathrm{var}(\mathcal{G})$ e $\mathrm{var}(UT_2)$ têm crescimento polino-

mial. Nesta seção, vamos apresentar a classificação de todas essas subvariedades que foi dada por La Mattina (2007). Dentre elas, destacamos as variedades minimais de crescimento polinomial, as quais definiremos a seguir.

Recordemos que o Teorema 4.2.14 nos diz que ao considerar uma álgebra de crescimento polinomial, temos que sua sequência de codimensões é dada por um polinômio de algum grau $k \geqslant 0$ com coeficientes racionais. Assim, a partir de agora, sempre que $\mathcal{V}$ for uma variedade de crescimento polinomial vamos dizer que $\mathcal{V}$ é uma variedade de crescimento n^k, para algum inteiro $k \geqslant 0$ e para sua sequência de codimensões, escreveremos $c_n(\mathcal{V}) \approx qn^k$ para algum $q \in \mathbb{Q}$.

Definição 6.2.1. Uma variedade $\mathcal{V}$ é minimal de crescimento polinomial n^k se $c_n(\mathcal{V}) \approx qn^k$, $k \geqslant 1$ e $q > 0$, e para qualquer subvariedade própria, $\mathcal{U} \subset \mathcal{V}$, temos que $c_n(\mathcal{U}) \approx q'n^t$ com $t < k$ para algum q'.

Para melhor explicar o conceito dado acima, vamos considerar as álgebras $\mathcal{G}_4$ e N_4 definidas na Seção 4.1. Pelos Teoremas 4.1.13 e 4.1.15, temos

$$\mathrm{Id}(\mathcal{G}_4) = \langle [x_1, x_2, x_3], [x_1, x_2][x_3, x_4][x_5, x_6] \rangle_T$$

e

$$\mathrm{Id}(N_4) = \langle [x_1, x_2, x_3, x_4], [x_1, x_2][x_3, x_4] \rangle_T.$$

Assim, vemos que $[x_1, x_2, x_3] \in \mathrm{Id}(\mathcal{G}_4)$, mas $[x_1, x_2, x_3] \notin \mathrm{Id}(N_4)$. Por outro lado, pelo Lema 4.1.3, temos $\mathrm{Id}(\mathcal{G}_4 \oplus N_4) = \mathrm{Id}(\mathcal{G}_4) \cap \mathrm{Id}(N_4)$ e, portanto, $\mathrm{var}(\mathcal{G}_4)$ é uma subvariedade própria de $\mathrm{var}(\mathcal{G}_4 \oplus N_4)$. Agora, pelas Proposições 4.2.12 e 4.2.13, temos

$$c_n(\mathcal{G}_4) \approx qn^4 \quad \text{e} \quad c_n(N_4) \approx q'n^3, \text{ com } q, q' \in \mathbb{Q}.$$

Usando que $\mathcal{G}_4 \in \mathrm{var}(\mathcal{G}_4 \oplus N_4)$ e a Proposição 4.2.4, temos

$$c_n(\mathcal{G}_4) \leqslant c_n(\mathcal{G}_4 \oplus N_4) \leqslant c_n(\mathcal{G}_4) + c_n(N_4)$$

e, com isso, podemos concluir que $c_n(\mathcal{G}_4 \oplus N_4) \approx \widetilde{q}n^4$, para algum $\widetilde{q} \in \mathbb{Q}$. Isto mostra que a variedade $\mathrm{var}(\mathcal{G}_4 \oplus N_4)$ é de crescimento n^4, mas não é minimal.

Em geral, as variedades $\mathrm{var}(\mathcal{G}_{2k})$ e $\mathrm{var}(N_s)$ são minimais, para $k \geqslant 1$ e $s \geqslant 3$, respectivamente. A classificação de todas as subvariedades próprias de $\mathrm{var}(\mathcal{G})$ e de $\mathrm{var}(UT_2)$, dada por La Mattina (ibid.), tem como destaque as subvariedades minimais e as álgebras $\mathcal{G}_{2k}$ e N_s têm papel fundamental, junto com outras álgebras que iremos definir. A relevância de tais variedades está no fato de que estas são vistas

como "blocos construtores", que permitiram à autora apresentar uma classificação completa das subvariedades das variedades de crescimento quase polinomial.

Iniciamos apresentando o resultado que classifica todas as subvariedades minimais da variedade $\mathrm{var}(\mathcal{G})$.

Teorema 6.2.2. *Uma subvariedade própria $\mathcal{V}$ de* $\mathrm{var}(\mathcal{G})$ *é uma variedade minimal se, e somente se, $\mathcal{V} = \mathrm{var}(\mathcal{G}_{2k})$, para algum $k \geqslant 1$.*

Vamos agora apresentar o resultado que classifica todas as subvariedades minimais da variedade $\mathrm{var}(UT_2)$ que finaliza a classificação dada por La Mattina. Para isso, para cada $k \geqslant 2$, vamos introduzir duas novas famílias de álgebras A_k e B_k, considerando, para $k \geqslant 2$ fixo, a matriz $H_k = \sum_{i=1}^{k-1} e_{i,i+1} \in UT_k$, assim como foi feito para a definição das álgebras N_k.

Definimos as seguintes subálgebras de UT_k:

$$\begin{aligned} A_k &= \mathrm{span}_F\{e_{11}, H_k, H_k^2, \ldots, H_k^{k-2}; e_{12}, e_{13}, \ldots, e_{1k}\} \quad \text{e} \\ B_k &= \mathrm{span}_F\{e_{kk}, H_k, H_k^2, \ldots, H_k^{k-2}; e_{1k}, e_{2k}, \ldots, e_{k-1,k}\}. \end{aligned} \tag{6.4}$$

Exemplo 6.2.3. Como um exemplo das álgebras definidas acima, para $k = 5$ temos

$$A_5 = \left\{ \begin{pmatrix} a & b & c & d & e \\ 0 & 0 & f & g & h \\ 0 & 0 & 0 & f & g \\ 0 & 0 & 0 & 0 & f \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} : a, b, c, d, e, f, g, h \in F \right\}$$

e

$$B_5 = \left\{ \begin{pmatrix} 0 & f & g & h & e \\ 0 & 0 & f & g & d \\ 0 & 0 & 0 & f & c \\ 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 & a \end{pmatrix} : a, b, c, d, e, f, g, h \in F \right\}$$

Podemos observar que, para cada $k \geqslant 2$, a álgebra B_k é a subálgebra de UT_k obtida ao refletir os elementos de A_k em relação a sua diagonal secundária, ou seja, obtemos B_k aplicando a involução ρ em A_k.

O próximo teorema classifica, a menos de PI-equivalência, todas as subvariedades minimais da variedade gerada pela álgebra UT_2.

Teorema 6.2.4. *Uma subvariedade própria $\mathcal{V}$ de* $\mathrm{var}(UT_2)$ *é uma variedade minimal se, e somente se, ou* $\mathcal{V} = \mathrm{var}(N_k)$ *ou* $\mathcal{V} = \mathrm{var}(A_r)$ *ou* $\mathcal{V} = \mathrm{var}(B_r)$*, para algum* $k \geqslant 3, r \geqslant 2$.

La Mattina (2007) utilizou a classificação feita nos dois últimos teoremas e também determinou, a menos de PI-equivalência, todas as álgebras que geram subvariedades das variedades $\mathrm{var}(\mathcal{G})$ e $\mathrm{var}(UT_2)$.

Teorema 6.2.5. *Seja* $A \in \mathrm{var}(\mathcal{G})$*. Então, ou* $A \sim_{PI} \mathcal{G}$ *ou* $A \sim_{PI} N$ *ou* $A \sim_{PI} C \oplus N$ *ou* $A \sim_{PI} \mathcal{G}_{2k} \oplus N$*, para algum* $k \geqslant 1$*, onde* N *é uma álgebra nilpotente e* C *é uma álgebra comutativa.*

Teorema 6.2.6. *Seja* $A \in \mathrm{var}(UT_2)$*. Então, ou* $A \sim_{PI} UT_2$ *ou* $A \sim_{PI} N$ *ou* $A \sim_{PI} N_k \oplus N$ *ou* $A \sim_{PI} N_k \oplus A_r \oplus N$ *ou* $A \sim_{PI} N_k \oplus B_s \oplus N$ *ou* $A \sim_{PI} N_k \oplus A_r \oplus B_s \oplus N$*, onde* N *é uma álgebra nilpotente e* $k, r, s \geqslant 2$.

Os resultados acima motivaram os estudos que visaram classificar variedades minimais de crescimento polinomial de modo geral. Giambruno, La Mattina e Zaicev (2014) estabeleceram tal classificação, no contexto de álgebras unitárias, mostrando que existe um número finito de tais variedades geradas por álgebras unitárias de crescimento assintótico no máximo n^4 e apresentaram explicitamente os T-ideais de cada uma dessas variedades. Para crescimento maior, os autores mostraram que a quantidade de variedades minimais sobre um corpo de característica zero é infinita e apresentaram ainda uma "receita" para a construção de T-ideais de identidades de variedades minimais de crescimento maior ou igual a n^5.

A respeito de álgebras com estrutura adicional, também já existem classificações semelhantes àquela dada no contexto geral. A definição de φ-variedade minimal é essencialmente a mesma, apenas considerando-se as φ-codimensões.

