Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Uma Classificação das Álgebras Graduadas Simples de Dimensão Finita por Identidades Polinomiais

por

Renato de Melo Filho [†]

sob orientação do

Prof. Dr. Diogo Diniz Pereira da Silva e Silva

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

[†]Este trabalho contou com apoio financeiro da CAPES por meio do programa PICME

M528c Melo Filho, Renato de.
Uma classificação das álgebras graduadas simples de dimensão finita por identidades polinomiais / Renato de Melo Filho. – Campina Grande, 2019.
73 f.

Dissertação (Mestrado em Matemática) – Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia, 2018.
"Orientação: Prof. Dr. Diogo Diniz Pereira da Silva e Silva".
Referências.

1. Álgebras graduadas simples. 2. Identidades polinomiais. 3. Álgebras graduadas. I. Silva, Diogo Diniz Pereira da Silva e. II. Título.

CDU 512(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA MARIA ANTONIA DE SOUSA CRB 15/398

Uma Classificação das Álgebras Graduadas Simples de dimensão finita por Identidades Polinomiais

por

Renato de Melo Filho

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

Área de Concentração: Matemática

Aprovada por:

Prof. Dr. Dimas José Gonçalves

Prof. Dr. Antônio Pereira Brandão Júnior

Prof. Dr. Diogo Diniz Pereira da Silva e Silva

Orientador

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Fevereiro de 2019

Agradecimentos

Poderá uma seção exceder o tamanho total do texto? Pois é o que me vem à mente ao pensar em todas as pessoas a quem devo agradecer por esta realização. Em primeiro lugar, Deus Pai, Filho e Espírito Santo e as intercessões de todos os Santos e irmãos do Corpo de Cristo, em particular à Virgem Santíssima. Depois ao sólido apoio sempre presente e contínuo da minha família, em especial minha mãe Maria do Socorro Pereira Marinho, que sempre sacrificou a si mesma pelo meu bem, e me permitiu estudar até este nível. Agradeço ao meu pai José Renato de Melo e aos meus irmãos Robson de Mélo e José Rellisson de Melo. Ainda entre minha família gostaria de agradecer a Severina Alves de Melo (in Memoriam) avó paterna que me criou durante certo período e aos meus tios Osmar Pereira Marinho (in Memoriam) e Francisco de Assis Pereira Marinho (in Memoriam), dois homens que perderam a vida prematuramente mas deixaram seu exemplo, um deles sendo vitimado no serviço à sociedade.

Tenho na universidade muitos amigos, cada um com sua contribuição. Sinto que sem eles nada disso seria possível. Alguns foram presentes durante o mestrado, outros, antes, na graduação e outros desde o Ensino Médio. Em primeiro lugar agradeço ao professor Diogo, que aceitou me orientar e dedicou bastante do seu tempo para nossas conversas. Agradeço a todos os professores que me deram aula no mestrado, os professores Claudemir, Antônio Brandão, Alânnio, Henrique e Marco Aurélio, do PPGMat-UFCG e ainda o Professor Antônio Ronaldo Gomes Garcia, que nos introduziu as belíssimas Álgebras de Colombeau, então bolsista de pós doutorado. Agradeço aos professores Dimas José Gonçalves e Antônio Brandão por aceitarem participar da banca e pelas suas valiosas contribuições que enriqueceram o texto. Muitos professores me ajudaram direta e indiretamente nesta fase, mas não posso deixar de citar especialmente os professores Daniel, Fábio, Romildo, Claudianor, José Luís e a professora Itailma.

Além dos professores, tenho agradecimentos aos funcionários da UAMat, que algumas vezes resolvem nossos problemas burocráticos, e muitas vezes alegram nosso dia com sua simpatia, fidelidade ao trabalho e alegria de sempre. Especialmente Andreza, Ana, Sóstenes, Renato, David, Dalvanira e Gislaine.

Por fim presto gratidão a todos os meus amigos mestrandos e doutorandos que compartilharam esta jornada. Em primeiro lugar, aos meus companheiros de mestrado, os que entraram comigo no mesmo semestre, Roseane da Silva Martins, uma baiana guerreira e o querido Pedro Fellype da Silva Pontes. Juntos, nós enfrentamos os primeiros semestres de disciplinas básicas como um verdadeiro time. Também cito os demais colegas de mestrado de semestres subsequentes, o meu amigo de Ensino Médio Wallace Ferreira Gomes, que também contribuiu bastante para o nosso time, o meu amigo de discussões filosóficas e teológicas, Ismael Sandro da Silva, e o "lendário" Caio Anthony Gomes de Matos Andrade. Também cito a segunda baiana guerreira Geisa Gama Oliveira. Além destes, há os doutorandos Geovany Fernandes Patricio, Franciélia Limeira de Sousa, Laise Dias Alves Araújo, Felipe Barbosa Cavalcante e André Felipe Araújo Ramalho. Há muitos que eu gostaria de citar, mas o espaço não permite. Sou grato pela passagem de cada um de vocês na minha vida neste período. Obrigado!

Dedicatória

A Jesus Ressuscitado.

Resumo

Dissertamos sobre as álgebras graduadas simples de dimensão finita sobre um corpo algebricamente fechado e as classificamos de acordo com suas identidades polinomiais. Em outras palavras, mostraremos que duas álgebras graduadas nestas condições são isomorfas se, e somente se, satisfazem as mesmas identidades polinomiais. Trazemos o conteúdo que lhe é necessário, que são as noções básicas de álgebras graduadas e de identidades polinomiais, uma demonstração do Teorema de Amitsur-Levitski e ainda uma do Teorema de Wedderburn-Artin.

Abstract

We have discussed the finite-dimensional graded simples algebras over an algebraically closed field and classify them according to their polynomial identities. In other words, we will show that two graded algebras under these conditions are isomorphic if and only if they satisfy the same polynomial identities. We bring out the content that is needed, which are the basics of graded algebras and polynomial identities, a demonstration of Amitsur-Levitski's Theorem and still one of Wedderburn-Artin's Theorem.

Conteúdo

Introdução 6

1 Prolegômenos **9**

1.1 Grupos e Anéis 9

1.1.1 Permutações 12

1.2 Álgebras 13

1.2.1 Graduação Elementar da Álgebra Matricial 19

1.2.2 Álgebras de Grupo *Twisted* 20

1.2.3 Módulos Graduados 22

1.2.4 Produto Tensorial 24

1.3 Identidades Polinomiais 30

1.4 O Teorema de Amitsur-Levitski 33

2 Álgebras Graduadas Simples e Identidades Polinomiais Graduadas **40**

2.1 Sobre Álgebras Graduadas Simples de Dimensão Finita 40

2.2 Classificação das Álgebras Graduadas Simples de Dimensão Finita . . . 48

2.3 Uma Condição para que Duas Álgebras Graduadas Simples de Dimensão Finita sejam Isomorfas 54

A Semissimplicidade de anéis e o Teorema de Wedderburn-Artin **61**

Bibliografia **72**

Introdução

A área de álgebra, na Matemática, é a disciplina cujos objetos de estudo são as estruturas algébricas, que são conjuntos nos quais se pode observar alguma relação entre seus elementos. Num primeiro curso de álgebra, muitas vezes chamado, não por acaso, de "estruturas algébricas", o aluno é apresentado ao mundo das estruturas mais simples, os Monóides e os Grupos, e, a partir destes, também se estudam os anéis. Naturalmente, apenas algumas propriedades mais básicas destas estruturas são apresentadas no primeiro contato, o suficiente para indicar a vastidão do que já se conhece e também para se ter um vislumbre da gigante floresta que ainda há para se explorar na pesquisa científica destes objetos matemáticos.

À medida em que as propriedades das estruturas algébricas se tornam conhecidas, elas passam a incorporar o leque das ferramentas matemáticas e, a partir daí, ficam disponíveis também para outras áreas e ciências. Neste sentido, pode-se dizer que um pesquisador de álgebra é um fabricante de ferramentas para as ciências exatas. Um exemplo célebre de estrutura cujas propriedades são amplamente difundidas é a de espaço vetorial, cujo estudo é fundamental para a maior parte das ciências exatas, ferramenta básica para qualquer pesquisador de Matemática, Física, Química, Engenharias, Ciências da Computação, entre outras.

Uma álgebra é um espaço vetorial onde, além da soma e produto por escalares naturais do espaço, observa-se ainda um produto entre os vetores. Uma álgebra graduada, no nosso caso álgebra graduada por um grupo, é uma decomposição em subespaços vetoriais indexados pelos elementos do grupo, que ocorre na forma de uma soma direta dos subespaços. Assim como existem subespaços, também observamos subálgebras. Se um subespaço da álgebra tem a propriedade absorvente para a multiplicação entre

vetores, então a chamamos de ideal, análogo aos ideais de anéis. Ora, se uma álgebra graduada não possui ideais graduados não triviais, dizemos que ela é simples. A pergunta (e resposta) que nos traz o artigo [13] é sobre a classificação de todas as álgebras graduadas simples possíveis de acordo com suas identidades polinomiais.

Na verdade, é conhecido o resultado chamado de Teorema de *Wedderburn-Artin* que classifica anéis semissimples à esquerda (que demonstraremos no Apêndice) e, particularmente, classifica anéis simples que contêm um ideal à esquerda minimal. Tais resultados são uma motivação para a nossa referência principal.

Entretanto, nada disso seria possível sem o desenvolvimento histórico do estudo das álgebras com identidades polinomiais. Dada uma álgebra e um polinômio não nulo, se para qualquer avaliação por elementos da álgebra o polinômio zera, então o chamamos de identidade polinomial e dizemos que tal álgebra é uma PI-álgebra. Esta sigla PI vem do inglês *polinomial identities* e, nada mais significa, do que álgebra com identidades polinomiais. Podemos apreender de maneira mais clara a utilidade de estudar identidades polinomiais para álgebras considerando, por exemplo, que uma álgebra é comutativa se, e somente se, satisfaz o polinômio $f(x, y) = xy - yx$. Assim, torna-se claro que as identidades podem trazer à tona informações valiosas da álgebra em questão.

Podemos colocar um marco zero na história das identidades polinomiais em 1948, quando o canadense Irving Kaplansky publicou seu artigo [12] classificando um conjunto especial, as PI-álgebras primitivas. Mas o artigo que fertilizou nossa referência principal foi publicado em 1950 pelos matemáticos israelenses Shimshon Avraham Amitsur e Yaakov Levitsky, que provaram que a álgebra das matrizes $n \times n$ satisfaz a identidade *standard* de grau $2n$. Todas as classificações que citamos utilizam direta ou indiretamente álgebras de matrizes e daí percebe-se a importância deste resultado.

Nesta dissertação tomamos como base o artigo [13], publicado em 2010, *Identities and isomorphisms of graded simple algebras*, ou, numa tradução livre, Identidades e isomorfismos de álgebras graduadas simples, do búlgaro Plamen Koshlukov em parceria com o russo Mikhail Zaicev, o qual apresenta uma classificação das álgebras graduadas simples utilizando resultados provenientes do estudo das identidades polinomiais. O nosso objetivo é expor a classificação para álgebras graduadas simples a partir de suas identidades polinomiais e trazer os resultados que são necessários para o entendimento

dele e de sua demonstração. Também trazemos um tópico que não é necessário para o entendimento do artigo, mas que pode ser relevante para auxiliar o entendimento do leitor, já que se trata de um caso particular e historicamente anterior, que é o Teorema de Wedderburn-Artin.

O texto foi dividido em três partes, que são os prolegômenos, o primeiro capítulo, que trata de todos os assuntos subjacentes ao nosso objetivo principal, o segundo com o cumprimento deste objetivo e, por fim, o apêndice, que traz uma motivação natural para o artigo que tomamos como referência principal.

Recomendamos para uma leitura proveitosa desta dissertação conhecimentos básicos de grupos, anéis e espaços vetoriais. Caso se faça necessário, recomendamos [10] para os primeiros e o premiado [15] para os espaços vetoriais.

Capítulo 1

Prolegômenos

Buscamos na composição e organização desta dissertação um equilíbrio entre o volume, quantidade de texto e autossuficiência de conteúdos, de modo que um aluno de nível superior de matemática, próximo ao final de seu curso, encontre neste capítulo a maior parte do que é necessário para o estudo que faremos das Álgebras Graduadas Simples. Algumas seções são, porém, introduções de assuntos mais gerais, como as permutações e os produtos tensoriais, mas que são necessários para as construções mais avançadas que utilizamos no decorrer do texto.

1.1 Grupos e Anéis

Definiremos e elencaremos algumas propriedades que nos serão úteis das estruturas algébricas mais simples.

Definição 1.1 *Seja G um conjunto não vazio juntamente com uma operação binária $+ : G \times G \to G$. Dizemos que $(G, +)$, ou, simplesmente, G é um grupo se a operação $+$ for associativa, existir elemento neutro e todo elemento possuir oposto. Em outras palavras,*

i) $(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$, *para quaisquer* $g_1, g_2, g_3 \in G$;

ii) Existe um elemento $e \in G$ *tal que* $g + e = g = e + g$, *para qualquer* $g \in G$;

iii) Para cada $g \in G$ *existe* $-g \in G$ *tal que* $g + (-g) = (-g) + g = e$.

Se um grupo for comutativo, ou seja, se, dados $g, h \in G$ vale $g + h = h + g$ então dizemos que o grupo é abeliano.

Exemplo 1.2

i) O conjunto dos números inteiros $\mathbb{Z}$ com a operação de adição é um grupo abeliano.

ii) O conjunto das matrizes $M_2(\mathbb{R})$ não é um grupo, se considerada a multiplicação usual de matrizes, pois a matriz E_{11}, por exemplo, não possui inverso. No entanto, o seu subconjunto $GL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid det(A) \neq 0\}$ munido com a multiplicação usual de matrizes é um grupo não abeliano. Exemplos de matrizes de $GL_2(\mathbb{R})$ que não comutam são $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ e $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Podemos definir o que significa ng para $n \in \mathbb{Z}$ e $g \in G$. Se $n = 1$, $ng := g$. Se $n > 1$ então $ng := \underbrace{g + g + \cdots + g}_{n \text{ parcelas}}$ e, por outro lado, se $n < 1$, então $ng := -n(-g)$. Se um grupo G for finito, chamamos o número de elementos de ordem do grupo. Dizemos que um grupo G é cíclico quando ele é gerado por apenas um elemento, ou seja, quando existe $g \in G$ tal que para qualquer $h \in G$, existe $n \in \mathbb{Z}$ com $h = ng$. Neste caso escrevemos $G = \langle g \rangle$. Assim, trazemos uma classificação para os grupos abelianos finitos em termos de decomposição em grupos cíclicos. Esse fato segue do Teorema Fundamental dos Grupos Abelianos Finitamente Gerados, que pode ser encontrado, por exemplo, como Teorema 11.12 da referência [10].

Devemos também recordar que dados G, H grupos, o produto direto $G \times H$ é o conjunto cujos elementos são pares ordenados (g, h) tais que $g \in G, h \in H$ e que esse conjunto munido da operação $(g_1, h_1) + (g_2, h_2) := (g_1 + g_2, h_1 + h_2)$ é um grupo.

Teorema 1.3 *Todo grupo abeliano finito é isomorfo a um produto direto de grupos cíclicos, e as ordens de cada um destes grupos é uma potência de um número primo. Além disso, a menos da posição dos fatores, esta decomposição é única.*

Utilizamos, até este ponto, a notação aditiva para os grupos para os utilizar na definição dos anéis. Porém, no decorrer do texto preferimos, como é mais comum na literatura, o uso da notação multiplicativa. Em vez de $g + h$, escrevemos gh e, em vez de ng, com $n \in \mathbb{Z}$, escrevemos g^n, para $g, h \in G$.

Definição 1.4 *Dado $(A, +)$ um grupo abeliano onde existe uma operação binária $\cdot : A \times A \to A$, chamamos $(A, +, \cdot)$, ou simplesmente A, de anel se para todos $a, a_1, a_2, a_3 \in A$ valem as propriedades:*

i) $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$;

ii) $a \cdot (a_1 + a_2) = (a \cdot a_1) + (a \cdot a_2)$;

iii) $(a_1 + a_2) \cdot a = (a_1 \cdot a) + (a_2 \cdot a)$.

Geralmente, por simplicidade, omitimos " $\cdot$ " e escrevemos ab em vez de $a \cdot b$. Dizemos ainda que A é um anel unitário se existe $1_A \in A$ tal que $a1_A = a = 1_A a$, para todo $a \in A$, que A é comutativo se $ab = ba$, para todos $a, b \in A$ e que A é um anel com divisão se todo elemento diferente do neutro da adição (também denotado por 0_A e chamado de zero) possui inverso multiplicativo. Em outras palavras, dado $a \in A \setminus \{0_A\}$, existe $a^{-1} \in A$ tal que $aa^{-1} = 1_A = a^{-1}a$.

Exemplo 1.5 *Um exemplo de anel comutativo e com unidade é o conjunto* $\mathbb{Z}$ *dos números inteiros munido de sua adição e multiplicação usuais. Um exemplo de anel comutativo com unidade e com divisão é o conjunto* $\mathbb{Q}$ *dos números racionais também munido de suas operações usuais de adição e multiplicação. Por fim, um exemplo de anel com unidade mas não comutativo é o conjunto* $M_n(\mathbb{R})$ *das matrizes* $n \times n$ *com entradas reais com as operações de adição e multiplicação de matrizes, onde* $n \geq 2$. *De fato, tal anel não é comutativo, pois* $E_{11}E_{12} = E_{12} \neq 0 = E_{12}E_{11}$, *onde* E_{ij} *representa a matriz elementar que tem* 1 *na entrada* ij *e* 0 *nas demais, para quaisquer* $i, j \in \{1, \ldots, n\}$.

Se $\mathbb{F}$ é um anel comutativo e com divisão, então dizemos que $\mathbb{F}$ é um corpo. Escolhemos esta notação por remeter à palavra em inglês para corpo, *field*.

Definição 1.6 *Seja* A *um anel. Dizemos que* A *tem característica positiva se existe* $n \in \mathbb{N}$ *tal que* $na = 0$, *para qualquer* $a \in A$. *Definimos a característica de* A *pondo*

$$char(A) := min\{n \in \mathbb{N} \mid na = 0, \forall a \in A\}.$$

Caso contrário, ou seja, se não existe tal n, *então dizemos que* A *tem característica zero, e denotamos* $char(A) := 0$

Exemplo 1.7 *O corpo* $\mathbb{Z}_2 = \{0, 1\}$, *tal que* $1 + 1 = 0$, 0 *é o neutro da adição e* 1 *é o neutro da multiplicação é um exemplo de corpo cuja característica é positiva, com* $char(\mathbb{Z}_2) = 2$.

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

Definição 1.8 *Dados* G *um grupo e* A *um anel, dizemos que* A *é um anel* G*-graduado quando* $A = \oplus_{g \in G} A_g$, *onde para cada* $g \in G$, A_g *é um subgrupo do grupo aditivo de* A *e, para todos* $g, h \in G$, *temos* $A_g A_h \subseteq A_{gh}$.

Exemplo 1.9 *Considere o anel* $A = \mathbb{F}[x_1, x_2, \ldots, x_k]$ *dos polinômios nas variáveis* $x_1, \ldots, x_k$ *e o grupo* $\mathbb{Z}$. *A é um anel* $\mathbb{Z}$*-graduado, pois podemos escrever* $A = \oplus_{n=1}^{\infty} A_n$, *onde, para cada* $n \in \mathbb{N}$, A_n *é o conjunto dos polinômios tais que os seus monômios possuem o mesmo número* n *de variáveis (contando também as potências), e para* $n \leq 0$ $A_n = 0$.

1.1.1 Permutações

Uma permutação é uma bijeção de um conjunto em si mesmo e é um exemplo célebre de grupo, cuja importância é ressaltada pelo conhecido Teorema de Cayley [10]. No nosso caso, definiremos apenas permutações em conjuntos finitos e, na verdade, apenas em subconjuntos de números naturais, visto que dado um conjunto U com n elementos, existe uma bijeção entre U e o subconjunto dos números naturais $I_n = \{1, 2, \cdots, n\}$, para algum $n \in \mathbb{N}$. No nosso caso não fará diferença se utilizamos U ou I_n e, portanto, utilizaremos I_n.

Definição 1.10 *Uma permutação em* I_n *é uma função bijetora de* I_n *em* I_n. *Denotamos o conjunto destas permutações por* S_n. *A identidade será denotada por* Id_n.

A notação para as permutações que utilizaremos posteriormente considera se determinada permutação fixa um elemento ou outro. Por exemplo, a permutação Id_n fixa todos os elementos. Por outro lado, a permutação

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 4 & 2 & 7 & 6 \end{pmatrix}$$

fixa apenas 1 e 4. Os números fixados não aparecerão na notação, mas perceba que $\sigma(2) = 3, \sigma(3) = 5$ e $\sigma(5) = 2$. Chamamos o conjunto destes três elementos de órbita e a denotamos (2 3 5). Poderia também ser (3 5 2) ou (5 2 3), importando apenas que o número sucessor seja imagem do anterior pela permutação. Ainda na permutação σ há a órbita (6 7). Uma órbita com apenas dois elementos, como (6 7), é também chamada de 2-ciclo, ou de transposição. As informações sobre esta permutação podem ser sumarizadas: σ fixa os elementos $1, 4$ e possui duas órbitas disjuntas (2 3 5) e (6 7). Uma maneira adequada para denotar σ é (2 3 5)(6 7).

Esta maneira de descrever uma permutação é adequada pois duas órbitas são disjuntas ou iguais. De fato, sejam $(i_1\ i_2\ \cdots\ i_n)$ e $(j_1\ j_2\ \cdots\ j_m)$ duas órbitas distintas

de uma permutação τ. Suponhamos que existem i_r, j_s com $i_r = j_s$. Por um comentário anterior, podemos supor, sem perda de generalidade, que $r = 1 = s$ e, assim, $i_1 = j_1$. Ora, sabemos que $i_2 = \tau(i_1) = \tau(j_1) = j_2$ e, analogamente, $i_r = j_s$, para todo r. Se $n < m$, então $j_1 = i_1 = \tau(i_n) = \tau(j_n) = j_{n+1}$, um absurdo, pois não repetimos elementos na notação. Segue que $n = m$. Portanto, as duas órbitas são representadas com os mesmos elementos nas mesmas posições, de onde segue que elas são, na verdade, iguais. Contrapositivamente, se duas órbitas são distintas, então elas são disjuntas.

Mais ainda, lembrando da operação de composição de funções, podemos denotar $(i_1\ i_2\ \cdots\ i_n) \circ (j_1\ j_2\ \cdots\ j_m)$ simplesmente por $(i_1\ i_2\ \cdots\ i_n)(j_1\ j_2\ \cdots\ j_m)$. Não é difícil ver que $(i_1\ i_2\ i_3\ \cdots\ i_n) = (i_1\ i_n)\cdots(i_1\ i_3)(i_1\ i_2)$, e portanto podemos modificar nossa notação de σ escrevendo $(2\ 5)(2\ 3)(6\ 7)$, mostrando que toda permutação pode ser escrita como produto de transposições. Um fato básico da teoria de permutações é que a paridade do número destas transposições é único para cada permutação, o que nos permite enunciar a definição que se segue.

Definição 1.11 *Dizemos que uma permutação $\sigma \in S_n$ é par se puder ser escrita como produto de um número par de transposições. Neste caso, denotamos $(-1)^\sigma := 1$. Caso contrário dizemos que σ é ímpar e escrevemos $(-1)^\sigma := -1$.*

Exemplo 1.12 *A permutação identidade é par, para qualquer n. A permutação $(2\ 5)(2\ 3)(6\ 7)$ é ímpar.*

É possível mostrar que o conjunto das permutações com a operação de composição é um grupo e possui importantes propriedades. Uma delas é que o conjunto das permutações pares é de igual número ao das permutações ímpares. De fato, fixados $i < j \in I_n$ a função f cujo domínio é conjunto das permutações pares definida por $f(\sigma) = (i\ j)\sigma$ é uma bijeção entre as permutações pares e as ímpares. Como no nosso caso o conjunto das permutações pares é finito, segue que eles têm o mesmo número de elementos.

1.2 Álgebras

Os objetos mais importantes desta dissertação são as álgebras e, em especial, as álgebras graduadas por um grupo. Deste modo, trazemos nesta seção algumas definições, propriedades e exemplos desta teoria que julgamos imprescindíveis para o

estudo a que nos destinamos. Levamos em consideração que o conhecimento, ainda que superficial, dos espaços vetoriais é um pré-requisito ao nosso público alvo, já que as álgebras são casos particulares daquelas estruturas.

Definição 1.13 *Seja $\mathbb{F}$ um corpo. Dizemos que um $\mathbb{F}$-espaço vetorial A com uma operação binária $* : A \times A \to A$, chamada multiplicação, é uma $\mathbb{F}$-álgebra, ou simplesmente, álgebra, se para quaisquer $a, b, c \in A$ e $\alpha \in \mathbb{F}$ valem:*

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

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

iii) $\alpha(a * b) = (\alpha a) * b = a * (\alpha b)$.

