UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

REBECA MARGARIDO VELOSO DOS SANTOS

ESTRUTURA DE ÁLGEBRAS ASSOCIATIVAS COM DIMENSÃO FINITA

SÃO CARLOS
2024

REBECA MARGARIDO VELOSO DOS SANTOS

ESTRUTURA DE ÁLGEBRAS ASSOCIATIVAS COM DIMENSÃO FINITA

Monografia apresentada ao Curso de Bacharelado em Matemática da Universidade Federal de São Carlos.

Orientador: Prof. Dr. Dimas José Gonçalves

SÃO CARLOS
2024

Margarido Veloso dos Santos, Rebeca

Estrutura de álgebras associativas com dimensão finita / Rebeca Margarido Veloso dos Santos -- 2024.
63f.

TCC (Graduação) - Universidade Federal de São Carlos, campus São Carlos, São Carlos
Orientador (a): Dimas José Gonçalves
Banca Examinadora: Fabio Ferrari Ruffino, Rafael Augusto dos Santos Kapp
Bibliografia

1. Álgebras associativas. 2. Teoremas de estrutura de Wedderburn. I. Margarido Veloso dos Santos, Rebeca. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Arildo Martins - CRB/8 7180

AGRADECIMENTOS

Aos meus pais, Patrícia e Elielcio, meus avós, Rita e Luiz e à minha irmã Sarah, por sempre serem meus maiores apoiadores;

Ao meu namorado Guilherme Sato, pela companhia e apoio que tornam as dificuldades mais fáceis de enfrentar;

Aos colegas do PET Matemática, cuja amizade e convivência me proporcionaram um suporte tão valioso durante a graduação;

Ao orientador Prof. Dr. Dimas José Gonçalves, por me despertar o interesse na área de álgebra e por toda a paciência e atenção durante a confecção deste trabalho;

A todos os professores do Departamento de Matemática, pela imensa contribuição à minha formação acadêmica e profissional.

"It is not knowledge, but the act of learning,
not possession but the act of getting there,
which grants the greatest enjoyment."
Carl Friedrich Gauss *(GAUSS, 1808).*

RESUMO

O presente trabalho tem por objetivo introduzir conceitos e propriedades de álgebras associativas com dimensão finita, com o intuito de descrever sua estrutura. No primeiro capítulo, apresentaremos algumas estruturas algébricas e suas propriedades, iniciando com a demonstração do teorema de Frobenius. Após isso, seguiremos definindo os conceitos de anéis simples, álgebras centrais, álgebras com multiplicação, automorfismos de álgebras centrais simples e subcorpos maximais, a fim de finalizar com as demonstrações dos teoremas de Skolem-Noether e de Wedderburn.

No segundo capítulo, daremos enfoque à teoria de estrutura de Wedderburn. Definiremos os conceitos de ideais nilpotentes, anéis primos e semiprimos, unitização de álgebras, representação regular, álgebras grupo, matrizes canônicas, idempotentes e ideais minimais, a fim de demonstrar o Teorema de Maschke e os Teoremas de Estrutura de Wedderburn, que descrevem de maneira concreta a estrutura de álgebras associativas com dimensão finita. O trabalho será finalizado com alguns exemplos práticos que ilustram estes resultados.

Palavras-chave: Álgebras associativas. Teorema de Frobenius. Teorema de Skolem-Noether. Teorema de Maschke. Teorema de Wedderburn.

ABSTRACT

The present work aims to introduce concepts and properties of finite-dimensional associative algebras, in order to describe their structure. In the first chapter, we will present properties of a few algebraic structures, starting with the proof of Frobenius' theorem. After that, we will define simple rings, central algebras, multiplication algebras, automorphisms of simple central algebras and maximal subfields, in order to finish with the proofs of the Skolem-Noether and Wedderburn theorems.

In the second chapter, we will focus on Wedderburn's structure theory. We will define the concepts of nilpotent ideals, prime and semiprime rings, unitization of algebras, regular representation, group algebras, matrix units, idempotents and minimal ideals, in order to prove Maschke's theorem and Wedderburn's structure theorems, which concretely describe the structure of finite-dimensional associative algebras. This work will conclude with some practical examples that illustrate these results.

Keywords: Associative algebras. Frobenius theorem. Skolem-Noether theorem. Maschke theorem. Wedderburn theorem.

SUMÁRIO

1 INTRODUÇÃO

A álgebra abstrata é o ramo da matemática que se dedica ao estudo de estruturas algébricas. Uma das estruturas mais importantes são as álgebras sobre um corpo, sendo um dos mais básicos objetos de estudo na área.

Neste trabalho faremos um estudo inicial sobre a noção de álgebra, com foco em álgebras associativas com dimensão finita e suas propriedades.

Tais estruturas estão inseridas na teoria das álgebras não comutativas. Estas são simplesmente as estruturas nas quais a operação de produto não é comutativa. Um dos primeiros exemplos deste tipo de estrutura visto na graduação é o dos anéis de matrizes, onde para duas matrizes $n \times n$, $n \geq 2$, geralmente ocorre que $AB \neq BA$. Ao longo do trabalho, iremos introduzir a álgebra não comutativa dos quatérnios, denotada por $\mathbb{H}$, em homenagem ao matemático irlandês William Rowan Hamilton, que a descreveu em 1843.

O assunto contido aqui foi estudado a partir da referência (BRESAR, 2014), e a estrutura do trabalho segue da seguinte forma:

Iniciaremos o Capítulo 3 construindo a demonstração do Teorema de Frobenius, que diz que uma álgebra com divisão de dimensão finita sobre o corpo $\mathbb{R}$ é isomorfa a $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$. Após isso, definiremos a noção de álgebras simples, introduzindo a álgebra de Weyl, denotada por $\mathscr{A}_1$, e suas propriedades.

As seguintes seções definem as noções de álgebras centrais e álgebras com multiplicação, utilizando-as para estudar automorfismos de álgebras centrais simples. Um resultado importante desta seção é o Teorema de Skolem-Noether, em nome de Thoralf Skolem e Emmy Noether. Finalizaremos o Capítulo 3 definindo subcorpos maximais e demonstrando um dos Teoremas de Wedderburn, que diz que todo anel com divisão finito é um corpo.

O Capítulo 4 é centrado na Teoria de Estrutura de Wedderburn que, sob certas restrições, descreve a forma de uma álgebra de dimensão finita e, em certo sentido, reduz o problema de compreensão de álgebras de dimensão finita ao problema de compreensão das álgebras com divisão de dimensão finita.

As primeiras seções definem as noções de ideais nilpotentes e ideais primos e semiprimos, com alguns exemplos destas estruturas. A seguir, definiremos as noções de unitização, representação regular e álgebras grupo. Um importante resultado desta seção é o Teorema de Maschke.

Por fim, definiremos os conceitos de matrizes canônicas, idempotentes e ideais minimais, finalizando o capítulo com as demonstrações dos Teoremas de Estrutura de Wedderburn.

2 PRELIMINARES

Neste pequeno capítulo, apresentaremos alguns conceitos e resultados básicos que serão utilizados ao longo deste trabalho. Aqui, F sempre denotará um corpo e, quando necessário, relembraremos o leitor deste fato.

Definição 2.0.1. Uma **álgebra** A sobre F (ou uma F-álgebra) é um conjunto $A \neq \varnothing$ munido de três operações

$$\begin{gathered} + : A \times A \to A,\ (x, y) \mapsto x + y \text{ (soma)}; \\ \cdot : A \times A \to A,\ (x, y) \mapsto xy \text{ (multiplicação)}; \\ \bullet : F \times A \to A,\ (\lambda, x) \mapsto \lambda x \text{ (multiplicação por escalar)}, \end{gathered}$$

que satisfazem as seguintes propriedades:

(a) $(A, +, \cdot)$ é um anel associativo;

(b) $(A, +, \bullet)$ é um F-espaço vetorial;

(c) $\lambda(xy) = (\lambda x)y = x(\lambda y)$ para todos $\lambda \in F$ e $x, y \in A$.

A seguir, daremos exemplos de algumas álgebras que serão utilizadas ao longo deste trabalho. Posteriormente, falaremos também de um importante exemplo: a álgebra de Weyl.

Exemplo 2.0.2. O anel dos polinômios $F[\omega]$ em uma variável comutativa ω é uma F-álgebra com as operações usuais de soma e produto de polinômios e produto por escalar. Relembramos que seus elementos têm a forma

$$f(\omega) = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_n\omega^n$$

onde $a_0, a_1, a_2, \ldots, a_n \in F$ e $n \in \mathbb{N}$.

Exemplo 2.0.3. Dada uma F-álgebra D, o conjunto $M_n(D)$ das matrizes $n \times n$ com entradas em D é uma F-álgebra com as operações usuais de soma e produto de matrizes e produto por escalar.

Exemplo 2.0.4. Dado um espaço vetorial V sobre F, denotamos por $End_F(V)$ o conjunto de todas as transformações lineares de V em V. Com as operações usuais de soma e composição de transformações lineares e produto por escalar, segue que $End_F(V)$ é uma F-álgebra.

Definição 2.0.5. Seja A uma F-álgebra.

(a) Se A é um anel unitário, dizemos que A é uma **álgebra unitária**.

(b) Se A é um anel com divisão, dizemos que A é uma **álgebra com divisão**.

Exemplo 2.0.6. Os $\mathbb{R}$ e $\mathbb{C}$ são $\mathbb{R}$-álgebras com divisão. No próximo capítulo também exibiremos outro importante exemplo: os quatérnios $\mathbb{H}$.

Um fato simples, mas que vale a pena ser citado, é que se A é uma álgebra com divisão e $u, v \in A$ satisfazem $uv = 0$, então $u = 0$ ou $v = 0$. De fato, se $u \neq 0$ e $v \neq 0$ seguem as implicações:

$$uv = 0 \Rightarrow u^{-1}uv = u^{-1}0 \Rightarrow 1v = 0 \Rightarrow v = 0,$$

o que contradiz a suposição.

Definição 2.0.7. Dizemos que a **dimensão** de uma F-álgebra A é a dimensão de A como espaço vetorial sobre F. Neste caso, denotamos ela por

$$[A : F] = \dim_F A.$$

Exemplo 2.0.8. Para alguns exemplos citados anteriormente, segue que

$$[\mathbb{C} : \mathbb{R}] = 2, \quad [M_n(F) : F] = n^2 \quad \text{e} \quad [F[\omega] : F] = \infty.$$

Definição 2.0.9. Um **homomorfismo de F-álgebras** é um homomorfismo de anéis que também é uma transformação linear. Um **isomorfismo de F-álgebras** é um homomorfismo de álgebras bijetivo.

Podemos definir de maneira análogo os conceitos de endomorfismo, monomorfismo, epimorfismo e automorfismo de álgebras.

Exemplo 2.0.10. Seja A uma álgebra unitária e $a \in A$ um elemento invertível. O homomorfismo $\varphi : A \to A$ dado por

$$\varphi(x) = axa^{-1}$$

é chamado de **automorfismo interno**.

Definição 2.0.11. Seja A uma F-álgebra e $S \subseteq A$. A **subálgebra de A gerada por S** é a intersecção de todas as subálgebras de A que contém S.

Pela definição podemos ver que a subálgebra de A gerada por S é a menor subálgebra de A que contém S. No próximo resultado descrevemos ela de maneira explícita.

Lema 2.0.12. *Seja A uma F-álgebra e $S \subseteq A$. A subálgebra de A gerada por S é o subespaço vetorial de A gerado pelos elementos*

$$s_1 s_2 \cdots s_n$$

onde $s_1, s_2, \ldots, s_n \in S$ e $n \in \mathbb{N}$.

3 ÁLGEBRAS COM DIVISÃO DE DIMENSÃO FINITA

Este capítulo tem por objetivo definir estruturas de álgebras e suas propriedades, bem como expor alguns exemplos de álgebras importantes. Os principais resultados demonstrados serão o Teorema de Frobenius, o Teorema de Skolem-Noether e o Teorema de Wedderburn.

3.1 UM RESULTADO DE FROBENIUS

Nesta seção, nos dedicaremos a demonstrar o Teorema de Frobenius, apresentando lemas que serão utilizados em sua demonstração.

Ao longo da seção, D denotará uma $\mathbb{R}$-álgebra com divisão de dimensão finita $n \geq 1$.

Um número real $\alpha \in \mathbb{R}$ será identificado com $\alpha \cdot 1_D$, onde 1_D é o elemento identidade de D.

Lema 3.1.1. *Para todo $x \in D$, existe $\lambda \in \mathbb{R}$ tal que $x^2 + \lambda x \in \mathbb{R}$.*

Demonstração. Como D tem dimensão n, os $n+1$ elementos $1, x, x^2, \ldots, x^n$ são linearmente dependentes. Assim, existe um polinômio não nulo $f(\omega) \in \mathbb{R}[\omega]$, de grau no máximo n, tal que $f(x) = 0$. A menos de um múltiplo, podemos assumir que o coeficiente líder do polinômio seja igual a 1, isto é,

$$f(\omega) = \omega^t + a_{t-1}\omega^{t-1} + a_{t-2}\omega^{t-2} + \cdots + a_1\omega + a_0,$$

onde $a_{t-1}, a_{t-2}, \ldots, a_1, a_0 \in \mathbb{R}$ e $t \leq n$. Pelo Teorema Fundamental da Álgebra, $f(\omega)$ pode ser fatorado como produto de polinômios de grau 1 e grau 2 irredutíveis em $\mathbb{R}[\omega]$:

$$f(\omega) = (\omega - \alpha_1)\cdots(\omega - \alpha_r)(\omega^2 + \lambda_1\omega + \mu_1)\cdots(\omega^2 + \lambda_s\omega + \mu_s)$$

onde $\alpha_i, \lambda_i, \mu_i \in \mathbb{R}$. Como $f(x) = 0$, temos

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_r)(x^2 + \lambda_1 x + \mu_1)\cdots(x^2 + \lambda_s x + \mu_s) = 0.$$

Como D é uma álgebra com divisão, um destes fatores deve ser 0. Logo, x é raiz de um polinômio linear ou quadrático em $\mathbb{R}[\omega]$.

Se para algum k ocorrer $(x - \alpha_k) = 0$, então teremos

$$x = \alpha_k \in \mathbb{R} \text{ e } x^2 + 1x \in \mathbb{R}.$$

Se para algum k ocorrer $(x^2 + \lambda_k x + \mu_k) = 0$, então teremos

$$x^2 + \lambda_k x = -\mu_k \in \mathbb{R}.$$

Nos dois casos acima existe $\lambda \in \mathbb{R}$ tal que $x^2 + \lambda x \in \mathbb{R}$, finalizando a demonstração. □

Antes do próximo lema, colocaremos um exemplo como motivação.

Exemplo 3.1.2. O conjunto $V = \{\, v \in \mathbb{C} : v^2 \in \mathbb{R} \text{ e } v^2 \leq 0 \,\}$ é formado pelos elementos $a + bi \in \mathbb{C}$ tal que $a = 0$ e $b \in \mathbb{R}$. Assim, V é um $\mathbb{R}$-subespaço vetorial de $\mathbb{C}$ e $\mathbb{C} = \mathbb{R} \oplus V$.

Lema 3.1.3. *O conjunto $V = \{\, v \in D \mid v^2 \in \mathbb{R} \text{ e } v^2 \leq 0 \,\}$ é um $\mathbb{R}$-subespaço vetorial de D. Além disso, $D = \mathbb{R} \oplus V$.*

Demonstração. Começaremos a demonstração com a importante afirmação.

Afirmação 1. Se $x \in D \setminus V$ e $x^2 \in \mathbb{R}$, então $x \in \mathbb{R}$.
Demonstração da afirmação. Se $x \in D \setminus V$, então $x^2 > 0$. Assim, $x^2 = \alpha^2$ para algum $\alpha \in \mathbb{R}$. Logo,

$$x^2 - \alpha^2 = 0 \Rightarrow (x - \alpha)(x + \alpha) = 0 \Rightarrow x = \pm\alpha \in \mathbb{R}.$$

Finalizamos a demonstração da afirmação.

Afirmação 2. $\mathbb{R} \cap V = \{0\}$.
Demonstração da afirmação. Se $x \in \mathbb{R} \cap V$, então $x^2 \geq 0$ e $x^2 \leq 0$. Logo, $x^2 = 0$ e $x = 0$. Finalizamos a demonstração da afirmação.

Afirmação 3. V é um subespaço vetorial de D.
Demonstração da afirmação. Sejam $v \in V$ e $\lambda \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Temos

$$(\lambda v)^2 = \lambda^2 v^2.$$

Como $\lambda \in \mathbb{R}^*$ ($\lambda^2 > 0$) e $v \in V$ ($v^2 \leq 0$), segue que

$$(\lambda v)^2 = \lambda^2 v^2 \leq 0,$$

ou seja, $\lambda v \in V$. Assim, V é fechado para multiplicação por escalar.

Resta mostrar que para $u, v \in V$ temos $u + v \in V$. Aqui temos dois casos a serem analisados: quando $\{u, v\}$ é linearmente dependente e quando $\{u, v\}$ é linearmente independente.

Caso 1: $\{u, v\}$ é linearmente dependente. Neste caso, existem $\alpha, \beta \in \mathbb{R}$ não todos nulos tais que

$$\alpha u + \beta v = 0.$$

Supomos, sem perda de generalidade, que $u = \lambda v$, para algum $\lambda \in \mathbb{R}$. Assim,

$$u + v = \lambda v + v = (\lambda + 1)v \in V$$

pois V é fechado para multiplicação por escalar.

Caso 2: $\{u, v\}$ é linearmente independente. Neste caso, afirmamos que $\{1, u, v\}$ também é linearmente independente. De fato, tomando α, β', $\gamma' \in \mathbb{R}$ tais que

$$\alpha u + \beta' v + \gamma' 1 = 0, \text{ obtemos } \alpha u = -\beta' v - \gamma'.$$

Redefinindo $-\beta' = \beta$ e $-\gamma' = \gamma$ obtemos a premissa e implicações seguintes:

$$\begin{gathered}\alpha u = \beta v + \gamma \Rightarrow (\alpha u)^2 = (\beta v + \gamma)^2 \\ \Rightarrow \alpha^2 u^2 = \beta^2 v^2 + 2\beta\gamma v + \gamma^2 \Rightarrow 2\beta\gamma v = \alpha^2 u^2 - \beta^2 v^2 - \gamma^2 \\ \Rightarrow \beta\gamma v = \frac{1}{2}(\alpha^2 u^2 - \beta^2 v^2 - \gamma^2)\end{gathered}$$

Como $u, v \in V$, segue que $u^2, v^2 \in \mathbb{R}$ e portanto $\beta\gamma v \in \mathbb{R}$. Como $\beta\gamma v \in \mathbb{R} \cap V$, segue da Afirmação 2 que $\beta = 0$ ou $\gamma = 0$. Novamente, temos dois casos a analisar:

Caso $\beta = 0$: Neste caso,

$$\alpha u = \gamma \in \mathbb{R} \cap V \Rightarrow \alpha = 0 \text{ e } \gamma = 0.$$

Caso $\gamma = 0$: Neste caso,

$$\alpha u = \beta v \Rightarrow \alpha = 0 \text{ e } \beta = 0$$

pois $\{u, v\}$ é linearmente independente.

Em ambos os casos, obtemos $\alpha = \beta = \gamma = 0$. Logo, $\{1, u, v\}$ é linearmente independente.

Pelo Lema 3.1.1, como $u - v, u + v \in D$, existem $\lambda, \mu \in \mathbb{R}$ tais que

$$(u+v)^2 + \lambda(u+v) \in \mathbb{R}, \tag{3.1}$$

$$(u-v)^2 + \mu(u-v) \in \mathbb{R}. \tag{3.2}$$

Por outro lado,

$$(u+v)^2 + (u-v)^2 = u^2 + uv + vu + v^2 + u^2 - uv - vu + v^2 = 2u^2 + 2v^2 \in \mathbb{R}.$$

Deste fato e de (3.1) e (3.2), obtemos a premissa e implicações a seguir:

$$\begin{gathered}(u+v)^2 + \lambda(u+v) + (u-v)^2 + \mu(u-v) = r \in \mathbb{R} \\ \Rightarrow \lambda(u+v) + \mu(u-v) = r - ((u+v)^2 + (u-v)^2) \in \mathbb{R} \\ \Rightarrow \lambda(u+v) + \mu(u-v) \in \mathbb{R} \\ \Rightarrow \lambda u + \lambda v + \mu u - \mu v \in \mathbb{R} \\ \Rightarrow (\lambda + \mu)u + (\lambda - \mu)v \in \mathbb{R}.\end{gathered}$$

Como $\{1, u, v\}$ é linearmente independente, obtemos

$$\lambda + \mu = \lambda - \mu = 0 \text{ e portanto } \lambda = \mu = 0.$$

Substituindo λ em (3.1), temos

$$(u+v)^2 \in \mathbb{R}.$$

Também, $(u+v)^2 \leq 0$. De fato, suponha $(u+v)^2 > 0$: Pela Afirmação 1, $u + v = \alpha \in \mathbb{R}$ e

$$u = \alpha 1 - 1v.$$

Assim, u é combinação linear de 1 e v. Mas $\{1, u, v\}$ são linearmente independentes, o que gera um absurdo. Assim, como $(u+v)^2 \in \mathbb{R}$ e $(u+v)^2 \leq 0$, segue que $(u+v) \in V$. Portanto, V é subespaço vetorial de D. Finalizamos a demonstração da afirmação.