Definição 6.2.7. Dizemos que $\mathcal{V}$ é uma φ-variedade minimal de crescimento polinomial n^k se $c_n^{\varphi}(\mathcal{V}) \approx q\, n^k$, para algum racional não nulo q e um inteiro $k > 0$, e $c_n^{\varphi}(\mathcal{U}) \approx b n^t$, com $t < k$ para qualquer subvariedade própria $\mathcal{U}$ de $\mathcal{V}$ e algum $b \in \mathbb{Q}$.

Vamos iniciar apresentando a lista das subvariedades minimais das $*$-variedades de crescimento quase polinomial, $\mathrm{var}^*(D_*)$ e $\mathrm{var}^*(M_*)$, e para isto, vamos definir mais algumas álgebras.

Para $k \geqslant 2$, consideremos a seguinte subálgebra comutativa da álgebra UT_k :

$$C_k = \mathrm{span}_F \left\{ I_k, H_k, H_k^2, \ldots, H_k^{k-1} \right\} \tag{6.5}$$

onde I_k denota a matriz identidade $k \times k$ e $H_k = \sum_{i=1}^{k-1} e_{i,i+1} \in UT_k$.

Exemplo 6.2.8. $C_5 = \left\{ \begin{pmatrix} a & b & c & d & e \\ 0 & a & b & c & d \\ 0 & 0 & a & b & c \\ 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & a \end{pmatrix} : a,b,c,d,e \in F \right\}$

Podemos definir uma involução sobre C_k de modo a ter uma $*$-álgebra. Tal involução é dada por

$$\left(\alpha I_k + \sum_{1 \leqslant i < k} \beta_i H_k^i\right)^* = \alpha I_k + \sum_{1 \leqslant i < k} (-1)^i \beta_i H_k^i, \text{ onde } \alpha, \beta_i \in F \quad (6.6)$$

e vamos denotar por $C_{k,*}$, a álgebra C_k munida desta involução.

Como exemplo, em $C_{5,*}$ temos

$$\begin{pmatrix} a & b & c & d & e \\ 0 & a & b & c & d \\ 0 & 0 & a & b & c \\ 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & a \end{pmatrix}^* = \begin{pmatrix} a & -b & c & -d & e \\ 0 & a & -b & c & -d \\ 0 & 0 & a & -b & c \\ 0 & 0 & 0 & a & -b \\ 0 & 0 & 0 & 0 & a \end{pmatrix}.$$

Utilizando as $*$-álgebras $C_{k,*}$ e as $*$-álgebras $Q_{k,\rho}$, $P_{k,\rho}$ e $R_{k,\rho}$ definidas na Seção 6.1, estamos prontos para apresentar a classificação das subvariedades minimais das $*$-variedades de crescimento quase polinomial dada por La Mattina e Martino (2016). Faremos isto nos próximos dois teoremas.

Teorema 6.2.9. *Seja $\mathcal{V}$ uma subvariedade própria de* $\mathrm{var}^*(D_*)$. *Então $\mathcal{V}$ é uma $*$-variedade minimal se, e somente se, $\mathcal{V} = \mathrm{var}^*(C_{k,*})$, para algum $k \geqslant 2$.*

Teorema 6.2.10. *Seja $\mathcal{V}$ uma subvariedade própria de* $\mathrm{var}^*(M_*)$. *Então $\mathcal{V}$ é uma $*$-variedade minimal se, e somente se, ou $\mathcal{V} = \mathrm{var}^*(Q_{r,\rho})$ ou $\mathcal{V} = \mathrm{var}^*(P_{k,\rho})$ ou $\mathcal{V} = \mathrm{var}^*(R_{k,\rho})$, para algum $k \geqslant 2, r > 2$.*

Vamos agora apresentar as álgebras que serão necessárias para enunciar os resultados de La Mattina (2011) sobre a classificação das subvariedades minimais das supervariedades de crescimento quase polinomial, $\mathrm{var}^{gr}(\mathcal{G})$, $\mathrm{var}^{gr}(UT_2)$,

$\mathrm{var}^{gr}(\mathcal{G}^{gr})$, $\mathrm{var}^{gr}(UT_2^{gr})$ e $\mathrm{var}^{gr}(D^{gr})$. Obviamente, como as superálgebras $\mathcal{G}$ e UT_2 têm graduação trivial, as subvariedades minimais já estão classificadas no contexto geral já apresentado.

Para a superálgebra de Grassmann com graduação canônica $\mathcal{G}^{gr}$, para $k \geqslant 1$, denotaremos por $\mathcal{G}_k^{gr}$ a superálgebra obtida da subálgebra de dimensão finita $\mathcal{G}_k$, definida em Equação (4.1), com a graduação induzida de $\mathcal{G}^{gr}$. Por exemplo, $\mathcal{G}_2^{gr} = (F + Fe_1e_2, Fe_1 + Fe_2)$.

Temos o seguinte.

Teorema 6.2.11. *Seja $\mathcal{V}$ uma subvariedade própria de* $\mathrm{var}^{gr}(\mathcal{G}^{gr})$. *Então $\mathcal{V}$ é uma supervariedade minimal se, e somente se, $\mathcal{V} = \mathrm{var}^{gr}(\mathcal{G}_k^{gr})$, para algum $k \geqslant 1$.*

Para definir as superálgebras que geram subvariedades minimais da variedade gerada por UT_2^{gr}, vamos considerar as subálgebras N_k, A_k e B_k de UT_k apresentadas nas Equações (4.4) e (6.4) munidas de uma graduação induzida de uma graduação elementar sobre UT_k.

Para $k \geqslant 2$, definimos as superálgebras N_k^{gr}, A_k^{gr} e B_k^{gr} como as álgebras N_k, A_k e B_k, respectivamente, com graduação elementar induzida por $g = (0, 1, \ldots, 1) \in \mathbb{Z}_2^k$.

Como exemplo, considerando $k = 5$, temos

$$N_5 = \left\{ \begin{pmatrix} a & b & c & d & e \\ 0 & a & f & g & h \\ 0 & 0 & a & f & g \\ 0 & 0 & 0 & a & f \\ 0 & 0 & 0 & 0 & a \end{pmatrix} : a, b, c, d, e, f, g, h \in F \right\}$$

com $(N_5^{gr})^{(0)} = F(e_{11}+e_{22}+e_{33}+e_{44}+e_{55})+F(e_{23}+e_{34}+e_{45})+F(e_{24}+e_{35})+e_{25}$ e $(N_5^{gr})^{(1)} = Fe_{12} + Fe_{13} + Fe_{14} + Fe_{15}$.

Também, observando o Exemplo 6.2.3, vemos que

$$(A_5^{gr})^{(0)} = Fe_{11} + F(e_{23} + e_{34} + e_{45}) + F(e_{24} + e_{35}) + Fe_{25}$$
$$(A_5^{gr})^{(1)} = Fe_{12} + Fe_{13} + Fe_{14} + Fe_{15}$$

e

$$(B_5^{gr})^{(0)} = Fe_{55} + F(e_{23} + e_{34} + e_{45}) + F(e_{24} + e_{35}) + Fe_{25}$$
$$(B_5^{gr})^{(1)} = Fe_{12} + Fe_{13} + Fe_{14} + Fe_{15}.$$

Com isso, a classificação dada por La Mattina (2011) foi a seguinte.

Teorema 6.2.12. *Uma subvariedade própria de* $\mathcal{V}$ *de* $\mathrm{var}^{gr}(UT_2^{gr})$ *é uma supervariedade minimal se, e somente se, ou* $\mathcal{V} = \mathrm{var}^{gr}(N_k^{gr})$ *ou* $\mathcal{V} = \mathrm{var}^{gr}(A_k^{gr})$ *ou* $\mathcal{V} = \mathrm{var}^{gr}(B_k^{gr})$*, para algum* $k \geqslant 2$*.*

Por fim, consideramos a subálgebra comutativa C_k da álgebra UT_k, definida na Equação (6.5), e definimos uma graduação elementar induzida por $g = (0, 1, 0, 1, ...) \in \mathbb{Z}_2^k$. Vamos denotar a superálgebra obtida por C_k^{gr}.

Por exemplo, para $k = 5$, temos

$$C_5 = \left\{ \begin{pmatrix} a & b & c & d & e \\ 0 & a & b & c & d \\ 0 & 0 & a & b & c \\ 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & a \end{pmatrix} : a, b, c, d, e \in F \right\}$$

com $(C_5^{gr})^{(0)} = F(e_{11} + e_{22} + e_{33} + e_{44} + e_{55}) + F(e_{13} + e_{24} + e_{35}) + Fe_{15}$ e $(C_5^{gr})^{(1)} = F(e_{12} + e_{23} + e_{34} + e_{45}) + F(e_{14} + e_{25})$.

Temos a seguinte classificação das subvariedades minimais de $\mathrm{var}^{gr}(D^{gr})$ dada por La Mattina (ibid.).

Teorema 6.2.13. *Seja* $\mathcal{V}$ *uma subvariedade própria de* $\mathrm{var}^{gr}(D^{gr})$*. Então* $\mathcal{V}$ *é uma supervariedade minimal se, e somente se,* $\mathcal{V} = \mathrm{var}^{gr}(C_k^{gr})$*, para algum* $k \geqslant 2$*.*

Assim como no caso geral, os resultados de classificação das subvariedades minimais das φ-variedades de crescimento quase polinomial, dados por La Mattina e Martino (2016) no contexto de $*$-álgebras, e por La Mattina (2011) no contexto de superálgebras, motivaram a busca por resultados de classificação de φ-variedades minimais de crescimento polinomial de modo geral.