Exemplo 1.14 *O conhecido espaço vetorial $\mathbb{R}^3$ dos vetores tridimensionais é uma álgebra se considerarmos o produto vetorial. Dado $\mathbb{F}$ um corpo, o conjunto das matrizes $M_n(\mathbb{F})$ com a soma, multiplicação por escalar e multiplicação de matrizes usuais é uma $\mathbb{F}$-álgebra.*

Dado um subconjunto $\beta \subset A$, dizemos que β é uma base para a álgebra A se é uma base para o espaço vetorial A e a dimensão da álgebra A é a dimensão do espaço A. No exemplo anterior, uma base para a álgebra $\mathbb{R}^3$ é a canônica $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ e para o conjunto das matrizes $M_n(\mathbb{F})$, temos a base formada pelas já mencionadas matrizes elementares

$$\{E_{11}, \ldots, E_{1n}, E_{21}, \ldots, E_{2n}, \ldots, E_{n1}, \ldots, E_{nn}\}.$$

Dizemos que uma álgebra A é:

i) Associativa, se $(ab)c = a(bc)$, para quaisquer $a, b, c \in A$;

ii) Unitária, se existe um elemento $1_A \in A$ tal que $1_A a = a = a1_A$, para todo $a \in A$;

iii) Comutativa, se $ab = ba$, para todos $a, b \in A$.

iv) De divisão (ou com divisão), se A é unitária e, para todo $a \in A \setminus \{0\}$, existe $a^{-1} \in A$ tal que $aa^{-1} = 1_A = a^{-1}a$.

Definição 1.15 *Dado $S \subset A$ um subespaço vetorial, dizemos que S é uma subálgebra de A se para quaisquer $a, b \in S$, temos $ab \in S$. Se A for unitária acrescentamos a condição $1_A \in S$ para que S seja subálgebra. Dado $I \subset A$ um subespaço vetorial, chamamos I de ideal de A se dados $r \in I$ e $a \in A$, temos $ar \in I$ e $ra \in I$. Analogamente, podemos definir ideal à direita se $ra \in I$ e ideal à esquerda se $ar \in I$.*

Dizemos que uma álgebra R satisfaz a condição de cadeia descendente para ideais à esquerda se toda cadeia descendente de ideais à esquerda é estacionária. Isto é, se para cada cadeia

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots$$

de ideais à esquerda existe $m \in \mathbb{N}$ tal que $I_m = I_{m+1} = \cdots$.

Dado $X \subseteq A$ um subconjunto de A, definimos a subálgebra de A gerada por X como sendo a interseção de todas as subálgebras de A que contêm X, a denotamos por $\langle X \rangle$.

Antes da próxima observação, precisamos definir a propriedade de minimalidade de ideais. Dizemos que um ideal (à esquerda) não nulo I é minimal quando não existe nenhum outro ideal (à esquerda) não nulo propriamente contido em I.

Observação 1.16 *Note que se R é uma álgebra que satisfaz a condição de cadeia descendente, então existe um ideal à esquerda minimal em R. De fato, tomando V_1 um ideal à esquerda não nulo de R, se V_1 não for minimal, então existe V_2 um ideal à esquerda não nulo de R contido propriamente em V_1. Procedendo indutivamente, obtemos a cadeia*

$$V_1 \supsetneq V_2 \supsetneq \cdots$$

de ideais à esquerda. Pela condição de cadeia descendente de R, existe $m \in \mathbb{N}$ tal que $V_m = V_{m+k}$, para todo $k \in \mathbb{N}$, uma contradição.

Utilizamos mais adiante as aplicações entre álgebras, que surgem também como casos particulares de transformações lineares. Assim, precisamos definir os homomorfismos de álgebras.

Definição 1.17 *Sejam A e B $\mathbb{F}$-álgebras e $\varphi : A \to B$ uma transformação linear. Chamamos φ de homomorfismo (de álgebras) sempre que $\varphi(ab) = \varphi(a)\varphi(b)$ para todos $a, b \in A$. Se ambas as álgebras são unitárias, acrescentamos que $\varphi(1_A) = 1_B$. Definimos o núcleo de φ e a imagem de φ, respectivamente, como*

$$Ker(\varphi) := \{a \in A \mid \varphi(a) = 0\} \quad e \quad Im(\varphi) := \{\varphi(a) \mid a \in A\} = \varphi(A).$$

Existem alguns tipos de homomorfismos que são mais comuns e, por isso recebem nomes especiais. Dizemos que φ é:

i) Um monomorfismo, ou mergulho, se for injetivo;

ii) Um epimorfismo, se for sobrejetivo;

iii) Um isomorfismo, se for um monomorfismo e um epimorfismo. Se existe um isomorfismo entre as álgebras A e B, dizemos que elas são isomorfas e denotamos este fato por $A \simeq B$;

iv) Um endomorfismo, se o domínio for também o contradomínio;

v) Um automorfismo, se for um endomorfismo e um isomorfismo.

Na estrutura de álgebra podemos ainda observar a ideia de graduação por um grupo. Na verdade, a ideia de graduação pode ser aplicada também em espaços vetoriais (ou em módulos) e a indexação pode ser por um conjunto qualquer. Para os nossos propósitos, é suficiente trazermos o conteúdo referente apenas para graduação de álgebras por grupos.

Definição 1.18 *Sejam A uma $\mathbb{F}$-álgebra e G um grupo. Uma graduação de A por G, ou uma G-graduação em A, é uma decomposição do espaço vetorial em subespaços*

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

que satisfaz $A_g A_h \subset A_{gh}$, para quaisquer $g, h \in G$. Fixada tal decomposição, chamaremos A de álgebra G-graduada.

No exemplo a seguir utilizamos o conceito de subespaço vetorial gerado por um subconjunto X do espaço vetorial V, que é o conjunto de todas as combinações lineares possíveis entre os elementos de X. Denotamos o subespaço de V gerado por X por $span\{X\}$.

Exemplo 1.19 *Dados G um grupo, podemos induzir uma G-graduação em $A = M_n(\mathbb{F})$ pondo*

$$A_g = span\{E_{ij} \mid g_i^{-1} g_j = g\},$$

onde E_{ij} são as matrizes unitárias e $g_i, g_j \in G$ para todos $i, j \in \{1, 2, \ldots, n\}$.

Definição 1.20 *Na Definição 1.18, chamamos os subespaços A_g de componentes homogêneas da álgebra G-graduada A. Se $a \in A_g \setminus \{0\}$ dizemos que a é um elemento graduado, ou homogêneo, de grau g. Denotamos o grau de a por $deg(a) = g$. Dizemos que o suporte da graduação é o conjunto*

$$Supp(A) = \{g \in G \mid A_g \neq 0\}.$$

Retomando o Exemplo 1.19, ao fixarmos $n = 3$, o corpo $\mathbb{R}$ dos números reais e o grupo $\mathbb{Z}_3$ dos inteiros módulo 3, temos

$$M_3(\mathbb{R}) = A_0 \oplus A_1 \oplus A_2,$$

onde $A_0 = span\{E_{11}, E_{22}, E_{33}\}$, $A_1 = span\{E_{21}, E_{32}, E_{13}\}$ e $A_2 = span\{E_{12}, E_{23}, E_{31}\}$. Neste caso, $Supp(A) = \mathbb{Z}_3$.

Definição 1.21 *Dizemos que um subespaço R de A é graduado se*

$$R = \bigoplus_{g \in G} (A_g \cap R).$$

Observação 1.22 *Um subespaço R de A é graduado se, e somente se, dado $\sum_{g \in G} r_g \in R$, com $r_g \in A_g$, temos $r_g \in R$, para todo $g \in G$.*

Exemplo 1.23 *Dado G um grupo, podemos considerar o conjunto $\mathbb{F}[G]$ de todas as somas formais $\sum_{g \in G} \alpha_g g$, onde $\alpha_g \in \mathbb{F}$ e $\{g \in G \mid \alpha_g \neq 0\}$ é finito. Diremos que $\sum_{g \in G} \alpha_g g = \sum_{g \in G} \beta_g g$ se $\alpha_g = \beta_g$, para todo $g \in G$. Definimos uma soma e um produto por escalar em $\mathbb{F}[G]$ pondo:*

$$\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g := \sum_{g \in G} (\alpha_g + \beta_g) g$$

$$\lambda \sum_{g \in G} \alpha_g g := \sum_{g \in G} (\lambda \alpha_g) g \ , \ onde \ \lambda \in \mathbb{F}.$$

Com tais operações $\mathbb{F}[G]$ é um espaço vetorial. Para que tal espaço vetorial se torne uma álgebra, consideramos o produto induzido pela operação do grupo G, ou seja, para os elementos da base, temos $g \cdot h := gh$.

A álgebra $\mathbb{F}[G]$ admite uma G-graduação, chamada de graduação canônica, dada por

$$\mathbb{F}[G] = \bigoplus_{g \in G} span\{g\}.$$

Definição 1.24 *Dizemos que uma álgebra graduada é de divisão se todo elemento homogêneo possuir inverso multiplicativo.*

Exemplo 1.25 *Temos que $\mathbb{F}[G]$ é uma álgebra graduada de divisão. De fato, dado $\alpha g \in span\{g\}$ não nulo, sendo $\alpha \in \mathbb{F}$, existe $\alpha^{-1} g^{-1}$ tal que*

$$(\alpha g)(\alpha^{-1} g^{-1}) = (\alpha \alpha^{-1})(g g^{-1}) = 1.$$

Definição 1.26 *Dizemos que uma álgebra G-graduada A é simples se $A^2 \neq 0$ e os únicos ideais graduados bilaterais são A e 0.*

Exemplo 1.27 *Toda álgebra G-graduada de divisão $A = \sum A_{g_i}$ é graduada simples. De fato, supondo que existe um ideal graduado bilateral não nulo $I \subseteq A$, podemos tomar $a = a_{g_1} + \cdots + a_{g_n} \in I \setminus \{0\}$. Como o ideal é graduado, então $a_{g_1} \in I$. Dado que a_{g_1} é homogêneo, existe um elemento $b = (a_{g_1})^{-1} \in A$. Ora, por ser ideal, temos $a_{g_1} b \in I$, de onde segue que $1_A \in I$ e, portanto, $I = A$.*

Na próxima definição utilizamos o conceito de avaliação de um elemento de uma álgebra em um polinômio. Dado $p \in \mathbb{F}[x]$ existem $n \in \mathbb{N}$ e $\alpha_i \in \mathbb{F}$ para todo $i = 0, 1, \ldots, n$ tais que $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$. Dado um elemento a de uma $\mathbb{F}$-álgebra, a avaliação de a em p, denotada por $p(a)$, é o elemento da álgebra

$$p(a) = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_n a^n.$$

Definição 1.28 *Seja A uma álgebra sobre um corpo $\mathbb{F}$. Dizemos que um elemento $a \in A$ é algébrico sobre $\mathbb{F}$ se existe um polinômio não nulo $p(x) \in \mathbb{F}[x]$ tal que $p(a) = 0$. Dizemos que a álgebra A é algébrica se todo elemento da álgebra for algébrico.*

Exemplo 1.29 *Toda álgebra de dimensão finita é algébrica. De fato, seja $dim(A) = n$. Dado $a \in A$ os elementos $a, a^2, \ldots, a^n, a^{n+1}$ formam um conjunto LD sobre $\mathbb{F}$, pois é um conjunto com mais de n elementos. Portanto existem $\alpha_i \in \mathbb{F}$, nem todos nulos, tais que $\alpha_1 a + \cdots + \alpha_n a^n + \alpha_{n+1} a^{n+1} = 0$. Ora, a é raiz do polinômio não nulo*

$$\alpha_1 x + \cdots + \alpha_n x^n + \alpha_{n+1} x^{n+1} \in \mathbb{F}[x],$$

mostrando que A é uma álgebra algébrica.

No próximo lema utilizaremos, como é frequente na literatura, a convenção de considerar $\mathbb{F} \subseteq A$. Podemos fazer iso pois como $span\{1_A\} \simeq \mathbb{F}$, identificamos $span\{1_A\}$ com $\mathbb{F}$ e assim podemos considerar $\mathbb{F} \subseteq A$.

Lema 1.30 *Seja A uma álgebra de divisão algébrica sobre um corpo $\mathbb{F}$, que é algebricamente fechado. Nestas condições $A = \mathbb{F}$.*

Demonstração. Seja $a \in A$, então $p(a) = 0$ para algum $p(x) \in \mathbb{F}[x]$ não constante. Como $\mathbb{F}$ é algebricamente fechado, $p(x) = \prod(x - \lambda_i), \lambda_i \in \mathbb{F}$. Ora,

$$0 = p(a) = \prod(a - \lambda_i).$$

Como A é um anel de divisão, concluímos que $a - \lambda_i = 0$ para algum i, de onde segue que $a = \lambda_i \in \mathbb{F}$. ∎

Observação 1.31 *Unindo o lema ao exemplo, obtemos que toda álgebra de divisão de dimensão finita sobre um corpo algebricamente fechado é, na verdade, o corpo.*

1.2.1 Graduação Elementar da Álgebra Matricial

A graduação do Exemplo 1.19 para álgebras de matrizes é chamada de graduação elementar, pois em tal graduação as matrizes unitárias são elementos homogêneos. De maneira mais geral, graduações elementares são exatamente as que mantêm as matrizes unitárias como elementos homogêneos. Um fato que nos será útil é percebermos que uma graduação elementar fica determinada por $deg(E_{12}), \ldots, deg(E_{n-1,n})$. Se tais graus forem conhecidos, poderemos obter o grau de qualquer matriz elementar a partir destes. De fato, se $i < j$, temos

$$E_{ij} = E_{i,i+1}E_{i+1,i+2}\cdots E_{j-1,j}$$

e, portanto,

$$deg(E_{ij}) = deg(E_{i,i+1})deg(E_{i+1,i+2})\cdots deg(E_{j-1,j}).$$

Se, por outro lado, $i > j$, basta relembrar que $deg(E_{ij})deg(E_{ji}) = deg(E_{ii}) = e$ e, assim, $deg(E_{ij}) = deg(E_{ji})^{-1}$. Veremos agora uma classificação para tais graduações.

Seja $V = \bigoplus_{g\in G} V_g$ um espaço vetorial de dimensão n graduado por um grupo G (isto é, uma decomposição de V em subespaços). Dizemos que uma transformação linear $f \in End(V)$ é homogênea de grau h se para todo $g \in G$, $f(V_g) \subseteq V_{hg}$.

Se $\{v_1, \ldots, v_n\}$ é uma base homogênea de V (que é uma base de V cujos elementos são homogêneos), com $deg(v_i) = g_i^{-1}$, $i = 1, \ldots, n$, considerando o conhecido isomorfismo de $End(V)$ com $M_n(V)$, uma base para $End(V)$ que podemos observar é o conjunto dos endomorfismos e_{ij} tais que, para cada $i, j \in \{1, \ldots, n\}$, $e_{ij}(v_j) = v_i$ e $e_{ij}(v_r) = 0$, para todo $r \neq j$. As imagens dos elementos desta base de $End(V)$ são exatamente as matrizes elementares E_{ij}. Com esta identificação em mente, podemos munir $M_n(\mathbb{F})$ com a graduação tal que todas as matrizes unitárias E_{ij} são homogêneas com $deg(E_{ij}) = g_i^{-1}g_j$. Claramente podemos identificar tal graduação de $M_n(\mathbb{F})$ com a n-upla $(g_1, \ldots, g_n) \in G^n$. Agora, dada um permutação $\sigma \in S_n$, se permutarmos $v_1, \ldots, v_n$ de acordo com σ, obtemos uma nova G-graduação para $M_n(\mathbb{F})$, mas agora definida pela n-upla $(g_{\sigma(1)}, \ldots, g_{\sigma(n)})$. Note que o grau de E_{ij} na nova graduação é $g_{\sigma(i)}^{-1}g_{\sigma(j)}$.

Podemos supor com base na discussão anterior e a menos de isomorfismos que

$$\underbrace{(g_1, \ldots, g_n)}_{n} = (\underbrace{g_{i_1}, \ldots, g_{i_1}}_{q_1}, \ldots, \underbrace{g_{i_m}, \ldots, g_{i_m}}_{q_m}),$$

com $g_{i_1}, \ldots, g_{i_m}$ distintos e $q_1 + \cdots + q_m = n$. Sejam $e \in G$ a unidade de G e $M_n(\mathbb{F}) = R = \bigoplus_{g \in G} R_g$ uma álgebra matricial com a G-graduação definida por $(g_1, \ldots, g_n)$. Então R_e é uma subálgebra de R e $R_e = M_{q_1}(\mathbb{F}) \oplus \cdots \oplus M_{q_m}(\mathbb{F})$. De fato, pois dados $a, b \in R_e$ temos $deg(ab) = deg(a)deg(b) = e$. Mostremos agora que

$$R_e = M_{q_1}(\mathbb{F}) \oplus \cdots \oplus M_{q_m}(\mathbb{F}). \tag{1.1}$$

Considere os conjuntos

$$\begin{aligned} I_1 &= \{1, \ldots, q_1\} \\ I_2 &= \{q_1 + 1, \ldots, q_1 + q_2\} \\ &\vdots \\ I_m &= \{q_1 + \cdots + q_{m-1} + 1, \ldots, q_1 + \cdots + q_m\}. \end{aligned}$$

É suficiente provar que $E_{ij} \in R_e$ se, e somente se, existe k tal que $i, j \in I_k$. Ora, mas isto é claro, pois $g_i g_j^{-1} = e$ se, e somente se, existe k tal que $i, j \in I_k$.

Se $e_1, \ldots, e_m$ são as matrizes identidade em $M_{q_1}(\mathbb{F}), \ldots, M_{q_m}(\mathbb{F})$, respectivamente, então $e_i R e_i$ é uma subálgebra de R que é homogênea nesta graduação, pois é isomorfa à álgebra de matriz $M_{q_i}(\mathbb{F})$.

Assumindo $q_1 \geq q_2 \geq \cdots \geq q_m > 0$, podemos utilizar a seguinte classificação, onde a graduação elementar é definida pela $(2m-1)$-upla

$$(q_1, \ldots, q_m; g_{12}, \ldots, g_{m-1,m}), \tag{1.2}$$

onde $g_{12}, \ldots, g_{m-1,m}$ satisfazem $g_{12} = g_{i_1}^{-1} g_{i_2}, \ldots, g_{m-1,m} = g_{i_{m-1}}^{-1} g_{i_m}$. Ademais, como $g_{i_1}, \ldots, g_{j-1,j}$ são distintos, então esses elementos também satisfazem $g_{i,i+1} \cdots g_{j-1,j} \neq e$, para quaisquer $1 \leq i < j \leq m$.

1.2.2 Álgebras de Grupo *Twisted*

Nesta seção introduzimos uma classe de álgebras que classifica todas as álgebras graduadas de divisão sobre um corpo algebricamente fechado, que são as álgebras *twisted*.

Um exemplo relevante de álgebra graduada é a álgebra de grupo $\mathbb{F}[G]$, que é o espaço vetorial que surge ao tomarmos os elementos do grupo como base e utilizarmos a multiplicação do grupo para induzir a multiplicação da álgebra.

Nosso objetivo é generalizar um pouco a noção de álgebra de grupo para introduzir as álgebras de grupo *twisted*. Para isto, consideramos uma aplicação $\sigma : G\times G \to \mathbb{F}\setminus\{0\}$ que chamamos de 2-cociclo em G com valores em $\mathbb{F} \setminus \{0\}$.

Agora, tomando apenas a estrutura de espaço vetorial de $\mathbb{F}[G]$ e definindo um produto distinto do anterior, a saber, induzido por

$$g \cdot h := \sigma(g,h)gh.$$

Dados $x, y, z \in G$, temos

$$\begin{aligned}(x\cdot y)\cdot z = x\cdot(y\cdot z) &\Leftrightarrow (\sigma(x,y)xy)\cdot z = x\cdot(\sigma(y,z)yz)\\ &\Leftrightarrow \sigma(x,y)\sigma(xy,z)xyz = \sigma(y,z)\sigma(x,yz)xyz\\ &\Leftrightarrow \sigma(x,y)\sigma(xy,z) = \sigma(y,z)\sigma(x,yz),\end{aligned}$$

mostrando que a relação

$$\sigma(x,y)\sigma(xy,z) = \sigma(y,z)\sigma(x,yz), \text{ para todos } x,y,z \in G \tag{1.3}$$

é suficiente e necessária para que a multiplicação " $\cdot$ " definida acima entre elementos do grupo seja associativa.

Com a multiplicação induzida por $g \cdot h := \sigma(g,h)gh$, o espaço vetorial $\mathbb{F}^\sigma[G]$ é, na verdade, uma álgebra. De fato, dados $a = \sum \alpha_i g_i, b = \sum \beta_i g_i, c = \sum \gamma_i g_i \in \mathbb{F}^\sigma[G]$ e $\lambda \in \mathbb{F}$, mostraremos que $(a+b)\cdot c = a\cdot c + b\cdot c$ e, de maneira análoga, pode-se provar que $a\cdot(b+c) = a\cdot b + a\cdot c$.

$$\begin{aligned}(a+b)\cdot c &= (\textstyle\sum \alpha_i g_i + \sum \beta_i g_i)\cdot \sum \gamma_i g_i = \sum(\alpha_i+\beta_i)g_i \cdot \sum \gamma_i g_i\\ &= \textstyle\sum_{i,j}((\alpha_i+\beta_i)\gamma_j)\sigma(g_i,g_j)g_ig_j\\ &= \textstyle\sum_{i,j}\alpha_i\gamma_j\sigma(g_i,g_j)g_ig_j + \sum_{i,j}\beta_i\gamma_j\sigma(g_i,g_j)g_ig_j\\ &= \textstyle\sum \alpha_i g_i \cdot \sum \gamma_i g_i + \sum \beta_i g_i \cdot \sum \gamma_i g_i = a\cdot c + b\cdot c.\end{aligned}$$

Assim como fizemos anteriormente, mostraremos que $\lambda(a\cdot b) = (\lambda a)\cdot b$ e pode-se provar analogamente que $\lambda(a\cdot b) = a\cdot(\lambda b)$.

$$\begin{aligned}\lambda(a\cdot b) &= \lambda(\textstyle\sum \alpha_i g_i \cdot \sum \beta_i g_i) = \lambda(\sum_{ij}\alpha_i\beta_j\sigma(g_i,g_j)g_ig_j)\\ &= \textstyle\sum_{i,j}\lambda\alpha_i\beta_j\sigma(g_i,g_j)g_ig_j = \sum \lambda\alpha_i g_i \cdot \sum \beta_i g_i\\ &= (\lambda\textstyle\sum \alpha_i g_i)\cdot \sum \beta_i g_i = (\lambda a)\cdot b.\end{aligned}$$

Chamamos $\mathbb{F}^\sigma[G]$ de álgebra de grupo *twisted* determinada por σ. Se σ é tal que vale a relação (1.3) então $\mathbb{F}^\sigma[G]$ é uma álgebra associativa, pois dados $a = \sum \alpha_i g_i, b = \sum \beta_i g_i, c = \sum \gamma_i g_i \in \mathbb{F}^\sigma[G]$,

$$\begin{aligned}(a \cdot b) \cdot c &= (\sum \alpha_i g_i \cdot \sum \beta_i g_i) \cdot \sum \gamma_i g_i = \sum_{i,j} \alpha_i \beta_j g_i \cdot g_j \cdot \sum \gamma_i g_i \\ &= \sum_{i,j,k} (\alpha_i \beta_j) \gamma_k (g_i \cdot g_j) \cdot g_k = \sum_{i,j,k} \alpha_i (\beta_j \gamma_k) g_i \cdot (g_j \cdot g_k) \\ &= \sum \alpha_i g_i \cdot (\sum_{i,j} \beta_i \gamma_j g_i \cdot g_j) = \sum \alpha_i g_i \cdot (\sum \beta_i g_i \cdot \sum \gamma_i g_i) \\ &= a \cdot (b \cdot c).\end{aligned}$$

Também podemos observar uma graduação natural em $A = \mathbb{F}^\sigma[G]$ se pusermos, por exemplo, $A_g = span\{g\}$, o que a torna uma álgebra graduada de divisão.

Observação 1.32 *No Teorema 2.6 mostraremos que uma álgebra é graduada de divisão se, e somente se, é isomorfa à álgebra de grupo twisted $\mathbb{F}^\sigma[H]$, para algum subgrupo H de G com a graduação acima mencionada.*

1.2.3 Módulos Graduados

Uma estrutura amplamente conhecida nas disciplinas universitárias mais básicas de matemática é o espaço vetorial. Nela, relacionam-se dois tipos (geralmente distintos) de objetos matemáticos, os vetores e os escalares. Na verdade, os espaços vetoriais são casos particulares da estrutura que definiremos nesta seção, os módulos.

Definição 1.33 *Seja R um anel com unidade. Dado um grupo abeliano $(M, +)$, dizemos que M é um R-módulo à esquerda quando existe uma aplicação $\cdot : R \times M \to M$, que chamamos ação de R em M, satisfazendo*

i) $1_R \cdot m = m$;

ii) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$;

iii) $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$;

iiii) $(r_1 + r_2) \cdot m = (r_1 \cdot m) + (r_2 \cdot m)$,

para todos $m, m_1, m_2 \in M$ e $r, r_1, r_2 \in R$. Denotamos o R-módulo à esquerda por ${}_RM$. Analogamente definimos o R-módulo à direita e o denotamos por M_R.

