Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Álgebras semissimples e suas aplicações em Combinatória e Otimização

Henrique Soares Assumpção e Silva

Orientador:
Gabriel Coutinho

Projeto Orientado em Computação

Março de 2024

Sumário

Introdução

Este trabalho consiste no Projeto Orientado em Computação (POC) necessário para a graduação em Ciência da Computação da Universidade Federal de Minas Gerais (UFMG). Nosso objetivo principal será entender como aplicar ferramentas de áreas da matemática pura, como álgebra não-comutativa e teoria dos anéis, em questões de teoria dos grafos e de otimização combinatória, que são de grande interesse para a computação como um todo.

Nós começamos com um *grafo* G, isto é, um conjunto V de vértices e um conjunto $E \subseteq V \times V$ de arestas que conectam os vértices. Grafos podem ser encontrados em diversas áreas de pesquisa diferentes: eles são utilizados para descrever moléculas e outras estruturas químicas, para modelar sistemas físicos de interações entre partículas, para entender as relações entre usuários de redes sociais, e diversas outras coisas mais. Essas estruturas também são de extrema importância para a ciência da computação: 10 dos 21 problemas NP-completos originais descritos em Karp (1972) são explicitamente sobre grafos, e essa diversidade de problemas interessantes e difíceis talvez seja um dos principais motivadores para o desenvolvimento da teoria dos grafos ao longo do século XX, que atualmente é uma área extremamente rica e profunda.

Existem diversas formas de criar uma matriz que capture a estrutura combinatória de G, e talvez a forma mais natural seja por meio da *matriz de adjacência*, denotada por $A(G)$. Se trata de uma matriz com linhas e colunas indexadas pelos vértices de G, tal que a entrada uv da matriz é igual a 1 se uv é aresta de G, e é igual a 0 caso contrário. A partir disso, podemos nos perguntar: que tipo de informação combinatória sobre o grafo pode ser extraída a partir das propriedades algébricas de sua matriz de adjacência? Perguntas desse tipo são características das áreas hoje conhecidas como teoria espectral e teoria algébrica dos grafos, e nossa abordagem utilizará diversas técnicas destas áreas.

O estudo de grafos regulares, isto é, grafos cujos vértices possuem um número fixo k de vizinhos, levou a descoberta de diversas conexões e interseções com áreas da álgebra abstrata, e estas interseções serão o foco principal deste trabalho. Certas famílias de grafos regulares, como os distância-regulares, possuem matrizes de adjacência que podem ser escritas como soma de outras matrizes, e essas outras matrizes formam a base de uma *álgebra*. Uma álgebra neste contexto é um subespaço vetorial do conjunto de todas as matrizes $n \times n$ que é fechado para produto de matrizes, onde n é o número de vértices do grafo, e de modo geral estaremos interessados em responder a seguinte pergunta: que tipo de informação combinatória podemos extrair das álgebras associadas à grafos?

Para responder essas perguntas, optamos por dividir este trabalho em duas partes. A primeira será dedicada inteiramente à compreensão do conceito de semissimplicidade em álgebras e anéis, e teremos como principal objetivo entender os teoremas estruturais de Wedderburn, o conceito do Radical de Jacobson, e como utilizar essas ferramentas para encontrar bloco-diagonalizações de certas álgebras de matrizes com entradas complexas. Utilizamos como referências principais os capítulos 4 e 5 de Cohn (2012), 13 e 17 de Lang (2005), 1 e 4 de Lam (2013), 4 de Curtis and Reiner (1966), 1 de Farb and Dennis (2012), 4 de Passman (2004), 1.2 e 1.3 de Vieira and Santos (2021), e também as notas de aula de Mendonça (2023) do curso de Álgebra não-comutativa da UFMG.

A segunda parte será dedicada à aplicações em problemas de combinatória, mais especificamente em teoria dos grafos, e também para problemas de otimização. O objetivo principal será entender como obter uma álgebra semissimples a partir de uma matriz de adjacência de um grafo, e entender quais grafos geram álgebras com certas propriedades especiais. Utilizamos como referências principais o capítulo 2 de Chen and Ponomarenko (2023), 1 e 2 de Bailey (2004), 12,13 e 16 de Godsil (2010), e 12 e 13 de Godsil (1993). Também iremos discutir os resultados de de Carli Silva et al. (2019) – sobre desigualdades do tipo clique-coclique e sobre o theta de Lovàsz – e de Proença et al. (2023) – relacionados ao corte-máximo e à cobertura por cortes fracionária. Ao longo dos próximos capítulos também discutiremos resultados de artigos científicos e de outros trabalhos, e estes serão propriamente referenciados quando necessário.

Este trabalho tenta ser o mais autocontido possível, e acreditamos que leitores com conhecimentos prévios em álgebra linear no nível de uma graduação em matemática, e.g. como apresentado em Axler (2014), sejam capazes de compreender o material na integra. Conhecimentos básicos em álgebra abstrata, combinatória e análise real também são bem-vindos, mas não estritamente necessários, e em caso de dúvidas as referências bibliográficas contém diversos materiais sobre os assuntos que serão discutidos.

1 Estruturas algébricas básicas

Neste capítulo, nosso objetivo principal é introduzir as estruturas algébricas básicas necessárias para os demais resultados apresentados ao longo do trabalho. O foco será em anéis, módulos e álgebras, mas também iremos discutir brevemente conceitos de grupos e corpos.

1.1 Grupos

Definição 1.1.1. Dado um conjunto G munido de uma operação binária $\cdot : G \times G \mapsto G$, dizemos que $(G, \cdot)$ é um *grupo* se para quaisquer a, b, c em G valem as seguintes condições:

(1) $a \cdot b \cdot c = a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(2) Existe elemento neutro e em G tal que $a \cdot e = e \cdot a = a$;

(3) Existe elemento a^{-1} em G tal que $a \cdot a^{-1} = e = a^{-1} \cdot a$.

Ambos elemento neutro e o inverso são únicos, e caso a operação seja comutativa, dizemos que o grupo é *abeliano*.

O item (1) nos diz que a operação do grupo é associativa, (2) nos garante a existência de um elemento neutro, e (3) nos mostra que todo elemento de um grupo é invertível. Existem diversos exemplos importantes de grupos: o *grupo simétrico* $\mathrm{Sym}(X)$ sobre um conjunto X consistindo de todas as bijeções de em X com a operação de composição de funções - e tal conjunto é denotado por $\mathrm{Sym}(n)$ ou S_n quando X é finito e com n elementos; o *grupo linear geral* $\mathrm{GL}_n(\mathbb{C})$ consistindo das matrizes invertíveis $n \times n$ com entradas nos número complexos com a operação de multiplicação de matrizes; o *grupo diedral* D_n das simetrias de um polígono regular com n vértices, e muitos outros mais.

Dado um subconjunto $H \subseteq G$, dizemos que H é *subgrupo* se H também é um grupo com respeito à mesma operação de G, e nesses caso podemos observar que H é subgrupo de G se, e somente se, H contém xy^{-1} para quaisquer x, y de H. No caso de grupos abelianos cuja operação representa algum tipo de adição, iremos representá-la pelo símbolo $+$, e o seu elemento neutro será denotado por 0. Dados grupos G, H, podemos estudar os mapas entre eles que preservar sua estrutura de grupos, isto é, funções da forma

$$\varphi : G \mapsto H,$$
$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y).$$

Essas funções recebem o nome de *homomorfismos* de grupos, e é imediato notar que $\varphi(e_G) = e_H$, e que $\varphi(x^{-1}) = \varphi(x)^{-1}$. Se um homomorfismo é injetivo ele é chamado de *monomorfismo*, se é sobrejetivo é dito *epimorfismo*, e se é bijetivo é dito *isomorfismo*, e escreveremos $G \cong H$ quando G e H forem grupos isomorfos. Um homomorfismo de um grupo para si próprio é dito *endomorfismo*, e quando esse mapa é bijetivo ele é chamado de *automorfismo*, e nesse caso denotamos o conjunto de automorfismos de um grupo por $\mathrm{Aut}(G)$, que também é um grupo com a operação de composição de funções. Dado um homomorfismo φ entre grupos G e H, definimos o seu *núcleo* e sua *imagem* como os conjuntos

$$\ker(\varphi) := \{x \in G | \varphi(x) = e_H\} \subseteq G,$$
$$\mathrm{Im}(\varphi) := \{\varphi(x) | x \in G\} \subseteq H,$$

respectivamente. A partir destas definições, podemos observar que um homomorfismo é injetivo se, e somente se, o seu núcleo contém somente o elemento neutro, e nesse caso diremos que o núcleo é *trivial*. A terminologia que apresentamos para funções entre grupos também será utilizada para funções entre os demais objetos algébricos discutidos nas próximas seções, com as devidas alterações que ficarão claras pelo contexto.

A construção a seguir também será extremamente importante.

Definição 1.1.2. Sejam G, H grupos, então definimos seu *produto direto externo* como sendo o conjunto

$$G \times H := \{(x, y) | x \in G, y \in H\},$$

com operação dada por

$$(x_1, y_1)(x_2, y_2) := (x_1x_2, y_1y_2).$$

Tal conjunto é um grupo com elemento neutro dado por (e_G, e_H).

Podemos generalizar a noção de produto direto para uma quantidade arbitrária de grupos, isto é, se $\{G_i\}_{i\in\mathcal{I}}$ é uma família arbitrária de grupos indexada por algum conjunto $\mathcal{I}$, definimos seu produto direto externo

$$\prod_{i\in\mathcal{I}} G_i := \{(x_i)_{i\in\mathcal{I}} | x_i \in G_i\},$$

com operação dada por

$$(x_i)_{i\in\mathcal{I}}(y_i)_{i\in\mathcal{I}} := (x_iy_i)_{i\in\mathcal{I}},$$

para quaisquer sequências $(x_i)_{i\in\mathcal{I}}, (y_i)_{i\in\mathcal{I}}$ de $\prod_{i\in\mathcal{I}} G_i$. O produto direto é um grupo onde o elemento neutro é apenas a sequência com cada elemento neutro dos respectivos G_i. Ele também é naturalmente acompanhado por uma família de homomorfismos de grupos: para cada índice i de $\mathcal{I}$, podemos definir o epimorfismo *projeção* que mapeia uma sequência qualquer do produto em seu i-ésimo elemento, e o monomorfismo *inclusão*, que mapeia um elemento x de G_i na sequência formada pelos elementos neutros na posições diferentes de i e por x na i-ésima posição.

No caso de grupos abelianos, definimos também a noção de *soma direta externa*. Se $\{G_i\}_{i\in\mathcal{I}}$ é uma família de grupos abelianos, então denotamos por

$$\bigoplus_{i\in\mathcal{I}} G_i \subseteq \prod_{i\in\mathcal{I}} G_i$$

como o subconjunto do produto direto formado por todas as sequências *quase-nulas*, isto é, sequências $(a_i)_{i\in\mathcal{I}}$ que possuem apenas uma quantidade finita de elementos diferentes do elemento neutro do respectivo grupo. Neste caso, esse conjunto forma um grupo com as mesmas operações e elemento neutro do produto direto externo, e vale notar que se $\mathcal{I}$ é finito, então o produto direto e a soma direta são iguais.

1.2 Anéis e Corpos

Neste trabalho não estaremos interessados em grupos de modo geral, mas sim em grupos com estrutura adicional que nos permite inferir mais informações sobre o conjunto em questão. O primeiro destes objetos são os anéis, que nada mais são que conjuntos onde se pode somar e multiplicar elementos de maneira associativa. Anéis também são chamados de sistemas numéricos, e historicamente a motivação por trás do seu estudo vem justamente do uso de sistemas numéricos alternativos aos inteiros – como os inteiros gaussianos – para demonstrar resultados em teoria dos números. Formalmente, temos a seguinte definição.

Definição 1.2.1. Seja $(R, +)$ um grupo abeliano. Dizemos que R é um *anel* se ele é munido de uma operação $\cdot : R \times R \mapsto R$ tal que para quaisquer elementos a, b, c de R:

(1) $a \cdot b \cdot c = a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(2) $a \cdot (b + c) = a \cdot b + a \cdot c$;

(3) $(a + b) \cdot c = a \cdot c + b \cdot c$;

(4) Existe elemento 1 em R tal que $a \cdot 1 = 1 \cdot a = a$.

Assim como no caso de grupos, é imediato verificar que o elemento unitário do anel é único. Iremos denotar $a \cdot b$ por ab quando for conveniente, e se a operação $\cdot$ é comutativa, R é dito *comutativo*.