Tal classificação foi feita por Gouveia, dos Santos e Vieira (2020) considerando φ-variedades minimais geradas por álgebras unitárias. A primeira pergunta é se existem φ-variedades minimais geradas por álgebras unitárias que não são subvariedades das φ-variedades de crescimento quase polinomial. A resposta é sim e, como um exemplo, consideramos a subálgebra $\mathcal{G}_2$ da álgebra de Grassmann $\mathcal{G}$ munida da involução

$$\tau : \mathcal{G}_2 \to \mathcal{G}_2 \text{ tal que } \tau(e_i) = -e_i, \text{ para } i \in \{1, 2\}.$$

Denotando essa $*$-álgebra por $\mathcal{G}_{2,\tau}$, La Mattina e Misso (2006) mostraram que

$$\mathrm{Id}^*(\mathcal{G}_{2,\tau}) = \langle [y_1, y_2], [y_1, z_2], z_1 \circ z_2, z_1 z_2 z_3 \rangle_{T_*}.$$

Com isso, vemos que $\mathcal{G}_{2,\tau}$ não satisfaz a $*$-identidade $z_1 z_2 \equiv 0$ e, portanto, $\mathcal{G}_{2,\tau} \notin \mathrm{var}^*(M_*)$. Também observamos que $[z_1, z_2] \notin \mathrm{Id}^*(\mathcal{G}_{2,\tau})$, ou seja, temos que $\mathcal{G}_{2,\tau} \notin \mathrm{var}^*(D_*)$.

Além de provar que $\mathcal{G}_{2,\tau}$ gera uma $*$-variedade minimal de crescimento quadrático, Gouveia, dos Santos e Vieira (2020) mostraram que existe um número finito de φ-variedades minimais geradas por álgebras unitárias de crescimento assintótico no máximo quadrático e apresentaram explicitamente uma álgebra geradora para cada uma destas φ-variedades. A partir de crescimento cúbico, os autores mostraram que a quantidade de φ-variedades minimais sobre um corpo de característica zero é infinita e explicitaram uma maneira de construir T_φ-ideais de φ-variedades minimais de crescimento maior ou igual a n^3.

É importante ressaltar que o conhecimento das φ-álgebras geradoras de subvariedades minimais das φ-variedades de crescimento polinomial foi fundamental para a classificação de todas as subvariedades dessas φ-variedades em cada caso.

Antes de apresentar os resultados correspondentes, para duas φ-álgebras A e B, vamos estabelecer que A e B geram a mesma φ-variedade se, e somente se, $\mathrm{Id}^\varphi(A) = \mathrm{Id}^\varphi(B)$. Neste caso, dizemos que A e B são T_φ-equivalentes. No caso em que A e B são $*$-álgebras, denotamos essa situação por $A \sim_{T_*} B$ e, quando A e B são superálgebras, a notação a ser usada será $A \sim_{T_2} B$.

A seguir temos os resultados sobre as subvariedades das $*$-variedades de crescimento quase polinomial dados por La Mattina e Martino (2016), onde os autores mostram que as $*$-álgebras que geram subvariedades minimais em $\mathrm{var}^*(M_*)$ e $\mathrm{var}^*(D_*)$ são fundamentais para determinar todas as outras.

Teorema 6.2.14. *Seja $A \in \mathrm{var}^*(M_*)$. Então ou $A \sim_{T_*} M_*$ ou $A \sim_{T_*} N$ ou $A \sim_{T_*} P_{k,\rho} \oplus N$ ou $A \sim_{T_*} Q_{k,\rho} \oplus N$ ou $A \sim_{T_*} R_{t,\rho} \oplus N$ ou $A \sim_{T_*} P_{k,\rho} \oplus Q_{k,\rho} \oplus N$ ou $A \sim_{T_*} P_{k,\rho} \oplus R_{t,\rho} \oplus N$ ou $A \sim_{T_*} Q_{k,\rho} \oplus R_{t,\rho} \oplus N$ ou $A \sim_{T_*} P_{k,\rho} \oplus Q_{k,\rho} \oplus R_{t,\rho} \oplus N$, onde $k, t \geqslant 1$ e N é uma $*$-álgebra nilpotente.*

Teorema 6.2.15. *Seja $A \in \mathrm{var}^*(D_*)$. Então ou $A \sim_{T_*} D_*$ ou $A \sim_{T_*} N$ ou $A \sim_{T_*} N \oplus C$ ou $A \sim_{T_*} C_{k,*} \oplus N$, para algum $k \geqslant 1$, onde N é uma $*$-álgebra nilpotente e C é uma álgebra comutativa com involução trivial.*

Para finalizar a seção, apresentamos os resultados de classificação das subvariedades das supervariedades de crescimento quase polinomial dados por La Mattina (2011). Novamente os resultados mostram que as superálgebras gerando subvariedades minimais em $\mathrm{var}^{gr}(\mathcal{G})$, $\mathrm{var}^{gr}(UT_2)$, $\mathrm{var}^{gr}(\mathcal{G}^{gr})$, $\mathrm{var}^{gr}(UT_2^{gr})$ e $\mathrm{var}^{gr}(D^{gr})$ determinam todas as outras. Obviamente, como a descrição das subvariedades de $\mathrm{var}^{gr}(\mathcal{G})$ e $\mathrm{var}^{gr}(UT_2)$ já foi apresentada na situação em que a

graduação é trivial, o que corresponde ao caso ordinário, vamos apenas descrever as subvariedades das demais com graduação não trivial.

Teorema 6.2.16. *Seja $A \in \mathrm{var}^{gr}(\mathcal{G}^{gr})$. Então ou $A \sim_{T_2} \mathcal{G}^{gr}$ ou $A \sim_{T_2} N$ ou $A \sim_{T_2} C \oplus N$ ou $A \sim_{T_2} \mathcal{G}_k^{gr} \oplus N$, para algum $k \geqslant 1$, onde N é uma superálgebra nilpotente e C é uma superálgebra comutativa com graduação trivial.*

Teorema 6.2.17. *Seja $A \in \mathrm{var}^{gr}(UT_2^{gr})$. Então ou $A \sim_{T_2} UT_2^{gr}$ ou $A \sim_{T_2} N$ ou $A \sim_{T_2} C \oplus N$ ou $A \sim_{T_2} N_t^{gr} \oplus N$ ou $A \sim_{T_2} A_k^{gr} \oplus N$ ou $A \sim_{T_2} B_r^{gr} \oplus N$ ou $A \sim_{T_2} N_t^{gr} \oplus A_k^{gr} \oplus N$ ou $A \sim_{T_2} N_t^{gr} \oplus B_r^{gr} \oplus N$ ou $A \sim_{T_2} A_k^{gr} \oplus B_r^{gr} \oplus N$ ou $A \sim_{T_2} N_t^{gr} \oplus A_k^{gr} \oplus B_r^{gr} \oplus N$, onde $k, r, t \geqslant 2$ com N uma superálgebra nilpotente e C uma superálgebra comutativa com graduação trivial.*

Teorema 6.2.18. *Seja $A \in \mathrm{var}^{gr}(D^{gr})$. Então ou $A \sim_{T_2} D^{gr}$ ou $A \sim_{T_2} N$ ou $A \sim_{T_2} C \oplus N$ ou $A \sim_{T_2} C_k^{gr} \oplus N$, para algum $k \geqslant 2$, onde N é uma superálgebra nilpotente e C é uma superálgebra comutativa com graduação trivial.*

As classificações de variedades apresentadas nesta seção nos levam a questionar sobre classificações mais gerais de variedades de crescimento polinomial. Uma pergunta relevante é se, de modo geral, as variedades minimais podem ser consideradas de fato como "blocos construtores" para todas as variedades de crescimento polinomial. Esta é uma questão em aberto até o presente momento.

6.3 Variedades de crescimento lento

Os resultados de classificações das subvariedades das variedades de crescimento quase polinomial estabeleceram um interesse na pesquisa por resultados mais gerais. Nesta seção, discutiremos sobre classificações que já são conhecidas tanto no âmbito ordinário quanto no contexto de álgebras com estruturas adicionais.

Neste sentido, podemos nos perguntar se é possível estabelecer classificações de variedades de crescimento polinomial considerando um valor assintótico específico para a codimensão da variedade. De fato, alguns resultados são conhecidos na tentativa de responder a pergunta: para $k \geqslant 0$ fixo e algum $q \in \mathbb{Q}$, a menos de PI-equivalência, quais são as álgebras A tais que $c_n(A) \approx q n^k$?

A seguir veremos os resultados que já foram provados nos diversos contextos estudados, todos eles para valores pequenos do inteiro $k \geqslant 0$. Desta forma, temos classificações para o que chamamos de variedades de crescimento lento das codimensões.

Iniciamos com o próximo teorema que classifica as variedades de crescimento no máximo cúbico geradas por álgebras unitárias, que foi explicitado em Giambruno, La Mattina e Petrogradsky (2007).

Teorema 6.3.1. *Seja A uma F-álgebra unitária. Se $c_n(A) \approx qn^k$, para algum $q \geqslant 1$ e $k \leqslant 3$, então ou $A \sim_{PI} F$ ou $A \sim_{PI} N_3$ ou $A \sim_{PI} N_4$.*

Observamos que as variedades de crescimento no máximo cúbico geradas por álgebras unitárias são todas minimais e vemos também que não existe álgebra unitária de crescimento linear. Do teorema anterior, usando a Proposição 4.2.13, segue imediatamente o seguinte corolário, que fornece os valores das codimensões possíveis de álgebras unitárias de crescimento no máximo cúbico.