Por último, provaremos que $D = \mathbb{R} + V$. Seja $x \in D \setminus \mathbb{R}$. Pelo Lema 3.1.1, $x^2 + kx \in \mathbb{R}$ para algum $k \in \mathbb{R}$. Temos que $x + \frac{k}{2} \in V$. De fato,

$$\left(x + \frac{k}{2}\right)^2 = x^2 + xk + \left(\frac{k}{2}\right)^2 \in \mathbb{R}.$$

Agora, se supomos $\left(x + \frac{k}{2}\right)^2 > 0$, então pela Afirmação 1,

$$\begin{aligned} x + \frac{k}{2} &= \alpha \text{ para algum } \alpha \in \mathbb{R} \\ \Rightarrow x &= \alpha - \frac{k}{2} \in \mathbb{R}. \end{aligned}$$

Mas $x \in D \setminus \mathbb{R}$, o que contraria a suposição. Logo, $\left(x + \frac{k}{2}\right)^2 \leq 0$. Assim,

$$\frac{k}{2} \in \mathbb{R} \quad \text{e} \quad x + \frac{k}{2} \in V \Rightarrow x = -\frac{k}{2} + \left(x + \frac{k}{2}\right) \in \mathbb{R} + V.$$

A demonstração do lema está completa. □

Considere o conjunto V do lema anterior. Defina a operação $\circ : V \times V \to \mathbb{R}$ por

$$u \circ v := uv + vu,$$

para todos $u, v \in V$. Como $u \circ v = (u+v)^2 - u^2 - v^2$, segue do Lema 3.1.3 que de fato $u \circ v \in \mathbb{R}$. Além disso, como D é álgebra com divisão, se $v \neq 0$ então $v \circ v = 2v^2 < 0$.

Lema 3.1.4. *Se $[D : \mathbb{R}] = n > 2$, então existem $i, j, k \in D$ tal que*

$$\begin{aligned} i^2 = j^2 = k^2 = -1, \\ ij = -ji = k,\ ki = -ik = j,\ jk = -kj = i, \end{aligned} \tag{3.3}$$

e $\{1, i, j, k\}$ é linearmente independente.

Demonstração. Pelo Lema 3.1.3, $D = \mathbb{R} \oplus V$. Como D tem dimensão n, e $\mathbb{R}$ tem dimensão 1, então V tem dimensão $n - 1 > 1$. Podemos tomar vetores $v, w \in V$ linearmente independentes. Seja

$$u := w - \frac{w \circ v}{v \circ v} v.$$

Temos que $u \neq 0$, pois

$$u = 0 \Rightarrow w - \frac{w \circ v}{v \circ v} v = 0 \Rightarrow 1w - \frac{w \circ v}{v \circ v} v = 0$$

de modo que existe uma combinação linear de v e w, com escalares não todos nulos, igual a 0. Como v, w são linearmente independentes, isto contradiz a suposição.

Agora, para a operação $\circ$, temos as seguinte propriedades para $a, b, c \in V$ e $\lambda \in \mathbb{R}$:

$$\begin{aligned} a \circ (b+c) &= a(b+c) + (b+c)a \\ &= ab + ac + ba + ca = ab + ba + ac + ca \\ &= a \circ b + a \circ c, \end{aligned}$$

$$\begin{aligned} (\lambda a) \circ b &= \lambda ab + b\lambda a \\ &= \lambda(ab + ba) = \lambda(a \circ b) \end{aligned}$$

e também

$$a \circ b = ab + ba = ba + ab = b \circ a.$$

Assim,

$$u \circ v = w \circ v + \left[-\left(\frac{w \circ v}{v \circ v} v \right) \right] \circ v = w \circ v - \left(\frac{w \circ v}{v \circ v} \right)(v \circ v) = w \circ v - w \circ v = 0.$$

Ou seja, seguindo a ideia de Álgebra Linear, partimos de dois vetores L.I. que chamamos de v e w, aplicamos o processo de ortogonalização de Gram-Schmidt e encontramos os vetores "ortogonais" v e u. Em particular, de $uv + vu = u \circ v = 0$ obtemos

$$uv = -vu.$$

Sejam

$$i = \frac{1}{\sqrt{-u^2}} u, \ \ j = \frac{1}{\sqrt{-v^2}} v \ \text{ e } \ k = ij.$$

Temos as seguintes igualdades:

$$\begin{aligned} i^2 &= \left(\frac{1}{\sqrt{-u^2}} u \right)^2 = \left(\frac{1}{\sqrt{-u^2}} u \right)\left(\frac{1}{\sqrt{-u^2}} u \right) = \frac{1}{-u^2} u^2 = -1, \\ j^2 &= \left(\frac{1}{\sqrt{-v^2}} v \right)^2 = \left(\frac{1}{\sqrt{-v^2}} v \right)\left(\frac{1}{\sqrt{-v^2}} v \right) = \frac{1}{-v^2} v^2 = -1, \\ ij &= \frac{u}{\sqrt{-u^2}} \frac{v}{\sqrt{-v^2}} = \left(\frac{1}{\sqrt{-u^2}} \frac{1}{\sqrt{-v^2}} \right)(uv) = \left(\frac{1}{\sqrt{-u^2}} \frac{1}{\sqrt{-v^2}} \right)(-vu) = -ji, \\ k^2 &= (ij)^2 = ijij = -iijj = -(-1)(-1) = -1, \\ ki &= iji = -iij = -ik = (-i^2)j = -(-1)j = 1j = j, \\ jk &= jij = -ijj = -kj = -i(j^2) = -i(-1) = i. \end{aligned}$$

Além disso, definidos desta forma, i, j, k e 1 são linearmente independentes. De fato, pelas igualdades acima temos para $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$:

$$\begin{aligned}
&\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k = 0 \\
\Rightarrow\ &(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = 0(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) \\
\Rightarrow\ &(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = 0 \\
\Rightarrow\ &\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0 \\
\Rightarrow\ &\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0.
\end{aligned}$$

Finalizamos a demonstração do lema. □

Como i, j, k e 1 são linearmente independentes, o caso em que $n = 3$ é descartado. Se $n = 4$, então D tem uma base $\{1, i, j, k\}$ que segue a relação definida no Lema 3.1.4.

Vamos supor então que temos um espaço vetorial real D de dimensão 4 com base $\{1, i, j, k\}$, sobre o qual definimos a multiplicação através de (3.3) com o requerimento que 1 seja uma unidade. Como os elementos da base são associativos, vemos que D é de fato uma $\mathbb{R}$-álgebra. Esta álgebra, denotada por $\mathbb{H}$, é a álgebra dos **quatérnios**. Ela foi descrita pelo matemático irlandês W. R. Hamilton em 1843.

Definimos o **conjugado** de um elemento arbitrário $h = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ em $\mathbb{H}$ por

$$\overline{h} := \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k.$$

Se $h \neq 0$, então

$$h\overline{h} = \overline{h}h = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$$

é um escalar não nulo. Logo, h é invertível com inversa $\left(\frac{1}{h\overline{h}}\right)\overline{h}$. Logo, $\mathbb{H}$ é uma álgebra com divisão, não comutativa, de dimensão 4.

O seguinte teorema foi provado em 1878 pelo matemático F. G. Frobenius.

Teorema 3.1.5 (Frobenius)**.** *Toda $\mathbb{R}$-álgebra D com divisão de dimensão finita é isomorfa a $\mathbb{R}$ ou $\mathbb{C}$ ou $\mathbb{H}$.*

Demonstração. Seja n a dimensão de D.

Se $n = 1$, então como $D = \mathbb{R} \oplus V$ e $\dim \mathbb{R} = 1$, segue que $V = \{0\}$ e $D \cong \mathbb{R}$.

Se $n = 2$, então $V \neq \{0\}$. Assim, pelo Lema 3.1.3, V contém um elemento i tal que $i^2 = -1$. Logo, $D \cong \mathbb{C}$.

Pelo Lema 3.1.4, obtemos que $n \neq 3$, pois para $n > 2$ os elementos i, j, k e 1 de D são linearmente independentes.

Se $n = 4$, então $D \cong \mathbb{H}$.

Supomos agora $n > 4$, e sejam i, j, k os elementos definidos no Lema 3.1.4. Como a dimensão de V é $n - 1$, existe $v \in V$ fora do subespaço vetorial gerado por i, j, k. Logo,

$$e := v + \frac{i \circ v}{2} i + \frac{j \circ v}{2} j + \frac{k \circ v}{2} k$$

é um elemento não nulo em V que satisfaz $i \circ e = j \circ e = k \circ e = 0$. De fato,

$$i \circ e = i \circ \left(v + \frac{i \circ v}{2} i + \frac{j \circ v}{2} j + \frac{k \circ v}{2} k \right) = i \circ v + i \circ \left(\frac{i \circ v}{2} i \right) + i \circ \left(\frac{j \circ v}{2} j \right) + i \circ \left(\frac{k \circ v}{2} k \right) =$$
$$i \circ v + \left(\frac{i \circ v}{2} \right) (i \circ i) + \left(\frac{j \circ v}{2} \right) (i \circ j) + \left(\frac{k \circ v}{2} \right) (i \circ k) = i \circ v + \left(\frac{i \circ v}{2} \right) (i \circ i) =$$
$$i \circ v + \left(\frac{i \circ v}{2} \right) (-2) = 0.$$

De maneira análoga,

$$j \circ e = 0 \text{ e } k \circ e = 0.$$

De $i \circ e = j \circ e = 0$ obtemos

$$ei + ie = 0 \Rightarrow ei = -ie \Rightarrow eij = -iej = -i(-je) = ije \Rightarrow eij = ije$$
$$\Rightarrow ek = ke$$

Por outro lado, de $k \circ e = 0$ obtemos $ke = -ek$. Assim,

$$ke = -ek = -ke \Rightarrow 2ke = 0 \Rightarrow ke = 0 \Rightarrow k = 0 \text{ ou } e = 0.$$

A última implicação vem do fato que D é álgebra com divisão. Como $e \neq 0$ e $k \neq 0$ temos um absurdo. Logo, n só pode ser 1, 2 ou 4.

A demonstração do teorema está finalizada. □

O Teorema de Frobenius classifica as $\mathbb{R}$-álgebras com divisão de dimensão finita. Uma pergunta natural agora seria: quais são as $\mathbb{C}$-álgebras com divisão de dimensão finita? Como $\mathbb{C}$ é um corpo algebricamente fechado, podemos fazer uma pergunta então um pouco mais geral: dado um corpo algebricamente fechado F, quais são as F-álgebras com divisão de dimensão finita? Para responder a esta pergunta, precisamos de alguns conceitos.

Definição 3.1.6. Seja F um corpo qualquer. Dizemos que um elemento x de uma F-álgebra A é **algébrico** se existe um polinômio não nulo $f(\omega) \in F[\omega]$ tal que $f(x) = 0$. Se todo elemento de uma álgebra A é algébrico, então A é chamada de **álgebra algébrica**.

Lema 3.1.7. *Toda F-álgebra de dimensão finita é uma álgebra algébrica.*

Demonstração. Denote por A tal F-álgebra de dimensão finita n. Se $x \in A$, então o conjunto de todas as potências de x,

$$\{1, x, x^2, \ldots, x^n, \ldots\},$$

é um conjunto linearmente dependente. Logo, existem $\alpha_0, \alpha_1, \ldots, \alpha_n \in F$ não todos nulos tal que

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n = 0.$$

Definindo o polinômio não nulo $f(\omega) \in F[\omega]$ por

$$f(\omega) = \alpha_0 + \alpha_1 \omega + \alpha_2 \omega^2 + \cdots + \alpha_n \omega^n,$$

segue que $f(x) = 0$. □

Proposição 3.1.8. *Se D é uma álgebra com divisão de dimensão finita sobre um corpo algebricamente fechado F, então D = F.*

Demonstração. Seja $x \in D$. Pelo Lema 3.1.7, existe um polinômio não nulo $f(\omega) \in F[\omega]$ tal que $f(x) = 0$. Podemos assumir o coeficiente líder como igual a 1. Como F é algebricamente fechado, temos

$$f(\omega) = (\omega - \alpha_1)\cdots(\omega - \alpha_r)$$

para alguns $\alpha_1, \ldots, \alpha_r \in F$. Consequentemente,

$$(x - \alpha_1)\cdots(x - \alpha_r) = 0.$$

Como D é uma álgebra com divisão, algum destes fatores lineares deve ser nulo. Isto nos dá que $x - \alpha_i = 0$ para algum i e, portanto, $x = \alpha_i \in F$. □

3.2 ANÉIS SIMPLES

Nesta seção, definiremos os conceitos de anéis simples e álgebras simples, exemplificando com a álgebra simples $\mathscr{A}_1$ (álgebra de Weyl).

Definição 3.2.1. Um subanel I de um anel R é dito ser um **ideal à esquerda de R** se $xu \in I$ para todo $x \in R$ e $u \in I$. Analogamente, é dito um **ideal à direita de R** se $ux \in I$ para todo $x \in R$ e $u \in I$. Se é um ideal à esquerda e à direita, então I é simplesmente chamado de **ideal de R**.

Exemplo 3.2.2. Dado um corpo F, considere $R = M_n(F)$. Se I é o subconjunto de R formado por todas as matrizes cujas colunas $2, 3, \ldots, n$ são nulas, então I é um ideal à esquerda de R. Se J é o subconjunto de R formado por todas as matrizes cujas linhas $2, 3, \ldots, n$ são nulas, então J é um ideal à direita de R.

Exemplo 3.2.3. Dado um corpo F, denote por $UT_n(F)$ o anel das matrizes triangulares superiores. O subconjunto I de $UT_n(F)$ formado pelas matrizes estritamente triangulares superiores é um ideal de $UT_n(F)$.

Definição 3.2.4. Um anel R é dito **simples** se $R^2 \neq 0$ e 0 e R são os únicos ideais de R.

Exemplo 3.2.5. Todo anel com divisão D é simples. Além disso, D não tem nenhum ideal lateral além de 0 e D. Isto segue do fato que ideais laterais próprios não podem conter elementos invertíveis.

Considere o anel de matrizes $M_n(S)$, onde S é um anel arbitrário unitário. Seja E_{ij} a matriz cuja entrada (i, j) é 1 e todas as outras são 0. Chamamos E_{ij}, com $1 \leq i, j \leq n$, as **matrizes canônicas**. Por aE_{ij} denotamos a matriz cuja entrada (i, j) é $a \in S$ e todas as outras entradas são 0. Toda matriz em $M_n(S)$ é uma soma de matrizes desta forma. Note que para todo $A = (a_{ij}) \in M_n(S)$ temos

$$E_{ij}AE_{kl} = a_{jk}E_{il} \text{ para todos } 1 \leq i, j, k, l \leq n.$$

Exemplo 3.2.6. Se D é um anel com divisão, então $M_n(D)$ é um anel simples para todo $n \in \mathbb{N}$. De fato, seja I um ideal não nulo de $M_n(D)$. Tome um elemento (a_{ij}) não nulo de I. Escolha j e k tal que $a_{jk} \neq 0$. Da observação anterior obtemos que $a_{jk}E_{il} \in I$ para todo i e l, e logo

$$\left[da_{jk}^{-1}E_{ii}\right] \cdot \left[a_{jk}E_{il}\right] = dE_{il} \in I$$

para todo $d \in D$. Consequentemente, $I = M_n(D)$.

Observação 3.2.7. Ao invés de anéis simples, tomaremos **álgebras simples**, ou seja, álgebras que satisfazem as condições da Definição 3.2.4.

Isto pode soar um pouco ambíguo, já que um ideal de uma álgebra A deve ser, em particular, um subespaço vetorial e a definição fala sobre ideais de um anel, os quais com a relação a operação de soma são meramente subgrupos aditivos. Porém, ambas as interpretações levam à mesma conclusão.

Pergunta: se A é um anel simples, então A é uma álgebra simples?
Sim, pois todo ideal da álgebra A é um ideal do anel A.

Pergunta: se A é uma álgebra simples, então A é um anel simples?
Suponhamos que A não é um anel simples. Neste caso, existe um ideal I do anel A tal que $I \neq 0$ e $I \neq A$. Temos que AI é um ideal da álgebra A. De fato, para $u \in AI$ e $a \in A$, temos

$$u \in AI \Rightarrow u = a_1i_1 + a_2i_2 + \cdots + a_ni_n, \text{ para alguns } a_1, \ldots, a_n \in A \text{ e } i_1, \ldots, i_n \in I$$
$$\Rightarrow au = aa_1i_1 + aa_2i_2 + \cdots + aa_ni_n$$

Como $aa_k \in A$ e $i_k \in I$ para todo k, segue que $au \in AI$. Também,

$$ua = a_1i_1a + a_2i_2a + \cdots + a_ni_na.$$

Como I é ideal do anel A, obtemos $i_ka = i'_k \in I$. Logo, $ua = a_1i'_1 + a_2i'_2 + \cdots + a_ni'_n \in AI$. Além disso, AI é um subespaço vetorial de A. Então, de fato, AI é um ideal da álgebra A.

Mas A é uma álgebra simples. Logo, AI tem que ser 0 ou A. Como $AI \subseteq I \neq A$, a possibilidade que resta é que $AI = 0$. Desta forma, o conjunto $J = \{x \in A : Ax = 0\}$ é não nulo. Como J é um ideal da álgebra A, segue que $J = A$. Ou seja, $A^2 = 0$. Esta possibilidade é excluída na definição, logo isto não é possível.

Concluindo, as nossas duas perguntas levam a seguinte sentença: uma álgebra A é simples como álgebra se, e somente se, é simples como anel.

O próximo objetivo é dar um exemplo de uma álgebra simples de dimensão infinita. Primeiramente algumas notações.

Definição 3.2.8. O **comutador** de elementos a e b de um anel R é o elemento

$$[a,b] := ab - ba.$$

Temos que a e b comutam se, e somente se, $[a,b] = 0$. Também notamos que

$$[a,b] = -[b,a] \ , \ [a,bc] = [a,b]c + b[a,c] \ \text{ e } \ [a,b+c] = [a,b] + [a,c]. \tag{3.4}$$

Exemplo 3.2.9. Seja F um corpo com característica $char(F) = 0$. Lembremos que $End_F(F[\omega])$ denota a álgebra de todos os operadores lineares do espaço vetorial $F[\omega]$. Definimos D, $L \in End_F(F[\omega])$ por

$$D(f(\omega)) = f'(\omega) \quad \text{e} \quad L(f(\omega)) = \omega f(\omega).$$

Aqui, $f'(\omega)$ é a derivada de $f(\omega)$. A subálgebra de $End_F(F[\omega])$ gerada por D e L é chamada **Álgebra de Weyl**, ou **primeira álgebra de Weyl**. Denotamos tal álgebra por $\mathscr{A}_1$.

Temos que

$$[D,L] = I,$$

onde I é o operador identidade. De fato,

$$[D,L](f(\omega)) = DL(f(\omega)) - LD(f(\omega)) = D(L(f(\omega))) - L(D(f(\omega))) =$$
$$D(\omega f(\omega)) - L(f'(\omega)) = f(\omega) + \omega f'(\omega) - \omega f'(\omega) = f(\omega).$$

Esta é a relação básica em $\mathscr{A}_1$. Os seguintes resultados serão deduzidos a partir deste. Em particular, vemos que $\mathscr{A}_1$ é uma álgebra unitária.