O item (1) nos diz que a operação de produto do anel é associativa, (2) e (3) nos dizem que a operação de produto é distributiva com respeito à operação de soma, e (4) nos garante a existência de um elemento unitário[1]. O conjunto $\mathbb{Z}$ dos números inteiros é um exemplo clássico de um anel comutativo. O conjunto $M_n(R)$ das matrizes $n \times n$ com entradas em um dado anel R também é um exemplo importante de um anel, e note que mesmo se R é comutativo o anel $M_n(R)$ não é se $n \geq 2$. Esse anel também é chamado de *álgebra completa de matrizes* $n \times n$ com entradas em R, por motivos que ficarão claros nas próximas seções.

Dados elementos a, b de R não-nulos tais que $ab = 1$, dizemos que a é *invertível à direita*, e analogamente que b é *invertível à esquerda*. Se um elemento é invertível tanto à esquerda quanto à direita, então os inversos são iguais, e daí dizemos que ele é *invertível*. O conjunto dos elementos invertíveis de um anel R é denotado por R^* ou por $U(R)$, e é usualmente chamado de *grupo unitário do anel*, pois de fato se trata de um grupo com operação de multiplicação e elemento neutro dado por 1. Se todo elemento não-nulo de um anel é invertível, isto é, se $R^* = R \setminus \{0\}$, dizemos que R é *anel de divisão*, e se ele também é comutativo ele é chamado de *corpo*.

Exemplo 1.2.2. Denote por $\mathbb{Z}_n$ o conjunto das classes de equivalência dos inteiros módulo n. Sabe-se que um elemento $x \in \mathbb{Z}_n$ possui inverso se, e somente se, x for coprimo com n, ou seja, $\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n | \gcd(x, n) = 1\}$ é o grupo unitário de $\mathbb{Z}_n$, também chamado de grupo multiplicativo do anel. Vale notar que a cardinalidade de $\mathbb{Z}_n^*$ é dada por $\varphi(n)$, onde φ é a função totiente de Euler. Se p é primo, então todo elemento não nulo será invertível, e portanto $\mathbb{Z}_p$ é corpo.

Dado um anel R qualquer e um subgrupo abeliano S de R, dizemos que ele é *subanel* se S também é um anel com as mesmas operações de R e contém a unidade 1 de R. Um subgrupo abeliano L é um *ideal à esquerda* de R se ele é fechado para multiplicação a esquerda por elementos de R, isto é, o produto ra pertence à L para quaisquer elementos r de R e a de L. Uma definição análoga vale para ideais à direita, e se um ideal é simultaneamente à esquerda e à direita, ele é dito *bilateral* (ou simplesmente ideal), e naturalmente se R é comutativo, todo ideal é bilateral. Disso é imediato que se L é um ideal à esquerda que contém a unidade 1, então $R = L$, ou seja, qualquer ideal próprio não-trivial de R necessariamente não-contém a unidade, e portanto não é um subanel. Um anel R é dito *simples* se seus únicos ideais bilaterais são R e $\{0\}$. Um ideal à esquerda próprio L é dito *maximal* se, dado qualquer outro ideal à esquerda J com $L \subseteq J$, vale que $J = L$ ou $J = R$, e um ideal à esquerda L é dito *minimal* se o único ideal à esquerda próprio de L é o ideal trivial $\{0\}$. Definições análogas se aplicam para ideais à direita e para ideais bilaterais.

Um homomorfismo φ entre dois anéis R, S é um homomorfismo de grupos entre $(R, +)$ e $(S, +)$ que também é compatível com as operações de multiplicação dos anéis, isto é,

$$\begin{aligned} \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b), \\ \varphi(1_R) &= 1_S, \end{aligned}$$

para quaisquer elementos a, b de R. Iremos denotar o conjunto de homomorfismos entre os anéis R e S por $\mathrm{Hom}(R, S)$, e se $R = S$, denotaremos este mesmo conjunto por $\mathrm{End}(R)$, que no caso também é um anel com operação de composição de funções e adição, com unidade dada pela função identidade.

Uma construção extremamente comum no estudo de álgebra abstrata são os chamados quocientes. No caso de anéis, dado um ideal I de um anel R, criamos um novo anel denotado por

$$R/I := \{a + I | a \in R\}$$

chamado de *anel quociente*. Os elementos $a + I := \{a + b | b \in I\}$ são chamados de *classes laterais*, e também podem ser denotados por $\overline{a}$. As operações de adição e multiplicação são definidas da seguinte forma:

$$\begin{aligned} (a + I) + (b + I) &:= (a + b) + I; \\ (a + I)(b + I) &:= ab + I. \end{aligned}$$

[1] Para este trabalho, um anel quer dizer um anel associativo com unidade. Em geral é possível se discutir anéis não unitários, mas não estaremos interessados nestes casos.

O elemento neutro aditivo de R/I é dado por $0+I=I$ – que também será denotado por 0 quando o contexto for claro –, e o elemento unitário é dado por $1+I$. Deixamos ao leitor verificar que R/I é anel se, e somente se, I for um ideal bilateral de R, ou seja, não podemos tomar quocientes sobre quaisquer ideais de um dado anel.

Podemos também considerar o conjunto de todos os elementos que comutam com os demais em R, usualmente chamado de *centro do anel*, e denotado por

$$Z(R) := \{a \in R | \forall b \in R : ab = ba\} \subseteq R,$$

que naturalmente forma um subanel de R. Nesse caso, também podemos definir o *comutador* entre dois elementos de R como

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

e dessa forma podemos descrever o centro do anel como

$$Z(R) = \{a \in R | \forall b \in R : [a,b] = 0\}.$$

Se $S \subseteq R$ é um subconjunto qualquer de um anel R, definimos o *centralizador* – também chamado de comutante – de S como o conjunto dos elementos de R que comutam com todos os elementos de S, isto é,

$$C_R(S) := \{a \in R | \forall b \in S : [a,b] = 0\} \subseteq R,$$

e note que $C_R(S)$ é um subanel de R.

Existem dois resultados extremamente importantes relativos a quocientes de anéis, e versões análogas de tais resultados também irão valer para os módulos que serão discutidos na próxima seção.

Teorema 1.2.3 (Primeiro Teorema do Isomorfismo para Anéis)**.** Sejam R, S anéis, e seja $\varphi \in \mathrm{Hom}(R,S)$ um homomorfismo entre eles. Então $\ker(\varphi)$ é ideal bilateral de R, $\mathrm{Im}(\varphi)$ é subanel de S, e

$$R/\ker(\varphi) \cong \mathrm{Im}(\varphi).$$

Demonstração. Nos deixamos ao leitor provar que $\ker(\varphi)$ é ideal bilateral de R, e que $\mathrm{Im}(\varphi)$ é subanel de S. Defina a seguinte função:

$$\overline{\varphi} : R/\ker(\varphi) \mapsto \mathrm{Im}(\varphi),$$
$$\overline{\varphi}(r + \ker(\varphi)) = \varphi(r),$$

e note que $\overline{\varphi}$ é homomorfismo de anéis.

Seja r elemento de R e assuma que $\overline{\varphi}(r+\ker(\varphi)) = 0$, logo por definição $\varphi(r) = 0$, portanto r é um elemento de núcleo $\ker(\varphi)$ de φ, que por sua vez é o elemento neutro de $R/\ker(\varphi)$, logo $\ker(\overline{\varphi}) = \{0\}$, implicando que $\overline{\varphi}$ é injetiva. Dado elemento $\varphi(r)$ qualquer da imagem $\mathrm{Im}(\varphi)$, onde r pertence à R, note que $r+\ker(\varphi)$ pertence à $R/\ker(\varphi)$, e que $\overline{\varphi}(r+\ker(\varphi)) = \varphi(r)$, logo $\overline{\varphi}$ é sobrejetiva. Dessas observações segue que $\overline{\varphi}$ é isomorfismo de anéis, o que nos permite concluir que $R/\ker(\varphi)$ é de fato isomorfo à $\mathrm{Im}(\varphi)$. ■

O teorema anterior essencialmente nos diz que para qualquer homomorfismo φ entre anéis R, S, sempre existe um homomorfismo $\overline{\varphi}$ tal que o diagrama

$$\begin{array}{ccc} R & \xrightarrow{\quad\varphi\quad} & S \\ \downarrow{\scriptstyle \pi} & & \uparrow{\scriptstyle \iota} \\ R/\ker(\varphi) & \xrightarrow{\overline{\varphi}} & \mathrm{Im}(\varphi) \end{array}$$

comuta, isto é, tal que $\varphi = \iota \circ \overline{\varphi} \circ \pi$, onde $\pi(a) = a + \ker(\varphi), \iota(b) = b$ denotam a projeção e inclusão canônicas, respectivamente. Também é importante notar que se φ é injetiva, o teorema anterior implica que R é isomorfo à $\mathrm{Im}(\varphi)$, e nesse caso dizemos que R este *isomorficamente imerso* em S, pois podemos identificar R como um subanel de S.

Agora mostramos que podemos identificar os ideais à esquerda de R com os ideais à esquerda do seu anel quociente com respeito à algum ideal.

Teorema 1.2.4 (Teorema da Correspondência para Anéis)**.** Seja R um anel, e I um ideal bilateral de R. Então existe uma bijeção entre os ideais à esquerda de R que contém I e os ideais à esquerda de R/I.

Demonstração. Considere os conjuntos

$$\mathcal{L}_R := \{L \subseteq R | L \text{ é ideal à esquerda de } R, I \subseteq L\},$$
$$\mathcal{L}_{R/I} := \{J \subseteq R/I | J \text{ é ideal à esquerda de } R/I\},$$

e defina as funções

$$f : \mathcal{L}_R \mapsto \mathcal{L}_{R/I} \qquad g : \mathcal{L}_{R/I} \mapsto \mathcal{L}_R,$$
$$f(L) = \{\pi(x) | x \in L\} \qquad g(J) = \{x \in R | \pi(x) \in J\},$$

onde π é a projeção canônica que leva x em $x + I$. Iremos mostrar que f e g são funções inversas, e daí concluir a afirmativa do teorema. Primeiro devemos mostrar que as funções estão bem definidas, e para isso considere L um ideal à esquerda de R em $\mathcal{L}_R$, e tome elementos $x + I, y + I$ na imagem $f(L)$ de L por f, logo

$$(x + I) - (y + I) = (x - y) + I = \pi(x - y) \in f(L),$$
$$(r + I)(x + I) = (rx) + I = \pi(rx) \in f(L),$$

e daí segue que $f(L)$ pertence à $\mathcal{L}_{R/I}$. Similarmente, note que se x é elemento de I então $\pi(x) = I = 0$ no quociente, e disso segue que $g(J)$ pertence à $\mathcal{L}_R$, portanto as funções estão bem-definidas. Agora note que se L é elemento de $\mathcal{L}_R$, então

$$g(f(L)) = g(\{\pi(x) | x \in L\}) = L,$$

e analogamente temos que $f(g(J)) = J$ para qualquer J em $\mathcal{L}_{R/I}$, portanto f, g são inversas uma da outra, e daí segue que f é uma bijeção. Isso implica que os ideais à esquerda de R que contém I correspondem unicamente aos ideais à esquerda de R/I. ■

Note que na demonstração anterior, a função f corresponde precisamente com a função projeção aplicada no ideal L, e a função g corresponde à pré-imagem de π com respeito à algum ideal J do quociente. É importante observar que a correspondência em questão pode ser estendida para ideais maximais, isto é, cada ideal maximal à esquerda de R que contém I corresponde à algum ideal maximal à esquerda de R/I. Em particular, se R, S são anéis isomorfos, então o teorema anterior nos diz que os ideais à esquerda de R correspondem aos ideais à esquerda de S. No caso de ideais bilaterais, obtemos todo ideal bilateral de R/I é da forma J/I para algum J ideal bilateral em R que contém I, e reciprocamente J/I é ideal bilateral de R/I para qualquer J ideal bilateral de R que contém I.

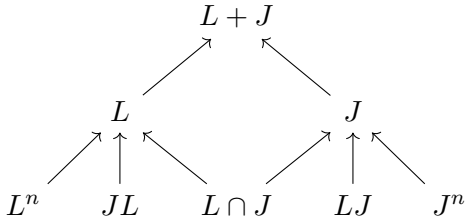
Existem algumas operações naturais que podem ser feitas com anéis e seus ideias. Dados ideais à esquerda L, J de R, podemos definir sua soma

$$L + J := \{a + b | a \in L, b \in J\} \subseteq R,$$

e note que a soma também é um ideal à esquerda, e se $\{L_i\}_{i \in \mathcal{I}}$ é uma família de ideais à esquerda indexada por um conjunto $\mathcal{I}$, denotamos por $\sum_{i \in \mathcal{I}} L_i$ o conjunto das somas finitas de elementos dos respectivos L_i. Também podemos definir o produto de ideais como

$$LJ := \{\sum_i a_i b_i | a_i \in L, b_i \in J\} \subseteq J,$$

onde todas as somas em questão são finitas, e nesse caso LJ é um ideal à esquerda de R. Portanto, para qualquer n natural, podemos definir o ideal à esquerda L^n como o produto de L consigo mesmo n vezes, ou seja, o conjunto de todas as possíveis somas finitas de produtos de n elementos de L. O diagrama a seguir ilustra as relações entre as diferentes operações que podemos fazer com ideais:



onde cada seta direcionada indica inclusão de conjuntos.