Corolário 6.3.2. *Seja A uma F-álgebra unitária. Se $c_n(A) \approx qn^k$, para algum $q \geqslant 1$ e $k \leqslant 3$, então ou $c_n(A) = 1$ ou $c_n(A) = 1 + \dfrac{n(n-1)}{2}$ ou $c_n(A) = 1 + \dfrac{n(n-1)}{2} + \dfrac{n(n-1)(n-2)}{3}$.*

A partir do corolário anterior, vemos que as possibilidades para o coeficiente líder do polinômio que descreve a codimensão de uma álgebra unitária de crescimento no máximo cúbico são

$$q = 1 \text{ ou } q = \frac{1}{2} \text{ ou } q = \frac{1}{3}.$$

Para crescimento assintótico n^4, de Oliveira e Vieira (2021) classificaram as variedades geradas por álgebras unitárias, mostrando que existem apenas 16 álgebras nessas condições, sendo obtidas como somas diretas de álgebras unitárias geradoras de variedades minimais de crescimento no máximo n^4. Para apresentar o resultado, vamos listar as variedades minimais de crescimento n^4 geradas por álgebras unitárias dadas por Giambruno, La Mattina e Zaicev (2014). Dos Teoremas 6.2.2 e 6.2.4, já sabemos que $\mathcal{G}_4$ e N_5 geram variedades minimais. A seguir, definiremos duas novas álgebras, a primeira delas é a seguinte subálgebra $\mathcal{K}_1$ de UT_5:

$$\mathcal{K}_1 = \left\{ \begin{pmatrix} a & b & d & e & f \\ 0 & a & c & g & h \\ 0 & 0 & a & c & i \\ 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & a \end{pmatrix} : a, b, c, d, e, f, g, h, i \in F \right\}$$

e a segunda é a álgebra unitária $\mathcal{K}_2$ cujo T-ideal é dado por

$$I = \langle [x_2, x_1, x_1, x_1], [x_1, x_2]^2, St_4(x_1, x_2, x_3, x_4) \rangle_T .$$

O teorema de classificação de Giambruno, La Mattina e Zaicev (ibid.) de variedades minimais de crescimento n^4 é o seguinte.

Teorema 6.3.3. *Seja $\mathcal{V} = \mathrm{var}(A)$ variedade de crescimento n^4 gerada por uma álgebra unitária A. Então $\mathcal{V}$ é minimal se, e somente se, ou $A \sim_{PI} \mathcal{G}_4$ ou $A \sim_{PI} N_5$ ou $A \sim_{PI} \mathcal{K}_1$ ou $A \sim_{PI} \mathcal{K}_2$.*

O resultado geral de classificação das variedades de crescimento n^4 geradas por álgebras unitárias dado por de Oliveira e Vieira (2021) segue abaixo.

Teorema 6.3.4. *Seja A um álgebra unitária. Então $\mathrm{var}(A)$ é uma variedade de crescimento n^4 se, e somente se, A é PI-equivalente ou a $\mathcal{G}_4$ ou N_5 ou $\mathcal{K}_1$ ou $\mathcal{K}_2$ ou $\mathcal{G}_4 \oplus N_4$ ou $\mathcal{G}_4 \oplus \mathcal{K}_1$ ou $\mathcal{G}_4 \oplus \mathcal{K}_2$ ou $\mathcal{G}_4 \oplus N_5$ ou $N_5 \oplus \mathcal{K}_1$ ou $N_5 \oplus \mathcal{K}_2$ ou $\mathcal{K}_1 \oplus \mathcal{K}_2$ ou $N_5 \oplus \mathcal{K}_1 \oplus \mathcal{G}_4$ ou $N_5 \oplus \mathcal{K}_2 \oplus \mathcal{G}_4$ ou $N_5 \oplus \mathcal{K}_1 \oplus \mathcal{K}_2$ ou $\mathcal{K}_1 \oplus \mathcal{K}_2 \oplus \mathcal{G}_4$ ou $N_5 \oplus \mathcal{K}_1 \oplus \mathcal{K}_2 \oplus \mathcal{G}_4$.*

Conforme observado anteriormente, não existem álgebras unitárias de crescimento linear, mas em um ambiente mais geral, tratando-se de álgebras não necessariamente unitárias, temos um resultado de classificação das variedades de crescimento no máximo linear dado por Giambruno e La Mattina (2005). Antes de enunciar este resultado, vamos recordar as seguintes álgebras definidas na Equação (6.4):

$$A_2 = \begin{pmatrix} F & F \\ 0 & 0 \end{pmatrix} \qquad \text{e} \qquad B_2 = \begin{pmatrix} 0 & F \\ 0 & F \end{pmatrix}.$$

Teorema 6.3.5. *Seja A uma F-álgebra. Então as seguintes condições são equivalentes:*

1. *$c_n(A) \leqslant kn$ para todo $n \geqslant 1$, para alguma constante k;*
2. *A é PI-equivalente ou a N ou $C \oplus N$ ou $A_2 \oplus N$ ou $B_2 \oplus N$ ou $A_2 \oplus B_2 \oplus N$, onde N é uma álgebra nilpotente e C é uma álgebra comutativa.*

Com isso, concluímos também que as variedades geradas por A_2 e B_2 são as únicas variedades minimais de crescimento linear geradas por álgebras não unitárias. Em relação às variedades minimais de crescimento quadrático, também

temos um resultado geral de classificação, considerando adicionalmente variedades geradas por álgebras não unitárias. Para enunciá-lo, consideramos as seguintes álgebras não unitárias:

$$M_5 = \begin{pmatrix} 0 & F & F \\ 0 & 0 & F \\ 0 & 0 & F \end{pmatrix}, \qquad M_6 = \begin{pmatrix} 0 & F & F \\ 0 & F & F \\ 0 & 0 & 0 \end{pmatrix}$$

$$M_7 = \left\{ \begin{pmatrix} a & b & c \\ 0 & 0 & d \\ 0 & 0 & a \end{pmatrix} : a, b, c, d \in F \right\}.$$

Já sabemos que N_3 é, a menos de PI-equivalência, a única álgebra unitária de crescimento quadrático. Agora o teorema a seguir, provado por Vieira e Jorge (2006), apresenta todas as álgebras geradoras de variedades minimais de crescimento quadrático, sem a exigência de serem unitárias.

Teorema 6.3.6. *As variedades* $\mathrm{var}(N_3)$, $\mathrm{var}(M_4)$, $\mathrm{var}(M_5)$, $\mathrm{var}(M_6)$ *e* $\mathrm{var}(M_7)$ *são as únicas varieadades minimais de crescimento quadrático.*

Em seguida apresentaremos brevemente os resultados sobre φ-variedades, onde fizemos a opção de não explicitar cada φ-álgebra geradora e indicamos apenas as referências de onde todos os detalhes podem ser encontrados.

- Giambruno, La Mattina e Misso (2006) apresentaram uma lista de 33 superálgebras que, a menos de equivalência, geram todas as supervariedades de crescimento no máximo linear.

- La Mattina e Misso (2006) exibiram uma lista completa de 5 álgebras com involução que, a menos de equivalência, geram todas $*$-variedades de crescimento no máximo linear.

- Bessades et al. (2021) mostraram que, a menos de equivalência, existem exatamente 16 superálgebras unitárias e 15 álgebras unitárias com involução gerando φ-variedades de crescimento quadrático. Cada φ-álgebra em cada uma das listas é equivalente a uma soma direta finita de φ-álgebras unitárias distintas gerando variedades minimais de crescimento no máximo quadrático.

6.4 Um pouco mais de estrutura

Esta seção finaliza este livro e nela introduziremos um novo objeto de estudo: as superálgebras munidas de involução graduada, que formam uma classe de álgebras com estrutura adicional, foco de investigação por diversos autores nos últimos anos. Vamos ver que vários conceitos e resultados sobre essa estrutura generalizam aqueles já trabalhados no contexto de PI-álgebras, superálgebras e álgebras com involução. Desta forma, nosso objetivo será apresentar os principais resultados a respeito das chamadas $*$-superálgebras de crescimento polinomial que foram obtidos recentemente.

Inicialmente, observamos que a involução reflexão ρ definida sobre a álgebra M com graduação

$$\left(\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & a \end{pmatrix}, \begin{pmatrix} 0 & c & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & d \\ 0 & 0 & 0 & 0 \end{pmatrix}\right) \tag{6.7}$$

é tal que $(M^{(0)})^{\rho} = M^{(0)}$ e $(M^{(1)})^{\rho} = M^{(1)}$. Com isso, temos um exemplo do que chamamos involução graduada sobre uma superálgebra, conforme a definição abaixo.

Definição 6.4.1. Uma involução $*$ sobre uma superálgebra $A = A^{(0)} \dotplus A^{(1)}$ tal que $(A^{(0)})^{*} = A^{(0)}$ e $(A^{(1)})^{*} = A^{(1)}$, é chamada de involução graduada. Uma superálgebra A munida com uma involução graduada $*$ é chamada de $*$-superálgebra.

Como exemplo, a álgebra M com graduação definida na Equação (6.7) munida da involução ρ é uma $*$-superálgebra, que denotaremos por M^{gri}.