A seguir, mostraremos por indução em n que

$$[D, L^n] = nL^{n-1}.$$

Para $n = 1$ temos $[D,L^1] = [D,L] = I = 1L^{1-1}$. Como hipótese de indução, assumimos que $[D,L^{k-1}] = (k-1)L^{k-2}$ e provaremos que a relação é válida para $n = k$:

$$[D,L^k] = [D,L^{k-1}L] \overset{(3.4)}{=} L^{k-1}[D,L] + [D,L^{k-1}]L \overset{HI}{=}$$
$$L^{k-1}I + (k-1)L^{k-2}L = L^{k-1} + (k-1)L^{k-1} = kL^{k-1}.$$

Similarmente, obtemos

$$[D^n, L] = nD^{n-1}.$$

Seja $\mathscr{L}$ a subálgebra de $\mathscr{A}_1$ gerada por I e L. Temos que $\mathscr{L}$ é formada pelos elementos

$$\alpha_0 I + \alpha_1 L + \alpha_2 L^2 + \cdots + \alpha_n L^n, \tag{3.5}$$

com $\alpha_0, \alpha_1, \ldots, \alpha_n \in F$. Além disso, $[D, \mathscr{L}] \subseteq \mathscr{L}$. De fato,

$$[D, \mathscr{L}] = \{[D, T] \mid T \in \mathscr{L}\},$$
$$[D, T] = [D, \alpha_0 I + \alpha_1 L + \alpha_2 L^2 + \cdots + \alpha_n L^n] = [D, \sum_{t=0}^{n} \alpha_t L^t] = \sum_{t=0}^{n} \alpha_t [D, L^t] = \sum_{t=1}^{n} \alpha_t t L^{t-1} =$$
$$\alpha_1 I + \alpha_2 2L + \alpha_3 3L^2 + \cdots + \alpha_n n L^{n-1} \in \mathscr{L}.$$

Em particular,

$$D\mathscr{L} \subseteq \mathscr{L} + \mathscr{L}D$$

De fato, seja $T \in \mathscr{L}$. Acabamos de ver que existe $H \in \mathscr{L}$ tal que $[D, T] = H$. Logo,

$$DT - TD = H \Rightarrow DT = H + TD \in \mathscr{L} + \mathscr{L}D.$$

Afirmação 1.

$$[D^m, \mathscr{L}] \subseteq \mathscr{L} + \mathscr{L}D + \cdots + \mathscr{L}D^{m-1} \text{ para todo } m \in \mathbb{N} \tag{3.6}$$

Demonstração da afirmação. A prova será feita por indução em m. O caso $m = 1$ já foi feito.

Suponhamos o resultado válido para $m = k - 1$, e vamos provar sua validade para k. Dado $T \in \mathscr{L}$, temos

$$[D^k, T] = [DD^{k-1}, T] = D[D^{k-1}, T] + [D, T]D^{k-1} \in D[D^{k-1}, \mathscr{L}] + [D, \mathscr{L}]D^{k-1} \subseteq$$
$$D(\mathscr{L} + \cdots + \mathscr{L}D^{k-2}) + \mathscr{L}D^{k-1} \subseteq D\mathscr{L} + D\mathscr{L}D + \cdots + D\mathscr{L}D^{k-2} + \mathscr{L}D^{k-1} \subseteq$$
$$\mathscr{L} + \mathscr{L}D + (\mathscr{L}D + \mathscr{L}D^2) + \cdots + (\mathscr{L}D^{k-2} + \mathscr{L}D^{k-1}) + \mathscr{L}D^{k-1}.$$

Finalizamos a demonstração da afirmação.

Da afirmação obtemos que o subespaço vetorial gerado por $\{TD^m \mid T \in \mathscr{L}, m \geq 0\}$ é uma subálgebra de $\mathscr{A}_1$ e, portanto, já que este contém L e D, é igual a $\mathscr{A}_1$. Ou seja, mostramos que:

a) *Todo elemento em $\mathscr{A}_1$ pode ser escrito como*

$$T_0 + T_1 D + \cdots + T_n D^n,$$

onde $n \geq 0$ e $T_0, T_1, \ldots, T_n \in \mathscr{L}$.

Afirmamos que os elementos T_i são unicamente determinados. Para provar isso, devemos mostrar que $T_0 + T_1 D + \cdots + T_n D^n = 0$ implica $T_i = 0$ para cada i. Aplicando o operador no polinômio $1 \in F[\omega]$, obtemos

$$0 = 0(1) = (T_0 + T_1 D + \cdots + T_n D^n)(1) = T_0(1).$$

Escrevendo T_0 como em (3.5) obtemos de $0 = T_0(1)$ que

$$\alpha_0 + \alpha_1 \omega + \cdots + \alpha_n \omega^n = 0,$$

isto é, $\alpha_0 = \alpha_1 = \cdots = \alpha_n = 0$ e portanto $T_0 = 0$ é o operador nulo. Similarmente, aplicando o operador $T_1 D + \cdots + T_n D^n = 0$ em $\omega \in F[\omega]$ obtemos $T_1 = 0$. Continuamos com $\omega^2, \omega^3, \ldots$. Note que a suposição $char(F) = 0$ é utilizada ao obter $T_2 = 0, T_3 = 0, \ldots$. Como $\{L^m \mid m \geq 0\}$ é base de $\mathscr{L}$, provamos então que:

b) *O conjunto* $\{L^m D^n \mid m, n \geq 0\}$ *é base de* $\mathscr{A}_1$.

Analogamente, pode ser mostrado que o conjunto $\{D^m L^n \mid m, n \geq 0\}$ também é base de $\mathscr{A}_1$.

Afirmação 2. $\mathscr{A}_1$ é uma álgebra simples.
Prova da afirmação. Seja $\mathscr{I}$ um ideal não nulo de $\mathscr{A}_1$. Tome $S = \sum_{k=0}^{n} T_k D^k \in \mathscr{I}$, $T_k \in \mathscr{L}$, tal que $T_n \neq 0$ e n é minimal. Suponha $n > 0$. Como L comuta com cada T_i, segue que

$$\begin{aligned}[S, L] = SL - LS = \sum_{k=0}^{n} T_k D^K L - L \sum_{k=0}^{n} T_k D^k = \sum_{k=0}^{n} T_k D^k L - L T_k D^k = \sum_{k=0}^{n} T_k D^k L - T_k L D^k \\ = \sum_{k=0}^{n} T_k (D^k L - L D^k) = \sum_{k=0}^{n} T_k [D^k, L] = \sum_{k=1}^{n} k T_k D^{k-1} \end{aligned} \tag{3.7}$$

No entanto, como $nT_n \neq 0$ e $[S, L] \in \mathscr{I}$, isto contradiz a minimalidade de n. Logo, $n = 0$ e $\mathscr{I} \cap \mathscr{L} \neq 0$. Agora tome $T = \sum_{j=0}^{m} \alpha_j L^j \in \mathscr{I} \cap \mathscr{L}$, $\alpha_j \in F$, tal que $\alpha_m \neq 0$ e m é minimal. Suponha $m > 0$. Obtemos

$$[D, T] = \sum_{j=1}^{m} j \alpha_j L^{j-1} \tag{3.8}$$

contradizendo a minimalidade de m. Logo, $m = 0$ e $I \in \mathscr{I}$, acarretando em $\mathscr{I} = \mathscr{A}_1$. A demonstração da afirmação está finalizada.

3.3 ÁLGEBRAS CENTRAIS

Nesta seção veremos os conceitos de centro, álgebra central e alguns exemplos relacionados ao tema. Começamos com o primeiro.

O **centro de uma álgebra** A é o conjunto

$$Z(A) := \{c \in A \mid cx = xc \text{ para todo } x \in A\}.$$

O centro de uma álgebra unitária trivialmente contém os múltiplos escalares da unidade. Em muitos exemplos importantes de álgebras, estes também são os únicos elementos centrais.

Definição 3.3.1. Uma F-álgebra unitária A com unidade 1_A é dita ser uma **álgebra central** se

$$Z(A) = \{\lambda 1_A \mid \lambda \in F\}.$$

A menos que seja dito o contrário, todas as álgebras consideradas serão sobre o corpo F e, neste caso, diremos simplesmente "álgebra". Se A é uma álgebra unitária, então identificamos F com $F \cdot 1_A$ e escrevemos λ ao invés de $\lambda 1_A$ para todo escalar $\lambda \in F$. Assim,

$$A \text{ é } F\text{-álgebra central se, e somente se, } Z(A) = F.$$

Lema 3.3.2. *Se A é uma álgebra unitária, então $Z(M_n(A)) = Z(A)I_n$.*

Demonstração. No que diz respeito a notação, $Z(A)I_n = \{cI_n \mid c \in Z(A)\}$, onde I_n é a matriz identidade. A inclusão $Z(M_n(A)) \supseteq Z(A)I_n$ é direta.

Referente a inclusão $(\subseteq)$, seja $C \in Z(M_n(A))$, onde $C = (c_{ij})$. Como $CE_{lk} = E_{lk}C$ para todo $k \neq l$, temos

$$\left(\sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}E_{ij}\right)E_{lk} = E_{lk}\left(\sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}E_{ij}\right).$$

De $E_{ij}E_{lk} = \delta_{jl}E_{ik}$, obtemos a premissa e implicações abaixo:

$\sum_{i=1}^{n} c_{il}E_{ik} = \sum_{j=1}^{n} c_{kj}E_{lj}$

$\Rightarrow c_{1l} = 0, c_{2l} = 0, \ldots, c_{ll} = c_{kk}, \ldots, c_{nl} = 0$ e também $c_{11} = c_{22} = \cdots = c_{nn} = \lambda$

$\Rightarrow C = \lambda I_n \Rightarrow C(aI_n) = (aI_n)C$ para todo $a \in A$

$\Rightarrow (\lambda I_n)(aI_n) = (aI_n)(\lambda I_n)$ para todo $a \in A$

$\Rightarrow \lambda a = a\lambda$ para todo $a \in A \Rightarrow \lambda \in Z(A)$.

Ou seja, $C \in Z(A)I_n$ como era o desejado. □

Corolário 3.3.3. *Seja A uma álgebra unitária e seja $n \in \mathbb{N}$. Então A é central se, e somente se, $M_n(A)$ é central.*

Exemplo 3.3.4. Como uma aplicação do Lema 3.3.3, temos que $M_n(F)$ é uma F-álgebra central.

Exemplo 3.3.5. $\mathbb{H}$ é uma $\mathbb{R}$-álgebra central.

De fato, seja $u \in Z(\mathbb{H})$, $u = a + bi + cj + dk$ com $a, b, c, d \in \mathbb{R}$. Então, valem as seguintes igualdades:

i) $ui = iu$,

ii) $uj = ju$,

iii) $uk = ku$.

Referente a cada item temos as seguintes informações:

i) $(a+bi+cj+dk)i = i(a+bi+cj+dk) \Rightarrow ai + bi^2 + cji + dki = ia + ibi + icj + idk$

$\Rightarrow ai + bi^2 + cji + dki = ai + bi^2 + cij + dik \Rightarrow ai + bi^2 + cji + dki - ai - bi^2 - cij - dik = 0$

$\Rightarrow ai - b - ck + dj - ai + b - ck + dj = 0 \Rightarrow 2dj - 2ck = 0 \Rightarrow dj - ck = 0$

ii) $(a+bi+cj+dk)j = j(a+bi+cj+dk) \Rightarrow aj + bij + cj^2 + dkj = ja + jbi + jcj + jdk$

$\Rightarrow aj + bij + cj^2 + dkj = aj + bji + cj^2 + djk \Rightarrow aj + bij + cj^2 + dkj - aj - bji - cj^2 - djk = 0$

$\Rightarrow aj + bk - c - di - aj + bk + c - di = 0 \Rightarrow 2bk - 2di = 0 \Rightarrow bk - di = 0$

iii) $(a+bi+cj+dk)k = k(a+bi+cj+dk) \Rightarrow ak + bik + cjk + dk^2 = ka + kbi + kcj + kdk$

$\Rightarrow ak + bik + cjk + dk^2 = ak + bik + cjk + dk^2 \Rightarrow ak + bik + cjk + dk^2 - ak - bki - ckj - dk^2 = 0$

$\Rightarrow ak - bj + ci - d - ak - bj + ci + d = 0 \Rightarrow 2ci - 2bj = 0 \Rightarrow ci - bj = 0$

Obtemos que $dj - ck = 0$, $bk - di = 0$ e $ci - bj = 0$. Da definição de $\mathbb{H}$, temos que i, j, k são linearmente independentes. Portanto, $b = c = d = 0$. Logo, um elemento $u \in Z(\mathbb{H})$ é da forma $u = a = a1_{\mathbb{H}}$.

Exemplo 3.3.6. $\mathbb{C}$ é central como $\mathbb{C}$-álgebra, mas não como $\mathbb{R}$-álgebra. Portanto, o Teorema 3.1.5 implica no próximo resultado.

Corolário 3.3.7. *Uma $\mathbb{R}$-álgebra central de dimensão finita é isomorfa a $\mathbb{R}$ ou $\mathbb{H}$.*

Exemplo 3.3.8. A álgebra de Weyl $\mathscr{A}_1$ é central. De fato, tome $S = \sum_{k=0}^{n} T_k D^k \in Z(\mathscr{A}_1)$, onde $T_0, T_1, \ldots, T_n \in \mathscr{L}$. Como $[S, L] = 0$, segue de (3.7) que $T_i = 0$ para $i \geq 1$. Então, $S = \sum_{j=0}^{m} \alpha_j L^j$. Utilizando o fato de que $[D, S] = 0$, segue de (3.8) que $\alpha_i = 0$ para $i \geq 1$. Logo, $S = \alpha_0 \in F$.

Exemplo 3.3.9. Se A é um anel unitário simples, então seu centro é um corpo. De fato, se c é um elemento central não nulo, então cA deve ser, como um ideal não nulo de A, igual a A. Isto implica que c é invertível. Se multiplicarmos $cx = xc$ pela direita e pela esquerda por c^{-1} vemos que c^{-1} é um elemento central. Consequentemente, *todo anel simples unitário pode ser visto como uma álgebra sobre seu centro*. Podemos definir a multiplicação por escalar simplesmente como a multiplicação ordinária de um elemento central por um elemento arbitrário de A, e todos os axiomas de álgebra são prontamente válidos.

3.4 ÁLGEBRA COM MULTIPLICAÇÃO

Seja A uma álgebra. Para todos $a, b \in A$ definimos as funções $L_a, R_b : A \to A$, chamadas **função multiplicativa à esquerda** e **função multiplicativa à direita**, como

$$L_a(x) := ax \quad \text{e} \quad R_b(x) := xb.$$

Estas funções podem ser consideradas elementos de $End_F(A)$.

Notemos que para todos $a, b \in A$ e $\lambda, \mu \in F$ temos

$$L_{ab} = L_a L_b,\ R_{ab} = R_b R_a,$$
$$L_a R_b = R_b L_a,$$
$$L_{\lambda a+\mu b} = \lambda L_a + \mu L_b,\ R_{\lambda a+\mu b} = \lambda R_a + \mu R_b.$$

Assim, concluímos que

$$M(A) := \{L_{a_1} R_{b_1} + \cdots + L_{a_n} R_{b_n} \mid a_i, b_i \in A, n \in \mathbb{N}\}$$

é uma subálgebra de $End_F(A)$.

Definição 3.4.1. A álgebra $M(A)$ é chamada **álgebra com multiplicação de** A.

Se A é unitária, então $L_a = L_a R_1$ e $R_b = L_1 R_b$ pertencem a $M(A)$ e, neste caso, $M(A)$ é a subálgebra de $End_F(A)$ gerada por todos as funções multiplicativas à direita e à esquerda. Também notamos que $a = L_a(1) = R_a(1)$, e então as condições $a = 0$, $L_a = 0$ e $R_a = 0$ são equivalentes se A é unitária.

Observação 3.4.2. Tome $f \in M(A)$. Então existem $a_i, b_i \in A$ tal que $f = \sum_{i=1}^{n} L_{a_i} R_{b_i}$, isto é,

$$f(x) = \sum_{i=1}^{n} a_i x b_i,\ x \in A.$$

Estes elementos não são únicos, f pode ser representada como uma soma de operadores da forma $L_a R_b$ de várias formas. Se $f \neq 0$, então a_i, b_i podem ser escolhidos de forma que o conjunto de todos os a_i's e o conjunto de todos os b_i's são linearmente independentes. Por exemplo, isto é alcançado se requeremos que n seja minimal. De fato, se sob esta suposição, um dos elementos, digamos b_n fosse uma combinação linear dos outros, $b_n = \sum_{i=1}^{n-1} \lambda_i b_i$, então f seria igual a

$$\sum_{i=1}^{n-1} L_{a_i+\lambda_i a_n} R_{b_i},$$

contradizendo a minimalidade de n. Além disso, se $\{u_i \mid i \in I\}$ é uma base de A, então podemos expressar cada R_b como uma combinação linear de R_{u_i}, de onde vemos que todo $f \in M(A)$ é uma soma (finita) de operadores da forma $L_{a_i} R_{u_i}$. Similarmente, f pode ser escrito como uma soma de operadores da forma $L_{u_i} R_{b_i}$, e também como uma combinação linear dos operadores $L_{u_i} R_{u_i}$.

O fato de que os elementos de $M(A)$ podem ser expressos de maneiras diferentes através das funções multiplicativas à direita e à esquerda pode causar confusão. O seguinte lema mostra que em álgebras centrais este problema é controlável.

Lema 3.4.3. *Seja A uma álgebra central simples, e sejam a_i, $b_i \in A$ tal que $\sum_{i=1}^{n} L_{a_i} R_{b_i} = 0$. Se os a_i's são linearmente independentes, então cada $b_i = 0$. Similarmente, se os b_i's são linearmente independentes, então cada $a_i = 0$.*

Demonstração. As duas afirmações do lema possuem demonstrações análogas, então consideremos apenas o caso onde os a_i's são linearmente independentes. Supomos $b_n \neq 0$. Como A é simples, o ideal gerado por b_n é igual a A. Ou seja, $\sum_{j=1}^{m} w_j b_n z_j = 1$ para alguns w_j, $z_j \in A$. Logo,

$$0 = \sum_{j=1}^{m} R_{z_j} \left(\sum_{i=1}^{n} L_{a_i} R_{b_i} \right) R_{w_j} = \sum_{i=1}^{n} L_{a_i} \left(\sum_{j=1}^{m} R_{w_j b_i z_j} \right) = \sum_{i=1}^{n} L_{a_i} R_{c_i}$$

onde $c_i = \sum_{j=1}^{m} w_j b_i z_j$; logo $c_n = 1$. Isto implica que $n > 1$. Podemos assumir que n é o menor natural para o qual o lema não vale. Como

$$0 = \left(\sum_{i=1}^{n} L_{a_i} R_{c_i} \right) R_x - R_x \left(\sum_{i=1}^{n} L_{a_i} R_{c_i} \right) = \sum_{i=1}^{n-1} L_{a_i} R_{x c_i - c_i x}$$

para todo $x \in A$, segue que $xc_i - c_i x = 0$. Consequentemente, $c_i \in F$. Mas então

$$0 = \sum_{i=1}^{n} L_{a_i} R_{c_i} = L_{c_1 a_1 + \cdots + c_n a_n}$$

o que contradiz a independência dos a_i's. □

No seguinte lema, consideremos a situação de dimensão finita. Lembremos que se $[A : F] = d$, então $[End_F(A) : F] = d^2$.

Lema 3.4.4. *Se A é uma álgebra central simples de dimensão finita, então $M(A) = End_F(A)$.*

Demonstração. Seja $\{u_1, ..., u_d\}$ uma base de A. O Lema 3.4.3 implica que os operadores $L_{u_i} R_{u_j}$, $1 \leq i, j \leq d$ são linearmente independentes. De fato, considere

$$\sum_{i=1}^{d} \sum_{j=1}^{d} \lambda_{ij} L_{u_i} R_{u_j} = 0, \ \lambda_{ij} \in F.$$

Denotando $b_i = \sum_{j=1}^{d} \lambda_{ij} u_j$, obtemos $\sum_{i=1}^{d} L_{u_i} R_{b_i} = 0$ e, pelo Lema 3.4.3, $b_i = 0$ para todo i. Logo, $\sum_{j=1}^{d} \lambda_{ij} u_j = 0$ implica em $\lambda_{ij} = 0$ para todos i, j. Assim,

$$d^2 \leq [M(A) : F] \leq [End_F(A) : F] = d^2$$

e $M(A) = End_F(A)$. □

3.5 AUTOMORFISMOS DE ÁLGEBRAS CENTRAIS SIMPLES

Nesta seção, definiremos o conceito de automorfismos internos e externos de álgebras simples expondo alguns exemplos, a fim de demonstrar o Teorema de Skolem-Noether.

Definição 3.5.1. Um automorfismo φ de um anel unitário R é dito ser um **automorfismo interno** se existe um elemento invertível $a \in R$ tal que

$$\varphi(x) = axa^{-1}$$

para todo $x \in R$. Um automorfismo que não é interno é chamado **externo**.

Exemplo 3.5.2. Se R é um anel comutativo, então o único automorfismo interno de R é a função identidade.