Também é possível estender a noção de produtos diretos de grupos para anéis.

Definição 1.2.5. Se $\{R_i\}_{i\in\mathcal{I}}$ é uma família arbitrária de anéis indexada por um conjunto $\mathcal{I}$, então definimos o *produto direto externo* como

$$\prod_{i\in\mathcal{I}} R_i := \{(a_i)_{i\in\mathcal{I}} | a_i \in R_i\},$$

com operações dadas por

$$(a_i)_{i\in\mathcal{I}} + (b_i)_{i\in\mathcal{I}} := (a_i + b_i)_{i\in\mathcal{I}},$$
$$(a_i)_{i\in\mathcal{I}}(b_i)_{i\in\mathcal{I}} := (a_i b_i)_{i\in\mathcal{I}},$$

para quaisquer sequências $(a_i)_{i\in\mathcal{I}}, (b_i)_{i\in\mathcal{I}}$ de $\prod_{i\in\mathcal{I}} M_i$. O elemento neutro aditivo do produto direto é dado por $(0_i)_{i\in\mathcal{I}}$, e o seu elemento unitário é dado por $(1_i)_{i\in\mathcal{I}}$.

Vale notar que as projeções canônicas que levam uma dada sequência do produto direto em seu i-ésimo elemento são epimorfismos de anéis, no entanto, as inclusões canônicas definidas para grupos não são. Isso segue do fato de que, por definição, um homomorfismo de anéis deve mapear a unidade do domínio na unidade do codomínio, e isso não é o caso para inclusões, pois elas levam a unidade 1_i de um anel R_i na sequência com 1_i na i-ésima posição e 0_j nas demais, e essa não é a unidade do produto direto. Por esse motivo que neste trabalhos não falamos de somas diretas de anéis, mesmo que em alguns contextos –particularmente quando está se tratando de anéis que não possuem unidade – tais objetos façam sentido.

Dado um anel $(R, +, \cdot)$, definimos o seu *anel oposto* $(R^{\mathrm{op}}, +, *)$ como o anel com a mesma operação de adição de R, mas onde para quaisquer elementos a, b em R, o produto é dado por

$$a * b := b \cdot a,$$

isto é, a multiplicação no anel oposto ocorre naturalmente no sentido oposto. A partir dessa definição, podemos demonstrar alguns fatos básicos sobre o anel oposto.

Proposição 1.2.6. Se R é um anel e R^{op} é seu anel oposto, então:

(1) $(R^{\mathrm{op}})^{\mathrm{op}}$ e R são anéis isomorfos;

(2) Se R é anel de divisão, então R^{op} também é;

(3) Se $\{R_i\}_{i\in\mathcal{I}}$ é uma família de anéis, então $(\prod_{i\in\mathcal{I}} R_i)^{\mathrm{op}}$ e $\prod_{i\in\mathcal{I}} R_i^{\mathrm{op}}$ são anéis isomorfos;

(4) Dado n natural, vale que $M_n(R)^{\mathrm{op}}$ e $M_n(R^{\mathrm{op}})$ são anéis isomorfos.

Demonstração.

(1) Basta notar que se $*_1$ e $*_2$ são as multiplicações em R^{op} e $(R^{\mathrm{op}})^{\mathrm{op}}$, respectivamente, então

$$a *_2 b = b *_1 a = ab,$$

logo a função identidade entre R e $(R^{\mathrm{op}})^{\mathrm{op}}$ será um isomorfismo de anéis.

(2) Se R é anel de divisão, sabemos que qualquer elemento a não-nulo é invertível, então existe b tal que $ab = 1 = ba$, logo $b * a = 1 = a * b$, e portanto a também é invertível em R^{op}.

(3) Assim como em (1), a função identidade será um isomorfismo de anéis. De fato, como o produto entre dois elementos de $\prod_{i\in\mathcal{I}} R_i$ é dado pela sequência dos produtos termo a termo de cada componente, teremos que o produto em seu anel oposto será dado pela sequência dos produtos termo a termo no anel oposto de cada componente.

(4) Considere o a aplicação de transposição

$$\varphi : M_n(R)^{\text{op}} \mapsto M_n(R^{\text{op}}),$$
$$\varphi(A) = A^T.$$

A função é claramente um isomorfismo de grupos abelianos, e também podemos notar que se A, B são elementos de $M_n(R)^{\text{op}}$, então

$$\varphi(A * B) = \varphi(BA) = (BA)^T = A^T B^T = \varphi(A)\varphi(B),$$

o que implica que os anéis são de fato isomorfos.

■

1.3 Módulos e Espaços Vetoriais

Vimos que anéis generalizam a noção de corpos, e de maneira semelhante agora estaremos interessados em estudar objetos que generalizam a noção de um espaço vetorial sobre um corpo.

Definição 1.3.1. Seja $(M, +)$ um grupo abeliano e R um anel. Dizemos que M é um R-módulo à esquerda se existe operação $\cdot : R \times M \mapsto M$ tal que para quaisquer elementos m_1, m_2 de M, e para quaisquer elementos α, β de R, vale que:

(1) $\alpha \cdot (m_1 + m_2) = \alpha \cdot m_1 + \alpha \cdot m_2$;

(2) $(\alpha + \beta) \cdot m_1 = \alpha \cdot m_1 + \beta \cdot m_1$;

(3) $\alpha\beta \cdot m_1 = \alpha \cdot (\beta \cdot m_1)$;

(4) $1 \cdot m_1 = m_1$.

Nesse caso, vale que $0m = 0 = \alpha 0$ e $(-1)m = -m$. Um R-módulo à direita é definido de forma análoga, e um R-módulo à esquerda e à direita é dito *bilateral*.

Os itens (1) e (2) nos dizem que $\cdot$ é compatível com as operações de soma do grupo abeliano M e do anel R, (3) nos diz que a operação é associativa com respeito ao produto do anel, e (4) simplesmente nos diz que a unidade de R também atua como unidade em M. O espaço euclidiano usual $\mathbb{R}^n$ é um $\mathbb{R}$-módulo bilateral, e também é um módulo à esquerda com respeito ao anel de matrizes $M_n(\mathbb{R})$. De modo geral, qualquer módulo sobre um anel comutativo é bilateral. Se G é um grupo abeliano qualquer, podemos tratá-lo como um $\mathbb{Z}$-módulo definindo a multiplicação de um elemento do grupo por um inteiro n simplesmente como a soma deste elemento com sigo mesmo n vezes, e caso n seja negativo, somamos o inverso aditivo do elemento. Qualquer anel R é um módulo bilateral sobre si mesmo, isto é, R é sempre um R-módulo bilateral.

Dado um subgrupo abeliano N de um R-módulo M, dizemos que ele é um *submódulo* se N também é um R-módulo com as mesmas operações de M. Um módulo M é dito *simples* – ou *minimal* – se seus únicos submódulos são M e $\{0\}$. Um submódulo próprio N de M é dito *maximal* se, dado qualquer outro submódulo N' tal que $N \subseteq N'$, então $N' = M$ ou $N' = N$.

Exemplo 1.3.2 (Simplicidade de $M_n(D)$)**.** Seja n um número natural e D um anel de divisão, e considere o anel $M_n(D)$. Note que se I é ideal bilateral, então podemos tomar uma matriz não nula A de I e multiplicá-la pela esquerda e pela direita por matrizes apropriadas da forma E_{xy}, isto é, com entrada xy igual a 1 e as demais iguais à zero, de modo a obter uma matriz com somente um elemento não-nulo. Daí podemos permutar as entradas desta nova matriz de modo a obter uma matriz diagonal com somente um elemento não-nulo, e como o anel é de divisão podemos obter uma matriz diagonal com somente uma entrada não-nula e igual a 1. Como todas as operações foram apenas multiplicações por matrizes em $M_n(D)$, mostramos que I contém todas as matrizes diagonais da forma E_{xx}, e portanto contém sua soma, isto é, contém a identidade de $M_n(D)$. Isso nos mostra que qualquer ideal próprio de $M_n(D)$ é trivial, ou seja, o anel em questão é simples.

A partir das definições dadas, segue que os R-submódulos de R são precisamente seus ideais à esquerda. Assim sendo, todo ideal minimal à esquerda de R é um R-submódulo simples de R, e reciprocamente qualquer R-submódulo simples de R é um ideal minimal à esquerda. Módulos simples são objetos de alto interesse para o estudo de álgebra não-comutativa, pois em muitos casos podemos escrever um módulo como uma composição de seus submódulos simples, mais precisamente, como uma soma direta, e ao longo dos próximos capítulos estaremos interessados em determinar quando tal decomposição é possível.

Agora iremos considerar funções φ entre R-módulos M, N que preservam a sua estrutura, isto é, homomorfismos de grupos aditivos onde

$$\varphi(\alpha m) = \alpha\varphi(m),$$

para quaisquer elementos α de R e m de M. Essas funções são chamadas de R-homomorfismos à esquerda, e o conjunto de todas as funções deste tipo será denotado por $\mathrm{Hom}_R(M, N)$. Note que tal conjunto sempre é um grupo abeliano com adição de funções e elemento neutro aditivo dado pela função identicamente nula, mas é um R-módulo somente quando R é comutativo, e o conjunto $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ é um anel com as operações de adição e composição de funções.

Dado um R-módulo M e um R-submódulo N, podemos também considerar o módulo quociente M/N, e deixamos ao leitor conferir que este novo conjunto é de fato um R-módulo, e nesse caso também podemos observar que a projeção canônica que leva um elemento m em sua classe lateral no quociente será um epimorfismo de módulos. Se R é um anel e L é um ideal à esquerda, podemos então considerar o R-módulo quociente R/L, pois L também é R-submódulo de R, mas vale lembrar que tal módulo será um anel se, e somente se, L for bilateral. Como ideais não são subanéis, iremos compará-los por meio homomorfismos de módulos, isto é, dois ideais de um anel são isomorfos se existe algum isomorfismo de módulos entre eles. Se M, N são isomorfos como R-módulos à esquerda, iremos indicar isto pela notação $M \cong_R N$. Disso, seguem versões análogas dos Teoremas 1.2.3 e 1.2.4 para R-módulos.

Teorema 1.3.3 (Primeiro Teorema do Isomorfismo para Módulos)**.** Sejam M, N módulos sobre um anel R, e seja φ em $\mathrm{Hom}_R(M, N)$ um homomorfismo entre eles. Então $\ker(\varphi)$ é submódulo de M, $\mathrm{Im}(\varphi)$ é submódulo de N, e

$$M/\ker(\varphi) \cong_R \mathrm{Im}(\varphi).$$

■

Teorema 1.3.4 (Teorema da Correspondência para Módulos)**.** Seja M um módulo sobre um anel R e N um submódulo de M. Então existe uma bijeção entre os R-submódulos de M que contém N e os R-submódulos à esquerda de M/N. Em particular, cada R-submódulo de M/N é da forma N'/N, para algum submódulo N' de M que contém N, e N'/N é submódulo de M/N para qualquer submódulo N' de M. ■

É importante ressaltar que a correspondência anterior também vale para submódulos maximais de M: se N' é submódulo maximal de M que contém N, então N'/N é submódulo maximal de M/N, e vice-versa. Também é possível mostrar que se M, N são módulos isomorfos, então tal isomorfismo induz um isomorfismo de anéis entre $\mathrm{End}_R(M)$ e $\mathrm{End}_R(N)$.

Proposição 1.3.5. Se M e N são R-módulos isomorfos, então os anéis $\mathrm{End}_R(M)$ e $\mathrm{End}_R(N)$ são isomorfos.