O estudo das $*$-superálgebras generaliza o estudo das álgebras com involução, uma vez que toda $*$-álgebra é uma $*$-superálgebra considerada com graduação trivial. Desta forma, a $*$-álgebra M_* com graduação trivial é uma $*$-superálgebra.

Observamos ainda que, para uma superálgebra comutativa A, a aplicação identidade é uma involução graduada sobre A, chamada de involução graduada trivial. Portanto, toda superálgebra comutativa é uma $*$-superálgebra considerada com involução graduada trivial. Reciprocamente, se a aplicação identidade é uma involução graduada sobre uma superálgebra A, então A é comutativa.

Exemplo 6.4.2. Considerando a álgebra comutativa $D = F \oplus F$, temos que D_* é uma $*$-superálgebra com graduação trivial e involução troca. Também a superálgebra D^{gr} com involução trivial é uma $*$-superálgebra. Por fim, a mesma álgebra

D, com graduação $(F(1,1),\ F(1,-1))$ e munida da involução troca, também é uma $*$-superálgebra, que denotaremos por D^{gri}.

É possível mostrar que uma superálgebra A munida de uma involução $*$ é uma $*$-superálgebra se, e somente se, os subespaços A^+ e A^- são graduados, isto é,

$$A^+ = (A^+)^{(0)} \dot{+} (A^+)^{(1)} \quad \text{e} \quad A^- = (A^-)^{(0)} \dot{+} (A^-)^{(1)}.$$

Com isso, obtemos que qualquer $*$-superálgebra A pode ser escrita como soma direta de 4 subespaços

$$A = (A^+)^{(0)} \dot{+} (A^+)^{(1)} \dot{+} (A^-)^{(0)} \dot{+} (A^-)^{(1)}.$$

Para nossos propósitos, estamos interessados em avaliar os elementos de uma $*$-superálgebra em polinômios de acordo com a decomposição acima. Para fazer isto, primeiramente escrevemos o conjunto enumerável de variáveis não comutativas X como uma união disjunta de quatro conjuntos

$$X = Y_0 \cup Y_1 \cup Z_0 \cup Z_1$$

onde $Y_0 = \{y_{1,0}, y_{2,0}, \ldots\}, Y_1 = \{y_{1,1}, y_{2,1}, \ldots\}, Z_0 = \{z_{1,0}, z_{2,0}, \ldots\}$ e $Z_1 = \{z_{1,1}, z_{2,1}, \ldots\}$. Em seguida definimos a $*$-superálgebra livre $\mathcal{F} = F\langle X|\mathbb{Z}_2, *\rangle$ dando uma superestrutura em $\mathcal{F}$ tal que

- as variáveis em $Y_0 \cup Z_0$ são homogêneas de grau 0
- as variáveis em $Y_1 \cup Z_1$ são homogêneas de grau 1

e definindo uma involução $*$ sobre $\mathcal{F}$ de modo que

- as variáveis em $Y_0 \cup Y_1$ são simétricas
- as variáveis em $Z_0 \cup Z_1$ são antissimétricas.

Dessa forma, definindo $\mathcal{F}^{(0)}$ como o subespaço gerado por todos os monômios nas variáveis em X, que têm um número par de variáveis de grau 1, e $\mathcal{F}^{(1)}$ como o subespaço gerado por todos os monômios nas variáveis em X, que têm um número ímpar de variáveis de grau 1, temos que $\mathcal{F} = \mathcal{F}^{(0)} \dot{+} \mathcal{F}^{(1)}$ e, assim, $(\mathcal{F}^{(0)})^* = \mathcal{F}^{(0)}$ e $(\mathcal{F}^{(1)})^* = \mathcal{F}^{(1)}$. Os elementos de $\mathcal{F}$ são chamados de $(\mathbb{Z}_2, *)$-polinômios.

Agora estamos aptos a estender a definição de identidade polinomial para a situação em que trabalhamos com $*$-superálgebras.

Definição 6.4.3. Dizemos que um $(\mathbb{Z}_2, *)$-polinômio

$$f = f(y_{1,0}, \ldots, y_{m,0}, y_{1,1}, \ldots, y_{n,1}, z_{1,0}, \ldots, z_{p,0}, z_{1,1}, \ldots, z_{q,1})$$

é uma $(\mathbb{Z}_2, *)$-identidade de uma $*$-superálgebra A, e escrevemos $f \equiv 0$ em A, se

$$f(a^+_{1,0}, \ldots, a^+_{m,0}, a^+_{1,1}, \ldots, a^+_{n,1}, a^-_{1,0}, \ldots, a^-_{p,0}, a^-_{1,1}, \ldots, a^-_{q,1}) = 0$$

para todos $a^+_{1,0}, \ldots, a^+_{m,0} \in (A^+)^{(0)}$, $a^+_{1,1}, \ldots, a^+_{n,1} \in (A^+)^{(1)}$, $a^-_{1,0}, \ldots, a^-_{p,0} \in (A^-)^{(0)}$ e $a^-_{1,1}, \ldots, a^-_{q,1} \in (A^-)^{(1)}$.

Observemos que sempre que uma $*$-superálgebra A tem graduação trivial, temos que $y_{1,1}$ e $z_{1,1}$ são $(\mathbb{Z}_2, *)$-identidades de A. Deste modo, estes são exemplos de $(\mathbb{Z}_2, *)$-identidades de M_* e de D_*. Também temos como exemplos que $z_{1,0}z_{2,0} \equiv 0$ em M_* e $[y_{1,0}, y_{2,0}] \equiv 0$, $[y_{1,0}, z_{2,0}] \equiv 0$ e $[z_{1,0}, z_{2,0}] \equiv 0$ em D_*.

Nosso objetivo agora é estender a definição de codimensões para o caso em que temos uma $*$-superálgebra. Para isso, consideramos o ideal das $(\mathbb{Z}_2, *)$-identidades de A:

$$\mathrm{Id}^{gri}(A) = \{f \in \mathcal{F} : f \equiv 0 \text{ em } A\}$$

denominado de T^*_2-ideal de A.

Como F é um corpo de característica zero, da mesma forma que o caso ordinário, $\mathrm{Id}^{gri}(A)$ é finitamente gerado como T^*_2-ideal e também neste contexto, temos que $\mathrm{Id}^{gri}(A)$ é completamente determinado por seus polinômios multilineares. Assim, para $n \geqslant 1$, definimos

$$P^{gri}_n = \mathrm{span}_F\{w_{\sigma(1)} \cdots w_{\sigma(n)} : w_i \in \{y_{i,0}, y_{i,1}, z_{i,0}, z_{i,1}\}, \sigma \in S_n\}$$

como o espaço dos $(\mathbb{Z}_2, *)$-polinômios multilineares de grau n nas variáveis $y_{1,0}, \ldots, y_{n,0}, y_{1,1}, \ldots, y_{n,1}, z_{1,0}, \ldots, z_{n,0}, z_{1,1}, \ldots, z_{n,1}$.

Para estudar o comportamento das $(\mathbb{Z}_2, *)$-identidades satisfeitas por uma $*$-superálgebra A, consideramos o espaço quociente

$$P^{gri}_n(A) = \frac{P^{gri}_n}{P^{gri}_n \cap \mathrm{Id}^{gri}(A)}$$

e estabelecemos a seguinte definição.

Definição 6.4.4. A n-ésima codimensão $*$-graduada de A é definida como o inteiro não negativo dado por

$$c_n^{gri}(A) = \dim_F(P_n^{gri}(A)),\ n \geqslant 1.$$

Novamente, como no caso ordinário, consideramos $\mathrm{var}^{gri}(A)$ a classe das $*$-superálgebras que satisfazem todas as $(\mathbb{Z}_2, *)$-identidades de A, chamada a $*$-supervariedade gerada por A. Quando $\mathcal{V} = \mathrm{var}^{gri}(A)$, definimos $c_n^{gri}(\mathcal{V}) = c_n^{gri}(A)$.

Vamos dizer que uma $*$-supervariedade $\mathcal{V}$ tem crescimento polinomial, se existem constantes q, k tais que $c_n^{gri}(\mathcal{V}) \leqslant qn^k$, para todo $n \geqslant 1$. Por outro lado, dizemos que uma $*$-supervariedade $\mathcal{V}$ tem crescimento exponencial, se existe um inteiro $\alpha \geqslant 2$ tal que $c_n^{gri}(\mathcal{V}) \geqslant \alpha^n$, para n suficientemente grande.

Dizemos ainda que a sequência de codimensões $*$-graduadas $\{c_n^{gri}(A)\}_{n\geqslant 1}$ de uma $*$-superálgebra A é limitada exponencialmente se existem constantes $a, \alpha > 0$ tais que $c_n^{gri}(A) \leqslant a\alpha^n$ para todo $n \geqslant 1$.

Observação 6.4.5. Giambruno, dos Santos e Vieira (2016) observaram que, dada A uma $*$-superálgebra, podemos considerar suas identidades ordinárias, suas $*$-identidades e suas identidades graduadas para estabelecer relações entre as codimensões correspondentes como abaixo:

1. $c_n(A) \leqslant c_n^*(A) \leqslant c_n^{gri}(A)$;
2. $c_n(A) \leqslant c_n^{gr}(A) \leqslant c_n^{gri}(A)$;
3. $c_n^{gri}(A) \leqslant 4^n c_n(A)$.

Com isso, os autores obtiveram o seguinte resultado.