Exemplo 3.5.3. A conjugação $z \mapsto \overline{z}$ é um automorfismo externo de $\mathbb{C}$, pois $\mathbb{C}$ é um anel comutativo. Também observamos que é um elemento de $End_{\mathbb{R}}(\mathbb{C})$, mas não de $M(\mathbb{C})$. De fato, seja $\varphi \in M(\mathbb{C})$. Assim, existem $a_1, ..., a_n, b_1, ..., b_n \in \mathbb{C}$ tal que

$$\varphi = \sum_{i=1}^{n} L_{a_i} R_{b_i}$$

$$\Rightarrow \varphi(x) = \sum_{i=1}^{n} a_i x b_i = \sum_{i=1}^{n} a_i b_i x = \left(\sum_{i=1}^{n} a_i b_i \right) x$$

$$\Rightarrow \varphi = L_a \text{ onde } a = \sum_{i=1}^{n} a_i b_i.$$

Suponhamos que φ seja a conjugação. Temos que φ não está em $M(\mathbb{C})$ pois, caso contrário, existiria $a \in \mathbb{C}$ tal que $\varphi = L_a$.

$$\begin{gathered} \Rightarrow \varphi(x) = \bar{x} = ax \text{ para todo } x \in \mathbb{C} \\ \Rightarrow \varphi(1) = \bar{1} = 1 = a \\ \Rightarrow \varphi(x) = \bar{x} = x, \end{gathered}$$

o que é um absurdo. Logo, a suposição de que A é central não pode ser omitida no Lema 3.4.4.

Exemplo 3.5.4. Para todo $\alpha \in F \setminus \{0\}$, a função

$$\varphi : F[\omega] \to F[\omega], f(\omega) \mapsto f(\omega + \alpha)$$

é um automorfismo externo de $F[\omega]$.

Exemplo 3.5.5. Seja $S \neq 0$ um anel com unidade e seja $R = S \times S$ o produto direto de duas cópias de S. Então a função

$$\tau : S \times S \to S \times S \text{ dada por } \tau(s,t) = (t,s)$$

é um automorfismo externo de R. De fato, suponhamos que exista $(s_1, s_2) \in S \times S$ tal que

$$\tau(x, y) = (s_1, s_2)(x, y)(s_1, s_2)^{-1}.$$

Neste caso, temos as implicações

$$\Rightarrow (y, x) = (s_1, s_2)(x, y)(s_1^{-1}, s_2^{-1})$$

$$\Rightarrow (y, x) = (s_1 x s_1^{-1}, s_2 x s_2^{-1})$$

$$\Rightarrow y = s_1 x s_1^{-1} \text{ e } x = s_2 y s_2^{-1}$$

para todos $x, y \in S$. Em particular, se $x = 1$ e $y = 0$, então

$$0 = s_1 1 s_1^{-1} = 1$$

o que é um absurdo.

Em vista destes exemplos, segue o teorema:

Teorema 3.5.6 (Skolem-Noether)**.** *Todo automorfismo de uma F-álgebra A central simples com dimensão finita é interno.*

Demonstração. Seja φ um automorfismo de A. O Lema 3.4.4 implica que $\varphi = \sum_{i=1}^{n} L_{a_i} R_{b_i}$ para alguns $a_i, b_i \in A$. Podemos assumir $a_i \neq 0$ e que os b_i's são linearmente independentes.

Afirmação. $L_{\varphi(x)}\varphi = \varphi L_x$ para todo $x \in A$.
Demonstração da afirmação. Para todo $y \in A$ temos

$$(L_{\varphi(x)} \circ \varphi)(y) = L_{\varphi(x)}(\varphi(y)) = \varphi(x)\varphi(y) = \varphi(xy) = \varphi(L_x(y)) = (\varphi \circ L_x)(y)$$

como era o desejado.

Temos as seguintes implicações:

$$L_{\varphi(x)} \circ \varphi = L_{\varphi(x)} \circ \sum_{i=1}^{n} L_{a_i} R_{b_i} = \left(\sum_{i=1}^{n} L_{a_i} R_{b_i} \right) \circ L_x$$

$$\Rightarrow \sum_{i=1}^{n} L_{\varphi(x)} L_{a_i} R_{b_i} = \sum_{i=1}^{n} L_{a_i} R_{b_i} L_x$$

$$\Rightarrow \sum_{i=1}^{n} \left(L_{\varphi(x)} L_{a_i} R_{b_i} - L_{a_i} L_x R_{b_i} \right) = 0$$

$$\Rightarrow \sum_{i=1}^{n} \left(L_{\varphi(x)} L_{a_i} - L_{a_i} L_x \right) R_{b_i} = 0$$

$$\Rightarrow \sum_{i=1}^{n} \left(L_{\varphi(x)a_i} - L_{a_i x} \right) R_{b_i} = 0$$

$$\Rightarrow \sum_{i=1}^{n} \left(L_{\varphi(x)a_i - a_i x} \right) R_{b_i} = 0$$

Como os $b_i's$ são linearmente independentes, o Lema 3.4.3 implica em particular que

$$\varphi(x)a_1 - a_1 x = 0 \text{ para todo } x \in A. \tag{3.9}$$

Resta mostrar que a_1 é invertível, pois daí

$$\varphi(x)a_1 = a_1 x \Rightarrow \varphi(x)a_1 a_1^{-1} = a_1 x a_1^{-1} \Rightarrow \varphi(x) = a_1 x a_1^{-1},$$

e obteremos o resultado desejado.

Seja I o ideal de A gerado por a_1. Temos que todo elemento em I é da forma $\sum_{j=1}^{m} w_j a_1 z_j$, para alguns $w_j, z_j \in A$. Como A é álgebra simples, $I = A$. Logo, o elemento 1 pode ser expresso como

$$1 = \sum_{j=1}^{m} w_j a_1 z_j.$$

De (3.9), temos

$$a_1 z_j = \varphi(z_j)a_1$$

Assim,

$$1 = \sum_{j=1}^{m} w_j a_1 z_j = \sum_{j=1}^{m} w_j \varphi(z_j) a_1 = \left[\sum_{j=1}^{m} w_j \varphi(z_j) \right] a_1$$

e a_1 tem um inverso à esquerda. De (3.9), temos

$$a_1 \varphi^{-1}(w_j) = w_j a_1$$

Assim,

$$1 = \sum_{j=1}^{m} w_j a_1 z_j = \sum_{j=1}^{m} a_1 \varphi^{-1}(w_j) z_j = a_1 \left[\sum_{j=1}^{m} \varphi^{-1}(w_j) z_j \right]$$

e a_1 tem um inverso à direita. Como a_1 tem inverso à direita e à esquerda, então a_1 é invertível e segue o resultado. □

3.6 SUBCORPOS MAXIMAIS

Esta seção se dedica a demonstrar algumas propriedades sobre a dimensão de álgebras unitárias de dimensão finita.

Se uma subálgebra K de uma F-álgebra unitária A é um corpo e $K \supseteq F$ (ou seja, K contém a unidade de A), então a chamamos de **subcorpo** de A. Neste caso, podemos considerar

A como um espaço vetorial sobre K. De fato, podemos considerar a multiplicação de elementos de K por elementos de A como um produto escalar $K \times A \to A$. Os axiomas de espaço vetorial são prontamente cumpridos. Observamos que isto ainda não implica que A também é uma K-álgebra, sendo isto uma verdade apenas se K estiver contido no centro $Z(A)$ de A (veja Exemplo 3.3.9).

Observação 3.6.1. Se K é um subcorpo de uma F-álgebra unitária de dimensão finita A, então temos

$$[A : F] = [A : K][K : F].$$

Esta fórmula é bem conhecida no caso em que A é uma extensão de corpos de K. A mesma prova funciona no caso geral. De fato, se $\{k_i \mid i = 1, \dots, m\}$ é uma base de K sobre F, e $\{a_j \mid j = 1, \dots, n\}$ é base de A sobre K, então $\{k_i a_j \mid i = 1, \dots, m,\ j = 1, \dots, n\}$ é uma base de A sobre F.

Definição 3.6.2. Um subcorpo que não está propriamente contido em um subcorpo maior de A é chamado **subcorpo maximal** de A.

Exemplo 3.6.3. Cada $\mathbb{R} \oplus \mathbb{R}i$, $\mathbb{R} \oplus \mathbb{R}j$ e $\mathbb{R} \oplus \mathbb{R}k$ é um subcorpo maximal de $\mathbb{H}$, de dimensão 2 e isomorfo a $\mathbb{C}$. Com algum abuso de notação, podemos então considerar $\mathbb{H}$ como um espaço vetorial complexo (mas não como uma álgebra complexa).

Se K é um subcorpo de A, então $R_u \in End_K(A)$ para todo $u \in A$. De fato, $R_u(kx) = kxu = kR_u(x)$ para todos $k \in K$, $x \in A$. Também observamos que dado $f \in End_K(A)$, seu escalar múltiplo kf, onde $k \in K$, pode ser interpretado como o operador $L_k f$. Esta observação é importante para a demonstração seguinte.

Teorema 3.6.4. *Seja D uma F-álgebra central com divisão de dimensão finita. Se K é um subcorpo maximal de D, então*

$$[D : F] = [K : F]^2.$$

Demonstração. Tomemos uma base $\{u_1, \dots, u_d\}$ da F-álgebra D. Afirmamos que $\{R_{u_1}, \dots, R_{u_d}\}$ é base da K-álgebra $End_K(D)$.

Primeiramente, vemos que $\{R_{u_1}, ..., R_{u_d}\}$ é um conjunto linearmente independente. De fato, se

$$\sum_{i=1}^{d} L_{a_i} R_{u_i} = 0,$$

como os u_i's são linearmente independentes, o Lema 3.4.3 nos diz que cada $a_i = 0$. Logo, resta mostrar que gera $End_K(D)$. Seja $f \in End_k(D)$. Em particular, $f \in End_F(D)$, então segue do Lema 3.4.4 e da Observação 3.4.2 que $f = \sum_{i=1}^{d} L_{a_i} R_{u_i}$ para algum $a_i \in D$. Como f é K-linear, isto é, $fL_k = L_k f$ é válido para todo $k \in K$, temos

$$\sum_{i=1}^{d} L_{a_i k - k a_i} R_{u_i} = 0.$$

Do Lema 3.4.3 temos que $a_i k - k a_i = 0$ para todo i e todo $k \in K$. Isto implica que $a_i \in K$, pois caso contrário a subálgebra gerada por a_i e K iria ser um corpo maior do que K. Logo, f é uma combinação K-linear dos R_{u_i}'s, provando nossa afirmação.

Da afirmação acima concluímos que

$$[D : F] = d = [End_K(D) : K] = [D : K]^2.$$

Por outro lado,

$$[D : F] = [D : K][K : F]$$

pela Observação 3.6.1, e assim

$$[D : K]^2 = [D : K][K : F] \Rightarrow [D : K] = [K : F] \Rightarrow [D : F] = [K : F]^2$$

Finalizamos a demonstração do teorema. □

Corolário 3.6.5. *A dimensão de uma álgebra central com divisão de dimensão finita é um quadrado perfeito.*

Demonstração. Uma álgebra central com divisão de dimensão finita certamente contém subcorpos maximais. De fato, estes são exatamente os subcorpos de dimensão maximal. A conclusão segue do Teorema 3.6.4. □

3.7 O TEOREMA DE WEDDERBURN SOBRE ANÉIS DE DIVISÃO FINITA

Nesta última seção, demonstraremos o Teorema de Wedderburn, que diz que todo anel com divisão finito é comutativo.

Corpos finitos existem e sua estrutura é bem conhecida. Pergunta: existem anéis com divisão finitos que são não comutativos? O conjunto de elementos não nulos de tal anel formaria um grupo finito não abeliano com o produto. Como grupos finitos são um dos objetos algébricos mais estudados, parece natural envolver técnicas da teoria de grupos para responder a pergunta acima.

Precisaremos da *equação de classes* da teoria elementar de grupos. Vamos relembrá-la e esboçar sua demonstração. Seja G um grupo finito com centro $\mathfrak{Z}(G)$. Para todo $a \in G$ seja

$$\mathfrak{C}(a) := \{g \in G \mid ag = ga\}.$$

Isto é um subgrupo de G. O conjunto $\{xax^{-1} \mid x \in G\}$ de todos os conjugados de a tem a mesma cardinalidade do conjunto de todas as classes laterais de $\mathfrak{C}(a)$ em G. De fato, $xax^{-1} \mapsto x\mathfrak{C}(a)$ é uma bijeção bem definida. Conjugação é uma relação de equivalência em G. Particionando G em suas classes de equivalência disjuntas (chamadas classes de conjugação) e utilizando o teorema de Lagrange que nos diz que o número de classes laterais é $\dfrac{|G|}{|\mathfrak{C}(a)|}$, obtemos a fórmula desejada

$$|G| = |\mathfrak{Z}(G)| + \sum \frac{|G|}{|\mathfrak{C}(a)|}, \tag{3.10}$$

onde a soma é tomada sobre representantes das classes de conjugação não triviais.

Podemos agora provar que a resposta da pergunta feita no primeiro parágrafo é "não". Isto foi estabelecido por J. H. M. Wedderburn em 1905.

Teorema 3.7.1 (Wedderburn)**.** *Todo anel com divisão finito é comutativo.*

Demonstração. Supomos que isto não é verdade. Então existe um anel D com divisão finito não comutativo de cardinalidade minimal; todos seus subanéis com divisão próprios são então comutativos. Podemos considerar D uma álgebra central com divisão sobre seu centro F.

Para todo $a \in D$ definimos

$$C(a) := \{x \in D : ax = xa\}.$$

Temos que $C(a)$ é um subanel com divisão, e logo um subcorpo de D se $a \notin F$. Já que os elementos em qualquer subcorpo que contém a comutam com a, $C(a)$ é na verdade um subcorpo maximal de D.

Seja $q = |F|$. Note que um espaço vetorial m-dimensional sobre F tem q^m elementos. De acordo com o Teorema 3.6.4, como $[D : F] = [C(a) : F]^2$, existe $d \geq 2$ tal que $|D| = q^{d^2}$ e $|C(a)| = q^d$ para todo $a \in D \setminus F$. Agora aplicamos a equação (3.10) para $G := D^* = D \setminus \{0\}$. Como $\mathfrak{Z}(G) = F \setminus \{0\}$ e $\mathfrak{C}(a) = C(a) \setminus \{0\}$ segue que existe $s \in \mathbb{N}$ tal que

$$q^{d^2} - 1 = q - 1 + s\frac{q^{d^2} - 1}{q^d - 1}.$$

Já que $q^{d^2} - 1$ é um múltiplo de $\dfrac{q^{d^2} - 1}{q^d - 1}$, isto segue à contradição que

$$\frac{q^{d^2} - 1}{q^d - 1} = \frac{(q^d)^d - 1}{q^d - 1} = 1 + q^d + \cdots + q^{d(d-2)} + q^{d(d-1)}$$

é um divisor de $q - 1$.

Finalizamos a demonstração do teorema. □

4 ESTRUTURA DE ÁLGEBRAS COM DIMENSÃO FINITA

Este capítulo tem por objetivo definir mais estruturas de anéis e álgebras, que serão utilizadas a fim de demonstrar os Teoremas de Estrutura de Wedderburn, os quais descrevem a estrutura de álgebras de dimensão finita.

4.1 IDEAIS NILPOTENTES

Nesta seção, trataremos de anéis que contêm ideais próprios não triviais cuja alguma potência se anula. Para que fique mais claro, segue abaixo algumas notações e posterior definição.

Sejam R um anel, I e J dois ideais de R, e $a \in R$. Denotamos por IJ o ideal de R formado por todas as somas de elementos ij tal que $i \in I$ e $j \in J$. Note que um elemento qualquer em IJ é da forma $i_1j_1 + i_2j_2 + \cdots + i_mj_m$ tal que $i_1, i_2, \ldots, i_m \in I$ e $j_1, j_2, \ldots, j_m \in J$. De maneira indutiva, definimos a potência I^n como sendo o produto dos dois ideais I e I^{n-1}. Também definimos o ideal RaR como sendo o conjunto formado pelas somas de todos os elementos da forma r_1ar_2 tal que $r_1, r_2 \in R$.

Definição 4.1.1. Sejam R um anel, I um ideal de R e $a \in R$.

(a) Dizemos que I é um **ideal nilpotente** se existe $n \in \mathbb{N}$ tal que $I^n = 0$.

(b) Dizemos que a é um **elemento nilpotente** se existe $n \in \mathbb{N}$ tal que $a^n = 0$.

(c) Dizemos que I é um **ideal nil** se todos os elementos em I são nilpotentes.

Na definição acima, vale ressaltar que a condição $I^n = 0$ é equivalente a

$$u_1u_2\cdots u_n = 0,$$

para todos $u_1, u_2, ..., u_n \in I$.

Note que todo ideal nilpotente é um ideal nil. De fato, seja I um ideal nilpotente de um anel R. Isto significa que existe $n \in \mathbb{N}$ tal que

$$a_1a_2\cdots a_n = 0, \text{ para todos } a_1, ..., a_n \in R.$$

Em particular,

$$a^n = aa\cdots a = 0, \text{ para todo } a \in R,$$

e portanto I é nil. A recíproca desta sentença nem sempre é verdadeira, como veremos no Exemplo 4.1.5.

Um exemplo trivial de um ideal nilpotente é $I = 0$. Por outro lado, um caso extremo é quando o próprio anel R é nilpotente.

Exemplo 4.1.2. Tomando qualquer grupo aditivo R e equipando-o com o produto trivial

$$xy = 0 \text{ para todos } x, y \in R,$$

temos $R^2 = 0$. Portanto, R é um ideal nilpotente.

Exemplo 4.1.3. Um elemento nilpotente no centro $Z(R)$ do anel R gera um ideal nilpotente. De fato, seja $a \in Z(R)$ e $\langle a \rangle$ o ideal gerado por a. Note que

$$\langle a \rangle = \mathbb{Z}a + Ra + aR + RaR = \mathbb{Z}a + Ra = \{za + ra \mid z \in \mathbb{Z} \text{ e } r \in R\}.$$

Como a é nilpotente, existe $n \in \mathbb{N}$ tal que $a^n = 0$. Afirmamos que $\langle a \rangle^n = 0$. De fato, dados $z_1, ..., z_n \in \mathbb{Z}$ e $r_1, ..., r_n \in R$,

$$(z_1a + r_1a)(z_2a + r_2a)\cdots(z_na + r_na) = (z_1z_2\cdots z_n)a^n + ra^n = 0$$

para algum $r \in R$.

Exemplo 4.1.4. Seja $A = T_n(F)$ a álgebra de todas as matrizes triangulares superiores $n \times n$ sobre um corpo F. Seja N o conjunto de todas as matrizes estritamente triangulares superiores. Então N é um ideal de A tal que $N^n = 0$ e $N^{n-1} \neq 0$.

De fato, sejam $A_1, A_2, ..., A_n \in N$. Como cada A_i pode ser escrito como combinação linear das matrizes canônicas E_{ij}, com $1 \leq i < j \leq n$, para provar que

$$A_1A_2\cdots A_n = 0,$$

basta provar que

$$E_{i_1j_1}E_{i_2j_2}\cdots E_{i_nj_n} = 0$$

para todos $i_1 < j_1, ..., i_n < j_n$. Suponha que $E_{i_1j_1}E_{i_2j_2}\cdots E_{i_nj_n} \neq 0$. Então

$$i_1 < j_1 = i_2 < j_2 = i_3 < j_3 = \cdots = i_n < j_n,$$

ou seja, $i_1, j_1, j_2, ..., j_n$ são $n + 1$ elementos distintos em $\{1, ..., n\}$, o que é um absurdo.

Agora,

$$E_{12}E_{23}E_{34}\cdots E_{(n-1)n} = E_{1n} \neq 0,$$

e portanto $N^{n-1} \neq 0$.

Exemplo 4.1.5. Seja A o conjunto de todas as matrizes infinitas, de tamanho $\mathbb{N} \times \mathbb{N}$, sobre F que são triangulares superiores e têm apenas um número finito de entradas não nulas. Note que A é

uma álgebra sob as operações usuais de matrizes. Seja I o conjunto de todas as matrizes em A que são estritamente triangulares superiores. Então I é um ideal nil de A que não é nilpotente.