Exemplo 1.34 *Dado um corpo $\mathbb{F}$, um $\mathbb{F}$-módulo é um $\mathbb{F}$-espaço vetorial.*

Dado N um subconjunto do R-módulo à esquerda M, dizemos que N é um submódulo de M se

i) $0 \in N$;

ii) $n_1 + n_2 \in N$, para quaisquer $n_1, n_2 \in N$;

iii) $rn \in N$, para todos $r \in R, n \in N$.

Também utilizaremos frequentemente o conceito de submódulo gerado por um conjunto. Dado $X \subseteq M$, chamamos de submódulo de M gerado pelo subconjunto X a interseção de todos os submódulos de M que contêm X, denotando-o por $\langle X \rangle$. Não é difícil verificar que tal conjunto é um submódulo de M.

Exemplo 1.35 *Dado um anel R, podemos vê-lo com um R-módulo à esquerda. Neste caso, chamamos este módulo de regular e o denotamos por ${}_RR$. Os submódulos de um módulo regular à esquerda são os ideais à esquerda do anel.*

Dados G um grupo e R um anel G-graduado, podemos observar em um R-módulo M uma graduação pelo grupo G. Basta decompor M em uma soma direta de submódulos indexados por G

$$M = \bigoplus_{g \in G} M_g,$$

tais que $R_g M_h \subseteq M_{gh}$, para quaisquer $g, h \in G$.

Sejam G um grupo, R uma álgebra associativa G-graduada, temos que R é também um anel e, assim, podemos falar sobre módulos sobre R. Sejam V, W R-módulos à esquerda graduados. Usaremos as seguintes notações:

- $Hom_R(V, W)$ é o conjunto dos R-homomorfismos de módulos entre V e W.
- $Hom_g(V, W) = \{f : V \to W; f \text{ é uma transformação linear e } (V_h)f \subset W_{hg}, \forall h \in G\}$;
- $Hom^{gr}(V, W) = \bigoplus_{g \in G} Hom_g(V, W)$;
- $Hom_R^{gr}(V, W) = Hom^{gr}(V, W) \cap Hom_R(V, W)$.

Pode-se provar (vide *Corollary I*.2.11 da referência [16]) que se a dimensão do R-módulo à esquerda graduado V é finita, então $Hom_R^{gr}(V, W) = Hom_R(V, W)$.

Dizemos que um R-módulo (à esquerda) graduado M é simples quando $M \neq 0$ e não existe nenhum submódulo (à esquerda) graduado próprio não nulo em M

Lema 1.36 *Seja R uma álgebra G-graduada. Se V é um R-módulo à esquerda graduado simples. Então $D = End_R^{gr}(V)$ é uma álgebra graduada de divisão*

Demonstração. Note que a aplicação identidade pertence a D, que é sua unidade. Seja $d \in D$ um elemento homogêneo não nulo com $deg(d) = g$. Então ambos $ker(d)$ e $Im(d)$ são submódulos graduados de V, donde segue que $Ker(d) = 0$ e $Im(d) = V$, e portanto d é invertível e possui inversa $d^{-1} \in End_{g^{-1}}(V) \cap End_R(V) \subset D$. ■

1.2.4 Produto Tensorial

Nesta seção trazemos um exemplo de álgebra com algumas propriedades bastante interessantes que nos servirão como ferramenta.

Na construção da álgebra de grupo $\mathbb{F}[G]$ na seção anterior, poderíamos, em vez de um grupo, tomarmos um conjunto S qualquer, mas considerando apenas o espaço vetorial que surge a partir das somas formais. A este espaço chamamos $\mathbb{F}$-espaço vetorial com base S, e o denotamos $\mathbb{F}[S]$.

Sejam agora V e W espaços vetoriais sobre $\mathbb{F}$ e considere $\mathbb{F}[V \times W]$ e o subespaço Λ gerado pelos elementos dos tipos

$$\begin{gathered}(v_1 + v_2, w) - (v_1, w) - (v_2, w) \\ (v, w_1 + w_2) - (v, w_1) - (v, w_2) \\ (\lambda v, w) - \lambda(v, w) \\ (v, \lambda w) - \lambda(v, w),\end{gathered} \tag{1.4}$$

onde $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$ e $\lambda \in \mathbb{F}$. Agora considere o espaço vetorial quociente $\dfrac{\mathbb{F}[V \times W]}{\Lambda}$. A este espaço chamamos produto tensorial entre os espaços V e W e o denotamos $V \otimes W$.

Antes de seguirmos com as propriedades deste espaço, devemos relembrar o que é o quociente de um espaço vetorial por um subespaço e quem são seus elementos. Sejam V um espaço vetorial e $V' \subseteq V$ um subespaço. Consideremos a relação definida por

$$v_1 \equiv v_2 (mod\ V') \Leftrightarrow v_1 - v_2 \in V',$$

onde $v_1, v_2 \in V$. Tal relação é de equivalência, pois para $v_1, v_2, v_3 \in V$,

i) $v_1 - v_1 = 0 \in V' \Rightarrow v_1 \equiv v_1 (mod\ V')$;

ii) Se $v_1 \equiv v_2 (mod\ V')$, então $v_1 - v_2 \in V'$. Como é um subespaço, $-(v_1 - v_2) \in V'$, e assim $v_2 - v_1 \in V'$, de onde segue que $v_2 \equiv v_1 (mod\ V')$.

iii) Suponhamos $v_1 \equiv v_2$ e $v_2 \equiv v_3 (mod\ V')$. Daí, $v_1 - v_2, v_2 - v_3 \in V' \Rightarrow v_1 - v_3 = (v_1 - v_2) + (v_2 - v_1) \in V'$, e, portanto, $v_1 \equiv v_3 (mod\ V')$.

Desta relação de equivalência podemos observar as classes laterais. Uma classe lateral é o conjunto de todos os elementos que se relacionam com um elemento dado, ou seja,

$$\overline{v} := \{w \in V \mid v \equiv w (mod\ V')\} = \{v + u \mid u \in V'\}.$$

Não é difícil ver que duas classes laterais são iguais ou disjuntas. As operações de adição $\overline{v_1} + \overline{v_2} := \overline{v_1 + v_2}$ e multiplicação por escalar $\alpha\overline{v_1} := \overline{\alpha v_1}$ estão bem definidas, para todos $\alpha \in \mathbb{F}$, e $v_1, v_2 \in V$ e portanto, com tais operações, o conjunto das classes é um espaço vetorial que chamamos de espaço quociente de V por V', e o denotamos por $\dfrac{V}{V'}$.

Um fato simples mas importante sobre o espaço quociente é que uma condição suficiente e necessária para que $\overline{v} = 0$ é que $v \in V'$.

Tendo feito esta pequena revisão podemos estabelecer os resultados para o nosso produto tensorial. Dados $v \in V$, $w \in W$, tendo em mente que $V \otimes W$ é um quociente de espaços vetoriais, chamamos a classe lateral de (v, w) de tensor e a denotamos por $v \otimes w$. Pela natureza dos elementos que escolhemos para gerarem Λ, as equações (1.4), obtemos algumas propriedades básicas dos tensores. Dados $\lambda \in \mathbb{F}$, $v, v_1, v_2 \in V$ e $w, w_1, w_2 \in W$, valem:

i) $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$;

ii) $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$;

iii) $\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w)$.

Dado $\bar{a} \in V \otimes W$, temos

$$\bar{a} = \sum_{v \in V, w \in W} \alpha_{v,w} v \otimes w = \sum_{v \in V, w \in W} (\alpha_{v,w} v) \otimes w = \sum_{v \in V, w \in W} v' \otimes w.$$

Assim, todos os elementos de $V \otimes W$ são da forma $\sum_{v \in V, w \in W} v \otimes w$.

Observação 1.37 *Se S_1 e S_2 são conjuntos geradores de V e W, respectivamente, então $\{u_1 \otimes u_2 \mid u_1 \in S_1,\ u_2 \in S_2\}$ é um conjunto gerador de $V \otimes W$.*

O teorema que usamos para mostrar que o tensor é uma álgebra e obter algumas das suas propriedades é conhecido como Propriedade Universal e segue.

Teorema 1.38 (Propriedade Universal) *Sejam U, V, W $\mathbb{F}$-espaços vetoriais e $f : V \times W \to U$ uma aplicação bilinear. Então existe uma única transformação linear $F : V \otimes W \to U$ tal que $F(v \otimes w) = f(v, w)$, onde $v \in V,\ w \in W$.*

Demonstração. Mencionamos anteriormente que o conjunto $V \times W$ é uma base para o espaço vetorial $\mathbb{F}[V \times W]$, então existe uma única transformação linear $\varphi : \mathbb{F}[V \times W] \to U$ tal que para todos $v \in V$ e $w \in W$, vale $\varphi((v, w)) = f(v, w)$. Note que os elementos de Λ pertencem ao $ker(\varphi)$, pois todos os geradores de Λ pertencem ao $ker(\varphi)$. De fato, todo gerador de Λ é de algum dos quatro tipos em (1.4). Seja u um gerador de Λ. Se existem $v_1, v_2 \in V$ e $w \in W$ tais que $u = (v_1 + v_2, w) - (v_1, w) - (v_2, w)$, então $\varphi(u) = \varphi((v_1 + v_2, w) - (v_1, w) - (v_2, w)) = \varphi((v_1 + v_2, w)) - \varphi((v_1, w)) + -\varphi((v_2, w)) = f((v_1 + v_2, w)) - f(v_1, w) - f(v_2, w) = 0$. O segundo caso é análogo ao primeiro. Se, porém, existem $\lambda \in \mathbb{F}, v \in V$ e $w \in W$ tais que $u = (\lambda v, w) - \lambda(v, w)$, então $\varphi(u) = \varphi((\lambda v, w) - \lambda(v, w)) = \varphi((\lambda v, w)) - \lambda\varphi((v, w)) = f(\lambda v, w) - \lambda f(v, w) = \lambda f(v, w) - \lambda f(v, w) = 0$ e o último caso é análogo a esse. Assim, $\Lambda \subseteq Ker(\varphi)$. Daí, se $u_1, u_2 \in \mathbb{F}[V \times W]$ satisfazem $u_1 \equiv u_2\ (mod \Lambda)$ então valem:

$$\begin{array}{rcl} u_1 - u_2 \in \Lambda \subseteq Ker(\varphi) & \Rightarrow & \varphi(u_1 - u_2) = 0 \\ & \Rightarrow & \varphi(u_1) = \varphi(u_2) \end{array}.$$

Dito isso, note que a aplicação

$$\begin{array}{rccl} F : & \dfrac{\mathbb{F}[V \times W]}{\Lambda} & \longrightarrow & U \\ & \overline{u} & \longmapsto & F(\overline{u}) := \varphi(u) \end{array}$$

está bem definida e herda a linearidade de φ. Além disso, dado $(v, w) \in V \times W$, temos

$$F(v \otimes w) = \varphi((v, w)) = f(v, w).$$

Provemos agora a unicidade de tal aplicação. Se $G : V \otimes W \to U$ é uma aplicação linear tal que $G(v \otimes w) = f(v, w)$ para todos $v \in V$ e $w \in W$, então dado $u \in V \otimes W$,

existem $v_i \in V$ e $w_i \in W$ tais que $u = \sum v_i \otimes w_i$ e, assim,

$$\begin{aligned} G(u) &= G\left(\sum v_i \otimes w_i\right) = \sum(G(v_i \otimes w_i)) \\ &= \sum(f(v_i, w_i)) = \sum(F(v_i \otimes w_i)) \\ &= F\left(\sum v_i \otimes w_i\right) = F(u). \end{aligned}$$

■

Abaixo apresentamos algumas propriedades dos produtos tensoriais.

Proposição 1.39 *Sejam U, V, W espaços vetoriais sobre $\mathbb{F}$. São válidas as seguintes propriedades:*

i) $V \simeq \mathbb{F} \otimes V$.

Considere $f : \mathbb{F} \times V \to V$ definida por $f(\lambda, v) := \lambda v$. Como f é claramente bilinear, pela propriedade universal, existe uma transformação linear $F : \mathbb{F} \otimes V \to V$ tal que $F(\lambda \otimes v) = \lambda v$. Mostraremos que F é um isomorfismo apresentando a inversa de F. Considere $G : V \to \mathbb{F} \otimes V$ dada por $G(v) = 1 \otimes v$. Claramente G é linear e

$$G \circ F(\lambda \otimes v) = G(\lambda v) = 1 \otimes \lambda v = \lambda \otimes v$$

$$F \circ G(v) = F(1 \otimes v) = v.$$

Segue-se que G é a inversa de F, provando que F é um isomorfismo.

ii) $V^n \simeq \mathbb{F}^n \otimes V$.

Tome $g : \mathbb{F}^n \times V \to V^n$, definida por $g((\lambda_1, \ldots, \lambda_n), v) := (\lambda_1 v, \ldots, \lambda_n v)$. Tal aplicação é claramente bilinear e, portanto (pela propriedade universal), existe uma transformação linear $G : \mathbb{F}^n \otimes V \to V^n$ tal que $G((\lambda_1, \ldots, \lambda_n) \otimes v) = (\lambda_1 v, \ldots, \lambda_n v)$. Considere agora, semelhante ao que fizemos no item anterior, a transformação linear $F : V^n \to \mathbb{F}^n \otimes V$ tal que $F(v_1, \ldots, v_n) = \sum_{j=1}^{n} e_j \otimes v_j$, onde e_j é a n-upla de $\mathbb{F}^n$ onde tem 1 na j-ésima entrada e zero nas demais. Temos

$$\begin{aligned} G \circ F(v_1, \ldots, v_n) &= G(\sum e_i \otimes v_i) = \sum(G(e_i \otimes v_i)) \\ &= (v_1, \ldots, v_n) \qquad \text{e} \\ F \circ G((\lambda_1, \ldots, \lambda_n) \otimes v) &= F(\lambda_1 v, \ldots, \lambda_n v) = \sum_{j=1}^{n} e_j \otimes \lambda_j v = (\lambda_1 \ldots, \lambda_n) \otimes v. \end{aligned}$$

Assim, G é inversa de F mostrando que F é um isomorfismo.

iii) $V \otimes W \simeq W \otimes V$.

Para a demonstração da validade desta proposição, basta considerar as aplicações bilineares

$$\begin{array}{rccc} f: & V \times W & \longrightarrow & W \otimes V \\ & (v,w) & \longmapsto & w \otimes v \end{array} \qquad \text{e} \qquad \begin{array}{rccc} g: & W \times V & \longrightarrow & V \otimes W \\ & (w,v) & \longmapsto & v \otimes w \end{array}$$

Existem transformações lineares $F : V \otimes W \to W \otimes V$ e $G : W \otimes V \to V \otimes W$ tais que $F(v \otimes w) = w \otimes v$ e $G(w \otimes v) = v \otimes w$. Note que G é a inversa de F, mostrando que existe um isomorfismo entre $V \otimes W$ e $W \otimes V$.

iv) $(V \otimes W) \otimes U \simeq V \otimes (W \otimes U)$.

Fixado $u_0 \in U$, a aplicação

$$\begin{array}{rccc} f_{u_0}: & V \times W & \longrightarrow & V \otimes (W \otimes U) \\ & (v,w) & \longmapsto & v \otimes (w \otimes u_0) \end{array}$$

é bilinear para cada u_0. Assim, existe uma transformação linear $F_{u_0} : V \otimes W \to V \otimes (W \otimes U)$ tal que $F_{u_0}(v \otimes w) = v \otimes (w \otimes u_0)$. Note que

$$\begin{array}{rccc} f: & U & \longrightarrow & \mathfrak{L}(V \otimes W, V \otimes (W \otimes U)) \\ & u & \longmapsto & F_u \end{array}$$

é linear. Com isto, podemos mostrar que

$$\begin{array}{rccc} F: & (V \otimes W) \times U & \longrightarrow & V \otimes (W \otimes U) \\ & (\alpha, u) & \longmapsto & F_u(\alpha) \end{array}$$

é bilinear. De fato, dados $\lambda \in \mathbb{F}, \alpha, \alpha_1, \alpha_2 \in V \otimes W$ e $u, u_1, u_2 \in U$,

$$F(\lambda\alpha_1 + \alpha_2, u) = F_u(\lambda\alpha_1 + \alpha_2) = \lambda F_u(\alpha_1) + F_u(\alpha_2) = \lambda F(\alpha_1, u) + F(\alpha_2, u) \text{ e}$$

$$F(\alpha, \lambda u_1 + u_2) = F_{\lambda u_1 + u_2}(\alpha) = \lambda F_{u_1}(\alpha) + F_{u_2}(\alpha) = \lambda F(\alpha, u_1) + F(\alpha, u_2).$$

Aplicando novamente a propriedade universal, existe uma aplicação linear $G : (V \otimes W) \otimes U \to V \otimes (W \otimes U)$ tal que $G(\alpha \otimes u) = F_u(\alpha)$ e, particularmente, $G((v \otimes w) \otimes u) = v \otimes (w \otimes u)$.

Analogamente, existe $G' : V \otimes (W \otimes U) \to (V \otimes W) \otimes U$ tal que $G(v \otimes (w \otimes u)) = (v \otimes w) \otimes u$. Não é difícil ver que G' é a inversa de G, de onde segue que G é um isomorfismo.

v) Se $S_1 = \{v_i \mid i \in I\}$ e $S_2 = \{w_j \mid j \in J\}$ são subconjuntos linearmente independentes de V e W respectivamente, então $S = \{v_i \otimes w_j \mid i \in I, j \in J\}$ é um conjunto linearmente independente de $V \otimes W$.

Suponhamos $\sum_{i\in I}\sum_{j\in J} \lambda_{ij}(v_i \otimes w_j) = 0$ e mostraremos que $\lambda_{ij} = 0$, para quaisquer $i \in I$ e $j \in J$. Fixe $i_0 \in I$, $j_0 \in J$ arbitrariamente e tome uma aplicação bilinear $f : V \times W \to \mathbb{F}$ tal que $f(v_{i_0}, w_{j_0}) = 1$ e $f(v_i, w_j) = 0$, caso $i \neq i_0$ ou $j \neq j_0$. Pela propriedade universal, existe uma transformação linear $F : V \otimes W \to \mathbb{F}$ tal que $F(v_{i_0} \otimes w_{j_0}) = 1$ e $F(v_i \otimes w_j) = 0$, se $i \neq i_0$ ou $j \neq j_0$. Segue que

$$0 = F\left(\sum_{i\in I}\sum_{j\in J} \lambda_{ij}(v_i \otimes w_j)\right) = \sum_{i\in I}\sum_{j\in J} \lambda_{ij}F(v_i \otimes w_j) = \lambda_{i_0,j_0}$$

o que é suficiente para mostrar que S é um conjunto de vetores linearmente independente sobre $\mathbb{F}$.

vi) Dados $X = \{v_i \mid i \in I\} \subset V$ e $Y = \{w_i \mid i \in I\} \subset W$ subconjuntos de vetores não nulos, se X ou Y é linearmente independente, então $Z = \{v_i \otimes w_i \mid i \in I\}$ é um conjunto de tensores linearmente independentes.

Suponhamos que X seja linearmente independente e seja β uma base do subespaço $\langle b \mid b \in Y\rangle$ de W. Tomemos uma combinação linear nula de elementos de Z:

$$\alpha_1 v_1 \otimes w_1 + \alpha_2 v_2 \otimes w_2 + \cdots + \alpha_k v_k \otimes w_k = 0.$$

Reescrevendo esta equação pondo cada w_i como combinação linear de elementos de β, temos

$$\begin{aligned} \alpha_1 v_1 \otimes (\textstyle\sum(\gamma_{1,i}b_i)) + \alpha_2 v_2 \otimes (\sum(\gamma_{2,i}b_i)) + \cdots + \alpha_k v_k \otimes (\sum(\gamma_{k,i}b_i)) &= 0 \\ \alpha_1\gamma_{1,1}v_1 \otimes b_1 + \cdots + \alpha_1\gamma_{1,l}v_1 \otimes b_l + \cdots + \alpha_k\gamma_{k,p}v_k \otimes b_p &= 0, \end{aligned}$$

onde $\alpha_1, \ldots, \alpha_k, \gamma_{1,1}, \ldots, \gamma_{k,p} \in \mathbb{F}$. Como cada w_i é não nulo, para cada r existe s tal que $\gamma_{r,s} \neq 0$. Como pelo item anterior $\alpha_r\gamma_{r,s} = 0$, segue que $\alpha_r = 0$, para todo $r \in \{1, \ldots, k\}$.

vii) Dadas $\beta_1 = \{v_i \mid i \in I\}$ uma base de V e $\beta_2 = \{w_j \mid j \in J\}$ uma base de W, então $\beta = \{v_i \otimes w_j \mid i \in I, j \in J\}$ é uma base de $V \otimes W$. Consequentemente, se $dim(V) = n$ e $dim(W) = m$, então $dim(V \otimes W) = nm$.

Dado qualquer elemento $a \in V \otimes W$, podemos escrever $a = \sum v \otimes w$, uma soma finita de tensores. Cada um destes vetores que compõem os tensores se escrevem como combinação linear finita de elementos de β_1 e de β_2 e assim vemos a escrito como uma combinação linear de elementos de β, mostrando que este conjunto gera $V \otimes W$. Tal conjunto é linearmente independente pelo item v).

Por fim, note que se V, W são $\mathbb{F}$-álgebras então o produto tensorial $V \otimes W$ também é uma álgebra. De fato, dadas $\beta_1 = \{v_i \mid i \in I\}$ uma base de V e $\beta_2 = \{w_j \mid j \in J\}$ uma base de W, então, pelo item *vii*) acima, $\beta = \{v_i \otimes w_j \mid i \in I, j \in J\}$ é uma base de $V \otimes W$. Podemos definir uma aplicação bilinear $\cdot : (V \otimes W) \times (V \otimes W) \longrightarrow V \otimes W$ tal que para elementos da base $\{((v_i \otimes w_j) \times (v_l \otimes w_m)) \mid i, l \in I, j, m \in J\}$ tenhamos $\cdot((v_i \otimes w_j), (v_l \otimes w_m)) := v_i v_l \otimes v_j v_m$. Tal operação faz de $V \otimes W$ uma $\mathbb{F}$-álgebra.

1.3 Identidades Polinomiais

Nesta seção apresentamos os polinômios e os polinômios graduados, que são as principais ferramentas que utilizamos para classificar as álgebras graduadas simples.

Definição 1.40 *Sejam B uma classe de álgebras, X um conjunto e F a álgebra gerada por X. Chamamos F de álgebra livre na classe B, livremente gerada pelo conjunto X se, para qualquer álgebra $R \in B$ toda aplicação $g : X \to R$ pode ser estendida para um homomorfismo $G : F \to R$. Dizemos que o posto de F é a cardinalidade do conjunto X.*

Exemplo 1.41 *Considerando a classe de todas as álgebras associativas unitárias, dado um conjunto X, podemos observar uma álgebra, que denotaremos por $\mathbb{F}\langle X\rangle$. É a álgebra cuja base é o conjunto de todas as palavras*

$$x_{i_1} \cdots x_{i_n},\ x_{i_j} \in X,\ \forall j \in \{1, \ldots, n\},\ n \in \mathbb{N} \cup \{0\}$$

e a multiplicação, chamada de concatenação, é definida por

$$(x_{i_1} \cdots x_{i_m})(x_{j_1} \cdots x_{j_n}) := x_{i_1} \cdots x_{i_m} x_{j_1} \cdots x_{j_n}, x_{i_k},\ x_{j_l} \in X.$$

A álgebra $\mathbb{F}\langle X\rangle$ é livre na classe de todas as álgebras associativas unitárias. Considerando o subespaço de $\mathbb{F}\langle X\rangle$ gerado por todas as palavras de tamanho maior do que ou igual a 1, obtemos uma álgebra não unitária livre, que é livre na classe de todas as álgebras associativas.

Mostremos que $\mathbb{F}\langle X\rangle$ é uma álgebra livre. Dadas uma álgebra R associativa e unitária e uma aplicação $g : X \to R$, podemos estender naturalmente g para $\mathbb{F}\langle X\rangle$ pondo $g(x_{i_1}\cdots x_{i_n}) = g(x_{i_1})\cdots g(x_{i_n})$ e considerando a linearidade. Não é difícil ver que tal extensão é um homomorfismo de álgebras.

Chamamos os elementos da álgebra $\mathbb{F}\langle X\rangle$ de polinômios e geralmente os identificamos por $f(x_{i_1},\ldots,x_{i_n}) \in \mathbb{F}\langle X\rangle$, ou com outra letra em vez de f, onde $x_{i_1},\ldots,x_{i_n}$ são os elementos de X que aparecem em f.

Definição 1.42 *Dados uma álgebra R e um polinômio $f(x_{i_1},\ldots,x_{i_n}) \in \mathbb{F}\langle X\rangle$, uma avaliação de uma lista ordenada de elementos $\{r_1,\ldots,r_n\} \in R$ em $f(x_{i_1},\ldots,x_{i_n})$ é o resultado que se obtém, em R, ao substituir no polinômio cada variável pelo elemento correspondente da lista, e denotamos tal avaliação por $f(r_1,\ldots,r_n)$.*

Definição 1.43 *Dada uma álgebra R, um polinômio $f(x_{i_1},\ldots,x_{i_n}) \in \mathbb{F}\langle X\rangle$ é chamado de identidade polinomial para R se, para qualquer lista de elementos de R, a sua avaliação em f é 0.*

Exemplo 1.44 *Se R é uma álgebra comutativa, então o polinômio $f(x_1,x_2) = x_1x_2 - x_2x_1$ é uma identidade polinomial para R. Na verdade, a recíproca é verdadeira, em suma, uma álgebra é comutativa se, e somente se, $f(x_1,x_2)$ é identidade polinomial. Com esse exemplo, podemos perceber que as propriedades de uma álgebra podem ser expressas por meio de identidades polinomiais. Também chamamos o polinômio f de comutador, e o denotamos $[x_1,x_2]$.*

Exemplo 1.45 *Um polinômio de central importância para o nosso estudo é o chamado Standard*

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

Para $n = 3$, $s_3(x_1,x_2,x_3) = x_1x_2x_3 + x_2x_3x_1 + x_3x_1x_2 - x_1x_3x_2 - x_2x_1x_3 - x_3x_2x_1$.