Corolário 6.4.6. *Seja A uma $*$-superálgebra. Então A é PI-álgebra se, e somente se, sua sequência de codimensões $*$-graduadas é limitada exponencialmente.*

De acordo com Equação (6.3), sabemos que $c_n(M)$ cresce exponencialmente e a partir das relações acima temos

$$c_n(M) \leqslant c_n^{gri}(M_*) \ \text{ e } \ c_n(M) \leqslant c_n^{gri}(M^{gri})$$

ou seja, M_* e M^{gri} são $*$-superálgebras de crescimento exponencial. Além disso, D_* e D^{gr} são φ-álgebras de crescimento exponencial e

$$c_n^*(D_*) \leqslant c_n^{gri}(D_*) \ \text{ e } \ c_n^{gr}(D^{gr}) \leqslant c_n^{gri}(D^{gr})$$

ou seja, D_* e D^{gr} são $*$-superálgebras de crescimento exponencial. Por fim, também temos $c_n^{gri}(D^{gri}) = 2^n$ para $n \geqslant 1$ e uma demonstração explícita está no artigo de do Nascimento e Vieira (2019).

O importante agora é questionar se podemos caracterizar $*$-supervariedades de crescimento polinomial provando um teorema do tipo Kemer. Com o próximo resultado de Giambruno, dos Santos e Vieira (2016) vemos que resposta é sim.

Teorema 6.4.7. *Uma $*$-supervariedade $\mathcal{V} = \mathrm{var}^{gri}(A)$ tem crescimento polinomial das codimensões $*$-graduadas se, e somente se, D_*, D^{gr}, D^{gri}, M_*, $M^{gri} \notin \mathcal{V}$.*

Usando a mesma linguagem utilizada no contexto ordinário apresentado na Seção 5.2 e no contexto de φ-álgebras da Seção 6.1, também podemos concluir que $\mathrm{var}^{gri}(D_*)$, $\mathrm{var}^{gri}(D^{gr})$, $\mathrm{var}^{gri}(D^{gri})$, $\mathrm{var}^{gri}(M_*)$ e $\mathrm{var}^{gri}(M^{gri})$ são as únicas $*$-supervariedades de crescimento quase polinomial das codimensões $*$-graduadas.

É importante comentar que as subvariedades das $*$-supervariedades de crescimento quase polinomial também já foram determinadas nos artigos de La Mattina (2011), Ioppolo e La Mattina (2017) e La Mattina e Martino (2016). Analogamente aos casos anteriores comentados, observa-se que a partir das subvariedades minimais das $*$-supervariedades de crescimento quase polinomial obtêm-se todas as demais subvariedades nas situações estudadas.

Em relação a classificações de $*$-supervariedades de crescimento lento, ressaltamos o resultado de Ioppolo e La Mattina (2017) que classifica, a menos de T_2^*-equivalência, todas as $*$-superálgebras de crescimento no máximo linear. Usaremos $A \sim_{T_2^*} B$ para dizer que A e B são $*$-superálgebras T_2^*-equivalentes, isto é, $\mathrm{Id}^{gri}(A) = \mathrm{Id}^{gri}(B)$.

Para apresentar a classificação feita, será necessário introduzir algumas $*$-superálgebras a partir de álgebras já anteriormente definidas.

Consideremos a seguinte álgebra dada pela Equação (6.5):

$$C_2 = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in F \right\}.$$

A partir de C_2, obtemos as seguintes $*$-superálgebras:

- $C_{2,*}$, a álgebra C_2 com graduação trivial e involução dada na Equação (6.6), ou seja,

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^* = \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix}. \tag{6.8}$$

- C_2^{gri}, a álgebra C_2 com graduação $(F(e_{11}+e_{22}), Fe_{12})$ e involução definida como na Equação (6.8).
- C_2^{gr}, a álgebra C_2 com graduação $(F(e_{11}+e_{22}), Fe_{12})$ e involução trivial.

Consideramos também a seguinte álgebra R_2 dada pela Equação (6.1)

$$R_2 = \left\{ \begin{pmatrix} a & b & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c \\ 0 & 0 & 0 & a \end{pmatrix} : a, b, c \in F \right\}$$

e construímos as $*$-superálgebras:

- $R_{2,\rho}$, a álgebra R_2 com graduação trivial e involução reflexão ρ.
- R_2^{gri}, a álgebra R_2 com graduação $(F(e_{11}+e_{44}), Fe_{12}+Fe_{34})$ e involução reflexão ρ.

Usando as $*$-superálgebras definidas acima, Ioppolo e La Mattina (2017) provaram o seguinte resultado que classifica as $*$-superálgebras de crescimento no máximo linear.

Teorema 6.4.8. *Seja A uma $*$-superálgebra tal que $c_n^{gri}(A) \leqslant an$, para alguma constante a. Então*

$$A \sim_{T_2^*} B_1 \oplus \cdots \oplus B_m$$

onde, para todo $i = 1, \ldots, m$, B_i é T_2^*-equivalente a uma das seguintes $*$-superálgebras:

N, $C \oplus N$, $C_{2,*} \oplus N$, $R_{2,\rho} \oplus N$, $R_{2,\rho} \oplus C_{2,*} \oplus N$, $C_2^{gri} \oplus N$, $C_2^{gr} \oplus N$, $R_2^{gri} \oplus N$, $C_2^{gri} \oplus C_2^{gr} \oplus N$, $C_2^{gri} \oplus R_2^{gri} \oplus N$, $C_2^{gr} \oplus R_2^{gri} \oplus N$, $C_2^{gri} \oplus C_2^{gr} \oplus R_2^{gri} \oplus N$, *onde C é uma $*$-superálgebra comutativa com graduação trivial e involução trivial e N é uma $*$-superálgebra nilpotente.*

Considerando que $*$-supervariedades minimais são definidas da mesma forma, como foi feito na Definição 6.2.7, apenas com diferença que consideramos codimensões $*$-graduadas, obtemos como consequência do teorema anterior que as $*$-superálgebras $R_{2,\rho}$, R_2^{gri}, $C_{2,*}$, C_2^{gri} e C_2^{gr} geram, a menos de T_2^*-equivalência, as únicas $*$-supervariedades minimais de crescimento linear. Além disso, cada

uma destas é subvariedade de alguma $*$-supervariedade de crescimento quase polinomial.

Para concluir as informações sobre as $*$-supervariedades minimais já obtidas até o presente momento, temos um resultado de Ioppolo, dos Santos et al. (2021) que determina de forma explícita as 36 $*$-superálgebras que geram, a menos de T_2^*-equivalência, as únicas $*$-supervariedades minimais de crescimento quadrático. Dentre essas 36 $*$-superálgebras minimais, 27 geram $*$-supervariedades que não são subvariedades das *-supervariedades de crescimento quase polinomial.

A classificação geral de $*$-supervariedades de crescimento quadrático, ou crescimento maior, até o momento, ainda não é conhecida.

Bibliografia

E. Aljadeff, A. Giambruno, C. Procesi e A. Regev (2020). *Rings with polynomial identities and finite dimensional representations of algebras*. Vol. 66. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, p. 630. MR: 4249615. Zbl: 07314181 (ver p. vii).

S. A. Amitsur (1953). "The identities of PI-rings". *Proc. Amer. Math. Soc.* 4, pp. 27–34. MR: 52397. Zbl: 0050.02902 (ver p. 224).

S. A. Amitsur e J. Levitzki (1950). "Minimal identities for algebras". *Proc. Amer. Math. Soc.* 1, pp. 449–463. MR: 36751. Zbl: 0040.01101 (ver pp. iii, 147).

Y. Bahturin e V. Drensky (2002). "Graded polynomial identities of matrices". *Linear Algebra Appl.* 357, pp. 15–34. MR: 1935223. Zbl: 1019.16011 (ver p. 170).

A. Y. Belov (2000). "Counterexamples to the Specht problem". *Mat. Sb.* 191.3, pp. 13–24. MR: 1773251. Zbl: 0960.16029 (ver p. 139).

A. Berele e A. Regev (1983). "Applications of hook Young diagrams to P.I. algebras". *J. Algebra* 82.2, pp. 559–567. MR: 704771. Zbl: 0517.16013 (ver p. 221).

— (2008). "Asymptotic behaviour of codimensions of p. i. algebras satisfying Capelli identities". *Trans. Amer. Math. Soc.* 360.10, pp. 5155–5172. MR: 2415069. Zbl: 1161.16016 (ver p. 198).

D. C. L. Bessades, R. B. dos Santos, M. L. O. Santos e A. C. Vieira (2021). "Superalgebras and algebras with involution: classifying varieties of quadratic growth". *Comm. Algebra* 49.6, pp. 2476–2490. MR: 4255008. Zbl: 07337672.

eprint: https://doi.org/10.1080/00927872.2021.1873354 (ver p. 258).

J. Colombo e P. Koshlukov (2004). "Central polynomials in the matrix algebra of order two". *Linear Algebra Appl.* 377, pp. 53–67. MR: 2021602. Zbl: 1044.16016 (ver p. 140).

C. W. Curtis e I. Reiner (1966). *Representation theory of finite groups and associative algebras*. Vol. 356. American Mathematical Soc. MR: 0144979 (ver pp. 77, 115).

M. Dehn (1922). "Über die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme". *Math. Ann.* 85.1, pp. 184–194. MR: 1512061 (ver p. iii).