Provaremos a afirmação acima. Todo elemento de A tem a forma

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} & 0 & 0 & \cdots \\ 0 & a_{22} & a_{23} & \cdots & a_{2n} & 0 & 0 & \cdots \\ 0 & 0 & a_{33} & \cdots & a_{3n} & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{nn} & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

para algum $n \in \mathbb{N}$. Note que podemos "identificar" tal matriz com uma matriz em $T_n(F)$. Se $X \in I$, então para algum $n \in \mathbb{N}$ temos

$$X = \begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} & 0 & 0 & \cdots \\ 0 & 0 & a_{23} & \cdots & a_{2n} & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots & a_{3n} & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

e portanto $X^n = 0$. Logo, I é nil. No entanto, I não é nilpotente. De fato, assuma que exista $n = k - 1 \in \mathbb{N}$ tal que $I^n = 0$. Seja $B = (b_{ij})_{ij}$ a matriz em I tal que

$$b_{12} = b_{23} = b_{34} = \cdots = b_{nk} = 1$$

e demais entradas iguais a 0. Então $B^n \neq 0$, o que é um absurdo.

Observação 4.1.6. Ideais unilaterais nilpotentes são definidos da mesma maneira que ideais (bilaterais) nilpotentes.

Se L é um ideal à esquerda nilpotente de R, então L está contido em um ideal nilpotente de R. De fato, $L + LR$ é ideal que contém L, e se $L^n = 0$, então $(L + LR)^n = 0$.

Similarmente, todo ideal à direita nilpotente está contido em um ideal nilpotente.

Esta observação mostra que um anel que contém um ideal unilateral nilpotente não nulo também contém um ideal bilateral nilpotente não nulo. O matemático austríaco Gottfried Köthe conjecturou em 1930 que o mesmo vale para ideais nil. O seguinte é conhecido como **Problema de Köthe**:

Problema 4.1.7. (Köthe): Se um anel R contém um ideal unilateral nil não nulo, então R também contém um ideal bilateral nil não nulo?

A resposta é afirmativa em várias situações, porém o problema segue em aberto.

Lema 4.1.8. *A soma de dois ideais nilpotentes é um ideal nilpotente.*

Demonstração. Sejam I e J ideais tais que $I^n = 0$ e $J^m = 0$.
Afirmação. $(I+J)^{n+m} = 0$.

Para a demonstração, devemos provar que o produto de $n+m$ elementos da forma $u+v$, com $u \in I$ e $v \in J$, é 0. Por meio da distributiva, tal produto pode ser escrito como uma soma de produtos

$$w = w_1 w_2 \cdots w_{n+m}$$

onde cada $w_i \in I \cup J$. Se ao menos n destes $w_i's$ estão em I, então $w = 0$ já que $I^n = 0$. Se o número de $w_i's$ pertencentes a I é menor que n, então ao menos m deles está em J, e logo $w = 0$ já que $J^m = 0$. □

Utilizaremos a terminologia **ideal nilpotente maximal** para nos referir a um ideal nilpotente que não está propriamente contido em um ideal nilpotente maior.

Lema 4.1.9. *Se um anel R tem um ideal nilpotente maximal N, então N contém todos os ideais nilpotentes de R.*

Demonstração. Se I é um ideal nilpotente, então $I+N$ é também um ideal nilpotente pelo Lema 4.1.8. Como N é maximal, devemos ter $I+N = N$, e portanto $I \subseteq N$. □

Assim, um ideal nilpotente maximal, se ele existe, é único e igual à soma de todos os ideais nilpotentes. No entanto, nem todo anel possui um ideal nilpotente maximal. Isso significa que a soma de todos os ideais nilpotentes de um anel nem sempre é um ideal nilpotente (no entanto, é nil, já que cada um de seus elementos está contido em um ideal nilpotente pelo Lema 4.1.8).

Exemplo 4.1.10. Sejam A e I a álgebra e seu ideal nil definidos no Exemplo 4.1.5. Para todo $k \in \mathbb{N}$, seja I_k o conjunto de todas as matrizes em I com a propriedade de que suas entradas não nulas aparecem apenas em suas primeiras k linhas e colunas. Como $I_k^k = 0$, segue que I_k é um ideal nilpotente de A. Se A tivesse um ideal nilpotente maximal N então, pelo Lema 4.1.9, N conteria todo I_k, e portanto

$$\bigcup_{k=1}^{\infty} I_k = I \subseteq N.$$

Em particular, I seria um ideal nilpotente, o que é um absurdo.

Uma álgebra de dimensão finita certamente contém um ideal nilpotente maximal. De fato, ela contém ao menos um ideal nilpotente (o ideal 0), e portanto o conjunto (não-vazio) de todos os ideais nilpotentes contém um elemento de dimensão maximal. Este portanto é um ideal nilpotente maximal.

Definição 4.1.11. O ideal nilpotente maximal de uma álgebra A de dimensão finita é chamado o **radical** de A.

Exemplo 4.1.12. O radical da álgebra $A = T_n(F)$ do Exemplo 4.1.4 é N, o conjunto de todas as matrizes estritamente triangulares superiores. De fato, N é um ideal nilpotente de A, e qualquer ideal de A que contém propriamente N não pode ser nilpotente já que ele necessariamente contém uma matriz com diagonal não nula.

Exemplo 4.1.13. O radical de uma álgebra simples de dimensão finita é 0. Suponha o contrário. Neste caso, o radical é A, pois trata-se de um ideal de uma álgebra simples. Denote por n o número natural tal que $A^n = 0$ e $A^{n-1} \neq 0$. Como $A^2 \neq 0$, pois A é simples, segue que $A^{n-1} \neq A$. Como A^{n-1} é um ideal de A, segue que $A^{n-1} = 0$, pois A é simples. Absurdo.

A partir daqui iremos focar em anéis que possuem ideais nilpotentes não nulos. Por fim, iremos descrever a estrutura de todas as álgebras de dimensão finita com essa propriedade.

4.2 ANÉIS PRIMOS E SEMIPRIMOS

O objetivo desta seção é introduzir duas classes importantes de anéis, os anéis primos e semiprimos. Primeiramente, relembremos a definição de domínio.

Definição 4.2.1. Um anel R é dito ser um **domínio** se, para todos $a, b \in R$,

$$ab = 0 \Rightarrow a = 0 \text{ ou } b = 0.$$

A saber, R é um domínio se não tem divisores de zero (à esquerda ou à direita). Equivalentemente, R é um domínio se possui a *propriedade do cancelamento*: se $a \neq 0$, então $ab = ac$ e $ba = ca$ implicam que $b = c$.

O lema a seguir introduzirá uma classe de anéis importantes que, como veremos no Lema 4.2.4, trata-se dos domínios no contexto comutativo.

Lema 4.2.2. *Seja R um anel. As seguintes condições são equivalentes:*

a) Para todos $a, b \in R$, $aRb = 0$ implica $a = 0$ ou $b = 0$;

b) Para todos os ideais à esquerda I e J de R, $IJ = 0$ implica $I = 0$ ou $J = 0$;

c) Para todos os ideais à direita I e J de R, $IJ = 0$ implica $I = 0$ ou $J = 0$;

d) Para todos os ideais I e J de R, $IJ = 0$ implica $I = 0$ ou $J = 0$.

Demonstração. Assumimos válido a), e tomemos ideais à esquerda I e J de R tais que $IJ = 0$. Como $RJ \subseteq J$, então particularmente $IRJ = 0$. Em outras palavras, $iRj = 0$, para todos $i \in I$ e $j \in J$.

Vamos assumir que $I \neq 0$ e $J \neq 0$. Então existem $0 \neq a \in I$, $0 \neq b \in J$ tais que $aRb = 0$. Mas pelo item $a)$, $a = 0$ ou $b = 0$, e logo temos um absurdo. Portanto $a)$ implica em $b)$.

De maneira análoga, $a)$ também implica $c)$, e de $b)$ e $c)$ obtemos $d)$.

Agora, assumimos válido $d)$ e supomos que para todos $a, b \in R$, $aRb = 0$. Então, também

$$RaRbR = 0 \Rightarrow (RaR)(RbR) = 0 \Rightarrow RaR = 0 \text{ ou } RbR = 0.$$

A última implicação se deve ao fato de termos o produto de dois ideais bilaterais. Suponhamos sem perda de generalidade que $RaR = 0$. Isto implica que Ra e aR são ideais bilaterais de R tais que

$$Ra \cdot R = R \cdot aR = 0.$$

Novamente, pelo item $d)$, temos que $Ra = aR = 0$, para todo $a \in R$. Assim, particularmente, $\mathbb{Z}a$ é um ideal de R satisfazendo $\mathbb{Z}a \cdot R = 0$. Daí, obtemos $\mathbb{Z}a = 0$ e, portanto, $a = 0$. Logo, $d)$ implica $a)$ e concluímos a demonstração. □

Definição 4.2.3. Um anel R é dito ser **primo** se satisfaz uma (e portanto, todas) as condições do Lema 4.2.2.

Lema 4.2.4. *Um anel comutativo é primo se, e somente se, é um domínio.*

Demonstração. Seja R um anel comutativo primo, e sejam $a, b \in R$ tais que $ab = 0$. Então $abR = aRb = 0$. Como R é primo, isto implica que $a = 0$ ou $b = 0$, ou seja, R é um domínio.

Agora suponhamos que R seja um domínio comutativo, e sejam $a, b \in R$ tais que $aRb = 0$. Sem perda de generalidade, consideremos $b \neq 0$. Em particular, $abb = 0$ e valem as implicações:

$$abb = 0 \Rightarrow (ab)b = 0 \Rightarrow ab = 0 \Rightarrow a = 0.$$

Portanto, como satisfaz o primeiro item do Lema 4.2.2, R é um anel primo. □

Observação 4.2.5. Seja R um anel primo com característica $char(R) \neq 0$. Primeiramente, temos que se $0 \neq a \in R$ e $n \in \mathbb{N}$ são tais que $na = 0$, então $aR(nb) = 0$ para todo $b \in R$, e portanto $nR = 0$. Em segundo lugar, se $nR = 0$ e $n = rs$ para alguns $r, s \in \mathbb{N}$, então $rR \cdot sR = 0$. Como rR e sR são ideais de R, devemos ter que $rR = 0$ ou $sR = 0$. Desta forma, concluímos que $char(R)$ é um número primo p. De fato, seja $char(R) = m$ não primo. Daí, m pode ser fatorado como kl, para alguns $k, l \in \mathbb{N}$. Logo, $kR \cdot lR = 0$ implica que $kR = 0$ ou $lR = 0$. Digamos que $kR = 0$. Então existe um número k menor que m tal que $kR = 0$. Absurdo, pois m é a característica de R.

Portanto, podemos considerar R como uma álgebra sobre $\mathbb{Z}_p$, definindo para $k \in \mathbb{Z}_p = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$ e $x \in R$ o produto

$$\overline{k}x = kx = \underbrace{x + \cdots + x}_{k \text{ parcelas}}.$$

Vejamos que este produto está bem definido:

$$\overline{z_1} = \overline{z_2} \in \mathbb{Z}_p \text{ e } r \in R \Rightarrow z_1 - z_2 = qp, \text{ para algum } q \in \mathbb{Z}, \text{ e } r \in R$$

$$\Rightarrow qpr = 0 \Rightarrow (z_1 - z_2)r = z_1 r - z_2 r = 0 \Rightarrow z_1 r = z_2 r.$$

A demonstração dos demais itens que garantem R ser uma álgebra sobre $\mathbb{Z}_p$ é de fácil argumentação.

Agora, prosseguimos com uma classe ainda mais ampla de anéis.

Lema 4.2.6. *Seja R um anel. As seguintes afirmações são equivalentes:*

a) Para todo $a \in R$, $aRa = 0$ implica $a = 0$.

b) Para todos os ideais à esquerda I de R, $I^2 = 0$ implica $I = 0$.

c) Para todos os ideais à direita I de R, $I^2 = 0$ implica $I = 0$.

d) Para todos os ideais I de R, $I^2 = 0$ implica $I = 0$.

e) R não tem nenhum ideal nilpotente não nulo.

Demonstração. De maneira similar à demonstração do Lema 4.2.2, assumimos válido $a)$ e tomemos I ideal à esquerda de R tal que $I^2 = 0$. Como $RI \subseteq I$, também $IRI = 0$. Assumimos $I \neq 0$. Assim, existe $0 \neq i \in I$ tal que $iRi = 0$. Mas por $a)$, $i = 0$ e obtemos um absurdo. Portanto $a)$ implica em $b)$.

De forma similar, obtemos que $a)$ também implica em $c)$, e de $b)$ e $c)$ obtemos $d)$.

Agora, assumimos válido $d)$, e seja I um ideal de R tal que $I^n = 0$ para algum $n \in \mathbb{N}$. Consideremos o ideal I^{n-1} formado pelas somas de todos os elementos $x_1 x_2 \cdots x_{n-1}$ tal que $x_1, x_2, \ldots, x_{n-1} \in I$. Temos que

$$(x_1 x_2 \cdots x_{n-1})(y_1 y_2 \cdots y_{n-1}), \text{ com } x_i, y_i \in I,$$

é um produto de $(n-1) + (n-1) = 2n - 2$ elementos de I. Mas por hipótese, I é nilpotente de grau n, então

$$(x_1 x_2 \cdots x_{n-1} y_1)(y_2 \cdots y_{n-1}) = 0 \cdot (y_2 \cdots y_{n-1}) = 0.$$

Ou seja, $(I^{n-1})^2 = 0$. Pelo item $d)$, segue que $I^{n-1} = 0$. De maneira indutiva, obtemos que $I = 0$. Logo, R não pode ter ideais nilpotentes não nulos, e portanto $d)$ implica $e)$.

Por fim, assumimos válido $e)$ e seja $a \in R$ tal que $aRa = 0$. Então, valem a premissa e as implicações seguintes:

$$RaRaR = 0 \Rightarrow (RaR)(RaR) = 0 \Rightarrow RaR = 0.$$

A última implicação se deve ao fato de termos um ideal nilpotente. Isto implica que Ra e aR são ideais bilaterais de R tais que

$$(Ra)^2 = (aR)^2 = 0.$$

Novamente, pelo item $e)$, temos que $Ra = aR = 0$, para todo $a \in R$. Assim, particularmente, $\mathbb{Z}a$ é um ideal de R satisfazendo $(\mathbb{Z}a)^2 = 0$. Daí, obtemos $\mathbb{Z}a = 0$ e, portanto, $a = 0$. Logo, $e)$ implica $a)$ e concluímos a demonstração. □

Definição 4.2.7. Um anel R é dito ser **semiprimo** se satisfaz uma (e portanto, todas) as condições do Lema 4.2.6.

O seguinte lema é análogo ao Lema 4.2.4.

Lema 4.2.8. *Um anel comutativo R é semiprimo se, e somente se, não contém nenhum elemento nilpotente não nulo.*

Demonstração. Para a ida, suponhamos que exista $n \in \mathbb{N}$ e $0 \neq a \in R$ tais que $a^n = 0$ e tomemos o ideal $I = \langle a \rangle = \{za + ra \mid z \in \mathbb{Z} \text{ e } r \in R\}$. Se $z_1, \dots, z_n \in \mathbb{Z}$ e $r_1, \dots, r_n \in R$, então

$$(z_1a + r_1a) \cdot (z_2a + r_2a) \cdots (z_na + r_na) = (z_1z_2 \cdots z_n)a^n + ra^n = 0$$

para algum $r \in R$. Logo, $I^n = 0$ e $0 \neq I$ é um ideal nilpotente de R, ou seja, R não é semiprimo.

Agora, para a recíproca, seja $a \in R$ tal que $aRa = 0$. Em particular, $0 = aaa = a^3$. Mas como R não contém nilpotentes não nulos, temos que $a = 0$. □

Observação 4.2.9. Se A é uma álgebra e I, J são ideais de A como anel tais que $IJ = 0$, então os espaços vetoriais gerados por I e J são ideais de A como álgebra, cujo produto é 0. Assim, segue que uma **álgebra prima** pode ser definida equivalentemente como uma álgebra que é prima como anel, ou como uma álgebra na qual o produto de quaisquer dois ideais não nulos é não nulo. Da mesma forma, vale a definição equivalente para álgebras semiprimas.

Observação 4.2.10. Seja I um ideal não nulo de um anel primo R, e seja $0 \neq u \in I$. Se $a, b \in R$ são tais que $aIb = 0$, então $aRuRb = 0$. Se $a \neq 0$, então através da condição $a)$ do Lema 4.2.2 segue que $uRb = 0$. Novamente por tal condição, obtemos $b = 0$. Isto mostra que um ideal não nulo de um anel primo é também um anel primo.

De forma similar, mostra-se que todo ideal não nulo de um anel semiprimo é também um anel semiprimo.

Lema 4.2.11. *Se N é o ideal nilpotente maximal de um anel R, então o anel quociente $\dfrac{R}{N}$ é semiprimo.*

Demonstração. Seja K um ideal nilpotente de $\dfrac{R}{N}$, e denote por J o seguinte conjunto:

$$J = \{x \in R \mid x + N \in K\}.$$

Temos que J é um ideal de R, $N \subseteq J$ e $K = \dfrac{J}{N}$. Como K é nilpotente, existe um natural n tal que $0 = K^n = \dfrac{J^n}{N}$. Logo, $J^n \subseteq N$. Por hipótese, N é nilpotente, isto é, existe um natural m tal que $N^m = 0$. Em particular, $J^{nm} = 0$ e J é nilpotente. Pelo Lema 4.1.9, temos que $J \subseteq N$. Já que $N \subseteq J$, obtemos $J = N$. Assim, $K = \dfrac{N}{N} = 0$. Concluímos então que $\dfrac{R}{N}$ é semiprimo. □

Exemplo 4.2.12. Sejam A e N definidos como no Exemplo 4.1.12. Então $\dfrac{A}{N}$ é isomorfo a F^n, o produto direto de n cópias de F. De fato, podemos construir a função $\varphi : A \to F^n$, por

$$\varphi((a_{ij})_{ij}) = (a_{11}, a_{22}, ..., a_{nn}), \quad (a_{ij})_{ij} \in A.$$

Temos que

$$\varphi((a_{ij})_{ij} + (b_{ij})_{ij}) = \varphi((a_{ij} + b_{ij})_{ij}) = (a_{11} + b_{11}, a_{22} + b_{22}, ..., a_{nn} + b_{nn})$$

$$= (a_{11}, a_{22}, ..., a_{nn}) + (b_{11}, b_{22}, ..., b_{nn}) = \varphi((a_{ij})_{ij}) + \varphi((b_{ij})_{ij});$$

$$\varphi((a_{ij})_{ij}(b_{ij})_{ij}) = (a_{11}b_{11}, a_{22}b_{22}, ..., a_{nn}b_{nn})$$

$$= (a_{11}, a_{22}, ..., a_{nn})(b_{11}, b_{22}, ..., b_{nn}) = \varphi((a_{ij})_{ij})\varphi((b_{ij})_{ij});$$

$$\varphi(\lambda(a_{ij})_{ij}) = \varphi((\lambda a_{ij})_{ij}) = (\lambda a_{11}, \lambda a_{22}, ..., \lambda a_{nn}) = \lambda(a_{11}, a_{22}, ..., a_{nn}) = \lambda\varphi((a_{ij})_{ij}).$$

Desta forma, φ é um homomorfismo de álgebras. Como $\ker(\varphi) = N$, aplicando o Primeiro Teorema do Isomorfismo, segue o resultado.

Obtemos as seguintes relações entre as classes de anéis já introduzidas:

$$\text{anel com divisão} \Rightarrow \text{simples e domínio};$$
$$\text{simples} \Rightarrow \text{primo};$$
$$\text{domínio} \Rightarrow \text{primo};$$
$$\text{primo} \Rightarrow \text{semiprimo}.$$

Conforme os exemplos abaixo, nenhuma das implicações pode ser invertida.

Exemplo 4.2.13. Pode ser mostrado que a álgebra de Weyl $\mathscr{A}_1$ é um domínio simples, porém não é com divisão. Vide (BRESAR, 2014, Exemplo 2.28).

Exemplo 4.2.14. O anel $\mathbb{Z}$ é um domínio que não é um anel simples.

Exemplo 4.2.15. O anel de matrizes $M_n(F)$, $n \geq 2$, é um anel simples (Exemplo 3.2.6) que não é um domínio. Note que

$$E_{11}E_{22} = 0, \text{ sendo que } E_{11}, E_{22} \neq 0.$$

Exemplo 4.2.16. O anel $M_n(\mathbb{Z})$, com $n \geq 2$ é primo. De fato, sejam $(a_{ij})_{ij}$ e $(b_{ij})_{ij}$ matrizes não nulas em $M_n(\mathbb{Z})$. Assim, existem entradas a_{pq} e b_{rs} não nulas. Temos que a entrada (p, s) da

matriz $(a_{ij})_{ij}E_{qr}(b_{ij})_{ij}$ é $a_{pq}b_{rs} \neq 0$. Logo, $(a_{ij})_{ij}M_n(\mathbb{Z})(b_{ij})_{ij} \neq 0$, e pelo item a) do Lema 4.2.2, segue que $M_n(\mathbb{Z})$ é primo.