Demonstração. Seja φ um R-isomorfismo entre M e N, e defina:

$$\begin{aligned} \psi : \mathrm{End}_R(M) &\mapsto \mathrm{End}_R(N), \\ \psi(f) &= \varphi \circ f \circ \varphi^{-1}. \end{aligned}$$

Note que $\psi(\mathrm{id}_M) = \mathrm{id}_N$ – onde id é a função identidade no respectivo módulo –, $\psi(f + g) = \psi(f) + \psi(g)$, e que

$$\begin{aligned} \psi(f \circ g) &= \varphi \circ f \circ g \circ \varphi^{-1} \\ &= (\varphi \circ f \circ \varphi^{-1})(\varphi \circ g \circ \varphi^{-1}) \\ &= \psi(f) \circ \psi(g), \end{aligned}$$

logo ψ é homomorfismo de anéis. Se $\psi(f) = 0$, isso implica que para qualquer elemento n de N

$$(\varphi \circ f \circ \varphi^{-1})(n) = 0,$$

mas sendo φ bijeção, temos que para qualquer elemento m de M

$$(\varphi \circ f)(m) = 0,$$

e novamente usando o fato de φ ser bijeção, obtemos que f é identicamente nula, logo ψ é injetiva. Se g é um elemento de $\mathrm{End}_R(N)$, podemos definir a função $\tilde{g} = \varphi^{-1} \circ g \circ \varphi$ e notar que ela é claramente um R-endomorfismo de M, e que $\psi(\tilde{g}) = g$. As duas observações anteriores nos garantem que ψ é de fato isomorfismo de anéis, como queríamos. ■

Dado um subconjunto S de um R-módulo M, definimos o submódulo gerado por S como o conjunto das somas finitas da forma

$$\langle S \rangle_R := \{\sum_j \alpha_{i_j} m_{i_j} | \alpha_{i_j} \in R, m_{i_j} \in S\} \subseteq M,$$

e note que se S é subconjunto de R, então $\langle S \rangle_R$ é o ideal à esquerda gerado por S em R. Se S gera M, ele é dito *conjunto gerador*, e caso seja finito dizemos que M é *finitamente gerado*. Se S possui somente um elemento m, M é dito *cíclico*, e é usualmente denotado por $M = Rm$.

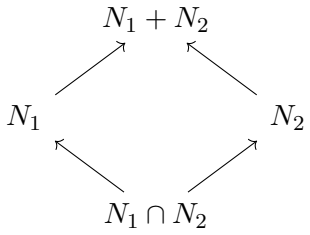
Dado um R-módulo M e R-submódulos N_1, N_2, podemos definir a sua soma

$$N_1 + N_2 := \{m + m' | m \in N_1, m' \in N_2\} \subseteq M,$$

que também é um R-submódulo, e caso $\{M_i\}_{i \in \mathcal{I}}$ seja uma família de submódulos de M indexada por um conjunto $\mathcal{I}$, podemos considerar a sua soma $\sum_{i \in \mathcal{I}} M_i$ como o conjunto de todas as somas finitas de elementos de M_i, que também será um R-submódulo. Se L é ideal à esquerda de R, podemos definir o submódulo

$$LM := \{\sum_i a_i m_i | a_i \in L, m_i \in M\} \subseteq M,$$

onde as somas em questão são finitas. Novamente, podemos ilustrar a relação entre esses conjuntos por meio de um diagrama:



onde as setas indicam inclusão de conjuntos.

Também é possível estender a noção de produtos diretos de grupos para produtos de R-módulos.

Definição 1.3.6. Se $\{M_i\}_{i \in \mathcal{I}}$ é uma família de R-módulos indexada por um conjunto $\mathcal{I}$, então definimos o *produto direto externo*

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

com operações dadas por

$$(m_i)_{i \in \mathcal{I}} + (n_i)_{i \in \mathcal{I}} := (m_i + n_i)_{i \in \mathcal{I}},$$
$$\alpha(m_i)_{i \in \mathcal{I}} := (\alpha m_i)_{i \in \mathcal{I}},$$

para quaisquer sequências $(m_i)_{i \in \mathcal{I}}, (n_i)_{i \in \mathcal{I}}$ de $\prod_{i \in \mathcal{I}} M_i$ e qualquer α de R. Tal conjunto é um R-módulo, e nesse caso note que as projeções e inclusões canônicas serão de fato homomorfismos de R-módulos.

No caso de módulos, podemos definir a sua *soma direta externa* de maneira similar a como fizemos para grupos abelianos: basta considerar o subconjunto do produto direto externo formado pelas sequências quase-nulas com as mesmas operações do produto direto. Esse conjunto será um R-módulo, e é denotado por $\bigoplus_{i\in\mathcal{I}} M_i$. Se n é número natural e M é R-módulo, denotamos por $M^{(n)}$ a soma direta externa de M consigo mesmo n vezes.

É possível encontrar um critério extremamente útil para identificar somas de submódulos com somas diretas externas.

Proposição 1.3.7. Se M é um R-módulo e $\{M_i\}_{i\in\mathcal{I}}$ é uma família de submódulos, as seguintes são equivalentes:

(1) $M = \sum_{i\in\mathcal{I}} M_i$ e $M_j \cap (\sum_{i\neq j} M_i) = \{0\}$ para qualquer j em $\mathcal{I}$;

(2) Todo elemento m de M pode ser escrito unicamente como soma finita $\sum_j m_{i_j}$, onde cada m_{i_j} é elemento do respectivo M_{i_j};

(3) $M \cong_R \bigoplus_{i\in\mathcal{I}} M_i$.

Demonstração.

(1) $\Rightarrow$ (2) Seja m elemento de M, e caso ele possa ser escrito de duas formas como soma finita de elementos dos ideais em questão, podemos assumir que

$$m = \sum_j m_{i_j} = \sum_j m'_{i_j},$$

pois basta tomar $m'_{i_j} = 0$ ou $m_{i_j} = 0$ se necessário para fazer com que o conjunto de índices seja igual. Daí, caso $\sum_j (m_{i_j} - m'_{i_j}) = 0$, segue que:

$$(m'_{i_j} - m_{i_j}) = \sum_{l\neq j} (m_{i_l} - m'_{i_l}) \in M_{i_j} \cap (\sum_{l\neq j} M_l),$$

logo por hipótese vale que $m_{i_j} = m'_{i_j}$, e se repetirmos o mesmo argumento para todos os índices i_j concluímos que a expressão para m é de fato única.

(2) $\Rightarrow$ (3) Caso cada elemento de M possa ser escrito unicamente como uma soma finita de elementos nos submódulos da família em questão, basta considerar o mapa que leva um elemento $m = \sum_j m_{i_j}$ na sequência com entradas m_{i_j} nos respectivos índices, e zero nos demais. É imediato verificar que tal mapa é de fato um isomorfismo de R-módulos, e portanto segue o resultado.

(3) $\Rightarrow$ (1) Basta notar que se m é um elemento de M e é identificado com a sequência quase-nula $(m_i)_{i\in\mathcal{I}}$ pelo isomorfismo de módulos, o elemento $\sum_{i\in\mathcal{I}} m_i$ que é finito também é identificado com essa mesma sequência, portanto $M = \sum_{i\in\mathcal{I}} M_i$. Além disso, se existe um elemento m_j de M_j tal que

$$m_j = \sum_{i\neq j} m_i \in M_j \cap (\sum_{i\neq j} M_i),$$

então m_j é identificado pelo isomorfismo com a sequência com apenas uma entrada não-nula igual à m_j, e a sequência identificada com $\sum_{i\neq j} m_i$ possui entrada relativa à j igual a zero, mas por hipótese ambas devem ser iguais, logo $m_j = 0$, como queríamos. ■

Este resultado nos mostra que caso cada elemento de M seja unicamente escrito como soma finita de elementos da família de submódulos, podemos naturalmente identificar M como uma soma direta externa de R-módulos. Nesse caso, escrevemos[2]

$$M = \bigoplus_{i\in\mathcal{I}} M_i,$$

[2]Iremos abusar da notação utilizar o mesmo símbolo para denotar somas diretas internas e externas de módulos, e quando for necessário iremos deixar explícito sobre qual soma estamos nos referindo.

e tal decomposição é chamada de *soma direta interna*, ou somente soma direta. No caso de módulos, a soma direta externa e interna são isomorfas, portanto podemos identificar elementos de uma soma direta de submódulos tanto como sequências quase-nulas quanto como somas finitas. Podemos também observar que se L é um ideal à esquerda de R e $M = \bigoplus_{i\in\mathcal{I}} M_i$, então $LM = \bigoplus_{i\in\mathcal{I}} LM_i$, pois certamente $LM = \sum_{i\in\mathcal{I}} LM_i$, e cada $LM_i \subseteq M_i$, logo $LM_i \cap (\sum_{j\neq i} LM_j) = \{0\}$.

Se R é um anel, então seus ideias à esquerda são precisamente seus submódulos, logo se R pode ser escrito como soma de submódulos

$$R = \sum_{i\in\mathcal{I}} L_i,$$

onde cada L_i é ideal à esquerda, e se vale que qualquer elemento em R pode ser escrito unicamente como soma finita de elementos em alguns dos ideais à esquerda L_i, podemos escrever

$$R = \bigoplus_{i\in\mathcal{I}} L_i$$

como soma direta de submódulos, e essa soma pode ser naturalmente identificada com a soma direta externa dos R-módulos L_i.

O seguinte resultado relaciona homomorfismos entre módulos expressos como somas e produtos diretos, e será de grande interesse para demonstrações futuras.

Proposição 1.3.8. Seja R anel, $\{M_i\}_{i\in\mathcal{I}}$ uma família de R-módulos indexada pelo conjunto $\mathcal{I}$, e N um R-módulo. Então valem os seguintes isomorfismos de grupos abelianos:

$$\mathrm{Hom}_R(\bigoplus_{i\in\mathcal{I}} M_i, N) \cong \prod_{i\in\mathcal{I}} \mathrm{Hom}_R(M_i, N);$$
$$\mathrm{Hom}_R(N, \prod_{i\in\mathcal{I}} M_i) \cong \prod_{i\in\mathcal{I}} \mathrm{Hom}_R(N, M_i).$$

Em particular

$$\mathrm{End}_R(\bigoplus_{i\in\mathcal{I}} M_i) \cong \prod_{i,j\in\mathcal{I}} \mathrm{Hom}_R(M_i, M_j)$$

é um isomorfismo de grupos abelianos, e caso $\mathrm{Hom}_R(M_i, M_j) = \{0\}$ se $i \neq j$, obtemos que

$$\mathrm{End}_R(\bigoplus_{i\in\mathcal{I}} M_i) \cong \prod_{i\in\mathcal{I}} \mathrm{End}_R(M_i)$$

é um isomorfismo de anéis, onde o lado direito é um produto direto de anéis.

Demonstração. Para vermos o primeiro isomorfismo, seja f um R-homomorfismo entre $\bigoplus_{i\in\mathcal{I}} M_i$ e N, e considere o seguinte mapa

$$\varphi : \mathrm{Hom}_R(\bigoplus_{i\in\mathcal{I}} M_i, N) \mapsto \prod_{i\in\mathcal{I}} \mathrm{Hom}_R(M_i, N),$$
$$\varphi(f) = (f \circ \iota_i)_{i\in\mathcal{I}},$$

onde ι_i denota a inclusão canônica que mapeia um elemento m_i de M_i para a sequência com apenas a i-ésima entrada não-nula igual à m_i – note que $f \circ \iota_i$ pode ser visto como a restrição de f em M_i, ou seja, φ simplesmente manda f na sequência de suas restrições nas respectivas componentes da soma direta. Dessa definição, segue que φ é homomorfismo de grupos abelianos, e portanto resta checar que ele é bijetivo. Se $\varphi(f) = 0$, significa que para qualquer i em $\mathcal{I}$, e para qualquer m_i em M_i, vale que

$$(f \circ \iota_i)(m_i) = 0.$$

Por outro lado, se $(m_i)_{i\in\mathcal{I}}$ é elemento de $\bigoplus_{i\in\mathcal{I}} M_i$, podemos escrevê-lo como

$$(m_i)_{i\in\mathcal{I}} = \sum_{i\in\mathcal{I}} \iota_i(m_i),$$

onde a soma do lado direito é finita pois a sequência é quase-nula, portanto

$$\begin{aligned} f((m_i)_{i\in\mathcal{I}}) &= f(\sum_{i\in\mathcal{I}} \iota_i(m_i)) \\ &= \sum_{i\in\mathcal{I}} (f\circ\iota_i)(m_i) = 0, \end{aligned}$$

logo f é identicamente nula, e então φ é injetiva. Agora se $(f_i)_{i\in\mathcal{I}}$ é elemento de $\prod_{i\in\mathcal{I}} \mathrm{Hom}_R(M_i, N)$, podemos definir um R-homomorfismo f tal que

$$f((m_i)_{i\in\mathcal{I}}) = \sum_{i\in\mathcal{I}} f_i(m_i) \in N,$$

para qualquer sequência $(m_i)_{i\in\mathcal{I}}$ em $\bigoplus_{i\in\mathcal{I}} M_i$, e como cada sequência é quase-nula a soma do lado direito da equação é finita. Disso, podemos observar que $(f\circ\iota_i)(m_i) = f_i(m_i)$, logo $\varphi(f) = (f_i)_{i\in\mathcal{I}}$, e então φ é sobrejetiva.