O. M. Di Vincenzo e A. Giambruno, ed. (2021). *Polynomial identities in algebras*. Vol. 44. Springer INdAM Series. Springer, Cham, p. 421. MR: 4237297 (ver p. vii).

V. Drensky (1981). "A minimal basis for identities of a second-order matrix algebra over a field of characteristic 0". *Algebra i Logika* 20.3, pp. 282–290, 361. MR: 648317 (ver p. 139).

— (1995). "New central polynomials for the matrix algebra". *Israel J. Math.* 92.1-3, pp. 235–248. MR: 1357754. Zbl: 0841.16027 (ver p. 156).

— (2000). *Free algebras and PI-algebras*. Graduate course in algebra. Springer-Verlag Singapore, Singapore, pp. xii+271. MR: 1712064. Zbl: 0936.16001 (ver pp. vii, 129, 162).

V. Drensky e A. Kasparian (1983). "Polynomial identities of eighth degree for 3×3 matrices". *Annuaire Univ. Sofia Fac. Math. Méc.* 77.1, 175–195 (1988). MR: 960570. Zbl: 0736.16012 (ver pp. 155, 156).

V. Drensky e A. Regev (1996). "Exact asymptotic behaviour of the codimensions of some P.I. algebras". *Israel J. Math.* 96.part A, pp. 231–242. MR: 1432733. Zbl: 0884.16014 (ver p. 173).

E. Formanek (1972). "Central polynomials for matrix rings". *J. Algebra* 23, pp. 129–132. MR: 302689. Zbl: 0242.15004 (ver p. 156).

— (1991). *The polynomial identities and invariants of $n \times n$ matrices*. Vol. 78. CBMS Regional Conference Series in Mathematics. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, pp. vi+57. MR: 1088481 (ver pp. vii, 156).

A. Giambruno e D. La Mattina (2005). "PI-algebras with slow codimension growth". *J. Algebra* 284.1, pp. 371–391. MR: 2115020. Zbl: 1071.16021 (ver p. 257).

A. Giambruno, D. La Mattina e P. Misso (2006). "Polynomial identities on superalgebras: classifying linear growth". *J. Pure Appl. Algebra* 207.1, pp. 215–240. MR: 2244391. Zbl: 1116.16028 (ver p. 258).

A. Giambruno, D. La Mattina e V. M. Petrogradsky (2007). "Matrix algebras of polynomial codimension growth". *Israel J. Math.* 158, pp. 367–378. MR: 2342471. Zbl: 1127.16018 (ver pp. 164–166, 172, 256).

A. Giambruno, D. La Mattina e M. V. Zaicev (2014). "Classifying the minimal varieties of polynomial growth". *Canad. J. Math.* 66.3, pp. 625–640. MR: 3194163. Zbl: 1323.16019 (ver pp. 250, 256, 257).

A. Giambruno e S. P. Mishchenko (2001). "Polynomial growth of the $*$-codimensions and Young diagrams". *Comm. Algebra* 29.1, pp. 277–284. MR: 1842497. Zbl: 0988.16018 (ver pp. 245, 247).

A. Giambruno, S. P. Mishchenko e M. V. Zaicev (2001). "Polynomial identities on superalgebras and almost polynomial growth". Em: vol. 29. 9. Special issue dedicated to Alexei Ivanovich Kostrikin, pp. 3787–3800. MR: 1857014. Zbl: 1006.16024 (ver pp. 245, 247).

A. Giambruno e A. Regev (1985). "Wreath products and P.I. algebras". *J. Pure Appl. Algebra* 35.2, pp. 133–149. MR: 775466. Zbl: 0563.16008 (ver p. 246).

A. Giambruno, R. B. dos Santos e A. C. Vieira (2016). "Identities of *-superalgebras and almost polynomial growth". *Linear Multilinear Algebra* 64.3, pp. 484–501. MR: 3439445. Zbl: 1342.16019 (ver pp. 262, 263).

A. Giambruno e M. V. Zaicev (1999). "Exponential codimension growth of PI algebras: an exact estimate". *Adv. Math.* 142.2, pp. 221–243. MR: 1680198. Zbl: 0920.16013 (ver pp. 197, 199).

— (2001). "A characterization of algebras with polynomial growth of the codimensions". *Proc. Amer. Math. Soc.* 129.1, pp. 59–67. MR: 1694862. Zbl: 0962.16018 (ver pp. 219, 228, 235).

— (2005). *Polynomial identities and asymptotic methods*. Vol. 122. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, pp. xiv+352. MR: 2176105. Zbl: 1105.16001 (ver pp. vii, 183, 221).

— (2014). "Growth of polynomial identities: is the sequence of codimensions eventually non-decreasing?" *Bull. Lond. Math. Soc.* 46.4, pp. 771–778. MR: 3239615. Zbl: 1302.16015 (ver p. 198).

A. Gonçalves (1979). *Introdução à álgebra*. Vol. 7. Projeto Euclides. Instituto de Matemática Pura e Aplicada, Rio de Janeiro, pp. xiv+194. MR: 651519 (ver p. 65).

T. A. Gouveia, R. B. dos Santos e A. C. Vieira (2020). "Minimal $*$-varieties and minimal supervarieties of polynomial growth". *J. Algebra* 552, pp. 107–133. MR: 4067466. Zbl: 1442.16024 (ver pp. 253, 254).

P. Halpin (1983). "Central and weak identities for matrices". *Comm. Algebra* 11.19, pp. 2237–2248. MR: 714201. Zbl: 0522.16016 (ver p. 156).

A. Henke e A. Regev (2003). "Explicit decompositions of the group algebras FS_n and FA_n". Em: *Polynomial identities and combinatorial methods (Pantelleria, 2001)*. Vol. 235. Lecture Notes in Pure and Appl. Math. Dekker, New York, pp. 329–357. MR: 2021806. Zbl: 1079.20016 (ver p. 117).

I. N. Herstein (1968). *Noncommutative rings*. The Carus Mathematical Monographs, No. 15. Published by The Mathematical Association of America; distributed by John Wiley & Sons, Inc., New York, pp. xi+199. MR: 0227205. Zbl: 0874.16001 (ver pp. vii, 38).

A. Ioppolo e D. La Mattina (2017). "Polynomial codimension growth of algebras with involutions and superinvolutions". *J. Algebra* 472, pp. 519–545. MR: 3584889. Zbl: 1400.16014 (ver pp. 263, 264).

A. Ioppolo, R. B. dos Santos, M. L. O. Santos e A. C. Vieira (2021). "Superalgebras with graded involution: Classifying minimal varieties of quadratic growth". *Linear Algebra Appl.* 621, pp. 105–134. MR: 4231569. Zbl: 07337672 (ver p. 265).

N. Jacobson (1975). PI-*algebras*. Lecture Notes in Mathematics, Vol. 441. An introduction. Springer-Verlag, Berlin–New York, pp. iv+115. MR: 0369421 (ver p. vi).

G. James e A. Kerber (1981). *The representation theory of the symmetric group*. Vol. 16. Encyclopedia of Mathematics and its Applications. With a foreword by P. M. Cohn, With an introduction by Gilbert de B. Robinson. Addison-Wesley Publishing Co., Reading, Mass., pp. xxviii+510. MR: 644144. Zbl: 1159.20012 (ver p. 112).

G. James e M. Liebeck (2001). *Representations and characters of groups*. Second. Cambridge University Press, New York, pp. viii+458. MR: 1864147. Zbl: 0981.20004 (ver pp. 104, 114).

I. Kaplansky (1948). "Rings with a polynomial identity". *Bull. Amer. Math. Soc.* 54, pp. 575–580. MR: 25451. Zbl: 0032.00701 (ver p. iii).

— (1957). *Problems in the theory of rings. Report of a conference on linear algebras, June, 1956, pp. 1-3*. National Academy of Sciences – National Research Council, Washington, Publ. 502, pp. v+60. MR: 0096696 (ver p. 156).

A. R. Kemer (1978). "The Spechtian nature of T-ideals whose condimensions have power growth". *Sibirsk. Mat. Ž.* 19.1, pp. 54–69, 237. MR: 0466190 (ver p. 145).

— (1979). "Varieties of finite rank". Em: *Proc. 15-th All the Union Algebraic Conf., Krasnoyarsk*. Vol. 2, p. 73 (ver pp. iv, 214).

— (1988). "Solution of the problem as to whether associative algebras have a finite basis of identities". *Dokl. Akad. Nauk SSSR* 298.2, pp. 273–277. MR: 937115 (ver pp. iv, 139).

— (1991). *Ideals of identities of associative algebras*. Vol. 87. Translations of Mathematical Monographs. Translated from the Russian by C. W. Kohls. American Mathematical Society, Providence, RI, pp. vi+81. MR: 1108620. Zbl: 0736.16013 (ver pp. vii, 195, 214).

B. Kostant (1958). "A theorem of Frobenius, a theorem of Amitsur–Levitski and cohomology theory". *J. Math. Mech.* 7, pp. 237–264. MR: 0092755 (ver p. 147).

D. Krakowski e A. Regev (1973). "The polynomial identities of the Grassmann algebra". *Trans. Amer. Math. Soc.* 181, pp. 429–438. MR: 325658. Zbl: 0289.16015 (ver p. 179).

D. La Mattina (2007). "Varieties of almost polynomial growth: classifying their subvarieties". *Manuscripta Math.* 123.2, pp. 185–203. MR: 2306632. Zbl: 1119.16022 (ver pp. 248, 250).