Existem polinômios especiais de $\mathbb{F}\langle X\rangle$, que são os monômios, ou seja, são os polinômios que se constituem de um escalar multiplicado por um produto de variáveis. Dado $m \in \mathbb{F}\langle X\rangle$ um monômio, podemos escrever

$$m(x_{i_1},x_{i_2},\ldots,x_{i_n}) = \alpha x_{j_1}^{\beta_1}x_{j_2}^{\beta_2}\cdots x_{j_m}^{\beta_m}$$

onde $\alpha \in \mathbb{F}$, cada j_l é igual a um i_r, podendo haver repetições de variáveis que não apareçam consecutivamente, $\beta_l \in \mathbb{N}$. Um exemplo prático de monômio é

$$m(x,y,z) = 7x^4yz^2y^2x.$$

Todo polinômio é, na verdade, uma soma de monômios.

Definição 1.46 *Dado $f \in \mathbb{F}\langle X\rangle$, dizemos que f é multilinear se em cada um de seus monômios não há repetição de variáveis e em cada monômio aparecem as mesmas variáveis.*

Note que um polinômio $f(x_1, x_2, \ldots, x_n)$ é multilinear se, e somente se, puder ser escrito na forma

$$f(x_1, x_2, \ldots, x_n) = \sum_{\sigma \in S_n} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)},$$

onde $\alpha_\sigma \in \mathbb{F}$. Deste modo, fica claro que o polinômio *standard* é multilinear.

Não é difícil ver que os polinômios multilineares possuem uma propriedade que justifica tal nome, são lineares em cada variável. Com isto queremos dizer, por exemplo, que para tais polinômios vale para a primeira variável (e para todas as demais)

$$f(y_1 + \alpha y_2, x_2, \ldots, x_n) = f(y_1, x_2, \ldots, x_n) + \alpha f(y_2, x_2, \ldots, x_n)$$

onde $\alpha \in \mathbb{F}, y_1, y_2 \in X$. A próxima observação sobre polinômios multilineares nos será útil mais adiante, na seção que trata do Teorema de Amitsur-Levitski.

Lema 1.47 *Sejam A uma álgebra sobre o corpo $\mathbb{F}$ e $B \subseteq A$ um subconjunto que gera A como espaço vetorial. Se f é um polinômio multilinear tal que toda avaliação por elementos de B é 0, então f é uma identidade polinomial para A.*

Demonstração. De fato, seja $f(x_1, x_2, \ldots, x_n)$ um polinômio com as qualidades descritas. Dados $a_1 = \sum \alpha_{1i} b_i, a_2 = \sum \alpha_{2i} b_i, \ldots, a_n = \sum \alpha_{ni} b_i \in A$, onde $b_i \in B$, como f é multilinear segue que

$$f(a_1, a_2, \ldots, a_n) = \sum \alpha_{1,i_1} \cdots \alpha_{n,i_n} f(b_{i_1}, \ldots, b_{i_n}) = 0.$$

■

Dados G um grupo e X um conjunto enumerável, defina X_g um subconjunto de X onde, para cada $g \neq h \in G$, X_g e X_h são disjuntos. Denotando $X_G = \bigcup_{g \in G} X_g$, podemos considerar a álgebra livre $\mathbb{F}\langle X_G\rangle$ e observar que naturalmente surge uma G-graduação para tal álgebra, pondo $deg(x) = g$, se $x \in X_g$. Além disso, definimos o grau do monômio $m = x_{i_1} x_{i_2} \cdots x_{i_n}$, com $x_{i_j} \in X_{g_j}$, pondo $deg(m) = g_1 g_2 \cdots g_n$, onde $g_k = deg(x_{i_k})$. Não é difícil mostrar que

$$\mathbb{F}\langle X_G\rangle = \bigoplus_{g \in G} \mathbb{F}\langle X_G\rangle_g,$$

onde $\mathbb{F}\langle X_G\rangle_g$ é o subespaço de $\mathbb{F}\langle X_G\rangle$ gerado por todos os monômios de grau g.

Chamamos os elementos de $\mathbb{F}\langle X_G\rangle$ de polinômios G-graduados. Dado $f \in \mathbb{F}\langle X_G\rangle$, escrevemos $f(x_1^{g_1}, x_2^{g_2}, \ldots, x_n^{g_n})$ para especificar que $x_1^{g_1}, x_2^{g_2}, \ldots, x_n^{g_n}$ são os elementos de X_G, ou variáveis, que aparecem no polinômio f, com $deg(x_i^{g_i}) = g_i$.

Dada R uma álgebra, anteriormente definimos a avaliação de uma lista ordenada $r_1, \ldots, r_n \in R$ em um polinômio $f(x_1, \ldots, x_n) \in \mathbb{F}\langle X\rangle$. Agora, de maneira análoga, dados uma álgebra G-graduada $R = \bigoplus_{g\in G} R_g$, uma lista ordenada $r_1, r_2, \ldots, r_n$ de elementos homogêneos de R e um polinômio G-graduado $f(x_1^{g_1}, x_2^{g_2}, \ldots, x_n^{g_n})$, dizemos que uma avaliação desta lista em f é admissível se $deg(r_i) = g_i$, para todo $i = 1, \ldots, n$. Lembremos que a avaliação é a substituição das variáveis pelos elementos da álgebra e, depois de feitas as operações induzidas por f, chamamos o resultado de avaliação f-admissível da lista $r_1, r_2, \ldots, r_n$ em f.

Definição 1.48 *Dados $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada e $f(x_1^{g_1}, x_2^{g_2}, \ldots, x_n^{g_n})$ um polinômio G-graduado, dizemos que f é uma identidade polinomial G-graduada para R se a avaliação f-admissível de qualquer lista $r_1, r_2, \ldots, r_n \in R$ em f é zero.*

Exemplo 1.49 *Seja R uma álgebra onde se observa uma graduação $R = R_0 \oplus R_1$, onde R_0 é o centro de R. Aqui, $G = \mathbb{Z}_2 = \{0, 1\}$. Um exemplo de álgebra que satisfaz tais condições é a álgebra de Grassmann, que será apresentada na próxima seção. Note que o polinômio $\mathbb{Z}_2$-graduado $f(x^0, y^1) = x^0y^1 - y^1x^0$ é uma identidade polinomial graduada para R.*

1.4 O Teorema de Amitsur-Levitski

O resultado principal do nosso texto deve uma parte do seu argumento à certeza de que toda álgebra matricial é uma PI-álgebra e, na verdade, a álgebra $M_n(\mathbb{F})$ satisfaz o polinômio *standard* s_{2n}. Utilizaremos este polinômio (e o fato de que ele é identidade para aquela álgebra) para construirmos, mais adiante, um polinômio graduado para a álgebra graduada que é o nosso objeto principal de estudos. Portanto, trazemos nesta seção uma demonstração simplificada trazida ao público em 1976 por Rosset [17] do famoso Teorema de Amitsur e Levitski.

Mas para atingirmos este objetivo, devemos primeiro tornar conhecidas algumas propriedades de uma álgebra que nos será muito útil, a álgebra de Grassmann, ou, como também é conhecida, álgebra exterior.

Exemplo 1.50 (Álgebra de Grassmann) *Apresentamos agora uma construção da álgebra de Grassmann. Sejam $\mathbb{F}$ um corpo de característica diferente de 2 e $X = \{x_1, x_2, \dots\}$ um conjunto de cardinalidade enumerável não finita. Dada a álgebra livre associativa $\mathbb{F}\langle X\rangle$ de posto enumerável, seja também I o ideal bilateral de $\mathbb{F}\langle X\rangle$ gerado pelo conjunto $\{x_i x_j + x_j x_i \mid i, j \in \mathbb{N}\}$. Podemos denotar $E := \dfrac{\mathbb{F}\langle X\rangle}{I}$ e $e_i := \overline{x_i}$, para $i \in \mathbb{N}$. Nesta notação, podemos afirmar que*

$$E = \langle 1, e_1, e_2, \cdots \mid e_i e_j = -e_j e_i, \text{ para todos } i, j \in \mathbb{N}\rangle.$$

Afirmamos agora que

$$\beta = \{1, e_{i_1} e_{i_2} \dots e_{i_k} \mid 1 \leq i_1 < i_2 < \cdots < i_k\}$$

é um conjunto gerador para E como espaço vetorial sobre $\mathbb{F}$. De fato, dado $a \in E$, $a = \sum_{j=(i_1,i_2,\dots)} \alpha_j e_{i_1} e_{i_2} \cdots e_{i_j}$ para algum $\alpha_j \in \mathbb{F}$, para todo $j \in \{1, \dots, k\}$. Visto que $e_i e_j = -e_j e_i$, para todos $i, j \in \mathbb{N}$, então podemos reorganizar cada parcela da soma de modo que os índices se apresentem de modo estritamente crescente, tendo o cuidado de verificarmos o sinal de menos que porventura apareça. Portanto podemos reescrever o elemento pondo

$$a = \sum_j (\pm\alpha_j) e_{l_1} e_{l_2} \cdots e_{l_j}, \text{ com } l_1 < l_2 < \cdots < l_j.$$

Daí concluímos que β é um conjunto gerador para E. Ademais, β é, na verdade, uma base para E. Isto pode ser verificado do seguinte modo. Em primeiro lugar, como $char(\mathbb{F}) \neq 2$, então $e_i^2 = 0$, pois $e_i e_i = -e_i e_i \Rightarrow 2e_i^2 = 0 \Rightarrow e_i^2 = 0$. Agora, para mostrar que β é linearmente independente, suponhamos por absurdo que exista uma soma $\sum_{i=1}^n \alpha_i w_i = 0$ com $w_i \in \beta$ e α_i escalares não nulos. Podemos, sem perda de generalidade, supor que tal relação é minimal no tocante ao número de coeficientes. Ora, se $n = 1$, temos $\alpha_1 = 0$. Suponha então que $n > 1$ e neste caso existe e_m que aparece em w_1 mas não em w_2, sem perda de generalidade. Note que $0 = e_m \sum_{i=1}^n \alpha_i w_i = \sum_{i=1}^n \alpha_i e_m w_i = \sum_{i=2}^n \pm\alpha_i w_i'$, pois como e_m aparece em w_1, $e_m w_1 = 0$. Ora, mas esta expressão também é nula, com coeficientes não nulos, mas com um número menor de coeficientes do que a expressão anterior, contradizendo a minimalidade desta quantidade. Portanto, β é uma base para E.

Dados dois elementos quaisquer da base β de E, digamos $a = e_{i_1} e_{i_2} \cdots e_{i_m}$ e $b = e_{j_1} e_{j_2} \cdots e_{j_n}$, utilizando a relação $e_i e_j = -e_j e_i$, obtemos

$$ab = (e_{i_1} e_{i_2} \cdots e_{i_m})(e_{j_1} e_{j_2} \cdots e_{j_n}) = (-1)^{mn} (e_{j_1} e_{j_2} \cdots e_{j_n})(e_{i_1} e_{i_2} \cdots e_{i_m}) = (-1)^{mn} ba$$

para $m, n \in \mathbb{N}$. Ora, note que se m ou n é par, vale $ab = ba$ e, por outro lado, se ambos m, n forem ímpares então $ab = -ba$. Considere os conjuntos

$$\beta_0 = \{1, e_{i_1} e_{i_2} \cdots e_{i_m} \mid m \text{ é par}, i_1 < i_2 < \cdots < i_m\} \text{ e}$$

$$\beta_1 = \{e_{i_1}e_{i_2}\cdots e_{i_m} |\ m \text{ é ímpar}, i_1 < i_2 < \cdots < i_m\}.$$

Chamando $E_0 = span\{\beta_0\}$ *e* $E_1 = span\{\beta_1\}$, *como* $\beta_0 \dot{\cup} \beta_1 = \beta$ *segue que* $E = E_0 \oplus E_1$. *Também não é difícil ver que* E_0 *é uma subálgebra comutativa de* E *e, mais ainda, é o seu centro.*

O objetivo desta seção é mostrarmos que o polinômio *standard* s_{2k} é uma identidade polinomial para a álgebra das matrizes $M_k(\mathbb{F})$, mas na verdade, é suficiente provarmos este fato para $\mathbb{F} = \mathbb{Q}$.

De fato, se s_{2k} é identidade para $M_k(\mathbb{Q})$, então, particularmente, também é identidade para o subconjunto $M_k(\mathbb{Z})$. Seja $\mathbb{Z}_p$ o corpo de p elementos e considere o homomorfismo sobrejetivo

$$\begin{array}{rccc} f: & M_k(\mathbb{Z}) & \longrightarrow & M_k(\mathbb{Z}_p) \\ & (a_{ij}) & \longmapsto & f((a_{ij})) := (\overline{a_{ij}}), \end{array}$$

onde $\overline{a_{ij}}$ é a classe de a_{ij} módulo p. Se $A = (a_{ij})$ então denotaremos $\overline{A} = (\overline{a_{ij}})$. Dada uma lista de classes de matrizes $\overline{A_1}, \overline{A_2}, \ldots, \overline{A_{2k}} \in M_k(\mathbb{Z}_p)$, temos

$$s_{2k}(\overline{A_1}, \overline{A_2}, \ldots, \overline{A_{2k}}) = f(s_{2k}(A_1, A_2, \ldots, A_{2k})) = f(0) = 0$$

mostrando que s_{2k} também é identidade para $M_k(\mathbb{Z}_p)$.

Pelo Lema 1.47, como s_{2k} é multilinear, para provar que este polinômio é uma identidade para $M_k(\mathbb{F})$, é suficiente mostrar que a avaliação nas matrizes unitárias E_{ij} é zero, pois tais matrizes geram a álgebra $M_k(\mathbb{F})$. Tais matrizes pertencem a $M_k(\mathbb{P})$, onde $\mathbb{P}$ é o subcorpo primo de $\mathbb{F}$, que é isomorfo a $\mathbb{Q}$, se for $char(\mathbb{F}) = 0$, e a $\mathbb{Z}_p$, caso contrário. Como s_{2k} é identidade tanto para $M_k(\mathbb{Z})$ quanto para $M_k(\mathbb{Z}_p)$, concluímos que s_{2k} é uma identidade polinomial para $M_k(\mathbb{F})$.

Utilizaremos um lema que trata da aplicação traço. Vale lembrar que dada uma matriz quadrada A, seu traço é a soma dos elementos da diagonal principal. A demonstração do lema pode ser encontrada na seção 1.7 de [11].

Lema 1.51 *Seja* C *uma* $\mathbb{Q}$*-álgebra comutativa. Se* $tr(A) = tr(A^2) = \cdots = tr(A^n) = 0$, *onde* A *é uma matriz de* $M_n(C)$, *então* $A^n = 0$.

Seja agora E a álgebra de Grassmann gerada por $\{e_1, e_2, \ldots\}$ sobre $\mathbb{Q}$ com a graduação que construímos $E = E_0 \oplus E_1$.

Lema 1.52 *Se A, B são matrizes com entradas em E_1, então $tr(AB) = -tr(BA)$.*

Demonstração. Podemos escrever $A = \sum A_i w_i$, $B = \sum B_i w_i$ onde $A_i, B_i \in M_n(\mathbb{F})$ e $w_i \in E_1$ são monômios nos elementos $e_1, e_2, \ldots$. Dados $w_i, w_j \in E_1$, temos $w_i w_j = -w_j w_i$ e, lembrando que $tr(RS) = tr(SR)$, para $R, S \in M_n(\mathbb{F})$, segue que

$$tr(AB) = \sum tr(A_i B_j) w_i w_j = -\sum tr(B_j A_i) w_j w_i = -tr(BA).$$

■

Observação 1.53 *Dados $e_1, e_2, \ldots, e_n \in E$ e σ uma permutação de S_n, então*

$$e_{\sigma(1)} e_{\sigma(2)} \cdots e_{\sigma(n)} = (-1)^{\sigma} e_1 e_2 \cdots e_n.$$

Demonstração. Toda representação de uma permutação qualquer como produto de transposições conserva a paridade do número das transposições. Assim, a observação estará demonstrada se pudermos mostrar que a troca da posição de dois elementos muda o sinal de um monômio de acordo com o sinal da transposição correspondente, em outras palavras, multiplica o monômio por (-1). Mas isto é exatamente o que acontece, pois para quaisquer $1 \leq k < l \leq n$,

$$e_{i_1} \cdots e_{i_{k-1}} e_{i_k} e_{i_{k+1}} \cdots e_{i_{l-1}} e_{i_l} e_{i_{l+1}} \cdots e_{i_n} = -e_{i_1} \cdots e_{i_{k-1}} e_{i_l} e_{i_{k+1}} \cdots e_{i_{l-1}} e_{i_k} e_{i_{l+1}} \cdots e_{i_n}.$$

■

Corolário 1.54 *Sejam $A_1, A_2, \ldots, A_{2k} \in M_n(\mathbb{F})$, onde $k \in \mathbb{N}$ e $char(\mathbb{F}) \neq 2$. Então $tr(s_{2k}(A_1, A_2, \ldots, A_{2k})) = 0$.*

Demonstração. Considere $A = \sum_{i=1}^{2k} A_i e_i \in M_n(E_1)$. Elevando A à potência $2k$, podemos fazer algumas observações,

$$A^{2k} = (A_1 e_1 + A_2 e_2 + \cdots + A_{2k} e_{2k})^{2k}.$$

Ao desenvolvermos esta potência, obteremos várias parcelas constituídas de produtos de $2k$ matrizes. Afirmamos que em todas as parcelas que houver alguma repetição de matrizes será nula. De fato, suponha que $A_{i_1} e_{i_1} A_{i_2} e_{i_2} \cdots A_{i_{2k}} e_{i_{2k}}$ é uma parcela onde há repetição e que $i_r = i_s$, com $r < s$. Ora,

$$\begin{aligned} A_{i_1} e_{i_1} A_{i_2} e_{i_2} \cdots A_{i_{2k}} e_{i_{2k}} &= A_{i_1} A_{i_2} \cdots A_{i_{2k}} e_{i_1} e_{i_2} \cdots e_{i_{2k}} \\ &= A_{i_1} A_{i_2} \cdots A_{i_{2k}} (-1)^{r+s-1} e_{i_r}^2 e_{i_1} e_{i_2} \cdots e_{i_{2k}} \\ &= 0, \end{aligned}$$

pois $e_i^2 = 0$. Assim as parcelas que talvez não se anulem são produtos de matrizes distintas em todas as permutações possíveis, em outras palavras,

$$A^{2k} = \sum_{\sigma \in S_{2k}} A_{\sigma(1)} e_{\sigma(1)} A_{\sigma(2)} e_{\sigma(2)} \cdots A_{\sigma(2k)} e_{\sigma(2k)}.$$

Dada $\sigma \in S_{2k}$, pela observação anterior,

$$e_{\sigma(1)} e_{\sigma(2)} \cdots e_{\sigma(2k)} = (-1)^{\sigma} e_1 e_2 \cdots e_{2k}$$

donde segue que

$$A^{2k} = \sum_{\sigma \in S_{2k}} (-1)^{\sigma} A_{\sigma(1)} A_{\sigma(2)} \cdots A_{\sigma(2k)} e_1 e_2 \cdots e_{2k}.$$

Por outro lado, pelo Lema 1.52,

$$tr(A^{2k}) = tr(AA^{2k-1}) = -tr(A^{2k-1}A) = -tr(A^{2k}).$$

Como $char(\mathbb{F}) \neq 2$ segue que

$$tr(A^{2k}) = 0 \Rightarrow tr\left(\sum_{\sigma \in S_{2k}} (-1)^{\sigma} A_{\sigma(1)} A_{\sigma(2)} \cdots A_{\sigma(2k)} e_1 e_2 \cdots e_{2k}\right) = 0 \Rightarrow$$

$$= tr\left(\sum_{\sigma \in S_{2k}} (-1)^{\sigma} A_{\sigma(1)} A_{\sigma(2)} \cdots A_{\sigma(2k)}\right) e_1 e_2 \cdots e_{2k} = 0$$

e, como $e_1 e_2 \cdots e_{2k} \neq 0$, segue, finalmente, que

$$0 = tr\left(\sum_{\sigma \in S_{2k}} (-1)^{\sigma} A_{\sigma(1)} A_{\sigma(2)} \cdots A_{\sigma(2k)}\right) = tr(s_{2k}(A_1, A_2, \ldots, A_{2k})).$$

■

Teorema 1.55 (Amitsur-Levitski) *O polinômio s_{2n} é uma identidade polinomial para a álgebra das matrizes $M_n(\mathbb{F})$.*

Demonstração. Pelo que já mencionamos anteriormente, é suficiente mostrar que s_{2n} se anula para avaliações em $M_n(\mathbb{Q})$. Tomemos $A_1, A_2, \ldots, A_{2n} \in M_n(\mathbb{Q})$ e considere a álgebra de Grassmann $E = E_0 \oplus E_1$ sobre o corpo dos números racionais. Pondo $A = \sum_{i=1}^{2n} A_i e_i \in M_n(E_1)$, temos, como se pode ver na demonstração do corolário anterior,

$$A^{2n} = s_{2n}(A_1, A_2, \ldots, A_{2n}) e_1 \cdots e_{2n}.$$

Mostraremos que $A^{2n} = 0$. De fato, pelo Lema 1.52, como $A, A^{2i-1} \in M_n(E_1)$, para todo $i \in \{1, \ldots, n\}$, então $tr(A^{2i}) = tr(AA^{2i-1}) = -tr(A^{2i-1}A) = -tr(A^{2i})$ e, assim, $tr(A^{2i}) = 0$. Além disso, como as entradas da matriz A pertencem todas a E_1; se $A = (a_{ij})$, então $A^2 = (\sum_{k=1}^{n} a_{ik}a_{kj})$. Como $a_{ik}, a_{kj} \in E_1$, então $a_{ik}a_{kj} \in E_0$, de onde segue que $A^2 \in M_n(E_0)$. Do Lema 1.51 obtemos que $A^{2n} = 0$. ■

Definimos o grau de um polinômio como a maior quantidade de variáveis (incluindo potências) que ocorrem em algum monômio do polinômio. Vimos que a álgebra $M_n(\mathbb{F})$ satisfaz uma identidade polinomial de grau $2n$. Na verdade, este é o menor grau possível com que um polinômio pode ser identidade polinomial para tal álgebra, que é a conclusão que segue da próxima proposição. Para mais detalhes, vide o Teorema 6.24 da referência [7].

Observação 1.56 (Processo de Multilinearização) *Dados uma álgebra A e um polinômio f que é identidade para A, podemos obter um polinômio multilinear que é também identidade para A e tem grau menor do que ou igual ao grau de f.*

De fato, se $f(x_1, x_2, \ldots, x_n)$ é identidade polinomial para A, supondo que o grau da variável x_1 é 2, então o polinômio

$$g(x_1, y_1, x_2, \ldots, x_n) := f(x_1 + y_1, x_2, \ldots, x_n) - f(x_1, x_2, \ldots, x_n) - f(y_1, x_2, \ldots, x_n)$$

é identidade para A, o grau de x_1 é 1 e o grau do polinômio g é menor do que ou igual ao de f. Caso o grau de x_1 seja maior do que 2, basta fazer este processo reiteradamente. Como o grau dos polinômios resultantes das etapas do processo está limitado pelo grau de f, então o processo para quando se obtiver um polinômio multilinear.

Ademais, vale a afirmação contra-positiva, que será usada na próxima proposição, se g não é identidade para A, então f também não é.

Proposição 1.57 *Não existe polinômio de grau menor do que $2n$ que seja identidade polinomial para $M_n(\mathbb{F})$.*

Demonstração. Suponha, por absurdo, que f é uma identidade polinomial de grau $d < 2n$ para $M_n(\mathbb{F})$. Podemos supor, pela observação anterior, que f é multilinear. Podemos também supor que o grau de f é exatamente $2n-1$. Se o grau de f fosse menor ainda, poderíamos multiplicar o polinômio por variáveis distintas que não ocorram em f, de modo que o grau se torne $2n-1$. Assim, podemos escrever f da seguinte maneira:

$$f(x_1, x_2, \ldots, x_{2n-1}) = \sum_{\sigma \in S_{2n-1}} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(2n-1)}.$$

E podemos supor que $\alpha_1 \neq 0$, renomeando as variáveis, se necessário. Fazendo a avaliação nas matrizes unitárias $(E_{11}, E_{12}, E_{22}, \ldots, E_{n-1,n}, E_{nn})$, obtemos

$$f(E_{11}, E_{12}, E_{22}, \ldots, E_{n-1,n}, E_{nn}) = \alpha_1 E_{1k} \neq 0.$$

De fato, pois a única permutação que não faz o produto das matrizes unitárias se anular é a identidade. Portanto este polinômio não é identidade para $M_n(\mathbb{F})$. ■

Capítulo 2

Álgebras Graduadas Simples e Identidades Polinomiais Graduadas

Neste capítulo, salvo em menção contrária, todas as álgebras utilizadas são associativas. Nas duas primeiras seções seguimos principalmente o livro [9] como referência e na última seção nos atemos à referência principal desta dissertação, o artigo [13].