Para vermos o segundo isomorfismo, seja $f \in \mathrm{Hom}_R(N, \prod_{i\in\mathcal{I}} M_i)$, e defina

$$\begin{aligned} \psi : \mathrm{Hom}_R(N, \prod_{i\in\mathcal{I}} M_i) &\mapsto \prod_{i\in\mathcal{I}} \mathrm{Hom}_R(N, M_i), \\ \psi(f) &= (\pi_i \circ f)_{i\in\mathcal{I}}, \end{aligned}$$

onde π_i denota a projeção canônica do produto direto em seu i-ésimo componente – note então que ψ nada mais é que o mapa que manda f na sequência das suas projeções nos respectivos componentes do produto direto. Novamente, a definição deixa claro que ψ é um homomorfismo de grupos abelianos, logo devemos checar se é uma bijeção. Se $\psi(f) = 0$, significa que para todo $i \in \mathcal{I}$ e para todo $n \in N$, vale que

$$(\pi_i \circ f)(n) = 0,$$

mas por outro lado, podemos escrever

$$f(n) = ((\pi_i \circ f)(n))_{i\in\mathcal{I}},$$

logo f é identicamente nula, e então ψ é injetiva. Agora se $(f_i)_{i\in\mathcal{I}}$ é elemento de $\prod_{i\in\mathcal{I}} \mathrm{Hom}_R(N, M_i)$, defina o R-homomorfismo f dado por

$$f(n) = (f_i(n))_{i\in\mathcal{I}} \in \prod_{i\in\mathcal{I}} M_i,$$

e então segue que $\pi_i \circ f = f_i$, logo

$$\psi(f) = ((\pi_i \circ f))_{i\in\mathcal{I}} = (f_i)_{i\in\mathcal{I}},$$

o que nos permite concluir que ψ é sobrejetiva.

O terceiro isomorfismo enunciado pode ser obtido notando que, a partir das considerações anteriores, temos

$$\mathrm{Hom}_R(\bigoplus_{i\in\mathcal{I}} M_i, \bigoplus_{i\in\mathcal{I}} M_i) \overset{\varphi}{\cong} \prod_{i\in\mathcal{I}} \mathrm{Hom}_R(M_i, \bigoplus_{i\in\mathcal{I}} M_i) \overset{\psi}{\cong} \prod_{i,j\in\mathcal{I}} \mathrm{Hom}_R(M_i, M_j),$$

onde os elementos de $\prod_{i,j\in\mathcal{I}} \mathrm{Hom}_R(M_i, M_j)$ são da forma

$$(\pi_j \circ f \circ \iota_i)_{i,j\in\mathcal{I}} = ((\pi_j \circ f \circ \iota_i)_{i\in\mathcal{I}})_{j\in\mathcal{I}},$$

pois a composição de isomorfismos de grupos aditivos compatíveis é um isomorfismo, logo $\rho = \psi \circ \phi$ é o isomorfismo desejado entre $\mathrm{End}_R(\bigoplus_{i\in\mathcal{I}} M_i)$ e $\prod_{i,j\in\mathcal{I}} \mathrm{Hom}_R(M_i, M_j)$. Agora note que se $\mathrm{Hom}_R(M_i, M_j) = \{0\}$ quando $i \neq j$, então vale que

$$(\pi_j \circ f \circ \iota_i)_{i,j\in\mathcal{I}} = (\pi_i \circ f \circ \iota_i)_{i\in\mathcal{I}},$$

pois $\pi_j \circ f \circ \iota_i = 0$ se $i \neq j$, logo $\prod_{i,j\in\mathcal{I}} \mathrm{Hom}_R(M_i, M_j) = \prod_{i\in\mathcal{I}} \mathrm{End}_R(M_i)$, e disso segue que

$$\mathrm{End}_R(\bigoplus_{i\in\mathcal{I}} M_i) \overset{\rho}{\cong} \prod_{i\in\mathcal{I}} \mathrm{End}_R(M_i),$$

onde $\rho(f) = (\pi_i \circ f \circ \iota_i)_{i\in\mathcal{I}}$, e os isomorfismos são de grupos aditivos, portanto para provarmos a última afirmativa basta verificar que também são homomorfismos de anéis. O elemento unitário em $\mathrm{End}_R(\bigoplus_{i\in\mathcal{I}} M_i)$ é a função identidade id, logo

$$\rho(\mathrm{id}) = (\pi_i \circ \mathrm{id} \circ \iota_i)_{i\in\mathcal{I}} = (\mathrm{id}_i)_{i\in\mathcal{I}},$$

pois $\pi_i \circ \iota_i = \mathrm{id}_i$ – onde id_i é a identidade em M_i –, logo a imagem da unidade do domínio é a unidade do codomínio. Se f, g são endomorfismos do domínio, então

$$\begin{aligned}
\rho(f \circ g) &= (\pi_i \circ f \circ \iota_i)_{i\in\mathcal{I}} \\
&= (\pi_i \circ f \circ \iota_i \circ \pi_i \circ g \circ \iota_i)_{i\in\mathcal{I}} \\
&= ((\pi_i \circ f \circ \iota_i) \circ (\pi_i \circ g \circ \iota_i))_{i\in\mathcal{I}} \\
&= \rho(f) \circ \rho(g),
\end{aligned}$$

portanto o isomorfismo é de fato de anéis, como queríamos. ■

O resultado anterior possui diversas implicações interessantes. Note que se o domínio de um R-homomorfismo f é uma soma direta de módulos, então f é unicamente determinado pelas restrições $(f \circ \iota_i)_{i\in\mathcal{I}}$ de f nas componentes do domínio. Analogamente, se seu codomínio é um produto direto de módulos, então f é determinado unicamente pelas funções $(\pi_i \circ f)_{i\in\mathcal{I}}$, e se ambos domínio e codomínio são somas diretas, segue que os elementos da forma $(\pi_i \circ f \circ \iota_j)_{i,j}$ determinam f unicamente, e no caso de somas diretas finitas, o isomorfismo nos permite identificar f unicamente com uma matriz com entrada ij dada por $(\pi_i \circ f \circ \iota_j)_{i,j}$. Também vale observar que se R é um anel comutativo, então os isomorfimos acima também serão isomorfismos de R-módulos.

O anel de R-endomorfimos de um anel R também se relaciona diretamente com o seu anel oposto.

Proposição 1.3.9. Os anéis $\mathrm{End}_R(R)$ e R^{op} são isomorfos.

Demonstração. Defina o seguinte homomorfismo de grupos abelianos:

$$\begin{aligned}
&\varphi : R^{\mathrm{op}} \mapsto \mathrm{End}_R(R); \\
&\varphi(a)(b) = b \cdot a.
\end{aligned}$$

Note que $\varphi(a * b) = \varphi(b \cdot a)$, logo para qualquer x em R temos que

$$\varphi(b \cdot a)(x) = x \cdot b \cdot a = \varphi(a) \circ \varphi(b)(x),$$

e também que $\varphi(1)$ é a função identidade em $\mathrm{End}_R(R)$, portanto o homomorfismo é de anéis. Se $\varphi(a) = 0$, temos que para qualquer b elemento de R vale que $b \cdot a = 0$, e como 1 também é elemento de R, isso implica que $a = 0$, e dado qualquer R-endomorfismo f de R, vale que para todo x em R

$$f(x) = f(x \cdot 1) = x \cdot f(1) = \varphi(f(1))(x),$$

implicando que φ é isomorfismo de anéis. ■

Agora iremos demonstrar um dos resultados mais importantes sobre de R-módulos simples.

Lema 1.3.10 (Lema de Schur)**.** Sejam M, N R-módulos simples não-nulos, e seja $\varphi : M \mapsto N$ um R-homomorfismo. Então φ ou é identicamente nulo ou é um isomorfismo. Em particular, o anel $\mathrm{End}_R(M)$ é um anel de divisão.

Demonstração. Sabemos que os conjuntos $\ker(\varphi), \mathrm{Im}(\varphi)$ são submódulos de M, N, respectivamente. Sendo M, N simples, segue que $\ker(\varphi) = \{0\}$ ou $\ker(\varphi) = M$, e que $\mathrm{Im}(\varphi) = \{0\}$ ou $\mathrm{Im}(\varphi) = N$. Se $\ker(\varphi) = \{0\}$, vale pelo Teorema 1.3.3 que $M \cong_R \mathrm{Im}(\varphi)$, e portanto $M \cong_R N$, pois M e N são não-nulos. Do contrario, segue que φ e identicamente nula.

Agora se tomarmos o conjunto $\mathrm{End}_R(M)$, sabemos que ele é de fato um anel com as operações de soma e composição de funções e com unidade dada pela função identidade, logo basta mostrar que todo elemento não-nulo é invertível. Dado elemento f qualquer do anel de endomorfismos, e sendo endo M simples, existem duas opções: $\ker(f) = \{0\}$, e nesse caso pelo mesmo argumento feito anteriormente segue que $\mathrm{Im}(f) = M$, ou $\ker(f) = M$ e nesse caso segue que $f = 0$. Logo, se f não é identicamente nulo então ele é bijeção, sendo portanto invertível, e então $\mathrm{End}_R(M)$ é anel de divisão. ■

O Lema de Schur também nos permite caracterizar módulos simples sobre um anel qualquer.

Teorema 1.3.11. Seja M um módulo sobre um anel R. As seguintes são equivalentes:

(1) M é simples;

(2) M é cíclico, e todo elemento não-nulo de M é um gerador;

(3) M é isomorfo como R-módulo à R/I, onde I é um ideal maximal à esquerda de R.

Demonstração.

(1)⇒(2) Assuma M simples, e note que dado qualquer elemento m de M não-nulo, Rm é R-submódulo que contém pelo menos 0 e m, logo $Rm \neq \{0\}$, e então por simplicidade segue que $Rm = M$.

(2)⇒(3) Assuma que M é cíclico e que todo elemento não nulo é gerador. Novamente considere um elemento não-nulo m de M, e defina

$$\varphi : R \mapsto M,$$
$$\varphi(r) = rm,$$

e note que tal função é claramente um R-epimorfismo, logo do Teorema 1.3.3 vale que

$$R/\ker(\varphi) \cong_R M.$$

Agora note que dados r_1, r_2 elementos de $\ker(\varphi)$,

$$\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2) = 0,$$

logo $r_1 - r_2$ está em $\ker(\varphi)$, e também vale que dado r de R qualquer,

$$\varphi(rr_1) = rr_1m = r(r_1m) = 0,$$

portanto rr_1 pertence a $\ker(\varphi)$, e então $\ker(\varphi)$ é ideal à esquerda de R. Se J é ideal à esquerda de R tal que $\ker(\varphi) \subsetneq J$, então existe r em $J \setminus \ker(\varphi)$, logo $\varphi(r) = rm \neq 0$ e por simplicidade teríamos que $M = R(rm)$. Mas então a restrição $\varphi|_J = \varphi \circ \iota$, onde ι é a inclusão de J em R, é sobrejetiva, e portanto

$$J/\ker(\varphi) \cong_R M \cong_R R/\ker(\varphi),$$

logo $J = R$, implicando que $\ker(\varphi)$ é ideal à esquerda maximal.

(3)⇒(1) Assuma que M é isomorfo à R/I, onde I é ideal maximal à esquerda de R. Se N é R-submódulo de M, então o isomorfismo em questão nos dá que N é isomorfo à algum submódulo de R/I, logo pelo Teorema 1.3.4 existe algum R-submódulo J de R que contém I tal que

$$N \cong_R J/I.$$

Por outro lado, sendo R anel, sabemos que seus R-submódulos são precisamente os seus ideais à esquerda, então J é um ideal à esquerda que contém o ideal maximal à esquerda I, implicando que $J = R$ ou $J = I$. Em ambos os casos, isso significa que N é R-isomorfo à R/I ou à $\{0\}$, e portanto pela arbitrariedade de N segue que M é módulo simples. ■

O resultado anterior nos permite identificar ideais maximais à esquerda de um anel R com os possíveis R-módulos simples. Em particular, como todo R-submódulo simples é um ideal minimal à esquerda de R, temos que cada ideal minimal à esquerda é isomorfo como R-módulo ao quociente de R por algum ideal maximal à esquerda. No entanto, não é verdade que um R-módulo simples qualquer (não necessariamente incluso em R) seja isomorfo à algum ideal minimal de R, simplesmente devido ao fato de que nem todos anéis possuem ideais minimais à esquerda, mas todos possuem ideais maximais à esquerda. Um exemplo disso é o anel $\mathbb{Z}$, que não possui ideais minimais pois seus ideais são da forma $n\mathbb{Z}$ para algum n inteiro, mas existem $\mathbb{Z}$-módulos simples, e.g., $\mathbb{Z}_p$ com p primo é simples pois é isomorfo à $\mathbb{Z}/p\mathbb{Z}$, e $p\mathbb{Z}$ é ideal maximal.

Agora podemos descrever de maneira mais detalhada os ideais minimais à esquerda de um anel.

Lema 1.3.12 (Lema de Brauer)**.** Seja L um ideal minimal à esquerda de um anel R. Então $L^2 = \{0\}$ ou existe elemento idempotente $e \in L$ tal que $L = Re$.