— (2011). "Varieties of superalgebras of almost polynomial growth". *J. Algebra* 336, pp. 209–226. MR: 2802538. Zbl: 1236.16020 (ver pp. 251–254, 263).

D. La Mattina e F. Martino (2016). "Polynomial growth and star-varieties". *J. Pure Appl. Algebra* 220.1, pp. 246–262. MR: 3393459. Zbl: 1336 . 16020 (ver pp. 251, 253, 254, 263).

D. La Mattina, S. Mauceri e P. Misso (2009). "Polynomial growth and identities of superalgebras and star-algebras". *J. Pure Appl. Algebra* 213.11, pp. 2087–2094. MR: 2533307. Zbl: 1178.16019 (ver p. 246).

D. La Mattina e P. Misso (2006). "Algebras with involution with linear codimension growth". *J. Algebra* 305.1, pp. 270–291. MR: 2262527. Zbl: 1113.16029 (ver pp. 253, 258).

T. Y. Lam (1991). *A first course in noncommutative rings*. Vol. 131. Graduate Texts in Mathematics. Springer-Verlag, New York, pp. xvi+397. MR: 1125071. Zbl: 0728.16001 (ver p. 74).

V. N. Latyšev (1972). "On Regev's theorem on identities in a tensor product of PI-algebras". *Uspehi Mat. Nauk* 27.4(166), pp. 213–214. MR: 0393114 (ver p. 170).

U. Leron (1973). "Multilinear identities of the matrix ring". *Trans. Amer. Math. Soc.* 183, pp. 175–202. MR: 332873. Zbl: 0278.16011 (ver p. 155).

J. N. Malcev (1971). "A basis for the identities of the algebra of upper triangular matrices". *Algebra i Logika* 10, pp. 393–400. MR: 0304426 (ver p. 177).

J. N. Malcev e E. N. Kuzmin (1978). "A basis for identities of the algebra of second-order matrices over a finite field". *Algebra i Logika* 17.1, pp. 28–32, 121. MR: 516388 (ver p. 140).

S. P. Mishchenko, A. Regev e M. V. Zaicev (1999). "A characterization of P.I. algebras with bounded multiplicities of the cocharacters". *J. Algebra* 219.1, pp. 356–368. MR: 1707676. Zbl: 0937.16037 (ver p. 233).

S. P. Mishchenko e A. Valenti (2000). "A star-variety with almost polynomial growth". *J. Algebra* 223.1, pp. 66–84. MR: 1738252. Zbl: 0947.16011 (ver p. 245).

T. S. do Nascimento e A. C. Vieira (2019). "Superalgebras with graded involution and star-graded colength bounded by 3". *Linear Multilinear Algebra* 67.10, pp. 1999–2020. MR: 3987576. Zbl: 1422.16045 (ver p. 263).

M. A. de Oliveira e A. C. Vieira (2021). "Varieties of unitary algebras with small growth of codimensions". *Internat. J. Algebra Comput.* 31.2, pp. 257–277. MR: 4242665 (ver pp. 256, 257).

D. S. Passman (1977). *The algebraic structure of group rings*. Pure and Applied Mathematics. Wiley Interscience [John Wiley & Sons], New York–London–Sydney, pp. xiv+720. MR: 470211 (ver p. vii).

C. Procesi (1973). *Rings with polynomial identities*. Pure and Applied Mathematics, 17. Marcel Dekker, Inc., New York, pp. viii+190. MR: 0366968 (ver p. vi).

J. P. Razmyslov (1973). "A certain problem of Kaplansky". *Izv. Akad. Nauk SSSR Ser. Mat.* 37, pp. 483–501. MR: 0338063 (ver pp. 139, 156).

— (1974). "Trace identities of full matrix algebras over a field of characteristic zero". Russo. *Izv. Akad. Nauk SSSR Ser. Mat.* 38, pp. 723–756. MR: 0506414. Zbl: 0311.16016 (ver p. 147).

A. Regev (1972). "Existence of identities in $A \otimes B$". *Israel J. Math.* 11, pp. 131–152. MR: 314893. Zbl: 0249.16007 (ver pp. iv, 158, 167, 169).

— (1984). "Codimensions and trace codimensions of matrices are asymptotically equal". *Israel J. Math.* 47.2-3, pp. 246–250. MR: 738172. Zbl: 0537.16014 (ver p. 182).

A. Regev e S. A. Amitsur (1982). "PI-algebras and their cocharacters". *J. Algebra* 78.1, pp. 248–254. MR: 677720. Zbl: 0495.16014 (ver p. 225).

D. J. S. Robinson (1982). *A course in the theory of groups*. Vol. 80. Graduate Texts in Mathematics. Springer-Verlag, New York–Berlin, pp. xvii+481. MR: 648604 (ver p. 84).

S. Rosset (1976). "A new proof of the Amitsur–Levitski identity". *Israel J. Math.* 23.2, pp. 187–188. MR: 401804 (ver p. 147).

L. H. Rowen (1980). *Polynomial identities in ring theory*. Vol. 84. Pure and Applied Mathematics. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York–London, pp. xx+365. MR: 576061 (ver pp. vi, 156).

— (1991). *Ring theory*. Student. Academic Press, Inc., Boston, MA, pp. xxviii+623. MR: 1095047. Zbl: 0743.16001 (ver p. vii).

B. E. Sagan (2001). *The symmetric group*. Second. Vol. 203. Graduate Texts in Mathematics. Representations, combinatorial algorithms, and symmetric functions. Springer-Verlag, New York, pp. xvi+238. MR: 1824028 (ver pp. 111, 113).

W. Specht (1950). "Gesetze in Ringen. I". *Math. Z.* 52, pp. 557–589. MR: 35274. Zbl: 0032.38901 (ver pp. iv, 139).

R. G. Swan (1963). "An application of graph theory to algebra". *Proc. Amer. Math. Soc.* 14, pp. 367–373. MR: 149468. Zbl: 0118.01802 (ver p. 147).

B. T. Tki (1981). "On the basis of the identities of the matrix algebra of second order over a field of characteristic zero". *Serdica* 7.3, pp. 187–194. MR: 649599. Zbl: 0486.16011 (ver p. 139).

A. Valenti (2002). "The graded identities of upper triangular matrices of size two". *J. Pure Appl. Algebra* 172.2-3, pp. 325–335. MR: 1906883. Zbl: 1007.16019 (ver p. 245).

A. C. Vieira e S. M. A. Jorge (2006). "On minimal varieties of quadratic growth". *Linear Algebra Appl.* 418.2-3, pp. 925–938. MR: 2260241. Zbl: 1107.15011 (ver p. 258).

W. Wagner (1937). "über die Grundlagen der projektiven Geometrie und allgemeine Zahlensysteme". *Math. Ann.* 113.1, pp. 528–567. MR: 1513106 (ver pp. iii, 156).

Índice de Notações

Índice de Autores

Índice Remissivo

Títulos Publicados — 33º Colóquio Brasileiro de Matemática

Geometria Lipschitz das singularidades – *Lev Birbrair e Edvalter Sena*

Combinatória – *Fábio Botler, Maurício Collares, Taísa Martins, Walner Mendonça, Rob Morris e Guilherme Mota*

Códigos Geométricos – *Gilberto Brito de Almeida Filho e Saeed Tafazolian*

Topologia e geometria de 3-variedades – *André Salles de Carvalho e Rafał Marian Siejakowski*

Ciência de Dados: Algoritmos e Aplicações – *Luerbio Faria, Fabiano de Souza Oliveira, Paulo Eustáquio Duarte Pinto e Jayme Luiz Szwarcfiter*

Discovering Euclidean Phenomena in Poncelet Families – *Ronaldo A. Garcia e Dan S. Reznik*

Introdução à geometria e topologia dos sistemas dinâmicos em superfícies e além – *Víctor León e Bruno Scárdua*

Equações diferenciais e modelos epidemiológicos – *Marlon M. López-Flores, Dan Marchesin, Vítor Matos e Stephen Schecter*

Differential Equation Models in Epidemiology – *Marlon M. López-Flores, Dan Marchesin, Vítor Matos e Stephen Schecter*

A friendly invitation to Fourier analysis on polytopes – *Sinai Robins*

PI-álgebras: uma introdução à PI-teoria – *Rafael Bezerra dos Santos e Ana Cristina Vieira*

First steps into Model Order Reduction – *Alessandro Alla*

The Einstein Constraint Equations – *Rodrigo Avalos e Jorge H. Lira*

Dynamics of Circle Mappings – *Edson de Faria e Pablo Guarino*

Statistical model selection for stochastic systems – *Antonio Galves, Florencia Leonardi e Guilherme Ost*

Transfer Operators in Hyperbolic Dynamics – *Mark F. Demers, Niloofar Kiamari e Carlangelo Liverani*

A Course in Hodge Theory Periods of Algebraic Cycles – *Hossein Movasati e Roberto Villaflor Loyola*

A dynamical system approach for Lane–Emden type problems – *Liliane Maia, Gabrielle Nornberg e Filomena Pacella*

Visualizing Thurston's Geometries – *Tiago Novello, Vinícius da Silva e Luiz Velho*

Scaling Problems, Algorithms and Applications to Computer Science and Statistics – *Rafael Oliveira e Akshay Ramachandran*

An Introduction to Characteristic Classes – *Jean-Paul Brasselet*

impa

Instituto de
Matemática
Pura e Aplicada

ISBN 978-65-89124-37-5