2.1 Sobre Álgebras Graduadas Simples de Dimensão Finita

Nesta seção nos dedicamos mais exclusivamente às álgebras graduadas simples, trazendo algumas proposições sobre tais estruturas que nos auxiliarão mais adiante para o nosso objetivo principal. Em primeiro lugar, por meio dos próximos dois lemas e do teorema que os segue, provaremos que toda álgebra graduada simples de dimensão finita é unitária. Utilizamos o artigo [4] como referência para esse resultado.

Mas antes cabe observar um fato interessante sobre o aniquilador à direita de um elemento em uma álgebra.

Observação 2.1 *Sejam $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada e $a \in R$ um elemento homogêneo de grau h. Então o aniquilador à direita de a em R, o conjunto $A = \{x \in R \mid ax = 0\}$, é um ideal à direita graduado.*

Demonstração. Mostremos em primeiro lugar que o conjunto A é um ideal à direita.

Claramente A é um subespaço de R. Quanto à propriedade absorvente do produto, dados $r \in R$ e $x \in A$, então $ax = 0$ e daí $a(xr) = (ax)r = 0$. Logo, $xr \in A$.

Agora resta mostrarmos que tal ideal é graduado. Dado $x_{g_1} + \cdots + x_{g_k} \in A$, temos $a(x_{g_1} + \cdots + x_{g_k}) = 0$, ou ainda, $ax_{g_1} + \cdots + ax_{g_k} = 0$. Como $deg(ax_{g_i}) = hg_i$ e $hg_i \neq hg_j$ para $i \neq j$, temos $ax_{g_i} = 0$ para todo i. Logo $x_{g_i} \in A$ para todo i ■

Lema 2.2 *Seja $R = \bigoplus_{g \in G} R_g$ uma álgebra graduada simples e $I \subseteq R$ um ideal graduado à direita minimal de R. Então $I = aR$ para algum idempotente homogêneo a.*

Demonstração. Suponhamos $I^2 = 0$. Como $(RI)^2 = R(IR)I \subseteq RII = RI^2 = 0$, o ideal bilateral RI de R é nilpotente. Note que RI é um ideal graduado. De fato, dado $b \in RI$, $b = b_1 + \cdots + b_n$, com $b_i \in R_{g_i}$, para $i \in \{1, \ldots, n\}$, existem $r_1, \ldots, r_k \in R$ e $a_1, \ldots, a_k \in I$ para algum $k \in \mathbb{N}$ tais que $b = \sum_{j=1}^{k} r_j a_j$. Também podemos escrever, para cada j, $r_j = r_{j1} + \cdots + r_{jl}$ e $a_j = a_{j1} + \cdots + a_{jl}$, com $r_{js} \in R_{g_s}$ e $a_{js} \in R_{g_s} \cap I$ para todo $s = 1, \ldots, l$. Segue que $b = \sum_{j=1}^{k}((r_{j1} + \cdots + r_{jl})(a_{j1} + \cdots + a_{jl}))$. Desenvolvendo a soma usando a distributividade e agrupando as parcelas de acordo com os graus, não é difícil ver que para cada i, $b_i = \sum r_p a_q$, para alguns $p, q \in \mathbb{N}$. Daí segue que $b_i \in RI$ e, portanto, RI é um ideal graduado.

Como R é graduada simples, devemos ter $RI = 0$ ou $RI = R$. Por definição, $R^2 \neq 0$. Como mostramos que $(RI)^2 = 0$, então resta a possibilidade $RI = 0 \subseteq I$. Assim, I é um ideal graduado bilateral não trivial, o que contradiz nossa hipótese de que R é graduado simples. Obtemos $I^2 \neq 0$ e assim existe um elemento homogêneo $x \neq 0$ em I tal que $xI \neq 0$. Como I é minimal e $xI \subseteq I$, então $xI = I$. Existe $a \in I$ um elemento homogêneo não nulo tal que $xa = x$.

Considerando agora o aniquilador à direita X de x em R, sabemos que X é um ideal à direita graduado e, da minimalidade de I, devemos ter $I \cap X = 0$ ou $I \cap X = I$. Como $xa = x \neq 0 \Rightarrow a \in I \setminus X$, então $I \cap X = 0$. Por fim,

$$xa^2 = xa = x \Rightarrow x(a^2 - a) = 0 \Rightarrow a^2 - a \in I \cap X = 0 \Rightarrow a^2 = a,$$

em outras palavras, a é idempotente. Como aI é um ideal à direita graduado não nulo, pois $a^2 \in aI \setminus \{0\}$ e aI está contido em I, então $aI = I$. Ora, $a \in I \Rightarrow aR \subset I$ e, por outro lado, $I = aI \subset aR$, de onde segue que $I = aR$. ■

Lema 2.3 *Seja $I \subset R$ um ideal à direita graduado não nulo de uma álgebra graduada simples de dimensão finita R. Então $I = bR$, onde $b \in R$ é um elemento homogêneo idempotente.*

Demonstração. Como $dimR < \infty$ todo ideal à direita contém um ideal à direita minimal. Pelo Lema 2.2 tal ideal contém um elemento homogêneo idempotente a. Dado $t \in I$ homogêneo e idempotente, denotamos por $A(t) = \{x \in I \mid tx = 0\}$, o aniquilador à direita de t em I. Afirmamos que existe um idempotente homogêneo $b \in I$ tal que $A(b) = 0$. Para isto, é suficiente mostrar que se $A(a) \neq 0$, então é possível encontrar outro idempotente homogêneo $t \in I$ com $dimA(t) < dimA(a)$. Como a é homogêneo, o aniquilador à direita T de a em R é um ideal à direita graduado. Assim, $A(a) = T \cap I$ é também um ideal à direita graduado. Novamente pelo Lema 2.2, podemos encontrar um idempotente homogêneo $c \in A(a)$. Então $c^2 = c$ e $ac = 0$. Considerando $t = a + c - ca$, segue que

$$t^2 = (a + c - ca)(a + c - ca) = a + c - ca = t \qquad \text{e} \qquad at = a,$$

mostrando que t é também idempotente. Agora mostraremos que $A(t)$ é um subespaço próprio de $A(a)$. Tomando $x \in A(t)$,

$$0 = tx = atx = a(a + c - ca)x = a^2x = ax,$$

donde x aniquila a, ou, $A(t) \subseteq A(a)$. Por outro lado, $ac = 0$, mas $tc = (a + c - ca)c = c^2 = c \neq 0$ e assim $c \in A(a) \setminus A(t)$, mostrando que $A(t) \subsetneq A(a)$. Repetindo este processo, obtemos um idempotente graduado $b \in I$ tal que $A(b) = 0$, ou seja, $bx \neq 0$, para todo $x \in I \setminus \{0\}$. Como $bx - b^2x = 0$, temos $b(x - bx) = 0$, ou seja, $(x - bx) \in A(b) = 0$, e obtemos $x = bx$, e assim, $bI = I$. Analogamente à conclusão do Lema 2.2, obtemos $I = bR$. ■

Teorema 2.4 *Seja R uma álgebra graduada simples de dimensão finita. Então R é unitária.*

Demonstração. Pelo Lema 2.3, existe um idempotente homogêneo $a \in R$ tal que $R = aR$. Dado $x \in R$, existe $y \in R$ tal que $x = ay$. Por outro lado, multiplicando ambos os membros pelo idempotente a, obtemos $ax = a^2y = ay$, de onde segue que $ax = x$, para todo $x \in R$. Note que $a \in R_e$, pois

$$a = a^2 \Rightarrow deg(a) = deg(a^2) \Rightarrow deg(a) = deg(a)^2 \Rightarrow e = deg(a).$$

Considere $I = \{x - xa \mid x \in R\}$. I é um subespaço graduado, pois dado $\sum x_g - (\sum x_g)a \in I$, cada componente homogênea $x_g - x_g a$ pertence a I. Claramente I é um ideal à esquerda e $Ia = 0$. Assim, $IR = IaR = 0 \subset I$, mostrando que I é um ideal graduado bilateral. Pela simplicidade de R, $I = 0$ ou $I = R$. Se $I = R$, então $R^2 = IR = 0$, o que não ocorre. Segue que $I = 0$ e, portanto, $xa = x$, para todo $x \in R$. Por outro lado, como $R = aR$, existe $y \in R$ tal que $y = ax$. Ora, $ay = aax = ax$, e assim $y = x$, ou seja, $x = ax$. Segue que R possui unidade a. ■

Lema 2.5 *Seja $R = \bigoplus_{g \in G} R_g$ uma álgebra graduada de divisão de dimensão finita sobre um corpo $\mathbb{F}$ algebricamente fechado. Então $H = Supp(R)$ é um subgrupo de G e $dim(R_h) = 1$, para todo $h \in H$.*

Demonstração. Em primeiro lugar, H é fechado à operação do grupo G. De fato, dados $g, h \in H$, existem $r_g \in R_g \setminus \{0\}$, $r_h \in R_h \setminus \{0\}$. Dado que ambos r_g, r_h são invertíveis, não são divisores de zero, donde segue que $r_g r_h \neq 0$. Como $R_g R_h \subset R_{gh}$, segue que $R_{gh} \neq 0$, ou, em outras palavras, $gh \in H$. Além disso, existe $(r_g)^{-1}$ tal que $r_g(r_g)^{-1} = 1$. Mostremos que $(r_g)^{-1}$ é homogêneo de grau g^{-1}. De fato, seja $(r_g)^{-1} = \sum_{t \in G} u_t$ onde $u_t \in R_t$ para todo $t \in G$. Assim, $1 = r_g(r_g)^{-1} = r_g \sum_{t \in G} u_t = \sum_{t \in G} r_g u_t$. Daí,

$$1 - r_g u_{g^{-1}} = \sum_{\substack{t \in G \\ t \neq g^{-1}}} \Rightarrow 1 - r_g u_{g^{-1}} = 0 \Rightarrow 1 = r_g u_{g^{-1}},$$

de onde segue que $(r_g)^{-1} = u_{g^{-1}}$, como queríamos mostrar. Ora, como $deg(r_g(r_g)^{-1}) = e \Rightarrow g\ deg((r_g)^{-1}) = e$, segue que o grau de $(r_g)^{-1}$ é g^{-1}, mostrando que se $g \in H$, então $g^{-1} \in H$, e, assim, H é um subgrupo de G.

Agora note que R_e é uma álgebra de divisão de dimensão finita sobre um corpo algebricamente fechado. Pela Observação 1.31 no capítulo anterior temos $R_e = \mathbb{F}$ e, em particular, $dim(R_e) = 1$.

Dados $g \neq e$ e $x \in R_g \setminus \{0\}$, existe um inverso x^{-1} que é homogêneo e $x^{-1} \in R_{g-1}$. Dado também $y \in R_g \setminus \{0\}$, temos $x^{-1}y \in R_e$ e, assim, $y = \lambda x$, para algum $\lambda \in \mathbb{F}$. Segue que $dim(R_g) = 1$. ■

No próximo teorema, podemos observar que se H é um subgrupo de G, a álgebra de grupo *twisted* $F^\sigma[H]$ além de álgebra H-graduada, também é G-graduada se definirmos $(F^\sigma[H])_g = 0$ para todo $g \in (G \setminus H)$. Consideraremos exatamente esta G-graduação em $F^\sigma[H]$.

Teorema 2.6 *Seja $R = \bigoplus_{g\in G} R_g$ uma álgebra G-graduada de dimensão finita sobre um corpo algebricamente fechado $\mathbb{F}$. R é uma álgebra graduada de divisão se, e somente se, R é isomorfa à álgebra de grupo twisted $\mathbb{F}^\sigma[H]$ com a H-graduação canônica, onde H é um subgrupo finito de G e $\sigma : H \times H \to \mathbb{F} \setminus \{0\}$ é um 2-cociclo em H.*

Demonstração. Sabendo que $\mathbb{F}^\sigma[H]$ é uma álgebra graduada de divisão, se existir tal isomorfismo, segue que R é uma álgebra graduada de divisão.

Reciprocamente, seja R uma álgebra graduada de divisão. Como R tem dimensão finita e pelo Lema 2.5, $dim(R_g) = 1$, para todo $g \in Supp(R) =: H$. Então a ordem de H é a dimensão de R, ou seja, H é finito. Para cada g, fixamos um $r_g \in R_g \setminus \{0\}$. Se $g, h \in H$, temos

$$r_g r_h = \sigma(g,h) r_{gh},$$

para algum escalar não nulo $\sigma(g,h) \in \mathbb{F}$, pois $R_g R_h \subset R_{gh}$ e $dim(R_{gh}) = 1$. Como R é associativa, devemos ter

$$\begin{aligned}
(r_g r_h) r_z = r_g (r_h r_z) &\Rightarrow \sigma(g,h) r_{gh} r_z = r_g(\sigma(h,z) r_{hz}) \\
&\Rightarrow \sigma(g,h)\sigma(gh,z) r_{ghz} = \sigma(h,z)\sigma(g,hz) r_{ghz} \\
&\Rightarrow \sigma(g,h)\sigma(gh,z) = \sigma(h,z)\sigma(g,hz),
\end{aligned}$$

mostrando que a multiplicação do grupo é associativa. Agora exibiremos um isomorfismo entre R e $\mathbb{F}^\sigma[H]$. Seja $\{r_{h_1}, r_{h_2}, \ldots, r_{h_n}\}$ uma base homogênea de R e definamos uma aplicação linear $f : R \to \mathbb{F}^\sigma[H]$ pondo $f(r_{h_i}) = h_i$, para todo $i = 1, \ldots, n$. Não é difícil ver que esta aplicação é um isomorfismo de espaços vetoriais. Mais ainda, considerando em R o produto induzido por $r_g r_h = \sigma(g,h) r_{gh}$, f se torna um isomorfismo de álgebras. De fato, dados $r_g, r_h \in R$, temos

$$\begin{aligned}
f(r_g) f(r_h) &= g \cdot h = \sigma(g,h) gh \\
&= f(\sigma(g,h) r_{gh}) = f(r_g r_h),
\end{aligned}$$

de onde segue que $R \simeq \mathbb{F}^\sigma[H]$. ■

Antes de enunciar o próximo resultado é conveniente lembrar que escrevemos os homomorfismos em um módulo do lado oposto aos escalares.

Teorema 2.7 *Seja R uma álgebra G-graduada. Suponha que V é um R-módulo à esquerda graduado simples e seja $D = End_R^{gr}(V)$. Se $v_1, \ldots, v_n \in V$ são elementos homogêneos LI sobre D, então para quaisquer $w_1, \ldots, w_n \in V$ existe $r \in R$ tal que $rv_i = w_i$, $i = 1, \ldots, n$.*

Demonstração. É suficiente provar que existe $s_1 \in R$ homogêneo tal que $s_1 v_1 \neq 0$ e $s_1 v_2 = \cdots = s_1 v_n = 0$. Neste caso, pela simplicidade de V, obtemos $< s_1 v_1 >= V$ e existe $t_1 \in R$ tal que $t_1 s_1 v_1 = w_1$. Procedendo de maneira análoga para cada i, obtemos $r_i := t_i s_i \in R$ tal que $r_i v_i = w_i$ e $r_i v_j = 0$, para todo $i \neq j$. Tomando $r := r_1 + r_2 + \cdots + r_n$, temos

$$rv_i = (r_1 + \cdots + r_n)v_i = r_1 v_i + \cdots + r_i v_i + \cdots + r_n v_i = r_i v_i = w_i,$$

o que prova o teorema.

Provaremos nossa afirmação por indução em n. Para $n = 1$, supondo por contradição que não existe $r \in R$ tal que $rv_1 \neq 0$ teríamos $Rv_1 = 0$. O subespaço gerado por v_1 seria um submódulo não nulo e portanto igual a V. Por outro lado, como $Rv_1 = 0$ teríamos $RV = 0$, o que seria um absurdo.

Para o passo de indução, considere I o aniquilador de $\{v_2, \ldots, v_{n-1}\}$, ou seja,

$$I = \{r \in R \mid rv_2 = \cdots = rv_{n-1} = 0\}.$$

Analogamente ao que fizemos na Observação 2.1, mas desta vez trocando direita por esquerda, e notando que I é a interseção dos anuladores de $v_2, \ldots, v_{n-1}$, segue que I é um ideal à esquerda graduado de R. Seja agora $W \subset V$ o aniquilador de I,

$$W = \{v \in V \mid Iv = 0\},$$

que é um D-submódulo graduado de V. Mostremos que $W = v_2 D \oplus \cdots \oplus v_{n-1} D$. De fato, como $v_2, \ldots, v_{n-1} \in W$, segue que $v_2 D \oplus \cdots \oplus v_{n-1} D \subset W$. Por outro lado, supondo por contradição que não haja a igualdade, deve existir $v \in W \setminus v_2 D \oplus \cdots \oplus v_{n-1} D$, de onde segue que $\{v, v_2, \ldots, v_{n-1}\}$ é LI. Por hipótese de indução, existe r com $rv \neq 0$ e $rv_2 = \cdots = rv_{n-1} = 0$. Neste caso $r \in I$, pela definição de I, e como $v \in W$ devemos ter $rv = 0$, pela definição de W, contradizendo o fato que $rv \neq 0$. Segue que $W = v_2 D \oplus \cdots \oplus v_{n-1} D$.

Em particular, $v_1, v_n \notin W$ e como V é simples, $Iv_1 = Iv_n = V$. Se existir $r \in I$ tal que $rv_1 \neq 0$ e $rv_n = 0$, o argumento estará completo. Se tal r não existir, podemos definir $d : Iv_n \to Iv_1$ tal que $rv_n \mapsto rv_1$. De fato, supondo por contradição que a função d não estivesse bem definida, existiriam $r_1, r_2 \in I$, com $r_1 v_n = r_2 v_n$ mas $(r_1 v_n)d = r_1 v_1 \neq r_2 v_1 = (r_2 v_n)d$. Considerando o elemento $r := (r_1 - r_2) \in I$, temos

$rv_1 = (r_1 - r_2)v_1 \neq 0$ e $rv_n = (r_1 - r_2)v_n = 0$, um absurdo, pois tal r não existe. Portanto d está bem definida.

Note que d é um homomorfismo de R-módulos e uma transformação homogênea de grau $(deg(v_n))^{-1}deg(v_1)$. Segue que $d \in D$. Pela definição de d, temos $r(v_n d - v_1) = 0$, para todo $r \in I$, o que implica $v_n d - v_1 \in W$, uma contradição. ■

Teorema 2.8 *Sejam G um grupo e R uma álgebra G-graduada. Se R é graduada simples e satisfaz a condição de cadeia descendente em ideais graduados à esquerda, então existem uma álgebra G-graduada D e um D-módulo à direita graduado V tais que D é uma álgebra graduada de divisão, V tem dimensão finita sobre D e R é isomorfo a $End_D(V)$ como uma álgebra G-graduada.*

Demonstração. Pela Observação 1.16, existe um ideal à esquerda graduado minimal V. Considerando o anulador de V em R, o conjunto $A = A_R(V) = \{r \in R \mid rV = 0\}$, temos que A é um ideal bilateral graduado de R. De fato, dados $a = a_e + a_{g_1} + \cdots + a_{g_m} \in A$, $r \in R$ e $v \in V$ um elemento homogêneo de grau g, $(ar)V = a(rV) = 0 \Rightarrow ar \in A$, $(ra)V = r(aV) = 0 \Rightarrow ra \in A$ e $0 = av = (a_e + a_{g_1} + \cdots + a_{g_m})v = a_e v + a_{g_1} v + \cdots + a_{g_m} v$. Daí segue que $a_{g_i} \in A$, para todo i, pois cada parcela tem grau distinto das demais, e assim todas são nulas. Ora, sendo A um ideal graduado de R, uma álgebra graduada simples, há duas possibilidades: $A = R$, o que é equivalente a $RV = 0$, ou $A = 0$, e R age fielmente em V. Se $RV = 0$, obtemos $V + VR$ é um ideal bilateral graduado não nulo, pois $R(V + VR) = RV + (RV)R = 0 \subset V + VR$. Ora, da simplicidade de R, segue que $(V + VR) = R$, um absurdo, pois neste caso $R^2 = R(V + VR) = 0$. Segue que R age fielmente em V e podemos ver V como um R-módulo à esquerda graduado simples. Também podemos enxergar R imerso em $End_D(V)$, onde $D = End_R^{gr}(V)$. Para isto, basta considerar, para cada $r \in R$, a aplicação $v \to rv$.

Mostraremos agora que V tem dimensão finita como um D-módulo. Se não tivesse, poderíamos construir uma cadeia infinita de ideais à esquerda graduados em R. Para isto, bastaria tomar uma sequência infinita $v_1, v_2, \ldots$ de elementos homogêneos LI sobre D e notar que as inclusões da cadeia

$$A_R(\{v_1\}) \supset A_R(\{v_1, v_2\}) \supset \cdots$$

seriam próprias, pois poderíamos, pelo Teorema 2.7, obter elementos que anulam $v_1, \ldots, v_n$ mas não anulam v_{n+1}.

Por fim, dados uma base $\{v_1, \ldots, v_n\}$ homogênea de V e um elemento $f \in End_D(V)$, sabemos que f pode ser identificado pela imagem dos elementos da base. Pelo Lema 2.7, como neste caso $End_D(V) = End_D^{gr}(V)$, existe um elemento $r \in R$ tal que $rv_i = f(v_i)$, e, portanto, f pode ser identificado com tal r. ■

Observação 2.9

- *Fixando-se uma D-base homogênea $\{v_1, \ldots, v_n\}$ em V e sendo g_i o grau de v_i, podemos identificar $End_D(V)$ com a álgebra de matrizes $M_n(D)$ construindo um isomorfismo entre as álgebras:*

  Dado $r \in End_D(V)$, para cada $j = 1, \ldots, n$, $rv_j = \sum_{i=1}^{n} v_i x_{ij}$, onde os x_{ij} são escalares em D. Podemos, a partir daí, associar o endomorfismo r com a matriz $(x_{ij}) \in M_n(D)$. Note que esta identificação depende da D-base escolhida, mas nesta base esta associação é, na verdade, um isomorfismo

$$\begin{array}{rccc} \varphi: & End_D(V) & \longrightarrow & M_n(D) \\ & r & \longmapsto & \varphi(r) := (x_{ij}). \end{array}$$

  Mostremos primeiro que φ é um homomorfismo de álgebras e depois que é injetivo e sobrejetivo. Sejam $r_1, r_2 \in End_D(V)$, $\alpha \in \mathbb{F}$, e $\varphi(r_1) = (x_{ij}), \varphi(r_2) = (y_{ij})$. Ora, como são endomorfismos, para cada $j = 1, \ldots, n$,

$$(r_1 + r_2\alpha)v_j = r_1 v_j + (r_2 v_j)\alpha = \sum_{i=1}^{n} v_i x_{ij} + (\sum_{i=1}^{n} v_i y_{ij})\alpha$$

  . Segue que

$$\begin{array}{rcl} \varphi(r_1 + r_2\alpha) & = & (x_{ij} + y_{ij}\alpha) = (x_{ij}) + (y_{ij})\alpha \\ & = & \varphi(r_1) + \varphi(r_2)\alpha. \end{array}$$

  Agora provaremos que φ é um isomorfismo com relação à multiplicação das álgebras, que no caso de $End_D(V)$ é a composição de funções. Ora, para cada $j = 1, \ldots, n$, temos

$$\begin{array}{rcl} r_1 r_2 v_j & = & r_1 \left(\sum_{k=1}^{n} v_k y_{kj}\right) = \sum (r_1 v_k y_{kj}) \\ & = & \sum_{k=1}^{n} \left(\left(\sum_{i=1}^{n} v_i x_{ik}\right) y_{kj}\right) = \sum_{i=1}^{n} \left(v_i \left(\sum_{k=1}^{n} x_{ik} y_{kj}\right)\right). \end{array}$$

  Obtemos que a matriz $\varphi(r_1 r_2) = (c_{ij})$, onde $c_{ij} = \sum_{k=1}^{n} x_{ik} y_{kj}$. Por outro lado, sabemos que esta é exatamente a matriz produto entre (x_{ij}) e (y_{ij}). Portanto,

$$\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2).$$

  Dado $r \in End_D(V)$ com $\varphi(r) = 0$, obtemos que todas as imagens rv_i são nulas, para todo i. Assim, dado $v = \sum v_i \alpha_i \in V \setminus \{0\}$, temos $rv = r(\sum v_i \alpha_i) =$

$\sum(rv_i)\alpha_i = 0$ *e, portanto,* r *é o endomorfismo nulo, o que é suficiente para provar que* φ *é injetora.*

Por fim, dada um matriz $(x_{ij}) \in M_n(D)$*, existe o endomorfismo* $r \in End_D(V)$ *tal que, para cada* $j = 1, \ldots, n$*,* $rv_j = \sum_{i=1}^{n} v_i x_{ij}$*, ou seja,* $\varphi(r) = (x_{ij})$*, concluindo que* φ *é um isomorfismo de álgebras.*

- *Também podemos identificar* $M_n(D)$ *com* $M_n(\mathbb{F}) \otimes D$ *da seguinte maneira: para cada* $(\lambda_{ij}) \otimes d \in M_n(\mathbb{F}) \otimes D$*, associamos a matriz* $(\lambda_{ij}d) \in M_n(D)$ *e a graduação é dada por*

$$deg(E_{ij} \otimes d) = g_i deg(d) g_j^{-1}.$$

Com esta graduação o isomorfismo φ *é um isomorfismo de álgebras graduadas.*

2.2 Classificação das Álgebras Graduadas Simples de Dimensão Finita

Sejam V um R-módulo à esquerda graduado, $g \in G$, e $v \in V$, denotemos a graduação de V por Γ. O *shift* à direita $V^{[g]}$, que é o mesmo conjunto V e cada componente homogênea é definida por $V^{[g]}_{hg} := V_h$ é um R-módulo à esquerda graduado e denotamos sua graduação $\Gamma^{[g]}$. Note que $deg_{\Gamma^{[g]}}(v) = deg_{\Gamma}(v)g$, para todo $v \in V$ homogêneo.