Demonstração. Assuma que $L^2 \neq \{0\}$, portanto existe elemento não-nulo a em L tal que $La \neq \{0\}$. No entanto, note que La é ideal à esquerda não-trivial de L, então por minimalidade segue que $La = L$, logo existe e em L tal que $ea = a$. Agora considere o conjunto

$$J = \{x \in L | xa = 0\}.$$

Note que $e \notin J$, e que J é ideal à esquerda de L, logo $J = \{0\}$, mas note também que $e^2 - e \in J$, então $e^2 - e = 0$, e portanto e é idempotente. Como L também é R-módulo à esquerda – e então é um R-módulo simples – segue do Teorema 1.3.11 que $L = Re$. ■

É importante ressaltar que o ideal Re, com e elemento idempotente, não é necessariamente um anel pois e não necessariamente é unitário. O elemento e certamente é uma unidade à direita, mas nada nos garante a princípio que $eRe = Re$, e isso de fato não será o caso para muitos dos exemplos neste trabalho. Os resultados anteriores nos permitem concluir fatos importantes sobre o anel de matrizes com entradas em algum anel de divisão.

Exemplo 1.3.13 (Semissimplicidade de $M_n(D)$)**.** Considere o anel de matrizes $M_n(D)$ com entradas em um anel de divisão D e com $n > 1$, e note que podemos escrever tal anel como

$$M_n(D) = C_1 \oplus ... \oplus C_n,$$

onde cada C_i é um submódulo das matrizes com i-ésima coluna não-nula dado por

$$C_i = \{ \begin{pmatrix} 0 & ... & a_{1i} & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & ... & a_{ni} & ... & 0 \end{pmatrix} | a_{1i}, ..., a_{ni} \in D \}.$$

Já vimos que os conjuntos C_i são de fato ideais à esquerda de $M_n(D)$, cada um naturalmente isomorfo à $D^{(n)}$ como $M_n(D)$-módulo, no entanto também podemos observar que tais ideais são minimais. De fato, tome um ideal à esquerda L contido em um C_i qualquer, e assuma que existe elemento y não-nulo em L, ou seja, existe índice j tal que a entrada $y_{ji} \neq 0$ na matriz y. Agora tome um elemento $x \in C_i$ qualquer, e note que a matriz

$$M = \begin{pmatrix} 0 & ... & x_{1i}y_{ji}^{-1} & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & ... & x_{ni}y_{ji}^{-1} & ... & 0 \end{pmatrix}$$

é tal que $My = x$, e sendo L ideal à esquerda segue que $My \in L$, logo $x \in L$, o que implica que $C_i = L$, e então C_i é ideal minimal à esquerda. Isso nos permite concluir que o conjunto de matrizes pode ser escrito como soma direta de ideais minimais à esquerda, algo que futuramente iremos definir como semissimplicidade. Como $C_i^2 \neq \{0\}$, o Lema de Brauer nos garante que tais ideais serão da forma $M_n(D)E$, onde E é alguma matriz idempotente, e no caso basta tomar para um C_i qualquer a matriz E_{ii}, que certamente é idempotente e pertence à C_i, logo de fato temos que

$$M_n(D) = M_n(D)E_{11} \oplus ... \oplus M_n(D)E_{nn}.$$

O exemplo anterior também ilustra um fato interessante: um anel R ser simples não necessariamente implica que ele é simples como um R-módulo. De fato, vimos anteriormente que $M_n(D)$ é um anel simples, mas o exemplo anterior nos mostra que, quando visto como um módulo sobre si mesmo, esse anel não é simples para os casos onde $n > 1$, pois pode ser escrito como soma direta de n submódulos simples distintos. A decomposição deste exemplo é relativamente fácil, no entanto ela captura a motivação principal por trás dos resultados dos próximos capítulos: descrever anéis como uma soma direta de objetos simples de maneira explícita. No caso anterior, a descrição foi em termos de elementos idempotentes que também são hermitianos, i.e., são matrizes de projeção ortogonal, e iremos ver em seções futuras que isso não é uma coincidência. Também é possível caracterizar todos os submódulos simples do anel de matrizes, algo que será particularmente útil para aplicações do Teorema de Wedderburn.

Exemplo 1.3.14 (Unicidade dos submódulos simples de $M_n(D)$)**.** Seja $R = M_n(D)$ o anel de matrizes sobre um anel de divisão D, e considere um R-módulo simples M. Pelo Teorema 1.3.11, segue que $M = RX$, onde X é uma matriz não-nula de M, e como $RX \neq 0$, certamente existe alguma matriz A de R não-nula tal que $AX \neq 0$. Fixe uma coluna j de A com alguma entrada não-nula, e considere o mapa φ entre M e $D^{(n)}$ que leva um elemento BX de M na j-ésima coluna de B, isto é, $\varphi(BX) = Be_j$, onde e_j é o vetor com um na j-ésima entrada e zero nas demais. Disso segue que esse mapa é um R-homomorfismo não-nulo, e do exemplo anterior vimos que $D^{(n)}$ é um R-módulo simples, portanto pelo Lema de Schur segue que φ deve ser um R-isomorfismo, logo $M \cong_R D^{(n)}$. Isso nos mostra que, a menos de isomorfismo, $D^{(n)}$ é o único $M_n(D)$-módulo simples.

Dado um R-módulo M e um conjunto $S \subseteq M$, dizemos que S é *linearmente independente* se $\sum_{i_j} \alpha_{i_j} m_{i_j} = 0$ implica que $\alpha_{i_j} = 0$ para todo i, j, onde $\alpha_{i_j} \in R, m_{i_j} \in S$, ou seja, toda combinação linear finita de elementos de S que resulta no elemento nulo deve ter todos coeficientes nulos. Um conjunto S é dito *linearmente dependente* se ele não é linearmente independente, ou seja, existe combinação linear finita que resulta no elemento nulo onde nem todos os coeficientes são nulos. Um conjunto gerador linearmente independente é dito *base* do R-módulo. Se $\mathbb{F}$ é um corpo, dizemos que qualquer módulo sobre $\mathbb{F}$ é um $\mathbb{F}$-*espaço vetorial*. Espaços vetoriais são os objetos de estudo de álgebra linear, e eles satisfazem uma série de propriedades básicas que, em geral, não são satisfeitas por R-módulos quaisquer.

Iremos agora enunciar sem prova um importante resultado para as seções futuras. Para isso, relembramos o leitor que dado um conjunto munido de uma relação binária entre seus elementos, dizemos que ele é um conjunto parcialmente ordenado – também dito *poset* – se a relação é reflexiva, antissimétrica e transitiva, e dizemos que um subconjunto é uma cadeia se ele é totalmente ordenado, ou seja, qualquer par de elementos é comparável.

Lema 1.3.15 (Lema de Zorn)**.** Seja $(X, \leq)$ um poset onde toda cadeia $C \subseteq X$ possui limitante superior em X, isto é, um elemento x em X tal que para todo y em C valha que $y \leq x$. Então X possui um elemento maximal.

O Lema de Zorn é uma ferramenta extremamente poderosa para demonstrar diversos resultados em álgebra linear, e ele será especialmente útil para demonstrar propriedades básicas de módulos e anéis semissimples. Abaixo fornecemos um exemplo de uso do Lema de Zorn para demonstrar que todo ideal em um anel está contido em algum ideal maximal.

Exemplo 1.3.16 (Existência de ideais maximais)**.** Seja R um anel, e fixe um ideal à esquerda L. Defina o conjunto

$$\mathcal{F} = \{J \subseteq R | L \subseteq J,\ J \text{ é ideal à esquerda de } R\}.$$

O conjunto em questão é um poset com operação $\subseteq$ de inclusão de conjuntos, e portanto tomaremos uma cadeia C em $\mathcal{F}$. Podemos tomar $\tilde{J} = \bigcup_{J \in C} J$, e afirmamos que tal elemento é um limitante superior de C. De fato, primeiro note que $L \subseteq \tilde{J}$ por definição, e se $a, b \in \tilde{J}$, existem $J_1, J_2 \in C$ tais que $a \in J_1, b \in J_2$, e assumindo sem perda de generalidade que $J_1 \subseteq J_2$, temos que $a, b \in J_2$, e portanto $a + b \in J_2$, implicando que $\tilde{J}$ é fechado para soma. Agora se $a \in R$ e $b \in \tilde{J}$, um argumento similar mostra que $ab \in \tilde{J}$, logo $\tilde{J}$ pertence à $\mathcal{F}$, e então pelo Lema de Zorn segue que existe elemento maximal de $\mathcal{F}$, que no caso será precisamente um ideal maximal à esquerda de R que contém L. Um argumento similar pode ser feito para ideais à direita e para ideais bilaterais.

1.4 Álgebras

O principal objeto de estudo deste trabalho são as chamadas álgebras sobre corpos, que nada mais são do que espaços vetoriais com alguma noção de produto bilinear entre seus elementos. A seguir damos sua definição formal.

Definição 1.4.1. Seja $(\mathcal{A}, +)$ um grupo abeliano e $\mathbb{F}$ um corpo. Dizemos que $\mathcal{A}$ é uma $\mathbb{F}$-álgebra se existem operações $\cdot : R \times \mathcal{A} \mapsto \mathcal{A}, * : \mathcal{A} \times \mathcal{A} \mapsto \mathcal{A}$ tais que:

(1) $(\mathcal{A}, +, \cdot)$ é um $\mathbb{F}$-espaço vetorial;

(2) $(\mathcal{A}, +, *)$ é um anel[3];

(3) Para quaisquer α em $\mathbb{F}$ e A, B em $\mathcal{A}$: $\alpha \cdot A * B = (\alpha A) * B = A * (\alpha B)$.

Os itens (1) e (2) nos dizem que uma álgebra nada mais é que um espaço vetorial com respeito à um corpo $\mathbb{F}$ que também é um anel, e (3) nos diz que a multiplicação entre elementos do anel é compatível com a multiplicação por escalares de $\mathbb{F}$, e portanto todas as construções e resultados vistos até então sobre anéis e módulos também se aplicam.

Exemplo 1.4.2. O conjunto $M_n(\mathbb{C})$ das matrizes $n \times n$ com entradas complexas é um anel com respeito às operações de adição e multiplicação de matrizes, e sua unidade é a matriz identidade. Além disso, esse conjunto também tem estrutura de $\mathbb{C}$-espaço vetorial com a multiplicação por escalares em $\mathbb{C}$, portanto ele é uma $\mathbb{C}$-álgebra. Podemos também considerar a operação de multiplicação termo-a-termo de matrizes, conhecida como produto de Schur, definida como $(A \circ B)_{ij} = A_{ij}B_{ij}$ para matrizes de mesmo tamanho, e podemos observar que $M_n(\mathbb{C})$ também é uma $\mathbb{C}$-álgebra com respeito ao produto de Schur, com unidade dada pela matriz com todos elementos iguais a um.

Dada uma álgebra $\mathcal{A}$ sobre um corpo $\mathbb{F}$, iremos representar sua unidade pelo símbolo E. Um subconjunto $\mathcal{B}$ de $\mathcal{A}$ que é simultaneamente um subespaço vetorial e um subanel é dito *subálgebra*, ou seja, $\mathcal{B}$ é um subespaço vetorial de $\mathbb{F}$ que é fechado para produto de matrizes, e que contém a unidade E de $\mathcal{A}$. Podemos dar a estrutura de $\mathbb{F}$-espaço para qualquer $\mathcal{A}$-módulo M, pois basta definir para quaisquer $X \in M, \alpha \in \mathbb{F} : \alpha X := (\alpha E)X$, e daí segue que M é $\mathbb{F}$-espaço vetorial, ou seja, qualquer $\mathcal{A}$-submódulo de $\mathcal{A}$ também é subespaço, e por motivos similares segue que qualquer homomorfismo de $\mathcal{A}$-módulos também é um homomorfismo de $\mathbb{F}$-espaços. No entanto, nem todo $\mathcal{A}$-submódulo é subálgebra, e para ver isso basta tomar o submódulo $M_n(\mathbb{C})E_{ii}$ das matrizes com i-ésima coluna não nula, e notar que a matriz identidade não pertence a tal conjunto. O centro $Z(\mathcal{A})$ de uma álgebra é sempre uma subálgebra – apesar de não necessariamente ser $\mathcal{A}$-módulo –, simplesmente devido à compatibilidade entre as operações da álgebra: se A comuta com todos elementos de $\mathcal{A}$, certamente αA também comuta para qualquer $\alpha \in \mathbb{F}$. Uma função φ entre $\mathbb{F}$-álgebras é dita *homomorfismo* se ela é simultaneamente um homomorfismo de $\mathbb{F}$-espaços e um homomorfismo de anéis.