No entanto, $M_n(\mathbb{Z})$ não é um domínio (pelas mesmas razões do exemplo anterior) nem um anel simples, pois $M_n(2\mathbb{Z})$ é um ideal, por exemplo.

Exemplo 4.2.17. Todo anel comutativo que possui divisores de zero mas não possui elementos nilpotentes não nulos, é semiprimo mas não primo (vide os Lemas 4.2.4 e 4.2.8). Um exemplo de tal anel é o anel das funções reais contínuas $C[-1,1]$ com as operações usuais de soma e produto de funções. Tomemos as funções $f, g \in C[-1,1]$, definidas da seguinte forma:

$$f(x) = \begin{cases} 0, & -1 \leq x < 0 \\ x, & 0 \leq x \leq 1 \end{cases}; \qquad g(x) = \begin{cases} -x, & -1 \leq x < 0 \\ 0, & 0 \leq x \leq 1 \end{cases}.$$

Temos que $f, g \neq 0$, mas $fg = 0$, provando que $C[-1,1]$ possui divisores de zero e, portanto, não é primo.

O próximo exemplo explicita uma diferença entre a classe dos anéis primos e semiprimos, e também aponta uma certa relação entre anéis primos e números primos.

Exemplo 4.2.18. Sejam R_1 e R_2 anéis não nulos. Seu produto direto $R = R_1 \times R_2$ não é um anel primo, já que $R_1 \times 0$ e $0 \times R_2$ são ideais não nulos de R cujo produto é 0. Por outro lado, se ambos R_1 e R_2 são semiprimos, então R também é semiprimo.

4.3 UNITIZAÇÃO

Nesta seção introduziremos uma maneira de estudar álgebras sem unidade de forma a reduzir certos problemas de álgebras gerais à álgebras unitárias, cuja estrutura é bem conhecida.

Seja A uma F-álgebra. Então o conjunto $F \times A = \{(\lambda, x) \mid \lambda \in F, x \in A\}$ se torna uma F-álgebra, a qual denotamos por $A^{\#}$, ao definirmos adição, produto por escalar e multiplicação da seguinte forma:

$$\begin{aligned} (\lambda, x) + (\mu, y) &:= (\lambda + \mu, x + y), \\ \mu(\lambda, x) &:= (\mu\lambda, \mu x), \\ (\lambda, x)(\mu, y) &:= (\lambda\mu, \mu x + \lambda y + xy). \end{aligned}$$

Consideramos A uma subálgebra de $A^{\#}$ através do mergulho $x \mapsto (0, x)$. Notemos que A é na verdade um ideal de $A^{\#}$. Verificaremos apenas um item deste fato, isto é, tomando $(0, x) \in A$ e $(\lambda, y) \in A^{\#}$, temos

$$\begin{aligned} (0, x)(\lambda, y) &= (0 \cdot \lambda, \lambda \cdot x + 0 \cdot y + x \cdot y) = (0, \lambda x + xy) \in A; \\ (\lambda, y)(0, x) &= (\lambda \cdot 0, 0 \cdot y + \lambda \cdot x + y \cdot x) = (0, \lambda x + yx) \in A. \end{aligned}$$

Uma observação crucial é a de que $A^{\#}$ é uma álgebra unitária. De fato, $(1, 0)$ é sua unidade:

$$(1,0)(\mu,y) = (1\cdot\mu, \mu\cdot 0 + 1\cdot y + 0\cdot y) = (\mu,y);$$
$$(\mu,y)(1,0) = (\mu\cdot 1, 1\cdot y + \mu\cdot 0 + y\cdot 0) = (\mu,y).$$

Definição 4.3.1. A álgebra $A^{\#}$ é chamada de **unitização** de A.

Observação 4.3.2. Considerando $F = \mathbb{Z}$, definimos a unitização $R^{\#}$ de um anel R de maneira similar, apenas desconsiderando a operação de produto por escalar.

Alternativamente, podemos tomar $\mathbb{Z}_n$ ao invés de $\mathbb{Z}$ se char(R)= $n > 0$.

Esta construção é destinada principalmente à álgebras (e anéis) sem unidade. O objetivo principal é reduzir certos problemas de álgebras gerais à álgebras unitárias. A princípio, é possível construir $A^{\#}$ mesmo se A for unitária.

Observação 4.3.3. A unitização de A não preserva as propriedades de A. Por exemplo, se A é uma álgebra simples, $A^{\#}$ não é simples já que A é um ideal de $A^{\#}$. Outro exemplo, se A é uma álgebra unitária prima não-nula, então $A^{\#}$ não é prima, já que $I = \{(\lambda,-\lambda) \mid \lambda \in F\}$ é um ideal de $A^{\#}$ tal que $IA = AI = 0$. De fato, se $(\mu,-\mu) \in I$ e $(0,x) \in A$, então

$$(\mu,-\mu)(0,x) = (\mu\cdot 0, 0\cdot(-\mu) + \mu\cdot x + (-\mu)\cdot x) = (0,0) \text{ e}$$
$$(0,x)(\mu,-\mu) = (0\cdot\mu, \mu\cdot x + 0\cdot(-\mu) + x\cdot(-\mu) = (0,0).$$

Portanto, encontramos dois ideais não nulos I e A de $A^{\#}$ cujo produto é zero.

Lema 4.3.4. *Seja A uma álgebra prima sem unidade. Então $A^{\#}$ também é prima.*

Demonstração. Sejam elementos (λ,a), $(\mu,b) \in A^{\#}$ tal que $(\lambda,a)A^{\#}(\mu,b) = \{(0,0)\}$. Particularmente, se isto vale, então vale a premissa e as implicações:

$$(\lambda,a)(1,0)(\mu,b) = (0,0) \Rightarrow (\lambda,a)(\mu,b) = (0,0) \Rightarrow \lambda\mu = 0 \text{ e } \mu a + \lambda b + ab = 0.$$

Logo, $\lambda = 0$ ou $\mu = 0$. Assumimos sem perda de generalidade que $\lambda = 0$, e vamos supor que $a \neq 0$. Então, para todo $x \in A$, vale que

$$(0,a)(0,x)(\mu,b) = (0,0) \Rightarrow (0,ax)(\mu,b) = (0,0) \Rightarrow (0,\mu ax + axb) = (0,0)$$
$$\Rightarrow \mu ax + axb = 0, \text{ para todo } x \in A.$$

Temos dois casos a analisar:

(1) Se $\mu = 0$, então $axb = 0$ para todo $x \in A$, ou seja, $aAb = 0$. Como A é álgebra prima, segue que $b = 0$ e, portanto, $(\mu,b) = (0,0)$, como desejado.

(2) Suponha $\mu \neq 0$. Definindo o elemento $e := -\mu^{-1}b$, temos

$$\mu ax + axb = 0 \Rightarrow \mu ax = -axb \Rightarrow ax = \frac{-axb}{\mu} = -ax(\mu^{-1}b) = axe, \text{ para todo } x \in A.$$

Assim, $a(xy)e = axy = (axe)y$, para todos $x, y \in A$. Em outras palavras,

$$axy - axye = ax(y - ye) = 0 = ax(y - ey) = axy - axey.$$

Mas como A é prima, segue que $y = ye$ e $y = ey$ para todo $y \in A$. Isto contradiz a hipótese de que A não tem unidade.

Pelos dois itens, finalizamos a demonstração. □

4.4 A REPRESENTAÇÃO REGULAR

Nesta seção introduziremos o conceito de representação regular. Partiremos da seguinte pergunta motivadora:

Pergunta. dada uma álgebra unitária A, é possível que

$$[a, b] = 1 \tag{4.1}$$

para algum $a, b \in A$?

Esta pergunta tem resposta positiva, por exemplo, para a álgebra de Weyl $\mathscr{A}_1$, que é uma álgebra de dimensão infinita. Estudaremos se é possível que (4.1) ocorra em uma álgebra de dimensão finita.

Utilizaremos as funções multiplicativas à esquerda $L_a : A \to A$, dadas por $L_a(x) = ax$. Relembrando que $L_{\lambda a+\mu b} = \lambda L_a + \mu L_b$ e $L_{ab} = L_a L_b$, vemos que a função $a \mapsto L_a$ é um homomorfismo de álgebras.

Definição 4.4.1. O homomorfismo $L : A \to End_F(A)$ dado por $L(a) = L_a$ é chamado de **representação regular** de A.

A representação regular é injetiva, a menos que $aA = 0$ para algum $0 \neq a \in A$. Esta última condição não pode ocorrer em uma álgebra unitária A. De fato, $aA = 0$ implica em particular que $a \cdot 1 = 0$, e assim $a = 0$. Logo, L é um mergulho de A em $End_F(A)$, o que torna possível identificar um elemento $a \in A$ com $L_a \in End_F(A)$. A vantagem obtida em considerar L_a vem das ferramentas já existentes para trabalhar com operadores lineares.

O lema a seguir justifica esta abordagem. Notemos a analogia com o Teorema de Cayley da teoria de grupos.

Proposição 4.4.2. *Toda F-álgebra A pode ser mergulhada na álgebra $End_F(V)$ para algum espaço vetorial V. Se A tem dimensão finita, então V pode ser escolhido de forma a ter dimensão finita, e então neste caso A pode ser mergulhado em $M_n(F)$ para algum $n \in \mathbb{N}$.*

Demonstração. Se A é unitária, basta tomar $V = A$ e utilizar a representação regular como um mergulho. Se A não é unitária, podemos mergulhar A em sua unitização $A^\#$, e então tomar $V = A^\#$. Em todo caso, V tem dimensão finita se A também tem; se V tem dimensão n, então $End_F(V) \cong M_n(F)$. □

Esta proposição torna possível considerar os elementos de uma álgebra de dimensão finita como matrizes.

Retornando à questão motivadora do início da seção, vamos assumir que existam elementos a, b de uma álgebra A com dimensão finita n tais que (4.1) vale. Então,

$$Id = L(1) = L([a,b]) = [L(a), L(b)] = [L_a, L_b].$$

Identificando L_a, L_b como matrizes em $M_n(F)$, como na Proposição 4.4.2, temos

$$n = tr(Id) = tr([L_a, L_b]) = 0,$$

onde tr é o traço da matriz. Se $char(F) = 0$, então isto é impossível, e logo (4.1) não pode ocorrer. Provamos então um caso particular do seguinte resultado:

Proposição 4.4.3. *Seja A uma álgebra unitária não nula de dimensão finita sobre um corpo F de característica 0. Então 1 não pode ser escrito como uma soma de comutadores de A.*

Demonstração. Segue a mesma ideia do parágrafo anterior. □

Pode ser mostrado que a proposição acima não é válida se a característica de F é diferente de 0. Para isso, veja (BRESAR, 2014, Exemplo 2.40).

Agora, provaremos um resultado do matemático estadunidense Nathan Jacobson, de 1935, que trata da condição $[[a,b],a] = 0$. Isto pode ocorrer em álgebras de dimensão finita mesmo que a e b não comutem, independentemente de $char(F)$.

Exemplo 4.4.4. As matrizes canônicas E_{11}, E_{12} satisfazem $[E_{12}, E_{11}] = -E_{12}$, e portanto $[[E_{12}, E_{11}], E_{12}] = 0$.

Definição 4.4.5. Seja A uma álgebra (respectivamente, um anel). Uma função linear (respectivamente aditiva) $d : A \to A$ é chamada uma **derivação** se

$$d(xy) = d(x)y + xd(y),$$

para todos $x, y \in A$.

Exemplo 4.4.6. O operador diferencial D no Exemplo 3.2.9 é uma derivação.

Exemplo 4.4.7. Fixado um elemento a em uma álgebra (ou anel) A, a função $d : A \to A$ dada por

$$d(x) = [a,x]$$

é uma derivação. De fato,

$$d(xy) = [a,xy] = axy - xya = axy - xay + xay - xya =$$
$$(ax - xa)y + x(ay - ya) = d(x)y + xd(y).$$

Uma derivação desta forma é chamada de **derivação interna de** A.

Proposição 4.4.8 (Jacobson)**.** *Seja A uma álgebra de dimensão finita sobre um corpo F de $char(F) = 0$. Se $a, b \in A$ satisfazem $[[a,b],a] = 0$, então $[a,b]$ é um elemento nilpotente.*

Demonstração. Seja d a derivação interna $d(x) = [a,x]$. Assim,

$$0 = [[a,b],a] = [a,[a,b]] = d([a,b]) = d(d(b)),$$

ou seja, $d^2(b) = 0$. Primeiramente, mostraremos por indução que

$$d(d(b)^k) = 0 \text{ para todo } k \in \mathbb{N}. \tag{4.2}$$

O caso $k = 1$ já está provado acima. Assumamos que a sentença é válida para k e provemos que vale para $k+1$. Temos

$$d(d(b)^{k+1}) = d(d(b)d(b)^k)) = d(d(b))d(b)^k + d(b)d(d(b)^k) = 0d(b)^k + d(b)0 = 0,$$

como era o desejado.

Agora, afirmamos que

$$d^n(b^n) = n!d(b)^n \text{ para todo } n \in \mathbb{N}. \tag{4.3}$$

Provaremos tal fato por indução em n. O caso $n = 1$ é óbvio. Seja $n > 1$ e vamos assumir que (4.3) vale para $n-1$. Antes de prosseguirmos, afirmamos que a Regra de Leibniz do Cálculo também vale aqui, ou seja,

$$d^n(uv) = \sum_{i=0}^{n} \binom{n}{i} d^i(u)d^{n-i}(v).$$

A demonstração deste fato é a mesma de Cálculo, feita por indução em n. Continuando, pela regra acima e por (4.2), temos

$$d^n(b^n) = d^n(bb^{n-1}) = \sum_{i=0}^{n} \binom{n}{i} d^i(b)d^{n-i}(b^{n-1}) = \sum_{i=0}^{1} \binom{n}{i} d^i(b)d^{n-i}(b^{n-1})$$

$$= bd^n(b^{n-1}) + nd(b)d^{n-1}(b^{n-1}) = bd(d^{n-1}(b^{n-1})) + nd(b)d^{n-1}(b^{n-1}).$$

Aplicando a hipótese de indução e (4.2), temos

$$d^n(b^n) = bd((n-1)!d(b)^{n-1}) + nd(b)(n-1)!d(b)^{n-1} = (n-1)!bd(d(b)^{n-1})) + n!d(b)^n = n!d(b)^n.$$

A afirmação está provada.

Como consequência de (4.2) e (4.3) obtemos

$$d^m(b^k) = d^{m-k}(d^k(b^k)) = d^{m-k}(k!d(b)^k) = k!d^{m-k}(d(b)^k) = k!d^{m-k-1}(d(d(b)^k)) = 0$$

sempre que $k < m$. Pelo Lema 3.1.7, existe $m \in \mathbb{N}$ tal que b^m é combinação linear de b^k, com $k < m$. Portanto, $d^m(b^m) = 0$, e logo $m!d(b)^m = 0$ por (4.3). Portanto, concluímos que $[a,b]^m = 0$ e então $[a,b]$ é nilpotente de grau m. □

4.5 ÁLGEBRAS GRUPO

Nesta seção introduziremos conceitos que conectam as noções de grupo e anel.

Seja G um conjunto arbitrário e F um corpo. Podemos considerar o espaço vetorial sobre F cuja base é G. Seus elementos são somas formais

$$\sum_{g\in G} \lambda_g g,\ \lambda_g \in F,$$

e a menos de uma quantidade finita de escalares λ_g, todos λ_g são nulos. Relembrando:

a) $\sum_{g\in G} \lambda_g g = \sum_{g\in G} \beta_g g$ se, e somente se, $\lambda_g = \beta_g$ para todo $g \in G$,

b) $\sum_{g\in G} \lambda_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\lambda_g + \beta_g) g$,

c) $\lambda \sum_{g\in G} \lambda_g g = \sum_{g\in G} (\lambda\lambda_g) g$ se $\lambda \in F$.

Assumimos agora que $(G,\cdot)$ é um grupo. Então o espaço vetorial acima torna-se uma álgebra ao estender o produto do grupo para o espaço inteiro por meio da distributividade. Em razão dos axiomas de álgebra isto pode ser feito de maneira única, ou seja,

$$\left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{h\in G} \mu_h h\right) = \sum_{k\in G} \nu_k k, \text{ onde } \nu_k = \sum_{g\cdot h = k} \lambda_g \mu_h.$$

Denotamos esta álgebra por $F[G]$.

Definição 4.5.1. A álgebra $F[G]$ é chamada de **álgebra grupo** de G sobre F.

É suficiente assumir que G seja um semigrupo para construir $F[G]$. Neste caso, denominamos $F[G]$ de **álgebra semigrupo**. De maneira similar, se G é um monóide, construímos a **álgebra monóide** de G. Ademais, podemos substituir o corpo F por qualquer anel R, e definir a soma e o produto formalmente da mesma maneira.

Há muitos exemplos de álgebras grupo que são domínios, como por exemplo $F[\mathbb{Z}]$. No entanto, se um grupo $(G,\cdot)$ tem um elemento $g \neq 1$ de ordem finita, então $F[G]$ não é um domínio. De fato, $g^n = 1$ implica $(1-g)(1+g+\cdots+g^{n-1}) = 0$. O problema a seguir permanece em aberto.

Problema 4.5.2. Se um grupo G não tem nenhum elemento de ordem finita além de 1, então $F[G]$ é um domínio?

Se G é um grupo não trivial, então o conjunto de todos $\sum_{g\in G} \lambda_g g$ tal que $\sum_{g\in G} \lambda_g = 0$ é um ideal próprio não nulo de $F[G]$. Ele é chamado de **ideal de aumento** de $F[G]$. A álgebra $F[G]$, portanto, não é simples. O objetivo principal desta seção é discutir se $F[G]$ é ou não semiprima.

Exemplo 4.5.3. Seja $G = \{1, g\}$, onde $g^2 = 1$, um grupo de ordem 2. A álgebra grupo $F[G]$ então consiste dos elementos da forma $\lambda 1 + \mu g$, onde $\lambda, \mu \in F$, cujo produto é dado por

$$(\lambda 1 + \mu g)(\lambda' 1 + \mu' g) = (\lambda\lambda' + \mu\mu')1 + (\lambda\mu' + \mu\lambda')g.$$

Seja $\varphi : F[G] \to F \times F$ a função dada por

$$\varphi(\lambda 1 + \mu g) = (\lambda + \mu, \lambda - \mu).$$

Provaremos que φ é um homomorfismo de álgebras. Temos:

a) Referente a soma,

$$\varphi((\lambda 1 + \mu g) + (\lambda' 1 + \mu' g)) = \varphi((\lambda + \lambda')1 + (\mu + \mu')g) = (\lambda + \lambda' + \mu + \mu', \lambda + \lambda' - \mu - \mu')$$

$$= (\lambda + \mu, \lambda - \mu) + (\lambda' + \mu', \lambda' - \mu') = \varphi(\lambda 1 + \mu g) + \varphi(\lambda' 1 + \mu' g);$$

b) Referente ao produto,

$$\varphi((\lambda 1+\mu g)(\lambda' 1+\mu' g)) = \varphi((\lambda\lambda'+\mu\mu')1+(\lambda\mu'+\mu\lambda')g) = (\lambda\lambda'+\mu\mu'+\lambda\mu'+\mu\lambda', \lambda\lambda'+\mu\mu'-\lambda\mu'-\mu\lambda')$$

$$= (\lambda\lambda' + \lambda\mu' + \mu\lambda' + \mu\mu', \lambda\lambda' - \lambda\mu' - \mu\lambda' + \mu\mu') = ((\lambda + \mu)(\lambda' + \mu'), (\lambda - \mu)(\lambda' - \mu'))$$

$$= (\lambda + \mu, \lambda - \mu)(\lambda' + \mu', \lambda' - \mu') = \varphi(\lambda 1 + \mu g)\varphi(\lambda' 1 + \mu' g);$$

c) Referente ao produto por escalar,

$$\alpha\varphi(\lambda 1 + \mu g) = \alpha(\lambda + \mu, \lambda - \mu) = (\alpha\lambda + \alpha\mu, \alpha\lambda - \alpha\mu) = \varphi(\alpha(\lambda 1 + \mu g)).$$

Agora suponha $\text{char}(F) \neq 2$. Neste caso, $\ker \varphi = 0$ e portanto φ é injetor. Sendo o domínio e contradomínio com mesma dimensão 2, segue que φ é um isomorfismo, ou seja, $F[G] \cong F \times F$. Em particular, $F[G]$ é semiprimo.