Se $f : V \to V$ é uma transformação homogênea de grau t, então f, vista como uma transformação $V^{[g]} \to V^{[g]}$ será homogênea de grau $g^{-1}tg$. De fato, dado $h \in G$, $(V_h)f \subset V_{ht} \Rightarrow (V^{[g]}_{hg})f \subseteq V^{[g]}_{htg}$. Segue que se $End^{gr}_R(V) = D$, então

$$End^{gr}_R(V^{[g]}) =^{[g^{-1}]} D^{[g]}.$$

Lema 2.10 *Seja* R *uma álgebra graduada simples que possui um ideal graduado à esquerda minimal* I*. Então* I *é um* R*-módulo graduado simples à esquerda gerado por um idempotente homogêneo de* R*. Mais ainda, se* V *é um* R*-módulo à esquerda graduado simples, então existe* $g \in G$ *tal que* V *é isomorfo a* $I^{[g]}$ *como um* R*-módulo graduado.*

Demonstração. Mostremos que I é um R-módulo graduado simples. Suponha por contradição $I^2 = 0$ e considere $J = I + IR$. Como I é um ideal à esquerda, então J também é. Por outro lado, dados $i_1 + i_2 s \in J = I + IR$, com $i_1, i_2 \in I, s \in R$ e $r \in R$, temos $(i_1 + i_2 s)r = i_1 r + i_2 sr \in IR \subset I + IR = J$, completando a prova de que J é

um ideal bilateral. Como R é uma álgebra graduada simples, $J \subseteq R$ é um ideal de R e $J \neq 0$ então $J = R$. Nesse caso,

$$R^2 = (I + IR)(I + IR) = I^2 + I^2R + I(RI) + I(RI)R \subset I^2 + I^2R = 0,$$

um absurdo. Segue que $I^2 \neq 0$. Como I é ideal à esquerda graduado minimal, segue que I é um R-módulo à esquerda graduado simples. Tome agora $x \in I$ homogêneo tal que $Ix \neq 0$. Pela minimalidade de I, $Ix = I$ e $A_I(\{x\}) = 0$, pois tal conjunto é um ideal propriamente contido em I. Assim existe $\varepsilon \in I$ tal que $\varepsilon x = x$. Note que podemos substituir ε pela componente de ε em R_e, pois as demais componentes multiplicadas por x são nulas. Como

$$\varepsilon x = x \Rightarrow \varepsilon^2 x = \varepsilon x \Rightarrow (\varepsilon^2 - \varepsilon)x = 0 \Rightarrow \varepsilon^2 - \varepsilon \in A_I(\{x\}) = 0,$$

temos $\varepsilon^2 = \varepsilon$. Como $R\varepsilon \neq 0$ e $R\varepsilon \subset I$, segue que $R\varepsilon = I$.

Seja agora V um R-módulo à esquerda graduado simples. Como IV é um submódulo graduado de V, devemos ter $IV = 0$ ou $IV = V$. Pelo mesmo argumento usado na demonstração do Teorema 2.8, R age fielmente em V, de onde segue que $IV = V$. Tome $v \in V$ tal que $Iv \neq 0$ e seja $deg(v) = g$. Então a transformação $f : I \to V$ definida por $r \mapsto rv$ é um homomorfismo de R-módulos e manda I_h em V_{hg}, para todo $h \in G$. Como ambos I e V são graduados simples, $ker(f) = 0$ e $Im(f) = V$, donde segue que I e V são isomorfos e $I^{[g]}$ é isomorfo a V como R-módulo graduado. ■

Lema 2.11 *Seja R uma álgebra graduada e $I = R\varepsilon$, onde ε é um idempotente homogêneo de R. Então a álgebra G-graduada $End_R^{gr}(I)$ é igual a $End_R(I)$ e isomorfa a $\varepsilon R\varepsilon$.*

Demonstração. Dado $a \in \varepsilon R\varepsilon$ um elemento homogêneo de grau $g \in G$ mostraremos que a aplicação multiplicação à direita por a

$$\begin{array}{rccc} f_a: & I & \longrightarrow & I \\ & x & \longmapsto & xf_a := xa \end{array}$$

é um endomorfismo graduado. De fato, sabendo que $End_R^{gr}(I) = End^{gr}(I) \cap End_R(I)$, e não é difícil ver que f_a é um R-endomorfismo. Agora, dados $h \in G$, e $b \in I_h$, $deg(bf_a) = deg(ba) = hg$, de onde segue que $(I_h)f_a \subseteq I_{hg}$, e assim, $f_a \in End_g(I) \subset End^{gr}(I)$, o que é suficiente para mostrar que $f_a \in End_R^{gr}(I)$.

Considere o homomorfismo $\varepsilon R\varepsilon \to End_R^{gr}(I)$ tal que a imagem de $a \in \varepsilon R\varepsilon$ é o endomorfismo f_a. Mostraremos que tal aplicação é, na verdade, um isomorfismo. De fato, se $xa = 0$, para todo $x \in I$, então $0 = \varepsilon a = a$, de onde segue que tal aplicação é injetora. Mais ainda, dado $f \in End_R(I)$ e $x \in I$, temos $xf = x(\varepsilon f)$ e f é a multiplicação à direita pelo elemento $a = \varepsilon f$. Por definição $a \in R\varepsilon$, mas $a = \varepsilon f = \varepsilon^2 f = \varepsilon(\varepsilon f) = \varepsilon a$, de onde segue que $a \in \varepsilon R\varepsilon$, mostrando a sobrejetividade do homomorfismo. ■

Observação 2.12 *Sob as condições do Teorema 2.8 o R-módulo graduado simples V e a álgebra graduada de divisão $D = End_R^{gr}(V) = End_R(V)$ são determinados a menos de shifts apropriados.*

Definição 2.13 *Sejam G um grupo, D, D' álgebras G-graduadas, V um D-módulo à esquerda graduado e V' um D'-módulo à esquerda graduado. Um isomorfismo de (D, V) em (D', V') é um par (f_0, f_1), onde $f_0 : D \to D'$ é um isomorfismo de álgebras G-graduadas e $f_1 : V \to V'$ é um isomorfismo de espaços G-graduados com a condição que $f_1(vd) = f_1(v)f_0(d)$, para todos $v \in V$ e $d \in D$.*

Exemplo 2.14 *Sejam $D = D' = \mathbb{F}$, V e W $\mathbb{F}$-espaços vetoriais graduados. Neste caso um isomorfismo de (D, V) em (D', W) é um par (f_0, f_1) onde f_0 é a identidade e $f_1 : V \to W$ uma transformação linear graduada. Fixada $\{v_1, \ldots, v_n\}$ uma base de V de elementos homogêneos de graus $g_1, \ldots, g_n$, respectivamente, temos que $End_{\mathbb{F}}(V)$ é isomorfa a $R = M_n(\mathbb{F})$ com a graduação elementar induzida por $(g_1, \ldots, g_n)$. Note que $\{w_1, \ldots, w_n\}$, com $w_i = f(v_i)$, é uma base de W, e como w_i é homogêneo de grau g_i concluímos que $End_{\mathbb{F}}(W)$ é isomorfa a R. Portanto as álgebras $End_{\mathbb{F}}(V)$ e $End_{\mathbb{F}}(W)$ são isomorfas.*

No próximo teorema provamos que, de modo geral, um isomorfismo de pares determina um isomorfismo nos anéis de endomorfismos correspondentes e que, reciprocamente, todo isomorfismo de anéis de endomorfismos é obtido de um isomorfismo de pares.

Teorema 2.15 *Sejam G um grupo, D, D' álgebras G-graduadas de divisão, V um D-módulo à direita graduado e V' um D'-módulo à direita graduado, ambos não nulos e de dimensão finita. Sejam também $R = End_D(V)$ e $R' = End_{D'}(V')$. Se $f : R \to R'$ é um isomorfismo de álgebras G-graduadas, então existem $g \in G$ e um isomorfismo (f_0, f_1) de $({}^{[g^{-1}]}D^{[g]}, V^{[g]})$ em (D', V') tais que $f_1(rv) = f(r)f_1(v)$, para quaisquer $r \in R$ e $v \in V$. Reciprocamente, dado um isomorfismo (f_0, f_1) de $({}^{[g^{-1}]}D^{[g]}, V^{[g]})$ em (D', V') existe um único isomorfismo $f : R \to R'$ de álgebras G-graduadas tal que $f_1(rv) = f(r)f_1(v)$,*

para todos $r \in R$ e $v \in V$. Dois isomorfismos (f_0, f_1) e (f_0', f_1') determinam o mesmo isomorfismo $R \to R'$ se, e somente se, existe um elemento homogêneo não nulo $d \in D'$ tal que $f_0'(x) = d^{-1}f_0(x)d$ e $f_1'(v) = f(v)d$, para todos $x \in D$ e $v \in V$.

Demonstração. Defina uma estrutura de R-módulo em V' pondo $rv' := f(r)v'$ para $r \in R$, $v' \in V'$. V' é um R-módulo graduado simples, pois como V' é um R'-módulo simples, segue que também o é em relação a R. De fato, supondo $W' \neq 0$ um R-submódulo de V', temos que W' é também um R'-submódulo e tomemos $w' \in W' \setminus \{0\}$. Dado $v' \in V'$, existe uma transformação linear sendo $r \in R$ tal que $f(r) = r'$, temos $rw' = f(r)w' = r'w' \in W'$, de onde segue que $W' = V'$ e V' é um R-módulo simples. Pelo Lema 2.10 existe um isomorfismo $f_1 : V^{[g]} \to V'$ para algum $g \in G$. Pela nossa definição de R-módulo em V', temos $f_1(rv) = f(r)f_1(v)$ para $r \in R$, $v \in V$. Como ${}^{[g^{-1}]}D^{[g]} = End_R(V^{[g]})$ e $D' = End_R(V')$ podemos definir $f_0 : End_R(V^{[g]}) \to End_R(V')$ pondo $(v')(f_0(d)) := f_1((f_1^{-1}(v'))d)$ para $v' \in V'$ e $d \in D$. Note que f_0 é um homomorfismo. Se $(v')(f_0(d)) = 0$, então $f_1((f_1^{-1}(v'))d) = 0$, para qualquer $v' \in V'$. Daí,$(f_1^{-1}(v'))d = 0$ e assim $d = 0$. É simples verificar que f_0 é um isomorfismo de álgebras. Por fim, mostraremos que $f_0(d)$ preserva o grau de v'. Se $deg(v') = g$ e $deg(d) = h$ então, como f_1 e sua inversa preservam o grau, $deg((v')(f_0(d))) = deg(f_1((f_1^{-1}(v'))d)) = gh$, de onde podemos concluir que $f_0(d)$ tem grau g.

Reciprocamente, dado (f_0, f_1), definamos $f(r) : V' \to V'$ para cada $r \in End_D(V)$ pondo $f(r)(v') := f_1(r(f_1^{-1}(v')))$. Assim, para $v' \in V'$ e $d' \in D'$, temos

$$\begin{aligned} f(r)(v'd') &= f_1(r(f_1^{-1}(v')f_0^{-1}(d'))) \\ &= f_1(r(f_1^{-1}(v'))f_0^{-1}(d')) \\ &= f_1(r(f_1^{-1}(v')))f_0(f_0^{-1}(d')) \\ &= (f(r)(v'))d', \end{aligned}$$

mostrando que $f(r) \in End_{D'}(V')$. Dado r homogêneo de grau $h \in G$, para qualquer $a \in G$, f_1^{-1} envia V_a' em $V_{ag^{-1}}$, r envia $V_{ag^{-1}}$ em $V_{hag^{-1}}$ e, finalmente, f_1 envia $V_{hag^{-1}}$ em V_{ha}', de onde segue que $f(r)$ é homogêneo de grau h, mostrando que $f : End_D(V) \to End_{D'}(V')$ é um isomorfismo de álgebras G-graduadas. A unicidade pode ser depreendida ponto a ponto pela igualdade $f_1(rv) = f(r)f_1(v)$.

Por fim, sendo $d \in D$ um elemento homogêneo não nulo de grau $t \in G$, $f_0' :^{[t^{-1}g^{-1}]} D^{[gt]} \to D'$, dado por $f_0'(x) = d^{-1}f_0(x)d$ é um isomorfismo. Também

$f_1' : V^{[gt]} \to V'$, dado por $f_1'(v) = f_1(v)d$, satisfaz $f_1(vx) = f_1'(v)f_0'(x)$. Desde que

$$f_1'(rv) = f_1(rv)d = (f(r)f_1(v))d = f(r)(f_1(v)d) = f(r)f_1'(v), \forall r \in R, v \in V,$$

concluímos que (f_0', f_1') determina o mesmo isomorfismo f. Reciprocamente, se (f_0', f_1') determina f, então $f_1' \circ f^{-1}$ é uma transformação homogênea de V' em V' e um isomorfismo de R-módulos. Assim, existe $d \in D'$ não nulo tal que $(f_1 \circ f_1^{-1})(v') = v'd$, para todo $v' \in V'$. Segue que $f_1'(v) = f_1(v)d$, para quaisquer $v \in V$ e $f_0'(x) = d^{-1}f_0(x)d$, para todo $x \in D$. ■

Observação 2.16

i) Utilizando a notação do Teorema 2.15, se $\beta = \{v_1, \ldots, v_n\}$ é uma D-base homogênea de V, então

$$\beta' = \{f_1(v_1), \ldots, f_1(v_n)\}$$

é uma D'-base homogênea de V' tal que $deg(f_1(v_i)) = (deg(v_i))g$.

ii) O isomorfismo f que corresponde a (f_0, f_1) pode ser expresso em linguagem de matrizes, semelhante ao que fizemos anteriormente e fixadas as bases do item anterior para V e V'.

Dado V um D-módulo à direita graduado simples, para qualquer $v \in V \setminus \{0\}$ homogêneo temos $V = vD$ e, portanto, V é isomorfo a um *shift* à esquerda do D-módulo à direita regular V, ou seja, ${}^{[g]}D \simeq V$, onde $g = deg(v)$. Ademais, sendo $T = supp(D)$, temos que ${}^{[g]}D$ é isomorfo a ${}^{[h]}D$ se, e somente se, $gT = hT$. De fato como $supp({}^{[g]}D) = gT$ e $supp({}^{[h]}D) = hT$, a igualdade $gT = hT$ segue do isomorfismo ${}^{[g]}D \simeq {}^{[h]}D$. Para mostrarmos que se as classes laterais gT e hT coincidem, então ${}^{[g]}D$ é isomorfo a ${}^{[h]}D$ basta notar que 1 tem grau g em ${}^{[g]}D$ e o conjunto $\{1\}$ é uma base para ${}^{[g]}D$. Como as classes coincidem, existe $t \in T$ tal que $g = ht$. Tome $d \in D_t$ não nulo. Note que o grau da unidade em ${}^{[h]}D$ é h e assim, o grau de $1d$ é $ht = g$. Lembrando que $\{d\}$ é uma base para ${}^{[h]}D$, podemos considerar a aplicação de ${}^{[g]}D$ em ${}^{[h]}D$ que leva x em dx. Não é difícil ver que tal aplicação é um isomorfismo graduado.

Seja $T \subset G$ o suporte de D. Se V é um D-módulo à direita graduado de dimensão finita, então existe uma decomposição canônica de V em uma soma direta

$$V = V_1 \oplus \cdots \oplus V_s,$$

onde V_i é a soma de todos os submódulos graduados que são isomorfos a algum ${}^{[g_i]}D$ fixo. Os elementos $g_1, \ldots, g_s$ não são unicamente determinados, mas suas classes laterais $g_1T, \ldots, g_sT$ são determinadas a menos de permutação. Escreva $\gamma = (g_1, \ldots, g_s)$, onde $g_i^{-1}g_j \notin T$, para $i \neq j$. Se $\{v_1, \ldots, v_n\}$ é uma D-base homogênea de V, então, para cada i o subconjunto

$$\{v_j \mid deg(v_j) \in g_iT\}$$

é uma D-base para V_i. Seja $k_i = dim_D(V_i)$ e escreva $k = (k_1, \ldots, k_s)$.

Por outro lado, dado um par (k, γ), seja $V(G, D, k, \gamma)$ o D-módulo à direita que possui uma D-base homogênea consistindo de k_i elementos tais que cada grau é g_i, para $i = 1, \ldots, s$. Isto prova que V é determinado como D-espaço vetorial por k e γ. Para uma exposição alternativa desse fato, confira a Proposição 2.5 da referência [19].

Se V e W são determinados por k e γ, então existem $\{v_1 \ldots, v_n\}$ e $\{w_1, \ldots, w_n\}$ bases homogêneas de V e W, respectivamente onde $\{v_j \mid deg(v_j) \in g_iT\}$ é uma D-base para V_i e $\{w_j \mid deg(w_j) \in g_iT\}$ é uma D-base para W_i, onde $dim_D(V_i) = k_i = dim_D(W_i)$. Nestas condições, e supondo sem perda de generalidade que $deg(v_j) = deg(w_j)$, a aplicação que, para cada i leva v_j em w_j é um isomorfismo, em outras palavras, V e W são isomorfas. A recíproca também é verdadeira, pois um isomorfismo f entre dois espaços V e W leva, para cada i, $\{v_j \mid deg(v_j) \in g_iT\}$ no conjunto $\{f(v_j) \mid deg(f(v_j)) \in g_iT\}$, que é uma D'-base para $f(V_i)$ e, a partir daí não é difícil ver que W também é determinado por k e γ. Portanto, a menos de isomorfismo, toda álgebra graduada simples de dimensão finita pode ser escrito dessa forma.

Além disso, denotamos a álgebra G-graduada $End_D(V)$ por $M(G, D, k, \gamma)$.

Notação 2.17 *Escreveremos $(D, k, \gamma) \sim (D', k', \gamma')$ se k e k' têm o mesmo número s de componentes e existem $g \in G$ e uma permutação σ dos símbolos $\{1, \ldots, s\}$ tais que $D' \simeq {}^{[g^{-1}]}D^{[g]}$, $k'_i = k_{\sigma(i)}$ e $g'_i \in g_{\sigma(i)}(Supp(D))g$, para todos $i = 1, \ldots, s$.*

Com esta notação e combinando o Teorema 2.8 e o Teorema 2.15, obtemos

Corolário 2.18 *Sejam G um grupo e R uma álgebra G-graduada. Se R é graduada simples e satisfaz a condição de cadeia descendente para ideais graduados à esquerda, então R é isomorfa a alguma $M(G, D, k, \gamma)$, onde D é uma álgebra graduada de divisão. Duas álgebras G-graduadas $M(G, D, k, \gamma)$ e $M(G, D', k', \gamma')$ são isomorfas se, e somente se, $(D, k, \gamma) \sim (D', k', \gamma')$.*

Demonstração. A primeira parte do corolário segue do Teorema 2.8, pois nestas hipóteses, existem uma álgebra G-graduada de divisão D e um D-módulo à direita graduado V de dimensão finita sobre D tais que $R \simeq End_D(V) = M(G, D, k, \gamma)$, para algum k e γ como nas construções anteriores. Já o Teorema 2.15 completa a segunda parte, pois $M(G, D, k, \gamma) = End_D(V) \simeq End_{D'}(V') = M(G, D', k', \gamma')$ se, e somente se, k e k' têm o mesmo número s de componentes e existem $g \in G$ e uma permutação σ dos símbolos $\{1, \ldots, s\}$ tais que $D' \simeq^{[g^{-1}]} D^{[g]}$, $k'_i = k_{\sigma(i)}$ e $g'_i \in g_{\sigma(i)}(Supp(D))g$, para todos $i = 1, \ldots, s$, o que denotamos por $(D, k, \gamma) \sim (D', k', \gamma')$. ■

Pela Observação 2.9, pelo corolário anterior e pelo Teorema 2.6, obtemos que $R \simeq End_D(V) \simeq M_n(D)$. Escrevendo este resultado em termos de matrizes, obtemos o seguinte teorema:

Teorema 2.19 *Seja $R = \bigoplus_{g \in G} R_g$ uma álgebra de dimensão finita sobre um corpo algebricamente fechado $\mathbb{F}$ graduada por um grupo G. Então R é graduada simples se, e somente se, R é isomorfa a $M_n(\mathbb{F}) \otimes D \simeq M_n(D)$, onde $D = \bigoplus_{h \in H} D_h$ é uma álgebra graduada de divisão com $Supp(D) = H$, um subgrupo de G, e $M_n(\mathbb{F})$ possui uma G-graduação elementar definida por uma n-upla $(g_1, \ldots, g_n) \in G^n$. Mais ainda, $D \simeq \mathbb{F}^\sigma[H]$ para algum 2-cociclo σ em H, com a H-graduação canônica, e a graduação em $M_n \otimes D$ é dada por $deg(E_{ij} \otimes d_h) = g_i^{-1} h g_j$, com $d_h \in D_h$.*

Observação 2.20 *Podemos decompor R pondo $R = AB \simeq A \otimes B$, onde $A = M_n(\mathbb{F})$ tem uma G-graduação elementar definida por $(q_1, \ldots, q_m; g_{12}, \ldots, g_{m-1,m})$, que definimos em (1.2) e B é uma álgebra graduada de divisão. Podemos, a menos de isomorfismo, supor que $g_i H = g_j H$ se, e somente se, $g_i = g_j$. No teorema anterior, dado um elemento $r = E_{ij} \otimes d_h \in R$ de grau e, temos $e = deg(r) = g_i^{-1} h g_j$ e daí, $g_i^{-1} g_j \in H$, de onde segue que $g_i H = g_j H$. Como isso acontece se, e somente se, $g_i = g_j$, obtemos que a matriz E_{ij} tem grau e na graduação de A e $h = e$. Mostramos portanto, que no nosso caso a decomposição $R = AB$ é tal que $R_e = A_e$.*

2.3 Uma Condição para que Duas Álgebras Graduadas Simples de Dimensão Finita sejam Isomorfas

Na seção anterior exibimos as álgebras graduadas simples de dimensão finita tanto em termos de endomorfismos quanto em termos de matrizes. Agora chegou o momento de cumprirmos com o objetivo principal da dissertação exibindo uma condição para que duas álgebras graduadas simples de dimensão finita sejam isomorfas. Antes

disso, porém, devemos estudar alguns lemas e teoremas que nos serão úteis quando demonstrarmos o resultado principal.

Doravante assumiremos as condições da Observação 2.20 e $\mathbb{F}$ um corpo algebricamente fechado, exceto se mencionarmos o contrário.

Lema 2.21 *Seja $R = \bigoplus_{g\in G} R_g = AB \simeq A \otimes B$ uma álgebra graduada simples de dimensão finita onde $A = M_n(\mathbb{F})$ tem uma G-graduação elementar definida por $(q_1, \ldots, q_m; g_{12}, \ldots, g_{m-1,m})$ e B é uma álgebra graduada de divisão e denote $S = Supp(A)$, $H = Supp(B)$. Se G é um grupo abeliano, então $S \cap H = \{e\}$.*

Demonstração. Suponha, por contradição, $h \in (S \cap H) \setminus \{e\}$. Pelo Teorema 2.19, H é um subgrupo de G e, pela Observação 2.20, $A_e = R_e$. Dados $x \in A_h \setminus \{0\}$, $r \in B_{h^{-1}} \setminus \{0\}$, pelo Teorema 2.19 e, como G é abeliano, B pode ser visto como subálgebra homogênea, de onde segue que $deg(xr) = e$, mas isto é um absurdo, pois se $xr \in A_e$ deveríamos ter $r = 1$, o que não ocorre. ■

Lema 2.22 *Seja R uma álgebra G-graduada simples de dimensão finita. Suponha que $R = AB \simeq A \otimes B, R = A'B' \simeq A' \otimes B'$ são duas decomposições de R em componente elementar e álgebra graduada de divisão com $H = Supp(B)$, $H' = Supp(B')$. Se G é abeliano, então $H = H'$ e B e B' são isomorfas como álgebras graduadas.*

Demonstração. Em primeiro lugar, temos que $A_e = R_e = A'_e$. Seja C o centralizador de R_e em R. Note que C é uma subálgebra graduada de R. De fato, dados $a, b \in C$, temos $ar = ra, bs = sb$, para todos $r, s \in R_e$. Daí, $abr = arb = rab$ e assim $ab \in C$. Dado $a = r_1 + \cdots + r_n \in C$, temos $ar = ra$, para qualquer $r \in R_e$. Ora, $r_1r + \cdots + r_nr = rr_1 + \cdots + rr_n$. Como as únicas parcelas com grau g_i em ambos os lados da equação são r_ir e rr_i, obtemos $r_ir = rr_i$, para todo i, donde segue que $r_i \in C$, o que é suficiente para concluir que C é subálgebra graduada.