As noções de somas diretas e de produtos diretos se traduzem naturalmente para o contexto de álgebras, mas nesse caso devemos fazer um esforço adicional para deixar claro sobre qual tipo de soma ou produto estamos nos referindo. Neste trabalho, uma soma direta de álgebras sobre um corpo $\mathbb{F}$ sempre irá se referir à uma soma direta de $\mathbb{F}$-espaços vetoriais, isto é, uma soma direta de $\mathbb{F}$-módulos, e um produto direto de álgebras irá se referir à um produto direto externo de anéis, pois cada álgebra é também um anel.

Uma álgebra $\mathcal{A}$ sobre um corpo $\mathbb{F}$ que é um $\mathbb{F}$-espaço vetorial de dimensão finita d é dita *álgebra de dimensão finita*. Neste caso, dado que fixemos uma base $\{A_1, ..., A_d\}$ de $\mathcal{A}$, temos que

$$A_i A_j = \sum_{k=1}^{d} c_{ij}^k A_k,$$

[3]Diversos outros trabalhos relacionados ao estudo de álgebras também estudam álgebras que não necessariamente possuem unidade, e nesse caso as álgebras aqui descritas seriam chamadas de *unitárias*.

para quaisquer $i, j \in [d] := \{1, ..., d\}$, onde $c_{ij}^k \in \mathbb{F}$. Portanto, note que dados elementos $A, B \in \mathcal{A}$ escritos como $A = \sum_i \alpha_i A_i$ e $B = \sum_j \beta_j A_j$, temos

$$\begin{aligned} AB &= (\sum_i \alpha_i A_i)(\sum_j \beta_j A_j) \\ &= \sum_{i,j} \alpha_i \beta_j A_i A_j \\ &= \sum_{ijk} \alpha_i \beta_j c_{ij}^k A_k, \end{aligned}$$

ou seja, se fixarmos uma base, as constantes $\{c_{ij}^k\}_{ijk}$ determinam completamente a álgebra $\mathcal{A}$, e elas são usualmente chamadas de *constantes estruturais* de $\mathcal{A}$.

2 O Teorema de Wedderburn

Usualmente em cursos de álgebra linear se estuda o famoso Teorema da Decomposição Primária, que nos diz que dado um endomorfismo de espaços vetoriais f em um espaço V sobre um corpo $\mathbb{F}$, sempre é possível decompor o espaço como

$$V = W_1 \oplus \ldots \oplus W_k,$$

onde cada W_i é um subespaço invariante por f, e em particular será um autoespaço generalizado, isto é, se escrevermos o polinômio minimal de f como

$$m_f(t) = p_1(t)^{r_1} \cdot \ldots \cdot p_k^{r_k}(t),$$

com cada p_i irredutível, então $W_i := \ker(p_i^{r_i}(f))$. Uma decomposição do espaço em uma soma direta de subespaços f-invariantes nos dá naturalmente uma diagonalização por blocos de f: basta escolher uma base para cada W_i e então tomar a união de tais bases.

No contexto de matrizes com entradas complexas, o teorema em questão nos garante que sempre é possível encontrar uma base bloco-diagonal para uma dada matriz, e muito do estudo básico de álgebra linear é dedicado à entender qual será a forma dos blocos em questão. Por exemplo, sobre os complexos sempre será possível triangularizar os blocos da decomposição primária de uma matriz, de modo que cada bloco tenha uma componente diagonal e uma componente nilpotente, e essa forma diagonal em blocos triangulares é semelhante à forma normal de Jordan da matriz. O caso onde a matriz é diagonalizável também fornece uma forma agradável para os blocos da decomposição primária: cada bloco terá tamanho 1 e sua única entrada será dada pelo autovalor associado ao autoespaço.

Podemos então nos perguntar como generalizar este resultado: se agora tivermos um conjunto de matrizes, será que também sempre é possível encontrar uma base que simultaneamente as coloca em uma forma bloco-diagonal? Essa será a pergunta motivadora para o nosso estudo de semissimplicidade ao longo deste capítulo, e veremos nas próximas seções diversas formas de determinar e caracterizar a existência de uma base bloco-diagonal.

2.1 Módulos semissimples

Dado um R-módulo M qualquer, dizemos que M é *semissimples* se ele pode ser escrito como soma direta de R-módulos simples. Estamos interessados em caracterizar módulos semissimples, e para isso iremos primeiro demonstrar o seguinte resultado auxiliar.

Lema 2.1.1. Seja M um R-módulo tal que todo N submódulo de M é um somando direto, isto é, existe N' submódulo de M tal que $M = N \oplus N'$. Então todo submódulo não-nulo de M possui submódulo simples.

Demonstração. Seja M um R-módulo que satisfaz a hipótese enunciada, N um submódulo não-nulo, e considere um elemento não-nulo $m \in N$. O módulo Rm é submódulo de N, então podemos tomar o seguinte epimorfismo de R-módulos:

$$\varphi : R \mapsto Rm;$$
$$\varphi(a) = am.$$

Sabemos que $\ker(\varphi)$ é R-submódulo de R e que $\ker(\varphi) \neq R$, pois $m \neq 0$, o que implica que $\ker(\varphi)$ é um ideal não-trivial à esquerda de R, e portanto existe algum ideal maximal à esquerda L em R que o contém. Pelo Teorema 1.3.4, sabemos que existe uma correspondência entre os submódulos de $R/\ker(\varphi)$ e os submódulos de R que contém $\ker(\varphi)$, logo segue que $L/\ker(\varphi)$ é submódulo maximal de $R/\ker(\varphi)$. Como φ é sobrejetivo, sabemos pelo Teorema 1.3.3 que

$$R/\ker(\varphi) \cong_R Rm.$$

Note que a imagem de $L/\ker(\varphi)$ por tal isomorfismo é o submódulo Lm de Rm, e como $L/\ker(\varphi)$ é maximal, segue que Lm é maximal em Rm.

Por hipótese, podemos escrever $M = Lm \oplus L'$, onde L' é um submódulo de M, ou seja, todo elemento $\alpha m \in Rm$ pode ser escrito unicamente como

$$\alpha m = \beta m + x',$$

para alguns $\beta \in L, x' \in L$, mas note então que podemos escrever

$$x' = \alpha m - \beta m \in Rm \cap L'$$

de maneira única. Disso segue que

$$\alpha m = \beta m + (\alpha m - \beta m),$$

com $\beta m \in Lm, \alpha m - \beta m \in Rm \cap L'$, ou seja,

$$Rm = Lm \oplus (Rm \cap L').$$

Afirmamos que $Rm \cap L'$ é simples. Suponha que não seja, isto é, suponha que exista um submódulo próprio U não-nulo. Note que por definição U é da forma $U = \{\alpha m | \alpha \in R' \subseteq R\}$ para algum subconjunto R' de R, mas como U é R-módulo, vale que R' é ideal à esquerda de R, e que $R' \cap L = \{0\}$ (pois a soma da equação anterior é direta). Vale então que

$$Lm \subsetneq Lm + R'm \subsetneq Rm,$$

onde a segunda inclusão é estrita pois assumimos que U é submódulo próprio de $Rm \cap L'$, e como a soma de submódulos é um submódulo, obtemos um submódulo próprio $Lm + R'm$ de Rm que contém propriamente o submódulo Lm, contradizendo a sua maximalidade. Portanto, $Rm \cap L'$ é de fato simples, e como $Rm \cap L'$ é submódulo de N, vale que N possui submódulo simples, como queríamos. ■

O resultado anterior em conjunto ao Lema de Zorn nos permite demonstrar a seguinte caracterização de módulos semissimples.

Proposição 2.1.2. Seja M um R-módulo. As seguintes são equivalentes:

(1) M é soma de R-módulos simples;

(2) M é semissimples;

(3) Todo R-submódulo de M é um somando direto.

Demonstração.

(1)⇒(2) Assuma que $M = \sum_{i \in \mathcal{I}} M_i$, onde cada M_i é R-módulo simples, e considere o conjunto

$$\mathcal{F} = \{\mathcal{J} \subseteq \mathcal{I} | \sum_{j \in \mathcal{J}} M_j \text{ é soma direta}\}.$$

Note que $\mathcal{F} \neq \emptyset$, pois cada $M_i \in \mathcal{F}$, e que $(\mathcal{F}, \subseteq)$ é um poset. Seja $C \subseteq \mathcal{F}$ uma cadeia, e note que $\bigcup_{\mathcal{J} \in C} \mathcal{J} \in \mathcal{F}$ é uma cota superior para C, ou seja, toda cadeia admite cota superior em $\mathcal{F}$. Segue do Lema de Zorn que existe $\mathcal{J}_m \in \mathcal{F}$ maximal, e note que dado um M_i qualquer, $M_i \cap \sum_{j \in \mathcal{J}_m} M_j$ é submódulo de M_i, logo

$$M_i \cap \sum_{j \in \mathcal{J}_m} M_j = M_i \qquad \text{ou} \qquad M_i \cap \sum_{j \in \mathcal{J}_m} M_j = \{0\},$$

pois M_i é simples. Assuma que existe algum $i \in \mathcal{I}$ tal que o segundo caso ocorra, e note então que $\mathcal{J}_m \cup \{i\} \in \mathcal{F}$ é um conjunto de índices que resulta em uma soma direta e que contém estritamente o conjunto maximal $\mathcal{J}_m$, algo que contradiz a definição deste conjunto, logo todo $M_i \subseteq \sum_{j \in \mathcal{J}_m} M_j$, e portanto $M = \sum_{j \in \mathcal{J}_m} M_j$, isto é, M é semissimples.

(2)⇒(3) Assuma que $M = \bigoplus_{i\in\mathcal{I}} M_i$, onde cada M_i é submódulo simples. Seja N um submódulo de M, e considere o conjunto

$$\mathcal{F} = \{\mathcal{J} \subseteq \mathcal{I} | N + \sum_{j\in\mathcal{J}} M_j \text{ é soma direta}\}.$$

De maneira análoga ao passo anterior, é imediato observar que $(\mathcal{F}, \subseteq)$ é um poset. Note que $\mathcal{F}$ é não-vazio, pois para cada M_i vale que $M_i \cap N = \{0\}$ ou $M_i \cap N = M_i$ (pois M_i é simples), e se para todo i vale que $M_i \cap N = M_i$, então $M = N$ e não há nada a se provar, logo podemos assumir que existe ao menos um i tal que $M_i \cap N = \{0\}$, e portanto $N + M_i$ é soma direta. Seja $C \subseteq \mathcal{F}$ uma cadeia, e note que $\bigcup_{\mathcal{J}\in C} \mathcal{J} \in \mathcal{F}$ é uma cota superior para C em $\mathcal{F}$, e então segue do Lema de Zorn que existe $\mathcal{J}_m \in \mathcal{F}$ maximal em $\mathcal{F}$. Note que se existe M_i tal que $M_i \cap (N + (\bigoplus_{j\in\mathcal{J}_m} M_j)) = \{0\}$, então $\mathcal{J}_m \cup \{i\} \in \mathcal{F}$, contrariando a maximalidade de $\mathcal{J}_m$ em $\mathcal{F}$, portanto todos os M_i's estão contidos na soma, então vale que

$$M = N \oplus (\bigoplus_{j\in\mathcal{J}_m} M_j),$$

e então N é somando direto.

(3)⇒(1) Assuma que todo submódulo de M é somando direto, e considere N_s o submódulo de M composto pela soma de todos os submódulos simples de M. Por hipótese, existe submódulo N' tal que

$$M = N_s \oplus N'.$$

Se $N' \neq \{0\}$, o Lema 2.1.1 nos garante que existe submódulo simples de N', algo que contradiz a definição de N_s, logo $N' = \{0\}$ e então M é semissimples. ■

A proposição anterior nos mostra que os R-módulos semissimples são precisamente aqueles que, de certa maneira, apresentam um comportamento semelhante aos de espaços vetoriais: dado qualquer submódulo, é possível encontrar um módulo complemento. A semissimplicidade também se comporta bem com respeito à submódulos e quocientes, como podemos verificar a seguir.

Corolário 2.1.3. Todo submódulo e todo quociente de um R-módulo semissimples é semissimples.

Demonstração. Seja $M = \bigoplus_{i\in\mathcal{I}} M_i$ R-módulo semissimples, com cada M_i simples, e tome um submódulo N qualquer. Considere o R-epimorfismo projeção $\pi : M \mapsto M/N$, e note que dado um $m \in M$ qualquer, existem únicos m_{i_j} tais que

$$m = \sum_j m_{i_j},$$

portanto $\pi(m) = \sum \pi(m_{i_j})$ de forma única, logo $M/N = \sum_{i\in\mathcal{I}} \pi(M_i)$, o que implica pela proposição anterior que M/N é semissimples. Da proposição anterior também sabemos que existe submódulo N' tal que $M = N \oplus N'$, logo vale que $M/N' \cong N$, então N é isomorfo à um quociente, e portanto também é semissimples. ■

Agora iremos formalizar uma forma de identificar endormorfismos de módulos semissimples com matrizes, que rapidamente mencionada logo após a prova da Proposição 1.3.8.