A conclusão acima não vale se $\text{char}(F) = 2$, pois $F(1 + g)$ seria um ideal nilpotente de $F[G]$. Neste caso, notamos que $F[G]$ é isomorfo à subálgebra $M_2(F)$ que consiste das matrizes da forma $\begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix}$. O isomorfismo é dado por $\lambda 1 + \mu g \mapsto \begin{pmatrix} \lambda + \mu & \mu \\ 0 & \lambda + \mu \end{pmatrix}$.

Logo, a álgebra grupo $F[G]$, quando a ordem de G é 2, é semiprima se, e somente se, $char(F) \neq 2$. Iremos generalizar este fato para álgebras grupo sobre grupos finitos arbitrários.

Primeiramente recordemos alguns fatos de álgebra linear. Seja V um espaço vetorial de dimensão finita n e $T : V \to V$ uma função linear. Tomando uma base β em V, podemos representar T como uma matriz $[T]_\beta$ em relação a esta base. Bases diferentes produzem matrizes similares. Logo, independente da base escolhida, o traço da matriz que representa T é

sempre o mesmo:

$$tr(X[T]_\beta X^{-1}) = tr([T]_\beta X^{-1}X) = tr([T]_\beta).$$

Podemos então definir $tr(T)$ como o traço de qualquer matriz que representa T. Usaremos o seguinte fato de Álgebra Linear: Se T é nilpotente, então $tr(T) = 0$. De fato, sendo $T^n = 0$ para algum n, segue que os autovalores de T são iguais a 0. Mergulhando F num corpo algebricamente fechado $\overline{F}$, temos que existe $X \in M_n(\overline{F})$ tal que $Y = X[T]_\beta X^{-1}$ está na forma de Jordan. A matriz Y é triangular superior com diagonal formada pelos autovalores de $[T]_\beta$, que no caso são nulos. Logo,

$$0 = tr(Y) = tr([T]_\beta),$$

como era o desejado.

O seguinte teorema foi provado em 1898 pelo matemático alemão Heinrich Maschke.

Teorema 4.5.4 (Maschke)**.** *Seja G um grupo finito. Então a álgebra grupo $F[G]$ é semiprima se, e somente se, $char(F) = 0$ ou $char(F)$ não divide $|G|$.*

Demonstração. Como $F[G]$ é um espaço vetorial de dimensão finita sobre F, podemos definir o funcional linear $\rho : F[G] \to F$ dado por

$$\rho(a) := tr(L_a).$$

Relembrando que L_a é a função multiplicativa à esquerda por a, e tr é o traço. Seja $n = |G|$ e denotemos os elementos de G por $g_1, g_2, ..., g_n$ onde $g_1 = 1$. Temos então

$$\rho(g_1) = \rho(1) = tr(L_1) = n.$$

Se $i \geq 2$, então

$$L_{g_i}(g_j) = g_i g_j \in G \setminus \{g_j\}$$

para todo j. A matriz que representa L_{g_i} em relação à base $\{g_1, g_2, ..., g_n\}$ portanto tem zeros na diagonal. Consequentemente, $\rho(g_i) = 0$.

Suponhamos agora que $F[G]$ tem um ideal nilpotente não nulo I. Queremos mostrar que F tem característica finita p que divide $n = |G|$. Tomemos $0 \neq a \in I$, e escrevamos $a = \sum_{i=1}^{n} \lambda_i g_i$. Sem perda de generalidade podemos assumir que $\lambda_1 \neq 0$. De fato, caso contrário escolhemos i tal que $\lambda_i \neq 0$ e substituímos a por ${g_i}^{-1}a$, que também é um elemento de I. Temos

$$\rho(a) = \lambda_1\rho(g_1) + \lambda_2\rho(g_2) + \cdots + \lambda_n\rho(g_n) = n\lambda_1.$$

Como todo elemento de um ideal nilpotente é nilpotente, segue que a é um elemento nilpotente. Logo, $L_a : F[G] \to F[G]$ é uma função linear nilpotente e, consequentemente, $\rho(a) = 0$. Isto é, $n\lambda_1 = 0$. Como $\lambda_1 \neq 0$, isto só é possível quando $p = \text{char}(F)$ divide n.

Por outro lado, assumimos que $p = \text{char}(F)$ divide $|\, G \,|$. Seja $r = \sum_{i=1}^{n} g_i$. Como $rg_j = g_j r = r$ para todo j, vemos que o espaço Fr, de dimensão 1, é um ideal de $F[G]$. Como

$$r^2 = \left(\sum_{i=1}^{n} g_i\right)\left(\sum_{j=1}^{n} g_j\right) = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} g_i\right) g_j = \sum_{j=1}^{n} rg_j = \sum_{j=1}^{n} r = |G|r = 0,$$

segue que Fr é um ideal nilpotente. □

4.6 MATRIZES CANÔNICAS

Nesta seção faremos uma generalização do conceito de matrizes canônicas.

Definição 4.6.1. Seja R um anel com unidade 1 e seja $n \in \mathbb{N}$. Um conjunto $\{e_{ij} \in R \mid 1 \leq i, j \leq n\}$ é chamado um **conjunto de matrizes canônicas** $n \times n$ se

$$e_{11} + e_{22} + \cdots + e_{nn} = 1 \quad \text{e} \quad e_{ij}e_{kl} = \delta_{jk}e_{il}$$

para todos $1 \leq i, j, k, l \leq n$, onde δ_{jk} é o delta de Kronecker: $\delta_{jk} = \begin{cases} 1, & \text{se } j = k \\ 0, & \text{se } j \neq k \end{cases}$.

Um exemplo básico do conceito acima são as matrizes canônicas usuais E_{ij} do anel $M_n(S)$, onde S é um anel unitário arbitrário. Este conjunto não é único, pois se e_{ij} são matrizes canônicas e p é um elemento invertível no anel R, então os elementos $f_{ij} := p^{-1}e_{ij}p$ também formam um conjunto de matrizes canônicas. De fato,

$$f_{11} + \cdots + f_{nn} = p^{-1}e_{11}p + \cdots + p^{-1}e_{nn}p = p^{-1}(e_{11} + \cdots + e_{nn})p = p^{-1}1p = p^{-1}p = 1,$$

e também

$$f_{ij}f_{kl} = p^{-1}e_{ij}pp^{-1}e_{kl}p = p^{-1}e_{ij}e_{kl}p = p^{-1}\delta_{jk}e_{il}p = \delta_{jk}p^{-1}e_{il}p = \delta_{jk}f_{il}.$$

As matrizes canônicas e_{ij} com $i \neq j$ se comportam de maneira significativamente diferente das matrizes canônicas da forma e_{ii}. Em particular, as e_{ij}'s são tais que $e_{ij}^2 = e_{ij}e_{ij} = \delta_{ji}e_{ij} = 0e_{ij} = 0$, e portanto são elementos nilpotentes, enquanto que as matrizes e_{ii}'s são tais que $e_{ii}^2 = e_{ii}e_{ii} = \delta_{ii}e_{ii} = 1e_{ii} = e_{ii}$.

Definição 4.6.2. Um elemento e em um anel R é dito **idempotente** se $e^2 = e$. Elementos idempotentes e e f são denominados **ortogonais** se $ef = fe = 0$.

Logo, num conjunto de matrizes canônicas, os elementos $e'_{ii}s$ são dois a dois idempotentes ortogonais cuja soma é 1.

Cada e_{ii} gera o subanel $e_{ii}Re_{ii} = \{e_{ii}ae_{ii} \mid a \in R\}$ de R, e todos estes subanéis gerados desta forma são isomorfos entre si. De fato, sejam $e_{ii}Re_{ii}$ e $e_{jj}Re_{jj}$ dois subanéis gerados desta

forma. Afirmamos que a aplicação $\varphi : e_{ii}Re_{ii} \to e_{jj}Re_{jj}$, dada por

$$\varphi(e_{ii}ae_{ii}) = e_{ji}(e_{ii}ae_{ii})e_{ij} = e_{jj}(e_{ji}ae_{ij})e_{jj},$$

é um isomorfismo. Provaremos isso, conforme os itens abaixo:

a) Referente a soma,

$$\varphi(e_{ii}xe_{ii} + e_{ii}ye_{ii}) = \varphi(e_{ii}[x+y]e_{ii}) = e_{ji}(e_{ii}(x+y)e_{ii})e_{ij}$$

$$= e_{ji}(e_{ii}xe_{ii} + e_{ii}ye_{ii})e_{ij} = e_{ji}e_{ii}xe_{ii}e_{ij} + e_{ji}e_{ii}ye_{ii}e_{ij} = \varphi(e_{ii}xe_{ii}) + \varphi(e_{ii}ye_{ii});$$

b) Referente ao produto,

$$\varphi(e_{ii}xe_{ii}e_{ii}ye_{ii}) = e_{ji}(e_{ii}xe_{ii}e_{ii}ye_{ii})e_{ij} = e_{ji}(e_{ii}xe_{ii}e_{ii}e_{ii}ye_{ii})e_{ij}$$

$$= e_{ji}(e_{ii}xe_{ii}e_{ij}e_{ji}e_{ii}ye_{ii})e_{ij} = [e_{ji}(e_{ii}xe_{ii})e_{ij}][e_{ji}(e_{ii}ye_{ii})e_{ij}] = \varphi(e_{ii}xe_{ii})\varphi(e_{ii}ye_{ii}).$$

Definimos conjunto de matrizes canônicas para anéis unitários arbitrários. Mostraremos a seguir que um anel que contém um conjunto de matrizes canônicas é de fato um anel de matrizes.

Proposição 4.6.3. *Se um anel unitário R contém um conjunto de matrizes canônicas $n \times n$, então $R \cong M_n(S)$ onde $S = e_{11}Re_{11}$.*

Demonstração. Definimos $\varphi : R \to M_n(e_{11}Re_{11})$ por

$$\varphi(a) := (a_{ij})_{ij}, \text{ onde } a_{ij} = e_{1i}ae_{j1}.$$

Temos que $a_{ij} = e_{11}a_{ij}e_{11}$ e portanto $a_{ij} \in e_{11}Re_{11}$, ou seja, φ está bem definida. Mostremos que φ é de fato um isomorfismo.

a) Referente a soma,

$$\varphi(a+b) = ((a+b)_{ij})_{ij}, \text{ onde } (a+b)_{ij} = e_{1i}(a+b)e_{j1} = e_{1i}ae_{j1} + e_{1i}be_{j1} = a_{ij} + b_{ij}.$$

Note que $a_{ij} + b_{ij}$ é a entrada (i,j) da matriz $(a_{ij})_{ij} + (b_{ij})_{ij} = \varphi(a) + \varphi(b)$. Portanto, $\varphi(a+b) = \varphi(a) + \varphi(b)$.

b) Referente ao produto,

$$\varphi(ab) = ((ab)_{ij})_{ij}, \text{ onde}(ab)_{ij} = e_{1i}abe_{j1}.$$

Olhemos para a entrada (i,j) da matriz $\varphi(a)\varphi(b)$. De acordo com o produto usual de matrizes,

ela é dada por

$$\sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} e_{1i}ae_{k1}e_{1k}be_{j1} = e_{1i}a\left(\sum_{k=1}^{n} e_{kk}\right)be_{j1} = e_{1i}a1be_{j1} = e_{1i}abe_{j1} = (ab)_{ij}.$$

Portanto, $\varphi(ab) = \varphi(a)\varphi(b)$.

c) Referente a injetividade, se $a_{ij} = 0$ para todos i, j, então

$$0 = e_{i1}a_{ij}e_{1j} = e_{i1}e_{1i}ae_{j1}e_{1j} = e_{ii}ae_{jj}$$

e portanto,

$$a = 1a1 = \left(\sum_{i=1}^{n} e_{ii}\right)a\left(\sum_{j=1}^{n} e_{jj}\right) = 0.$$

Assim, $\varphi(a) = 0$ implica que $a = 0$, e portanto φ é injetiva.

d) Referente a sobrejetividade, se $r \in R$, então

$$\varphi(e_{k1}re_{1l}) = (e_{1i}e_{k1}re_{1l}e_{j1})_{ij} = (\delta_{ik}e_{11}re_{11}\delta_{lj})_{ij},$$

e observemos que esta é a matriz cuja entrada (k, l) é igual a $e_{11}re_{11}$ e todas as outras entradas são nulas. Portanto, se $y \in M_n(S)$, então $y = (e_{11}r_{ij}e_{11})_{ij}$ para certos $r_{ij} \in R$ e

$$\varphi\left(\sum_{k=1}^{n}\sum_{l=1}^{n} e_{k1}r_{kl}e_{1l}\right) = y.$$

Finalizamos a demonstração. □

Observação 4.6.4. Se R é uma álgebra, então o isomorfismo da Proposição 4.6.3 é um isomorfismo de álgebras.

4.7 IDEMPOTENTES

Nesta seção discutiremos elementos idempotentes, suas propriedades e a decomposição de Pierce.

Denotaremos um elemento idempotente arbitrário em um anel R por e. Chamamos o anel eRe de **corner ring** correspondente a e. Este anel tem unidade, mesmo que R não seja um anel unitário, sendo sua unidade e. Veremos ao longo da seção outros três subanéis de R que são naturalmente conectados a e.

Iremos assumir que R é um anel unitário e que e é um **idempotente não trivial**, ou seja, um idempotente diferente de 0 e 1. Logo,

$$f := 1 - e$$

também é um idempotente não trivial, e e f são ortogonais e sua soma é igual a 1. De fato,

$$f^2 = (1-e)(1-e) = 1 - e - e + e^2 = 1 - e - e + e = 1 - e = f;$$

$$fe = (1-e)e = e - ee = e - e = 0;$$

$$ef = e(1-e) = e - ee = e - e = 0.$$

Como exemplo de tal par de idempotentes, podemos considerar as matrizes canônicas e_{11} e e_{22} em um anel de matrizes 2×2. De fato, sejam $e = e_{11}$ e $f = Id - e_{11}$. Temos

$$f = Id - e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = e_{22}$$

e

$$e_{11}^2 = e_{11}e_{11} = e_{11}, e_{22}^2 = e_{22}e_{22} = e_{22}, e_{11}e_{22} = 0 = e_{22}e_{21}.$$

Retornando para a teoria, vamos supor que existam $x_1, x_2, x_3, x_4 \in R$ tais que

$$ex_1e + ex_2f + fx_3e + fx_4f = 0.$$

Ao multiplicarmos a igualdade à esquerda e à direita por e, temos

$$eex_1ee + eex_2fe + efx_3ee + efx_4fe = ex_1e = 0.$$

Procedendo de maneira similar, obtemos que todos os outros termos também são iguais a 0. Por outro lado, cada $x \in R$ pode ser escrito como

$$x = exe + exf + fxe + fxf.$$

De fato,

$$exe + exf + fxe + fxf = (e+f)x(e+f) = 1x1 = x.$$

Desta forma, segue que

$$R = eRe \oplus eRf \oplus fRe \oplus fRf. \tag{4.4}$$

Chamamos (4.4) de **Decomposição de Peirce** de R em relação a e. Sejam

$$R_{11} \coloneqq eRe \text{ , } R_{12} \coloneqq eRf, R_{21} \coloneqq fRe, R_{22} \coloneqq fRf.$$

Assim, R_{11} e R_{22} são corner rings com respeito a e e f, respectivamente, enquanto que R_{12} e R_{21}

são subanéis cujas multiplicações são nulas. Além disso, temos

$$R_{ij}R_{kl} \subseteq \delta_{jk}R_{il}$$

para todos $1 \leq i, j, k, l \leq 2$, o que corresponde ao produto das matrizes canônicas do anel de matrizes.

Assim, ao tomar um idempotente não trivial e em um anel R, podemos construir $f := 1 - e$ e desta forma "imitar" a estrutura de $M_2(eRe)$. No entanto, isto não garante que um anel R com um idempotente e é isomorfo ao anel $M_2(eRe)$, é necessário ainda construir, segundo a Proposição 4.6.3, os outros dois elementos $e_{12} \in eRf$ e $e_{21} \in fRe$ de modo que $\{e = e_{11}, f = e_{22}, e_{12}, e_{21}\}$ seja um conjunto de matrizes canônicas de R. Note, precisamos encontrar $x, y \in R$ tais que exf e fye façam os papéis de e_{12} e e_{21}, respectivamente. Para isso, é suficiente e necessário encontrar $x, y \in R$ tais que

$$exfye = e \text{ e } fyexf = f.$$

Exemplos de anéis que não têm idempotentes não triviais são domínios, e em particular anéis com divisão. A existência de um idempotente não trivial garante a existência de "vários" idempotentes se os termos eRf e fRe da decomposição de Peirce forem não nulos. De uma forma mais clara, se e é um idempotente, então $e + exf$ e $e + fxe$ também são idempotentes, para todo $x \in R$. Ademais, para todo elemento invertível $p \in R$, $p^{-1}ep$ também é um idempotente.

No caso em que e é um **idempotente central**, ou seja, $e \in Z(R)$ (centro de R), temos que

$$eRf = Ref = 0 = feR = fRe$$

e a decomposição de Peirce se reduz aos termos $I := eR = eRe$ e $J := fR = fRf$. Temos que I e J são ideais de R, $R = I \oplus J$ e a função $\varphi : R \to I \times J$ dada por $\varphi(x) = (ex, fx)$ é um isomorfismo de anéis. De fato,

a) φ preserva a soma;

b) φ preserva o produto, pois

$$\varphi(xy) = (exy, fxy) = (e^2xy, f^2xy) = (exey, fxfy) = \varphi(x)\varphi(y);$$

c) φ é injetora, pois

$$\varphi(x) = 0 \Rightarrow ex = fx = 0 \Rightarrow 0 = ex + fx = (e + f)x = 1x = x;$$

d) φ é sobrejetora, pois para todos $x, y \in R$ temos

$$\varphi(ex + fy) = (ex, fy).$$

Assim, através de um idempotente central é possível decompor o anel.

Observação 4.7.1. Ao assumir que R é um anel unitário, pudemos tomar o idempotente $f := 1 - e$ e tomar produtos de f com elementos de R. Retirando a hipótese de R ser unitário, e substituindo fx por $x - ex$, fxf por $x - ex - xe + exe$ e outros produtos de maneira similar, os resultados anteriores seguem válidos e em particular a decomposição de Peirce ainda se aplica. Assim, se e é um idempotente central em R, então $I = eR$ e $J = \{x - ex \mid x \in R\}$ são ideais de R tais que

$$R = I \oplus J \cong I \times J.$$

Ao considerar I como anel, temos que e é sua unidade.

Lema 4.7.2. *Seja I um ideal de um anel R. Se I é anel com unidade, então sua unidade e é um idempotente central em R, $I = eR$, e existe um ideal J de R tal que $R = I \oplus J$. Além disso, $R \cong I \times J$.*

Demonstração. Como $e \in I$, temos que $eR \subseteq I$. Por outro lado, $I = eI \subseteq eR$. Assim, $I = eR$. Também, como $ex, xe \in I$ para todo $x \in R$, temos $ex = (ex)e$ e $xe = e(xe)$. Portanto, $ex = xe$ e logo e é um idempotente central. Partindo da Observação 4.7.1, obtemos o resultado desejado. □

4.8 IDEAIS MINIMAIS À ESQUERDA

Nesta seção trataremos de ideais unilaterais, dando preferência a ideais à esquerda.

Definição 4.8.1. Um ideal à esquerda L de um anel R é chamado um **ideal à esquerda minimal** se $L \neq 0$ e L não contém propriamente nenhum ideal à esquerda não nulo de R.

Ideais à direita minimais e **ideais bilaterais minimais** são definidos analogamente.

Exemplo 4.8.2. O único ideal à esquerda minimal de um anel com divisão D é o próprio D.

Exemplo 4.8.3. Seja $R = M_n(D)$, com D um anel com divisão, e seja L o conjunto de matrizes em R que têm entradas arbitrárias na i-ésima coluna e zeros nas outras. Temos que L é um ideal à esquerda minimal de R. De fato, sejam a, b matrizes em L:

$$a = \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ji} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix}, \; b = \begin{pmatrix} 0 & \cdots & 0 & b_{1i} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & b_{ji} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & b_{ni} & 0 & \cdots & 0 \end{pmatrix}.$$

Então

$$a - b = \begin{pmatrix} 0 & \cdots & 0 & a_{1i} - b_{1i} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ji} - b_{ji} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ni} - b_{ni} & 0 & \cdots & 0 \end{pmatrix} \in L.$$

Também, seja r uma matriz qualquer de R. Então

$$ra = \begin{pmatrix} r_{11} & \cdots & r_{1i-1} & r_{1i} & r_{1i+1} & \cdots & r_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ r_{j1} & \cdots & r_{ji-1} & r_{ji} & r_{ji+1} & \cdots & r_{jn} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ r_{n1} & \cdots & r_{ni-1} & r_{ni} & r_{ni+1} & \cdots & r_{nn} \end{pmatrix} \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ji} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & \cdots & 0 & \sum_{k=1}^{n} r_{1k}a_{ki} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \sum_{k=1}^{n} r_{jk}a_{ki} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \sum_{k=1}^{n} r_{nk}a_{ki} & 0 & \cdots & 0 \end{pmatrix} \in L.$$

Vale ressaltar que $L = RE_{ii}$, onde E_{ii} é a matriz canônica usual (com entrada (i,i) igual a 1 e demais entradas iguais a 0), e $E_{ii}RE_{ii} = \{dE_{ii} \mid d \in D\}$ é um subanel com divisão de R isomorfo a D.