Como $R \simeq A \otimes B$, então $C \simeq \tilde{C} \otimes B$, onde $\tilde{C} = C_A(A_e)$. De fato, podemos identificar C com $C_R(A_e \otimes 1)$ e mostraremos que $C_R(A_e \otimes 1) = C_A(A_e) \otimes B$. Dado $a \otimes b \in C_A(A_e) \otimes B$, como a comuta com todo elemento de A_e, então $a \otimes b$ comuta com todo elemento de $A_e \otimes 1$, de onde segue que $C_A(A_e) \otimes B \subseteq C_R(A_e \otimes 1)$. Por outro lado, dado $x = \sum a_i \otimes b_i \in C_R(A_e \otimes 1)$, onde o conjunto dos b'_is é linearmente independente, e dado $a \otimes 1 \in A_e \otimes 1$, temos

$$x(a \otimes 1) = (a \otimes 1)x \Rightarrow \sum (a_ia - aa_i) \otimes b_i = 0.$$

Como os b_i's são $L.I.$, obtemos $a_i a = a a_i$ para cada i e, assim, $x \in C_A(A_e) \otimes B$.

Analogamente ao que foi feito na Equação (1.1), na seção sobre graduações elementares em álgebras de matrizes, temos $\tilde{C} \simeq \underbrace{\mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{m \text{ parcelas}}$, de onde segue que $C \simeq \underbrace{B \oplus \cdots \oplus B}_{m \text{ parcelas}}$ e, similarmente, $C \simeq B' \oplus \cdots \oplus B'$, de onde segue que

$$H = Supp(C) = Supp(B) = Supp(B')$$

e $B \simeq B'$ como álgebras graduadas. ■

Lema 2.23 *Sejam G um grupo abeliano e $\mathbb{F}$ um corpo algebricamente fechado tal que a ordem de todo subgrupo finito de G é invertível em $\mathbb{F}$. Se duas álgebras G-graduadas simples e de dimensões finitas $R \simeq A \otimes B$ e $R' \simeq A' \otimes B'$, satisfazem as mesmas identidades polinomiais graduadas, onde A, A' possuem graduações elementares, B, B' são álgebras graduadas de divisão com $Supp(B) = Supp(B') =: H$, então $B \simeq B'$.*

Nesse lema, a hipótese de que a ordem de todo subgrupo finito de G é invertível em $\mathbb{F}$ foi usada pea referência [4] para provar que toda álgebra graduada simples é isomorfa a um tensor da forma $A \otimes B$.

Demonstração. Sejam $\overline{A} = M_q(\mathbb{F})$ com uma graduação trivial e B uma álgebra graduada de divisão. Mostraremos que $\overline{A} \otimes B$ satisfaz uma identidade polinomial graduada especial, que definiremos mais adiante na Equação 2.2. Sejam $H = supp(B)$ e $\sigma : H \times H \to \mathbb{F} \setminus \{0\}$ o 2-cociclo que define a estrutura de álgebra graduada de divisão em B (vide Observação 1.32, identificando B com $\mathbb{F}^\sigma[G]$). Existe uma base $\{b_h \mid h \in H\}$ de B tal que $b_g b_h = \sigma(g,h) b_{gh}$ e ainda $b_h b_g = \sigma(h,g) b_{hg}$. Segue que

$$b_g b_h = \lambda(g,h) b_h b_g, \text{ onde } \lambda(g,h) = \frac{\sigma(g,h)}{\sigma(h,g)}. \tag{2.1}$$

Pelo Teorema de Amitsur-Levitski sabemos que $\overline{A}$ satisfaz a identidade *Standard*

$$s_{2q} = s_{2q}(x_1, x_2, \ldots, x_{2q}) = \sum_{\sigma \in S_{2q}} (-1)^\sigma x_{\sigma(1)} \cdots x_{\sigma(2q)}.$$

Chamemos $x_{2q-1} = y_1$ e $x_{2q} = y_2$. Podemos agrupar as parcelas do somatório levando em consideração as posições de y_1 e y_2. Por exemplo, ao fixarmos y_1 na primeira posição do monômio e y_2 na segunda, as demais variáveis variarão de acordo com todas as permutações de S_{2q-2}. Assim, uma das partes deste agrupamento é o somatório

$$(-1)^\alpha \sum_{\tau \in S_{2q-2}} (-1)^\tau x_{\tau(1)} \cdots x_{\tau(i-1)} y_1 x_{\tau(i)} \cdots x_{\tau(j-2)} y_2 x_{\tau(j-1)} \cdots x_{\tau(2q-2)}.$$

Podemos usar o número $\alpha = i + j + 1$, onde i é a posição de y_1 e j é a de y_2.

Desse modo, podemos definir

$$s_{i,j} = s_{i,j}(x_1, \ldots, x_{2q-2}, y_1, y_2) =$$

$$= (-1)^{i+j+1} \sum_{\tau \in S_{2q-2}} (-1)^{\tau} x_{\tau(1)} \cdots x_{\tau(i-1)} y_1 x_{\tau(i)} \cdots x_{\tau(j-2)} y_2 x_{\tau(j-1)} \cdots x_{\tau(2q-2)}.$$

Note que trocando y_1 e y_2 de posição, obtemos as mesmas permutações, mas com o sinal invertido. Ao consideramos todas as possíveis posições de y_1 e y_2, obtemos

$$s_{2q}(x_1, \ldots, x_{2q-2}, y_1, y_2) = \sum_{1 \leq i < j \leq 2q} (s_{i,j}(x_1, \ldots, x_{2q-2}, y_1, y_2) - s_{i,j}(x_1, \ldots, x_{2q-2}, y_2, y_1)).$$

Agora definimos uma identidade *standard* modificada como segue:

$$s^*_{2q}(x^e_1, \ldots, x^e_{2q-2}, y^g_1, y^h_2) :=$$

$$= \sum_{1 \leq i < j \leq 2q} (s_{i,j}(x^e_1, \ldots, x^e_{2q-2}, y^g_1, y^h_2) - \lambda(g,h) s_{i,j}(x^e_1, \ldots, x^e_{2q-2}, y^h_2, y^g_1)). \tag{2.2}$$

Mostraremos que $s^*_{2q} \equiv 0$ é uma identidade graduada para $\overline{A} \otimes B$. De fato, avaliando $(x^e_1, \ldots, x^e_{2q-2}, y^g_1, y^h_2) = (a_1 \otimes 1, \ldots, a_{2q-2} \otimes 1, a_{2q-1} \otimes b_g, a_{2q} \otimes b_h)$ em s^*_{2q} obtemos

$$\begin{aligned}
& \sum_{1 \leq i < j \leq 2q} (s_{i,j}(a_1, \ldots, a_{2q-1}, a_{2q}) \otimes b_g b_h - \lambda(g,h) s_{i,j}(a_1, \ldots, a_{2q}, a_{2q-1}) \otimes b_h b_g) = \\
= & \sum_{1 \leq i < j \leq 2q} (s_{i,j}(a_1, \ldots, a_{2q-1}, a_{2q}) \otimes b_g b_h - s_{i,j}(a_1, \ldots, a_{2q}, a_{2q-1}) \otimes b_g b_h) = \\
= & \sum_{1 \leq i < j \leq 2q} (s_{i,j}(a_1, \ldots, a_{2q-1}, a_{2q}) - s_{i,j}(a_1, \ldots, a_{2q})) \otimes b_g b_h \\
= & \; s_{2q}(a_1, \ldots, a_{2q}, a_{2q-1}) \otimes b_g b_h = 0.
\end{aligned}$$

Ademais, claramente tal polinômio também é identidade polinomial graduada para $M_{q'}(\mathbb{F}) \otimes B'$ se $q' < q$. No entanto, mostraremos que ela não é identidade graduada se $q' > q$ ou $q' = q$, mas $\lambda'(g,h) \neq \lambda(g,h)$, onde $\lambda'(g,h) := \dfrac{\sigma'(g,h)}{\sigma'(h,g)}$ e σ' é o cociclo que define a H-graduação em B'.

Supondo primeiro $q' > q$, podemos avaliar

$$s^*_{2q}(E_{11} \otimes 1, E_{12} \otimes 1, E_{22} \otimes 1, \ldots, E_{q-1,q} \otimes 1, E_{q,q} \otimes b'_g, E_{q,q+1} \otimes b'_h) = E_{1,q+1} \otimes b'_g b'_h \neq 0.$$

Agora, supondo $q' = q$ e $\lambda'(g,h) \neq \lambda(g,h)$, tomamos $x^e_1 = a_1 \otimes 1, \ldots, x^e_{2q-2} = a_{2q-2} \otimes 1, y_1 = a \otimes b'_g, y_2 = a \otimes b'_h$, com $a_1 = E_{11}, a_2 = E_{12}, a_3 = E_{22}, \ldots, a_{2q-2} =$

$E_{q-1,q}, a = E_{q,q}$. Neste caso, a avaliação de tais valores em s_{2q}^* é

$$\sum_{i<j}(s_{ij}(a_1,\ldots,a_{2q-2},a,a)\otimes b'_g b'_h - \lambda(g,h)s_{ij}(a_1,\ldots,a_{2q-2},a,a)\otimes b'_h b'_g) =$$
$$\left(1-\frac{\lambda(g,h)}{\lambda'(g,h)}\right)(s_{2q-2}(a_1,\ldots,a_{2q-2})E_{qq}^2\otimes b'_g b'_h) = \left(1-\frac{\lambda(g,h)}{\lambda'(g,h)}\right)E_{1q}\otimes b'_g b'_h \neq 0.$$

Relembrando que A_e, A'_e são somas diretas de álgebras matriciais sobre $\mathbb{F}$, consideremos $M_q(\mathbb{F})$ o somando matricial de A_e de maior dimensão e $M_{q'}(\mathbb{F})$ o somando de A'_e de maior dimensão. Como R satisfaz as mesmas identidades que R', pelo exposto acima, obtemos que $q = q'$ e $\lambda(g,h) = \lambda'(g,h)$ para quaisquer $g, h \in H$. Em particular sejam b'_g, com $g \in H$, elementos de uma base de B' satisfazendo as relações (2.1). Como H é um grupo abeliano finito, pelo Teorema 1.3, existe uma decomposição em um produto direto de grupos cíclicos de ordens $k_1, k_2, \ldots, k_t$

$$H = \langle h_1\rangle_{k_1}\times\langle h_2\rangle_{k_2}\times\cdots\times\langle h_t\rangle_{k_t}$$

e tomemos $b_1, b_2, \ldots, b_t \in B$ tais que $deg(b_i) = h_i, 1 \leq i \leq t$ e $b_i^{k_i} = 1$. Não é difícil ver que o conjunto $\beta = \{b_1^{j_1}b_2^{j_2}\cdots b_t^{j_t} \mid 1 \leq j_r \leq k_r, r = 1,\ldots,t\}$ é uma base para B. Note que as relações (2.1) e as igualdades $b_1^{k_1} = b_2^{k_2} = \cdots = b_t^{k_t} = 1$ fazem com que a multiplicação definida nos elementos da base β seja completamente conhecida.

Analogamente, podemos tomar $c_1, c_2, \ldots, c_t \in B'$, com $c_i = b'_{h_i} \in B'_{h_i}$ e $c_i^{k_i} = 1$, para $i = 1, 2, \ldots, t$. O conjunto $\beta' = \{c_1^{j_1}c_2^{j_2}\cdots c_t^{j_t} \mid 1 \leq j_r \leq k_r, r = 1,\ldots,t\}$ é uma base para B' cuja multiplicação satisfaz as relações 2.1 e $c_1^{k_1} = c_2^{k_2} = \cdots = c_t^{k_t} = 1$, de onde segue que a multiplicação de B é a mesma de B', em outras palavras, $B \simeq B'$. ■

Não é difícil provar que se duas álgebras graduadas simples de dimensão finita são isomorfas, elas satisfazem as mesmas identidades polinomiais. O próximo Teorema é sobre a recíproca deste fato e constitui a condição que queríamos exibir.

Teorema 2.24 *Sejam G um grupo abeliano e $\mathbb{F}$ um corpo algebricamente fechado tal que a ordem de todo subgrupo finito de G é invertível em $\mathbb{F}$. Se duas álgebras G-graduadas simples e de dimensões finitas R e R' satisfazem as mesmas identidades polinomiais graduadas, então elas são isomorfas.*

Demonstração. Sejam $R = AB \simeq A\otimes B$, $R' = A'B' \simeq A'\otimes B'$ decomposições onde A e A' possuem graduações elementares e B e B' são álgebras graduadas de divisão. Suponha que $(q_1,\ldots,q_m; g_{12},\ldots,g_{m-1,m})$ define uma graduação elementar em

A e $(q'_1, \ldots, q'_{m'}; g'_{12}, \ldots, g'_{m'-1,m'})$ define uma graduação elementar em A'. Se $S = supp(A)$, $H = supp(B)$, $S' = supp(A')$ e $H' = supp(B')$, então $SH = S'H'$. De fato, note que $x^g \equiv 0$ é identidade graduada de R para todo $g \in G \setminus SH$. Como R e R' satisfazem as mesmas identidades graduadas, então tal polinômio também é identidade para R', mas neste caso, para $g \in G \setminus S'H'$. Daí segue que $G \setminus SH = G \setminus S'H'$, donde $SH = S'H'$.

Na verdade, provaremos que $H = H'$ e que $B \simeq B'$. Considere C o centralizador de R_e em R. Por um argumento já usado anteriormente (veja demonstração do Lema 2.22), C é uma subálgebra graduada e $H = Supp(C)$. Por outro lado, $g \in Supp(C)$ se, e somente se, $g \in SH$ e $[x^e, x^g] \equiv 0$ é uma identidade graduada de R. Como $SH = S'H'$ e as identidades graduadas de R e R' são as mesmas, segue que $H = H'$. Agora, tendo provado que todas as condições do Lema 2.23 se aplicam neste caso, obtemos $B \simeq B'$ como álgebras graduadas.

Mostraremos que $q_i = q'_i$ e $m = m'$. Pela graduação elementar em A que definimos, a componente $A_e = R_e$ é $M_{q_1}(\mathbb{F}) \oplus M_{q_2}(\mathbb{F}) \oplus \cdots \oplus M_{q_m}(\mathbb{F})$. Sejam

$$\begin{aligned} p_1 &= q_1 \\ p_2 &= p_1 + q_2 = q_1 + q_2 \\ &\vdots \\ p_{m-1} &= p_{m-2} + q_{m-1} = q_1 + q_2 + \cdots + q_{m-1} \\ p_m &= p_{m-1} + q_m = q_1 + q_2 + \cdots + q_m = n, \end{aligned}$$

e considere o subgrupo de S_{2n-1}

$$S^*_{2n-1} = \{\sigma \in S_{2n-1} \mid \sigma(2p_1) = 2p_1, \sigma(2p_2) = 2p_2, \ldots, \sigma(2p_{m-1}) = 2p_{m-1}\}.$$

Mostraremos que R não satisfaz a identidade polinomial graduada

$$\sum_{\sigma \in S^*_{2n-1}} (-1)^\sigma x^e_{\sigma(1)} \cdots x^e_{\sigma(2p_1-1)} x^{g_{12}}_{2p_1} x^e_{\sigma(2p_1+1)} \cdots x^e_{\sigma(2p_2-1)} x^{g_{23}}_{2p_2} x^e_{\sigma(2p_2+1)} \cdots$$
$$\cdots x^e_{\sigma(2p_{m-1}-1)} x^{g_{m-1,m}}_{2p_{m-1}} x^e_{\sigma(2p_{m-1}+1)} \cdots x^e_{\sigma(2n-1)} \equiv 0. \qquad (2.3)$$

De fato, se fizermos a avaliação de

$$(x_1, x_2, \ldots, x_{2n-1}) = (E_{11}, E_{12}, E_{22}, E_{23}, \ldots, E_{n-1,n}, E_{nn})$$

no polinômio, existe apenas uma permutação do subgrupo de permutações que não anula os produtos destes elementos, que é a identidade, e, portanto, obtemos o valor

$E_{1n} \neq 0$. Agora considere a decomposição análoga $A'_e = R'_e = M_{q'_1}(\mathbb{F}) \oplus M_{q'_2}(\mathbb{F}) \oplus \cdots \oplus M_{q'_{m'}}(\mathbb{F}) = A'_1 \oplus A'_2 \oplus \cdots \oplus A'_{m'}$, onde $q'_1 \geq q'_2 \geq \cdots \geq q'_{m'} > 0$. Se $q_1 > q'_1$ então o polinômio (2.3) é identidade graduada para R', pois $A'_i A'_j = 0$, para todo $i \neq j$ e todo A'_i satisfaz a identidade $s_{2q'_1} \equiv 0$, o que contradiz o fato de R e R' satisfazerem as mesmas identidades.

Temos ainda que $g_{12}, \ldots, g_{m-1,m}$ são tais que $g_{i,i+1} \cdots g_{j-1,j} \neq e$ para quaisquer $1 \leq i < j \leq m$. Dados $a_1 \in A'_{i_1}, \ldots, a_m \in A'_{i_m}$, temos $a_1 c_{12} a_2 \cdots a_{m-1} c_{m-1} a_m = 0$ em A', onde $deg(c_{12}) = g_{12}, \ldots, deg(c_{m-1,m}) = g_{m-1,m}$. Assim, pelo menos dois dos índices $i_1, \ldots, i_m$ coincidem e, quando isto acontece, o produto se anula. Se, porém, $q'_1 = q_1$ mas $q'_2 < q_2$, podemos usar o mesmo argumento anterior, chegando à mesma contradição. Portanto, $m = m'$ e $q_1 = q'_1, \ldots, q_m = q'_m$. Em particular, A e A' devem ser álgebras de matrizes de mesmo tamanho $n = q_1 + \cdots + q_m$. Por fim, sejam $e_1 \in A'_1 = M_{q_1}(\mathbb{F}), \ldots, e_m \in A'_m = M_{q_m}(\mathbb{F})$ as unidades das álgebras $A'_1, \ldots, A'_m$ respectivamente. Como o polinômio (2.3) não é identidade graduada para R', então existem uma permutação $\tau \in S_m$, $a_1 \in A'_1, \ldots, a_m \in A'_m$ e elementos homogêneos $c_1 \in R'_{g_{12}}, \ldots, c_{m-1} \in R'_{g_{m-1,m}}$ tais que

$$a_{\tau(1)} c_1 a_{\tau(2)} \cdots a_{\tau(m-1)} c_{m-1} a_{\tau(m)} \neq 0$$

em R'. Ademais, $q'_{\tau(i)} = q_i$ para todo $i = 1, \ldots, m$ e $c_i = a'_i b_i$, $i = 1, \ldots, m-1$, onde $a'_i \in e_{\tau(i)} A' e_{\tau(i+1)}$, $deg(a'_i) = g'_{\tau(i),\tau(i+1)}$, $b_i \in B'_{h_i}$ e $g'_{\tau(i),\tau(i+1)} h_i = g_{i,i+1}$ para $1 \leq i \leq m-1$.

Portanto mostramos que R e R' são isomorfas como álgebras graduadas. ■

Apêndice A

Semissimplicidade de anéis e o Teorema de Wedderburn-Artin

Nos dedicamos, neste apêndice, a trazer o assunto que influenciou o nosso resultado principal. A referência que mais utilizamos para esta parte do texto foi [18]. Apresentamos uma propriedade dos anéis, a semissimplicidade (que tem como um caso particular a simplicidade), e classificaremos todos os anéis semissimples por meio de anéis de matrizes com entradas em anéis com divisão. Para isto, é necessário primeiro elencar teoremas relacionados aos módulos, que generalizam os espaços vetoriais, que foram definidos no primeiro capítulo.

Agora introduzimos um conceito bastante importante desta seção que é a semissimplicidade. Nós a definimos em relação a módulos, mas mais adiante a semissimplicidade de anéis tomará a de módulos como base. Neste apêndice consideraremos, salvo menção contrária, anéis com unidade.

Definição A.1 *Sejam R um anel e M um R-módulo à esquerda. Dizemos que M é um módulo*

i) simples, se $RM \neq 0$ e os únicos submódulos de M são os triviais;

ii) semissimples, se todo R-submódulo de M é um somando direto de M.

Doravante, salvo menção contrária, R representará um anel e M um R-módulo à esquerda.

Lema A.2 *Se M é semissimples, então*

i) Todo submódulo de M é um R-módulo semissimples;

ii) Toda imagem homomórfica de M é um R-módulo semissimples.

Demonstração.

i) Seja L um submódulo de M. Dado N um submódulo de L, como N é também submódulo de M, existe K um submódulo de m tal que $M = N \oplus K$. Assim, $L = M \cap L = (N \oplus K) \cap L = N \oplus (K \cap L)$. Mostremos a validade da última igualdade. Dado $x \in (N \oplus K) \cap L$, $x \in L$ e existem $n \in N$ e $k \in K$ tais que $x = n + k$. Como $N \subseteq L$, então $k = x - n \in L$. Segue que $x \in N \oplus (K \cap L)$. Por outro lado, dado $x \in N \oplus (K \cap L)$, existem $n \in N$, $k \in K \cap L$ tais que $x = n + k$. Como $n \in N \subseteq L$, então $x = n + k \in L$, de onde segue que $x \in (N \oplus K) \cap L$.

ii) Sejam $f : M \to L$ um R-epimorfismo e N um R-submódulo de L. Sabemos que $f^{-1}(N)$ é um submódulo de M e como M é semissimples, $M = f^{-1} \oplus K$, para algum submódulo K de M. Dado $y \in L$, existe $x \in M$ tal que $y = f(x)$ e existem $x_1 \in f^{-1}(N)$, $x_2 \in K$ tais que $x = x_1 + x_2$. Assim, $y = f(x) = f(x_1) + f(x_2) \in N + f(K)$, ou seja, $L = N + f(K)$. Resta mostrar que a soma é direta. Dado $z \in N \cap f(K)$, existe $a \in K$ tal que $z = f(a)$. Ora, $a \in f^{-1}(N) \cap K = 0$ e assim $z = f(a) = f(0) = 0$, o que é suficiente para concluir que L é semissimples.

■

Corolário A.3 *Se M é semissimples, estão todo módulo fator de M é semissimples.*

Demonstração. De fato, basta observar que um módulo fator é imagem de M pelo homomorfismo sobrejetivo projeção canônica. ■

Lema A.4 *Todo módulo semissimples não nulo possui algum submódulo simples.*

Demonstração. Sejam R um anel e M um R-módulo à esquerda semissimples não nulo. Dado $m \in M \setminus \{0\}$, mostraremos que o submódulo Rm contém um submódulo simples. Seja F a família de todos os submódulos de Rm que não contêm m. Note que $F \neq \emptyset$, pois $\{0\} \in F$, e que qualquer cadeia de elementos de F possui cota superior. De fato, para a segunda afirmação basta notar que a união de todos os submódulos de

uma cadeia em F é ainda um submódulo pertencente a F e que contém toda a cadeia. Pelo Lema de Zorn, considerando F ordenado pela inclusão de conjuntos, existe um elemento maximal $N \in F$. Pelo lema A.2, Rm é semissimples e assim existe N' um submódulo de Rm tal que $Rm = N \oplus N'$. Afirmamos que N' é simples. De fato, existem $n \in N, n' \in N'$ tais que $m = n + n'$. Como $m \notin N$, temos $n' \neq 0$, mostrando que $N' \neq 0$. Sendo N'' um submódulo não nulo de N', mostraremos que $N'' = N'$. Aplicando novamente o Lema A.2, N' é semissimples e existe P um submódulo de N' tal que $N' = N'' \oplus P$. Afirmamos que $m \in N \oplus N''$, pois se isto não fosse verdade, teríamos $N \oplus N'' \in F$, mas $N \subsetneq N \oplus N''$ contrariaria a maximalidade de N em F. Como $m \in N \oplus N''$ segue que $N \oplus N'' = Rm$. Daí,

$$N \oplus N'' = Rm = N \oplus N' = N \oplus (N'' \oplus P) \Rightarrow N'' = N'' \oplus P,$$

de onde segue que $P = 0$, e assim, $N'' = N'$, mostrando que N' é simples. ■

Teorema A.5 *Se M é um R-módulo não nulo, são equivalentes:*

i) M é semissimples;

ii) M é soma de uma família de submódulos simples;

iii) M é soma direta de uma família de submódulos simples

Demonstração.

i) $\Rightarrow$ ii) Seja $\{S_i\}_{i \in I}$ a família de todos os R-submódulos simples de M. Tal família é não vazia pelo Lema A.4. Denotando $N = \sum_{i \in I} S_i$, como M é semissimples, existe um submódulo $P \subset M$ tal que $M = N \oplus P$. Se $P = 0$, o resultado segue. Se, por outro lado, $P \neq 0$, pelo Lema A.2 P é semissimples e, novamente usando o lema A.4, existe T um R-submódulo simples de P. Neste caso, existe $j \in I$ tal que $T = S_j$ e assim $T \subset N \cap P = 0$, um absurdo.

ii) $\Rightarrow$ iii) Seja $M = \sum_{i \in I} M_i$, onde $\{M_i\}_{i \in I}$ é uma família de submódulos simples de M. Consideremos $F = \left\{ J \subseteq I \mid \sum_{j \in J} M_j \text{ é uma soma direta} \right\}$ ordenado pela inclusão. Note que $F \neq \emptyset$ pois cada conjunto unitário de I pertence a F. Toda cadeia de elementos de F possui cota superior, a saber, a união dos seus membros e,

portanto, pelo Lema de Zorn existe um elemento maximal $I' \in F$. Considere $M' = \bigoplus_{j \in I'} M_j$. Mostraremos que $M' = M$. De fato, para cada $i \in I$, M_i é um módulo simples e, assim, $M_i \cap M' = 0$ ou $M_i \cap M' = M_i$. Se para algum i tivermos $M_i \cap M' = 0$, então $i \notin I'$, a soma $M' + M_i$ é direta e, portanto, $I' \subsetneq I' \cup \{i\} \in F$, o que contradiz a maximalidade de I'. Segue que $M_i \subset M'$, para todo $i \in I$, mostrando que $M \subseteq M'$, o que é suficiente para concluir a igualdade entre os dois conjuntos.

iii) $\Rightarrow$ i) Denote $M = \bigoplus_{i \in I} M_i$, onde M_i é um submódulo simples de M para cada i, e seja N um submódulo de M. Como M_i é simples, $N \cap M_i = 0$ ou $N \cap M_i = M_i$. Assim, $N = \bigoplus_{j \in J} M_j$, onde $J = \{i \in I \mid M_i \cap N = M_i\}$. De fato, a inclusão $\bigoplus_{j \in J} M_j \subseteq N$ é clara. Por outro lado, supondo, por contradição, que $N \not\subseteq \bigoplus_{j \in J} M_j$ existe $n \in N \setminus \bigoplus_{j \in J} M_j$. Ora, existe $i \in I$ tal que $n \in M_i \cap N$. Pelo que dissemos anteriormente, $M_i \cap N = M_i$, de onde segue que $i \in J$ e, portanto, $n \in \bigoplus_{j \in J} M_j$, um absurdo, o que mostra a igualdade. Assim, podemos escrever

$$M = \left(\bigoplus_{j \in J} M_j \right) \oplus \left(\bigoplus_{j \in I \setminus J} M_j \right) = N \oplus K,$$

donde segue que M é semissimples.