Lema 4.8.4. *Se L é um ideal minimal à esquerda de um anel semiprimo R, então existe um idempotente $e \in R$ tal que $L = Re$ e eRe é um anel com divisão.*

Demonstração. Pela existência de L obtemos $R \neq \{0\}$, e pelo fato de R ser semiprimo existem $x, y \in L$ tais que $xy \neq 0$. Desta forma, temos que $Ly \neq 0$. Como Ly é um ideal à esquerda de R, com $Ly \subseteq L$, pela hipótese de minimalidade de L obtemos $Ly = L$. Logo, existe $e \in L$ tal que $ey = y$.

Construa agora o conjunto $J = \{z \in L \mid zy = 0\}$. Ao tomar o elemento $e^2 - e$, vemos que $(e^2 - e)y = e^2y - ey = eey - ey = ey - y = y - y = 0$. Portanto $e^2 - e \in J$. Vemos também que J é um ideal à esquerda de R, com $J \subseteq L$. Como $x \in L \setminus J$, e L é minimal, então $J = 0$. Assim, $e^2 - e = 0$ implica que $e^2 = e$, e portanto e é o idempotente procurado. Já que $e \in L$, temos $Re \subseteq L$, e como $0 \neq e = ee \in Re$, novamente pela minimalidade de L obtemos $L = Re$.

Agora consideremos o corner ring eRe. Seja $a \in R$ tal que $eae \neq 0$. Iremos mostrar que eae tem inverso em eRe. Temos que $0 \neq Reae \subseteq Re = L$, o que implica que $Reae = L$. Assim, para algum $b \in R$, $beae = e$, e também $(ebe)(eae) = ebe^2ae = ebeae = ee = e$. Como ebe é um elemento não nulo de eRe, através de um argumento análogo existe $c \in R$ tal que $(ece)(ebe) = e$. Como o inverso é único, segue que $eae = ece$ é invertível em eRe, e seu inverso é ebe. □

De maneira análoga, o resultado vale para ideais à direita minimais. Vale ressaltar que o Lema 4.8.4 também é válido para ideais à esquerda minimais de álgebras, que são definidos da mesma maneira que ideais minimais de anéis.

Vemos por este resultado que como álgebras não nulas com dimensão finita sempre possuem ideais à esquerda minimais, podemos construir seus respectivos corner rings com

divisão.

O resultado a seguir segue do Lema 4.8.4 aplicado a álgebras.

Corolário 4.8.5. *Se A é uma álgebra semiprima não nula de dimensão finita, então existe um idempotente $e \in A$ tal que eAe é uma álgebra com divisão.*

O seguinte resultado é a "volta"do Lema 4.8.4.

Corolário 4.8.6. *As afirmações seguintes são equivalentes para um idempotente e em um anel semiprimo R:*

a) eRe é um anel com divisão;

b) Re é um ideal minimal à esquerda de R;

c) eR é um ideal minimal à direita de R.

Demonstração. A implicação $b) \Rightarrow a)$ provém do Lema 4.8.4, e a implicação $c) \Rightarrow a)$ se faz por argumentos análogos. Faremos a prova de $a) \Rightarrow b)$ e omitiremos a implicação $a) \Rightarrow c)$, pois a segunda se faz por meio de argumentos análogos.

Seja eRe um anel com divisão e tomemos um ideal à esquerda I de R tal que $0 \neq I \subseteq Re$. Vamos mostrar que $e \in I$, pois assim teremos $I = Re$. Tomemos $0 \neq u \in I$. Como R é semiprimo, temos que $uRu \neq 0$, e portanto $uru \neq 0$ para algum $r \in R$. Como $u \in I \subseteq Re$, $u = ue$ e portanto

$$0 \neq uru = uerue.$$

Assim, $eru = erue$ é um elemento não nulo de eRe. Como eRe é um anel com divisão por hipótese, então existe $v \in R$ tal que $(eve)(eru) = e$. Desta forma, como $eru \in Ru$, temos $e \in Ru \subseteq I$ e segue o resultado desejado.

□

4.9 TEOREMAS DE ESTRUTURA DE WEDDERBURN

Nesta seção, através dos Teoremas de Wedderburn veremos como caracterizar a estrutura das álgebras com dimensão finita. Os teoremas desta seção foram provados pelo matemático escocês Joseph Wedderburn, em 1907.

Teorema 4.9.1 (Teorema de Wedderburn)**.** *Seja A uma álgebra não nula com dimensão finita sobre F. As seguintes afirmações são equivalentes:*

a) A é prima;

b) A é simples;

c) Existe $n \in \mathbb{N}$ e uma álgebra com divisão D tais que $A \cong M_n(D)$.

Demonstração. Para provarmos que b) implica a), sejam I e J dois ideais de A. Como A é simples, segue que $I = 0$ ou $I = A$, sendo que o mesmo vale para J. Se $I = J = A$, então $A^2 = 0$, absurdo pela definição de ser simples. Logo, $I = 0$ ou $J = 0$.

Vimos anteriormente, no Exemplo 3.2.6, que c) implica b).

Resta mostrar que a) implica c). Esta demonstração será feita em partes. Primeiramente, vamos assumir que A é uma álgebra unitária, e faremos indução sobre $d := [A : F]$.

Se $d = 1$, podemos exibir o isomorfismo trivial

$$\varphi : F \to A, \text{ dado por } \varphi(\lambda) = \lambda 1,$$

e desta forma, tomando $n = 1$ e $D = F$, temos $A \cong M_1(F)$.

Se $d > 1$, pelo Corolário 4.8.5 existe um idempotente $e \in A$ tal que eAe é uma álgebra com divisão. Se e é a unidade de A, então o resultado vale para $n = 1$, com $A \cong M_1(A)$. Se e é um idempotente não trivial, podemos tomar o idempotente $f := 1 - e$. Temos então que fAf é uma álgebra prima, não nula, com unidade f. De fato, tomando dois elementos $fxf, fyf \in fAf$,

$$fxffAffyf = 0 \Rightarrow fxfAfyf = 0 \Rightarrow (fxf)(A)(fyf) = 0$$

e, como A é prima por hipótese, segue que $fxf = 0$ ou $fyf = 0$.

Também vemos que $e \notin fAf$, já que, caso contrário, $e = fxf$ para algum $x \in A$ e

$$e = e^2 = efxf = 0$$

o que seria um absurdo. Desta forma, como $fAf \subsetneq A$, $[fAf : F] < d$.

Aplicamos sobre fAf a hipótese de indução: $fAf \cong M_m(D)$ para algum $m \in \mathbb{N}$ e D álgebra com divisão. Desta maneira, fAf contém matrizes canônicas e_{ij}, $i, j = 1, 2, ..., m$, tais que $e_{11}fAfe_{11} = e_{11}Ae_{11}$ é uma álgebra com divisão. O objetivo é estender as matrizes canônicas de fAf para matrizes canônicas de A.

Definimos $n := m + 1$ e $e_{nn} := e$. Assim, $\sum_{i=1}^{n} e_{ii} = f + e = 1$, e $e_{nn}e_{ij} = e_{ij}e_{nn} = 0$ para todos $i, j < n$. Resta-nos encontrar e_{in} e e_{ni}, $i \leq n - 1$. Em outras palavras, resta-nos construir a última linha e a última coluna das matrizes desta álgebra.

Vamos então encontrar e_{1n} e e_{n1}. Temos $e_{11}ae_{nn}a'e_{11} \neq 0$ para alguns $a, a' \in A$. De fato, seja $e_{11}Ae_{nn}Ae_{11}$. Temos que $e_{11}Ae_{nn} \neq 0$, já que A é prima por hipótese e $e_{11}, e_{nn} \neq 0$. Então existe $a \in A$ tal que $e_{11}ae_{nn} \neq 0$. Chamamos este elemento de u. Agora, também temos que $uAe_{11} \neq 0$. Então existe $a' \in A$ tal que $ua'e_{11} \neq 0$, e portanto $e_{11}ae_{nn}a'e_{11} \neq 0$.

Como $e_{11}Ae_{11}$ é uma álgebra com divisão e unidade e_{11}, existe $a'' \in A$ tal que

$$(e_{11}ae_{nn}a'e_{11})(e_{11}a''e_{11}) = e_{11}.$$

Daí, denotando $e_{1n} := e_{11}ae_{nn}$ e $e_{n1} := e_{nn}a'e_{11}a''e_{11}$, temos

$$e_{1n}e_{n1} = e_{11}.$$

Já que $e_{n1} \in e_{nn}Ae_{11}$, temos $e_{n1} = e_{nn}e_{n1}$ e $e_{n1} = e_{n1}e_{11} = e_{n1}e_{1n}e_{n1}$. Assim, vale a premissa e implicação:

$$e_{n1}e_{1n}e_{n1} = e_{nn}e_{n1} \Rightarrow (e_{n1}e_{1n} - e_{nn})e_{n1} = 0.$$

O elemento $(e_{n1}e_{1n} - e_{nn})$ está na álgebra com divisão $e_{nn}Ae_{nn}$. Se ele fosse não nulo, então poderíamos multiplicar a última igualdade (lado direito da última implicação) pelo seu inverso em $e_{nn}Ae_{nn}$, levando a contradição $0 = e_{nn}e_{n1} = e_{n1}$. Portanto,

$$e_{n1}e_{1n} = e_{nn}.$$

Finalmente, definimos $e_{nj} := e_{n1}e_{1j}$ e $e_{jn} := e_{j1}e_{1n}$ para $j = 2, ..., n-1$. Vemos que $e_{ij} = e_{i1}e_{1j}$ e $e_{1j}e_{k1} = \delta_{jk}e_{11}$ são válidos para todos $i, j, k = 1, ..., n$. Desta forma, para todos $i, j, k, l = 1, ..., n$ vale:

$$e_{ij}e_{kl} = e_{i1}e_{1j}e_{k1}e_{1l} = \delta_{jk}e_{i1}e_{11}e_{1l} = \delta_{jk}e_{i1}e_{1l} = \delta_{jk}e_{il}.$$

Portanto e_{ij}, $i, j = 1, ..., n$ são de fato matrizes canônicas de A. Com a Proposição 4.6.3 e a Observação 4.6.4 obtemos a conclusão desejada, $A \cong M_n(D)$, onde $D = e_{11}Ae_{11}$.

Por fim, resta mostrar que a) implica c) sem a suposição de que A é unitária. Vamos supor que A é prima e não unitária. Pelo Lema 4.3.4, $A^{\#}$ é uma álgebra prima e unitária. Como a) implica c) (e portanto b)) para todas álgebras unitárias, segue que $A^{\#}$ é simples. Porém, isto é uma contradição já que A é um ideal próprio não nulo de $A^{\#}$. □

Podemos adicionar ao Teorema 4.9.1 o fato de que D também tem dimensão finita, e que $[A : F] = n^2[D : F]$.

Vale observar que álgebras primas de dimensão finita coincidem com álgebras simples de dimensão finita. De modo geral, a classe de álgebras primas é muito maior do que a classe de álgebras simples.

Outra observação é a de que a restrição à álgebras de dimensão finita é necessária. A Álgebra de Weyl é um exemplo de uma álgebra que é um domínio simples, porém não é uma álgebra com divisão, veja o Exemplo 4.2.13.

Corolário 4.9.2. *Uma álgebra de dimensão finita A é uma álgebra central simples se, e somente se, existe $n \in \mathbb{N}$ e uma álgebra central com divisão D tal que $A \cong M_n(D)$.*

Demonstração. No que se refere a implicação, sendo A simples, obtemos que $A \cong M_n(D)$ para alguma álgebra com divisão D, veja o último teorema. Sendo A central, do Lema 3.3.3 obtemos que D é central. Para a recíproca usamos os mesmos resultados. □

Corolário 4.9.3. *A dimensão de uma álgebra central simples com dimensão finita é um quadrado perfeito.*

Demonstração. Seja A uma álgebra central simples sobre F. Como $A \cong M_n(D)$ para alguma álgebra com divisão D, temos que $[A:F] = n^2[D:F]$. Pelo Corolário 3.6.4, como D é com divisão, $[D:F] = [K:F]^2$, para um subcorpo maximal K de D. Logo, $[A:F] = n^2[K:F]^2 = (n[K:F])^2$, que é um quadrado perfeito. □

O produto direto de álgebras primas é uma álgebra semiprima, como podemos ver no Exemplo 4.2.18. O resultado a seguir mostra que todas as álgebras semiprimas têm esta estrutura.

Teorema 4.9.4 (Wedderburn)**.** *Seja A uma álgebra não nula com dimensão finita. Então A é semiprima se, e somente se, existem $n_1, n_2, ..., n_r \in \mathbb{N}$ e álgebras com divisão $D_1, D_2, ..., D_r$ tal que $A \cong M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_r}(D_r)$.*

Demonstração. Como cada D_i é uma álgebra com divisão, temos que cada $M_{n_i}(D_i)$ é simples, e em particular semiprima. Como visto no Exemplo 4.2.18, o produto direto de álgebras semiprimas é semiprimo.

No que se refere a implicação, faremos a demonstração por indução em $d = [A:F]$. Se $d = 1$, então $A = Fa$ para algum $a \in A$, e $a^2 \neq 0$. Assim, a^2 é da forma λa, com $\lambda \neq 0$, de modo que $\lambda^{-1}a$ é a unidade de A. Portanto, $A \cong F$. Seja agora $d > 1$. Se A é prima, o resultado segue do Teorema 4.9.1. Iremos assumir então que existe $0 \neq a \in A$ tal que $I = \{x \in A \mid aAx = 0\}$ é um conjunto não nulo. Como I é um ideal de A, também é uma álgebra semiprima (de acordo com a Observação 4.2.10). Como $a \notin I$, temos $[I:F] < d$. Pela hipótese de indução,

$$I \cong M_{n_1}(D_1) \times \cdots \times M_{n_p}(D_p)$$

para alguns $n_i \in \mathbb{N}$ e álgebras com divisão D_i, $i = 1, ..., p$. Como cada fator $M_{n_i}(D_i)$ do produto tem unidade, então I também tem. Pelo Lema 4.7.2, existe um ideal J de A tal que $A \cong I \times J$. Aplicando a hipótese de indução em J, obtemos que $J \cong M_{n_{p+1}}(D_{p+1}) \times \cdots \times M_{n_r}(D_r)$ para alguns $n_i \in \mathbb{N}$ e álgebras com divisão D_i, $i = p+1, ..., r$. Segue o resultado. □

O Teorema 4.9.4 mostra, em particular, que uma álgebra não nula semiprima com dimensão finita automaticamente é unitária.

Outra denominação para álgebras semiprimas com dimensão finita é **álgebras semisimples**. Desta forma, o Teorema 4.9.4 pode ser enunciado da seguinte forma:

$$A \text{ é semisimples} \iff A \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r).$$

Se uma álgebra A com dimensão finita possui ideais nilpotentes não nulos, então podemos tomar o quociente de A pelo seu radical e obter uma álgebra semiprima, veja o Lema 4.2.11. Isto implica no seguinte resultado:

Teorema 4.9.5. *Seja A uma álgebra com dimensão finita. Se N é seu radical e $A \neq N$, então*

$$\frac{A}{N} \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$$

para alguns $n_1, ..., n_r \in \mathbb{N}$ e álgebras com divisão $D_1, ..., D_r$.

4.10 ÁLGEBRAS SOBRE CORPOS ESPECIAIS

Nesta seção, aplicaremos os teoremas de Wedderburn a álgebras sobre certos corpos.

Começaremos com corpos algebricamente fechados. O seguinte resultado foi provado pelo matemático russo Theodor Molien, em 1892, para $F = \mathbb{C}$.

Corolário 4.10.1 (Molien)**.** *Seja A uma álgebra não nula semiprima de dimensão finita sobre um corpo algebricamente fechado F. Então $A \cong M_{n_1}(F) \times \cdots \times M_{n_r}(F)$ para alguns $n_1, ..., n_r \in \mathbb{N}$. Além disso, se A é prima, então $r = 1$.*

Demonstração. Pelo Teorema 4.9.4, temos que $A \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ para algumas álgebras com divisão $D_1, ..., D_r$. A Proposição 3.1.8 implica que, como cada D_i é uma álgebra sobre F e F é algebricamente fechado, então $D_1 = \cdots = D_r = F$. Se A é prima, o resultado segue do Teorema 4.9.1, ou seja, $A \cong M_n(F)$ e logo $r = 1$. □

O próximo resultado irá combinar o Corolário 4.10.1 com o Teorema de Maschke 4.5.4. Dado um grupo finito G, podemos construir a álgebra grupo $F[G]$. Se $F = \mathbb{C}$, então F é um corpo algebricamente fechado de $\text{char}(F) = 0$. Logo, $F[G]$ é semiprima e segue o resultado abaixo.

Corolário 4.10.2. *Se G é um grupo finito, então existem $n_1, ..., n_r \in \mathbb{N}$ tais que*

$$\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}).$$

Este resultado mostra que, ao tomar um grupo arbitrário G finito, seu elementos podem ser interpretados como r-uplas de matrizes com entradas em $\mathbb{C}$.

Exemplo 4.10.3. Consideremos a álgebra grupo $\mathbb{C}[S_3]$, onde S_3 é o grupo simétrico de $\{1, 2, 3\}$. Encontraremos os números $n_1, \ldots, n_r \in \mathbb{N}$ tais que $\mathbb{C}[S_3] \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$. Temos

$$6 = 3! = |S_3| = [\mathbb{C}[S_3] : \mathbb{C}] = [M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C}) : \mathbb{C}] = \sum_{i=1}^{r} n_i^2.$$

Além disso, ao menos um n_i deve ser diferente de 1, já que $\mathbb{C}[S_3]$ não é comutativo. A única possibilidade é que $\mathbb{C}[S_3] \cong M_2(\mathbb{C}) \times \mathbb{C} \times \mathbb{C}$.

Os próximos resultados são referentes a álgebras simples.

Corolário 4.10.4. *Uma $\mathbb{R}$-álgebra simples com dimensão finita A é isomorfa a $M_n(\mathbb{R})$, $M_n(\mathbb{C})$ ou $M_n(\mathbb{H})$, para algum $n \in \mathbb{N}$.*

Demonstração. Como A é simples, pelo Teorema 4.9.4 temos que $A \cong M_n(D)$ para algum n natural e alguma álgebra com divisão D de dimensão finita sobre $\mathbb{R}$. Pelo Teorema 3.1.5 temos que D é isomorfa a $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, e segue o resultado. □

Em relação ao Corolário 4.9.2 e Corolário 3.3.7, obtemos o seguinte resultado.

Corolário 4.10.5. *Uma $\mathbb{R}$-álgebra central simples com dimensão finita é isomorfa a $M_n(\mathbb{R})$ ou $M_n(\mathbb{H})$ para algum $n \in \mathbb{N}$.*

Corolário 4.10.6. *Um anel R simples e finito é isomorfo a $M_n(F)$ para algum $n \in \mathbb{N}$ e algum corpo finito F.*

Demonstração. Como visto na Observação 4.2.5, $\text{char}(R)$ é um número primo p, e podemos considerar R como uma álgebra sobre $\mathbb{Z}_p$. Pelo Teorema 4.9.1, temos que $R \cong M_n(D)$, onde D é uma álgebra com divisão de dimensão finita sobre $\mathbb{Z}_p$. Por fim, pelo Teorema 3.7.1, como D é um anel com divisão finito, D é um corpo. □

Através dos exemplos vistos nesta seção, pudemos observar que os Teoremas de Wedderburn reduzem o problema de classificar F-álgebras (semi)primas com dimensão finita a classificar F-álgebras com divisão com dimensão finita.

REFERÊNCIAS

BRESAR, M. **Introduction to Noncommutative Algebra**. [S.l.]: Springer, 2014. (Universitext). ISBN 978-3-319-08692-7. Citado 3 vezes nas páginas 8, 41 e 45.

GAUSS, C. F. 1808. Carta à Bolyai. Disponível em: <https://mathshistory.st-andrews.ac.uk/Biographies/Gauss/quotations/>. Citado na página 4.