■

Definição A.6 *dizemos que R é um anel semissimples à esquerda se, visto como um $R-$módulo à esquerda (respectivamente à direita), for semissimples.*

Proposição A.7 *Todo anel com unidade semissimples à esquerda ou à direita é simultaneamente artiniano e noetheriano.*

Demonstração. Provaremos que se R é semissimples à esquerda então é artiniano e noetheriano. De fato, seja R um anel semissimples à esquerda. Pelo Teorema A.5 existe $\{I_j\}_{j \in J}$ uma família de submódulos à esquerda minimais de R tais que $R = \bigoplus_{j \in J} I_j$. Note que os submódulos I_j de R são, na verdade, ideais à esquerda minimais do anel R. Sejam $a_j \in I_{i_j}$ e $n \in \mathbb{N}$ tais que $1_R = 1 = \sum_{j=1}^{n} a_j$. Dado $r \in R$, temos

$r = r\cdot 1 = r\sum_{j=1}^{n} a_j = \sum_{j=1}^{n} ra_j \in \sum_{j=1}^{n} I_{i_j}$, donde podemos concluir que $R = \bigoplus_{j=1}^{n} I_{i_j}$. Assim, R possui uma série de composição. De fato, consideremos a cadeia

$$R \supseteq \bigoplus_{j=1}^{n-1} I_j \supseteq \cdots \supseteq I_1 \oplus I_2 \supseteq I_1 \supseteq 0$$

e perceba que

$$\frac{I_1 \oplus \cdots \oplus I_k}{I_1 \oplus \cdots \oplus I_{k-1}} \simeq I_k,$$

que é um submódulo simples para todo $k \in \{1, 2, \ldots, n\}$. Como o anel R possui uma série de composição finita, segue que R é artiniano e noetheriano. ■

Teorema A.8 *Seja R um anel com unidade. São equivalentes:*

i) R é semissimples;

ii) Todos os R-módulos à esquerda são semissimples;

iii) Todos os R-módulos à esquerda finitamente gerados são semissimples;

iv) Todos os R-módulos à esquerda cíclicos são semissimples.

Demonstração. As implicações *ii)* $\Rightarrow$ *iii)* $\Rightarrow$ *iv)* são triviais. Quanto a *iv)* $\Rightarrow$ *i)* basta notar que R é um R-módulo cíclico gerado por $1 \in R$. Resta provarmos *i)* $\Rightarrow$ *ii)*. Sejam R semissimples e M um R-módulo à esquerda. Temos $M = \sum_{m\in M} Rm$ e mostraremos que para cada $m \in M$ temos Rm semissimples. Pelo Teorema A.5 podemos escrever $R = \bigoplus_{i=1}^{k} I_i$, onde I_i é um ideal à esquerda minimal de R para todo $i \in \{1, 2, \ldots, k\}$. Segue que

$$Rm = (I_1 \oplus \cdots \oplus I_k)m = I_1m + \cdots + I_km.$$

Mostraremos que cada I_im é um R-submódulo simples de Rm. Para isto, fixemos $i \in \{1, 2, \ldots, k\}$ e consideremos L um R-submódulo de I_im. Se $L \neq 0$, tomemos $x \in L \setminus \{0\}$ e assim existe $a_i \in I_i$ tal que $x = a_im$. Neste caso, o conjunto $(L : m)_i = \{r \in I_i \mid rm \in L\}$ é um $R-$submódulo não nulo de I_i, de onde segue que $(L : m)_i = I_i$, visto que I_i é simples. Segue que $L = I_im$, mostrando que I_im é simples. ■

Notação A.9 *Dados R um anel semissimples e I um ideal à esquerda minimal de R denotaremos*

$$R_I := \sum\{J \lhd_l R \mid J \simeq I\},$$

onde o símbolo $\lhd_l$ significa "ideal à esquerda de"e "$\simeq$"é isomorfismo de R-módulos.

Lema A.10 *Se R é um anel semissimples e I é um ideal à esquerda minimal de R, então valem:*

i) R_I é um ideal de R;

ii) Se I e J são ideais à esquerda minimais de R tais que $I \not\simeq J$ como R-módulos, então $R_I R_J = 0$.

Demonstração.

i) É claro que R_I é fechado à soma e é um ideal à esquerda de R. Mostremos que é também um ideal à direita. Para isto, é suficiente mostrar que $Jr \subseteq R_I$, para todo $r \in R$ e todo $J \lhd_l R$ tal que $J \simeq I$. Dado $r \in R$, consideremos a aplicação $f_r : J \to R$ dada por $f_r(x) = xr$, para todo $x \in J$. Note que f_r é um R-homomorfismo, pois dados $a \in R$, $x, y \in J$, então

$$f_r(x + ay) = (x + ay)r = xr + ayr = f_r(x) + af_r(y).$$

Como J é um ideal à esquerda minimal de R, então $kerf_r = 0$ ou $kerf_r = J$, pois $kerf_r$ é um R-submódulo de J. Se $kerf_r = 0$, então $Jr = Imf_r \simeq J \simeq I$. Neste caso, $Jr \subseteq R_I$. Se, por outro lado, $kerf_r = J_I$ então $Jr = 0$ e, com maior razão, $Jr \subseteq R_I$.

ii) Sejam I e J ideais à esquerda minimais de R tais que $I \not\simeq J$. Dados $x \in R_I$, $y \in R_J$, temos

$$x = \sum_{i=1}^{n} a_i, \qquad\qquad y = \sum_{j=1}^{m} b_j,$$

onde $a_i \in L_i$, $b_j \in K_j$, L_i é um ideal à esquerda minimal de R isomorfo a I e K_j é um ideal à esquerda minimal de R isomorfo a J, para cada $i \in \{1, \ldots, n\}$ e $j \in \{1, \ldots, m\}$. É suficiente provar que se $L, K \lhd_l R$ com $L \simeq I$, $K \simeq J$, então $LK = 0$. Dado $y \in K$, devemos ter $Ly = 0$ ou $Ly = K$, pois K é minimal. Se $Ly = K$, temos $I \simeq L \simeq Ly = K \simeq J$, o que contradiz nossa hipótese. Segue que $Ly = 0$, para todp $y \in K$. Segue que $LK = 0$, e, portanto, $R_I R_J = 0$.

■

Definição A.11 *Dado R um anel semissimples à esquerda, então o módulo regular ${}_R R$ é semissimples e podemos escrever*

$${}_R R = \underbrace{I_{1,1} \oplus \cdots \oplus I_{1,n_1}}_{R_{I_1}} \oplus \cdots \oplus \underbrace{I_{r,1} \oplus \cdots \oplus I_{r,n_r}}_{R_{I_r}} = \oplus R_{I_p},$$

onde $R_{I_k} = \sum\{J \lhd_l R \mid J \text{ é minimal e } J \simeq I_k\}$. *Ora,* $R = R_{I_1} \oplus \cdots \oplus R_{I_r}$ *como soma de submódulos. Dizemos que as parcelas* R_{I_i} *são as componentes homogêneas de* R.

Observação A.12 *Se* $R = I_1 \oplus \cdots \oplus I_n$ *com* $I_j \lhd R$, *para todo* j *e* $J \lhd R$, *então* $J = J_1 \oplus \cdots \oplus J_n$, *onde* $J_k \lhd I_k$. *De fato,* $1 = e_1 + e_2 + \cdots + e_n$, *com* $e_i \in I_i$, *e assim* $1 = 1^2 = \sum e_i e_j = \sum e_i^2$, *pois se* $i \neq j$, $e_i e_j \in I_i I_j \subseteq I_i \cap I_j = 0$. *Da unicidade da representação em uma soma direta, obtemos* $e_i^2 = e_i$ *e, assim,* $\{e_1, e_2, \ldots, e_n\}$ *é um conjunto de elementos idempotentes ortogonais de* R. *Além disso, tais elementos são centrais pois, para qualquer* $r \in R$, $r1 = 1r$. *Portanto*

$$J = RJ = (I_1 \oplus \cdots \oplus I_n)J = Je_1 \oplus \cdots \oplus Je_n, \text{ onde } Je_i \lhd Re_i.$$

Lema A.13 *Sejam* R *um anel e* $I_1, \ldots, I_r, J_1, \ldots, J_s$ *ideais indecomponíveis de* R *tais que* $R = I_1 \oplus \cdots \oplus I_r = J_1 \oplus \cdots \oplus J_s$. *Então* $r = s$ *e, a menos de uma permutação de índices,* $I_i = J_i$, *para todos* $i = 1, \ldots, r$.

Demonstração. Note que $J_1 \lhd R$ e, pela observação, temos $J_1 = I_1' \oplus \cdots \oplus I_r'$ com $I_i' \lhd I_i$. Como J_1 é um ideal indecomponível, existe $k \in \{1, \ldots, r\}$ tal que $J_1 = I_k'$. Reordenando os índices, se necessário, podemos escrever $J_1 = I_1'$ e, assim, $J_1 \subseteq I_1$. Analogamente, obtemos $I_1 \subseteq J_1$. Repetindo a argumentação finitas vezes obtemos o resultado. ■

Lema A.14 *Seja* R *um anel semissimples à esquerda. Então* $R = R_1 \oplus \cdots \oplus R_r$, *onde cada* R_i, $1 \leq i \leq r$, *é um anel simples com unidade que possui um único ideal à esquerda minimal a menos de isomorfismos.*

Demonstração. Como R é semissimples, podemos escrever $R = R_1 \oplus \cdots \oplus R_r$, onde , pelo Lema A.10, cada R_i é ideal que, a menos de isomorfismo, contém apenas um ideal à esquerda minimal. Pela observação anterior, existem elementos idempotentes e_i tais que $R_i = e_i R = Re_i$ e, portanto, e_i é unidade para o anel R_i. Resta mostrar que R_i é simples para cada i. Fixado $i \in \{1, 2, \ldots, r\}$, tomando $I \lhd R_i$, $I \neq 0$, temos $I \lhd R$. De fato, dados $e_1 s_1 + \cdots + e_r s_r \in R$ e $e_i s \in I$, temos $(e_1 s_1 + \cdots + e_i s_i + \cdots + e_r s_r) e_i s = e_i s_i s \in R_i I \subset I$. O outro lado é análogo. Como todo ideal de R é ideal à esquerda, então I é um R-submódulo de ${}_R R$ e, portanto, I é semissimples. Pelo Teorema A.5, I é a soma direta de submódulos simples, em outras palavras, I contém um ideal à esquerda minimal I_0 de R. Ainda da soma direta de I e da observação anterior, como I_0 é um submódulo à esquerda minimal de ${}_R R$, existe um elemento idempotente $e \in R$ tal que $I_0 = Re$. Considere a componente homogênea $R_{I_0} = \sum\{J \lhd_l R \mid J \text{ é minimal e } J \simeq I_0\}$. Pelo

Lema A.13, devemos ter $R_{I_0} = R_j$ para algum $j \in \{1, \ldots, r\}$. Como $I_0 \subset R_i$, devemos ter $R_{I_0} = R_i$. Seja agora $J \lhd_l R$ minimal tal que $J \subseteq R_i$. Como $R_i = I_{I_)}$, existe um R-isomorfismo $f : I_0 \to J$ e, assim,

$$J \simeq f(I_0) = f(Re) = f(Ree) = f(I_0 e) = I_0 f(e) \subseteq I.$$

Assim, $R_i = R_{I_0} = \sum\{J \lhd_l R \mid J \text{ é minimal e } J \simeq I_0\} \subset I$, de onde segue que $I = R_i$ e, portanto, R_i é simples para todo $i = 1, \ldots, r$. ■

Lema A.15 (Schur) *Sejam R um anel e M um R-módulo à esquerda simples. $End_R(M)$ é um anel de divisão.*

Demonstração. Seja $f : M \to M$ um R-endomorfismo. Sabemos que $Kerf$ e Imf são R-submódulos de M. Supondo f não nula, da simplicidade de M devemos ter $Kerf = 0$ e $Imf = M$, de onde segue que f é bijetora e possui inversa, mostrando que $End_R(M)$ é um anel de divisão. ■

No próximo resultado, dado I um ideal à esquerda não nulo do anel R, mostraremos que R é isomorfo ao anel de endomorfismos de I visto como D-módulo, onde $D = End_R(I)$, que denotamos por $End_D(I)$.

Proposição A.16 (Rieffel) *Seja R um anel simples. Suponhamos que R contenha um ideal à esquerda não nulo I. Então $R \simeq End_D(I)$.*

Demonstração. Consideremos

$$\begin{array}{rccl} f: & R & \longrightarrow & End_D(I) \\ & r & \longmapsto & \begin{array}{rccl} f_r: & I & \longrightarrow & I \\ & a & \longmapsto & ra \end{array} \end{array} .$$

Não é difícil ver que f_r é um D-endomorfismo de I. Mostremos que f é um isomomorfismo de anéis. De fato, dados $r, s \in R$ e $a \in I$, temos

$$f(r+s)(a) = f_{r+s}(a) = (r+s)a = ra + sa = f_r(a) + f_s(a) = (f(r) + f(s))(a) \quad e$$

$$f(rs)(a) = f_{rs}(a) = rsa = f_r(sa) = f_r(f_s(a)) = (f_r \circ f_s)(a).$$

Como R é um anel simples, então $Kerf = 0$ ou $Kerf = R$. Mas como $f(1_R) = Id_I \neq 0$, obtemos $Kerf = 0$, de onde segue que f é injetora. Antes de provarmos a sobrejetividade de f, mostraremos que $f(I)$ é um ideal à esquerda de $End_R(I_D)$. Note

que a multiplicação à direita por um elemento de I é um elemento do anel D. De fato, dado $a \in I$, consideremos $g_a : I \to I$ dado por $g_a(x) = xa$. Dados $x, y \in I$ e $r \in R$, então

$$g_a(x+y) = (x+y)a = xa + ya = g_a(x) + g_a(y) \quad \text{e} \quad g_a(rx) = rxa = rg_a(x)$$

mostrando que $g_a \in D$, para todo $a \in I$. Tomando agora $a, b \in I$ e $h \in End_D(I)$, como $g_b \in D$, obtemos

$$h(f_a(b)) = h(ab) = h(a)b = f_{h(a)}(b)$$

e assim, $h \circ f_a = f_{h(a)} \in f(I)$, para quaisquer $a \in I, h \in End_D(I)$. Em outras palavras,

$$End_D(I)f(I) \subseteq f(I) \text{ e, portanto, } f(I) \lhd_l End_D(I).$$

Por fim, como R é simples e $I \neq 0$, temos $IR = R$, pois $IR \lhd R$. Ora, $f(R) = f(IR) = f(I)f(R)$ e

$$End_D(I)f(R) = End_D(I)f(I)f(R) \subseteq f(I)f(R) = f(R).$$

Portanto $f(R) \lhd_l End_D(I)$. Agora observemos que $1_{End_D(I)} = Id_I = f(1_R) \in f(R)$ e assim $f(R) = End_D(I)$, mostrando a sobrejetividade de f. ■

Corolário A.17 *Se R é um anel simples que contém um ideal à esquerda minimal, então $R \simeq M_n(D)$, para algum $n \geq 1$ e D um anel de divisão.*

Demonstração. Seja $I \subseteq R$ um ideal à esquerda minimal. Pelo lema de Schur, $D := End_R(I)$ é um anel de divisão. Assim, considerando em I sua estrutura de (R, D)-bimódulo, pela Proposição de Rieffel, podemos concluir que $End_D(I)$ é simples, pois é isomorfo a um anel simples. Mostraremos que $dim_D I < \infty$, pois, neste caso, $End_D(I)$ é o anel das transformações lineares de I em I e, naturalmente, obteremos o isomorfismo desejado.

Supondo, por absurdo, que $dim_D I = \infty$. O conjunto

$$K = \{f \in End_R(I_D) \mid dim_D(Im(f)) < \infty\}$$

é um ideal próprio de $End_D(I)$. De fato, pois na composição de funções, se a dimensão de uma das imagens for finita, a da imagem da composição também será e, além disso, é próprio por que a imagem da identidade tem dimensão infinita. Ora, é fácil ver que

$K \neq 0$, bastando tomar, por exemplo, uma aplicação que leve qualquer vetor num múltiplo escalar de um vetor fixo, uma projeção. Mas isto contradiz a simplicidade de $End_D(I)$, o que conclui a demonstração. ■

Lema A.18 *Seja R um anel simples que possui um ideal à esquerda minimal I. Então R possui, a menos de isomorfismo, um único módulo à esquerda simples e fiel isomorfo a I. Ademais, nestas condições, $R \simeq I^{(n)}$, onde $I^{(n)}$ é a soma direta de n cópias de I.*

Demonstração. Sabemos que $A(I) = \{r \in R \mid rI = 0\} \lhd R$ e R tem unidade. Pela simplicidade de R, $A(I) = 0$ ou $A(I) = R$. Se $A(I) = R$, então $1 \in A(I)$, ou seja, $I = 1I = 0$, o que não ocorre. Portanto, I é um R-módulo à esquerda simples e fiel.

seja M um R-módulo à esquerda simples e fiel. Como $A(M) = 0$, existe $m \in M$ tal que $Im \neq 0$. Pela simplicidade de M segue que $Im = M$. Assim a aplicação $f : I \to M$ definida por $f(x) = xm$ é um R-epimorfismo. Porém, como $Kerf \lhd I$ e I é simples, obtemos que $Kerf = 0$ e f é um isomorfismo de R-módulos. Portanto, a menos de isomorfismos, R possui apenas um módulo à esquerda simples e fiel.

Ademais, pelos resultados anteriores, $R \simeq M_n(D)$, onde $D = End_R(I)$ e $n = dim_D I$. Assim, $R \simeq M_n(D) \simeq I^{(n)}$, onde $I = \{(a_{ij}) \in M_n(D) \mid a_{ij} = 0, \text{ se } j \neq 1\}$. ■

Teorema A.19 (Teorema de Wedderburn-Artin) *Seja R um anel semissimples à esquerda. Então*

$$R \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k),$$

onde $D_1, D_2, \ldots, D_k$ são anéis de divisão e $n_1, n_2, \ldots, n_k$ são naturais. O número k e os pares ordenados (D_i, n_i) são unicamente determinados a menos de permutações. Além disso, existem exatamente k R-módulos à esquerda simples e fiéis dois a dois não isomorfos.

Demonstração. Pelo Lema A.14, podemos escrever $R = R_1 \oplus \cdots \oplus R_n$, onde cada R_i é anel simples com unidade que possui, a menos de isomorfismos, um único ideal à esquerda minimal. Ora, pelo comentário anterior, como cada R_i é isomorfo a $M_{n_i}(D_i)$, com D_i anel de divisão, segue que

$$R \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k).$$

Resta apenas mostrar a unicidade desta representação. Suponhamos $R \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k)$ e que $R \simeq M_{m_1}(D'_1) \times M_{m_2}(D'_2) \times \cdots \times M_{m_s}(D'_s)$, onde

cada D_i e cada D'_j é anel de divisão. Seja V_i o único módulo simples e fiel sobre $R_i = M_{n_i}(D_i)$ (vide Lema A.18). Estendendo a multiplicação de V_i como R_i-módulo para R pondo $R_i \cdot V_j = 0$, se $j \neq i$, obtemos V_i como um R-módulo à esquerda simples. Mostremos agora que se $i \neq j$, então $V_i \not\simeq V_j$. Suponhamos, por contradição que $f : V_i \to V_j$ é um R-homomorfismo. Para todo $r \in R$ e $v \in V_i$ teríamos $f(rv) = rf(v)$. Tomando $r = (0, \ldots, 0, 1_{R_j}, 0, \ldots, 0) \in R$, obtemos $rf(v) = f(rv) = f(0) = 0$ e assim $r \in A(V_j) = 0$, pois $v \in V_i$ é arbitrário, o que contradiz a sobrejetividade de f. Segue que $V_i \not\simeq v_j$. Pelo Lema A.18, $M_{n_i}(D_i) \simeq V_i^{(n_i)}$. Repetindo o argumento com a outra decomposição obtemos

$$V_1^{(n_1)} \oplus \cdots \oplus V_k^{(n_k)} \simeq_R R \simeq V_1'^{(m_1)} \oplus \cdots \oplus V_s'^{(m_s)}.$$

Mas pelo teorema de Jordan-Hölder, sobre a unicidade de séries de composição, segue que $s = k, n_i = m_i$ e ${}_RV_i \simeq_R V'_i$. Por fim, observe que

$$D'_i = End_{R'_i}(V'_i) \simeq End_R(V'_i) \simeq End_R(V_i) \simeq End_{R_i}(V_i) = D_i.$$

■

Bibliografia

[1] Alves, S. T.,*Identidades Polinomiais Graduadas para Álgebras de Matrizes*, Dissertação (Mestrado em Matemática), UFCG, Campina Grande (2012)

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

[3] Araújo, L. D. A., *Identidades polinomiais para álgebras de matrizes triangulares superiores em blocos*, Dissertação (Mestrado em Matemática), UFCG, Campina Grande (2017).

[4] Bahturin, Y. A., Zaicev, M. V. e Sehgal, S. K., *Finite-dimensional graded simple algebras*, Sbornik: Mathematics 199:7, 965-983 (2008).

[5] Bezerra, C. F., *Introdução a PI-Álgebras*, Notas de aula, UAMat - UFCG, (2018).

[6] Brandão, A. P., *Representações de Grupos* Notas de aula, UAMat - UFCG.

[7] Bresar, M. *Introduction to Noncommutative Algebra*, Springer, (2014).

[8] Drensky, V., *Free Algebras and PI-Algebras*, Graduate Course in Algebra, Springer-Verlag (2000).

[9] Elduque, A. e Kochetov, M., *Gradings on Simple Lie Algebras*, Mathematical Surveys and Monographs, Volune 189, AMS - Providence, AARMS - Halifax (2013).

[10] Fraleigh, J. B., *A First Course in Abstract Algebra*, 6ª edição. New York: Addison-Wesley (2000).

[11] Giambruno, A. e Zaicev, M., *Polynomial identities and asymptotic methods*, Mathematical Surveys and Monographs, Volune 122, AMS (2005).

[12] Kaplanski, I., *Rings with a polinomial identity.* Bull. Amer. Math. Soc. 54 220, 496-500 (1948).

[13] Koshlukov, P. e Zaicev, M., *Identities and isomorphisms of graded simple algebras*, Linear Algebra and its Applications 432, Elsevier, 3141-3148 (2010).

[14] Lang, S., *Algebra*, Graduate Texts in Mathematics 211 3^{rd} ed., New York: Springer-Velag, (2002).

[15] Lima, E. L., *Álgebra Linear*, 1. ed. Rio de Janeiro: IMPA, (2014).

[16] Nastasescu, C. e Van Oystaeyen, F., *Graded Ring Theory.* North-Holland Mathematical Library, Volume 28, (1982).

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

[18] Sant'ana, A., *Uma introdução ao estudo dos anéis semissimples*, IV Colóquio de Matemática da Região Sul. 1ª edição, Rio Grande, SBM (2016).

[19] Tignol, J.-P. e Wadsworth, A. R., *Value Functions on Simple Algebras, and Associated Graded Rings*, Springer, (2015).