Proposição 2.1.4. Seja M um módulo sobre um anel R, e considere $M^{(n)}$, onde n é um número natural. Então $\mathrm{End}_R(M^{(n)})$ e $M_n(\mathrm{End}_R(M))$ são anéis isomorfos.

Demonstração. Considere $f \in \mathrm{End}_R(M^{(n)})$, e sejam π_i, ι_j a projeção e a inclusão canônicas na i-ésima e j-ésima cópias de M, respectivamente, onde $\pi_i \circ f \circ \iota_j \in \mathrm{End}_R(M)$. Vale notar que apesar de se tratarem de cópias de M, as funções $\pi_i \circ f \circ \iota_j$ em geral não são iguais. Observe que se $m = (m_1, ..., m_n)$ é elemento de $M^{(n)}$, então

$$f(m) = (\sum_{j=1}^{n} (\pi_1 \circ f \circ \iota_j)(m_j), ..., \sum_{j=1}^{n} (\pi_n \circ f \circ \iota_j)(m_j)),$$

logo se identificarmos m com um vetor coluna, temos que

$$f(m) = \begin{pmatrix} \pi_1 \circ f \circ \iota_1 & \pi_1 \circ f \circ \iota_2 & \dots & \pi_1 \circ f \circ \iota_n \\ \vdots & \vdots & \vdots & \vdots \\ \pi_n \circ f \circ \iota_1 & \pi_n \circ f \circ \iota_2 & \dots & \pi_n \circ f \circ \iota_n \end{pmatrix} \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}.$$

Portanto, se considerarmos o mapa

$$\varphi : \mathrm{End}_R(M^{(n)}) \mapsto M_n(\mathrm{End}_R(M)),$$
$$\varphi(f) = \begin{pmatrix} \pi_1 \circ f \circ \iota_1 & \pi_1 \circ f \circ \iota_2 & \dots & \pi_1 \circ f \circ \iota_n \\ \vdots & \vdots & \vdots & \vdots \\ \pi_n \circ f \circ \iota_1 & \pi_n \circ f \circ \iota_2 & \dots & \pi_n \circ f \circ \iota_n \end{pmatrix},$$

é imediato observar que se trata de um homomorfismo de grupos aditivos, e se $f, g \in \mathrm{End}_R(M^{(n)})$, as observações anteriores nos garantem que $\varphi(f \circ g) = \varphi(f) \cdot \varphi(g)$, e como $\varphi(\mathrm{id}) = I$, segue que temos um homomorfismo de anéis. Se $\varphi(f) = 0$, como vimos na Proposição 1.3.8 que f é unicamente determinado pelas entradas da matriz $\varphi(f)$, segue que $f = 0$. Dado qualquer matriz M de $M_n(\mathrm{End}_R(M))$, observe que existe um único R-homomorfismo f tal que $\pi_i \circ f \circ \iota_j = M_{ij}$, logo $\varphi(f) = M$. Portanto, concluímos que φ é bijeção, e então

$$\mathrm{End}_R(M^{(n)}) \cong M_n(\mathrm{End}_R(M))$$

são anéis isomorfos. ■

2.2 Anéis semissimples

Nesta seção estaremos interessados em demonstrar teoremas estruturais para anéis semissimples, com o objetivo de obter descrições úteis das diversas componentes algébricas de um anel. Em particular, iremos demonstrar o Teorema de Wedderburn para anéis semissimples, e discutir em detalhes suas consequências e ramificações. O teorema será apresentado em sua forma geral, e nas próximas seções iremos discutir sua versão para álgebras de matrizes.

Dado um anel R, dizemos que ele é semissimples se ele é um R-modulo semissimples. Ou seja, anéis semissimples são apenas aqueles que, quando vistos como módulos sobre si mesmos, podem ser escritos como soma direta de R-submódulos simples, e ressaltamos novamente que os R-submódulos simples de R são precisamente seus ideias minimais à esquerda. Provaremos agora uma caracterização básica para estes anéis.

Proposição 2.2.1. Um anel R é semissimples se, e somente se, todo R-módulo é semissimples.

Demonstração. Seja R um anel, e note que sendo R um R-módulo, a volta da afirmação segue imediatamente. Agora assuma que R é semissimples e tome um R-módulo M qualquer. Considere o seguinte R-homomorfismo:

$$\varphi : \bigoplus_{m \in M} R \mapsto M;$$
$$\varphi((r_m)_{m \in M}) = \sum_{m \in M, r_m \neq 0} r_m \cdot m.$$

Note que dado $x \in M$, basta tomar a sequência $(\delta_{xm})_{m \in M}$, onde $\delta_{xm} = 1$ se e somente se $m = x$, e notar que $\varphi((\delta_{xm})_{m \in M}) = x$, logo φ é sobrejetiva. Portanto temos que

$$\bigoplus_{m \in M} R/\ker(\varphi) \cong_R M,$$

e como a soma direta de módulos semissimples é semissimples, concluímos que M é isomorfo à um quociente de um módulo semissimples, logo pelo Corolário 2.1.3 segue que M é semissimples. ■

A semissimplicidade em anéis também implica em uma versão mais forte do Lema de Brauer.

Proposição 2.2.2. Seja R um anel semissimples. Então todo ideal à esquerda de R é da forma Re, onde $e^2 = e$ é elemento idempotente. Em particular, todo ideal bilateral é um anel da forma Re com unidade e pertencente ao centro de R.

Demonstração. Seja L ideal à esquerda de R, e sendo R semissimples sabemos da Proposição 2.1.2 que existe outro ideal à esquerda J tal que $R = L \oplus J$. Sejam $e \in L, x \in J$ tais que $e + x = 1$. Dado qualquer $a \in L$, segue que

$$a = ae + ax,$$

o que implica que

$$ax = a - ae \in J \cap L,$$

mas como $J \cap L = \{0\}$, segue que $ax = 0$ e $a = ae$. Isso implica que $e^2 = e$, e também que $L = Re$, e um resultado análogo vale para ideais à direita. Agora assuma que I é ideal bilateral, portanto sabemos que existem elementos idempotentes e, e' tais que

$$I = Re = e'R,$$

logo vale que $ee = e'e$ e que $e'e = e'e'$, mas como ambos são idempotentes, segue que $e = e'e = e'$, portanto $I = Re = eR$. Note que se $x \in I$, existem $a_1, a_2 \in R$ tais que

$$x = a_1 e = e a_2$$

logo

$$xe = a_1 e = x \qquad \text{e} \qquad ex = e a_2 = x$$

portanto $xe = ex$, implicando que e comuta com qualquer elemento de I, ou seja, I é um anel com unidade e. Se tomarmos um elemento $a \in R$ qualquer, temos

$$ae = (ae)e = eae \qquad \text{e} \qquad ea = e(ea) = eae$$

logo $ae = ea$, ou seja, e é um elemento do centro de R, como queríamos. ■

Agora mostramos que a decomposição em submódulos simples de um anel é sempre finita.

Proposição 2.2.3. Se R é um anel semissimples, então ele pode ser escrito como soma direta finita submódulos simples. Ademais, todo R-módulo simples é isomorfo à algum dos somandos diretos de R.

Demonstração. Seja $R = \bigoplus_i L_i$, onde cara L_i é R-submódulo simples. Note que, por definição, existem únicos $r_{i_1}, ..., r_{i_m}, r_{i_j} \in L_{i_j}$ tal que

$$1 = r_{i_1} + ... + r_{i_m}.$$

Logo, qualquer elemento $x \in R$ pode ser escrito unicamente como

$$x = x r_{i_1} + ... + x r_{i_m},$$

e como cada L_{i_j} é R-submódulo de R, vale que $x r_{i_j} \in L_{i_j}$, o que implica que $R = \bigoplus_{j=1}^{m} L_{i_j}$.

Agora seja M um R-módulo simples, logo sabemos que qualquer elemento m não nulo de M é tal que $M = Rm$, portanto o R-homomorfismo $\varphi : R \mapsto M$ dado por $\varphi(a) = am$ é não nulo. Por outro lado, temos pela Proposição 1.3.8 que

$$\{0\} \neq \mathrm{Hom}_R(R, M) \cong \prod_{i=1}^{m} \mathrm{Hom}_R(L_i, M),$$

onde o isomorfismo em questão é de grupos abelianos, mas note que de qualquer forma isso implica que existe algum i tal que $\mathrm{Hom}_R(L_i, M) \neq \{0\}$, logo pelo Lema de Schur segue que $M \cong_R L_i$. ■

Uma consequência imediata da proposição anterior é que existem uma quantidade finita de classes de isomorfismo de módulos simples em um anel semissimples. Se escrevermos um anel semissimples R como

$$R = \bigoplus_{i=1}^{l} L_i,$$

onde cada L_i é R-submódulo simples, e então podemos considerar os submódulos

$$R_i := \bigoplus_{L \cong_R L_i} L \cong_R L_i^{(d_i)}$$

que agrupam todos os d_i somandos isomorfos à L_i na soma direta de R, para algum d_i inteiro não-negativo. Dessa forma, cada R_i é um ideal à esquerda de R que é semissimples, e portanto podemos escrever

$$R = \bigoplus_{i=1}^{m} R_i \cong_R \bigoplus_{i=1}^{m} L_i^{(d_i)},$$

onde $L_i \ncong_R L_j$ se $i \neq j$. Também podemos notar que cada R_i é um ideal bilateral de R. De fato, se $i \neq j$, tomamos

$$R_i R_j = \bigoplus_{L \cong_R L_j} RL = \bigoplus_{L \cong_R L_j} \bigoplus_{L' \cong_R L_i} L'L.$$

Sabemos que ambos L, L' são submódulos simples, logo se existe $a \in L', b \in L$ tal que $ab \neq 0$, o mapa que leva qualquer $a \in L'$ em $ab \in L$ seria um R-homomorfismo não-nulo, e portanto pelo Lema de Schur L e L' seriam isomorfos, algo que contradiz o fato de que $i \neq j$, logo $L'L = \{0\}$, implicando que $R_i R_j = \{0\}$. Disso segue que

$$R_i \subseteq R_i R = R_i \bigoplus_{j=1}^{m} R_j = \bigoplus_{j=1}^{m} R_i R_j = R_i R_i \subseteq R_i,$$

onde a última inclusão seguem do fato de R_i ser ideal à esquerda de R, portanto $R_i R = R_i$, implicando que R_i é ideal bilateral. Disso e pela proposição anterior, segue que cada R_i é um anel com unidade dada por algum idempotente e_i pertencente ao centro de R, e como $R_i R_j = \{0\}$ se $i \neq j$, segue que $e_i e_j = 0$.

Como R é soma direta dos R_i, temos que a unidade de R pode ser unicamente escrita como

$$1 = e_1 + ... + e_m.$$

Além disso, se tomarmos elementos $r, s \in R$, eles podem ser unicamente decompostos como $r = r_1 + ... + r_m$ e $s = s_1 + ... + s_m$, com $r_i, s_i \in R_i$, logo sua multiplicação será dada por

$$rs = r_1 s_1 + ... + r_m s_m,$$

pois os produtos da forma $r_i s_j$ com $i \neq j$ serão nulos. Portanto, se considerarmos o mapa canônico que leva r em $(r_1, ..., r_m)$ – ou seja, que identifica a soma direta interna de submódulos com a soma direta externa – também será um isomorfismo de anéis, pois a unidade 1 será mapeada em $(e_1, ..., e_m)$, que é justamente a unidade do produto direto dos R_i. Isso nos mostra que o anel R é isomorfo à um produto direto externo dos anéis R_i, e como cada anel corresponde à um ideal bilateral de R, diremos que

$$R = \prod_{i=1}^{m} R_i,$$

isto é, diremos que R é igual ao produto direto dos R_i. Essa é uma das possíveis definições de produtos diretos internos em anéis, mas como sua construção é um tanto específica para o caso de anéis semissimples, optamos por introduzi-la somente agora.

Essa discussão nos leva a demonstração o Teorema de Wedderburn.

Teorema 2.2.4 (Teorema de Wedderburn)**.** Seja R um anel semissimples escrito como

$$R = \bigoplus_{i=1}^{m} R_i,$$

onde $R_i \cong_R L_i^{(d_i)}$, cada L_i é submódulo simples, e $L_i \ncong_R L_j$ se $i \neq j$. Então cada R_i é um anel simples isomorfo à $M_{d_i}(D_i)$, onde D_i é um anel de divisão, e também temos que

$$R \cong \prod_{i=1}^{m} M_{d_i}(D_i),$$

ou seja, R é isomorfo à um produto direto de anéis de matrizes sobre anéis de divisão. Reciprocamente, todo produto direto de anéis de matrizes sobre anéis de divisão é semissimples.

Demonstração. Pelas Proposições 1.3.5 e 2.1.4, temos que

$$\mathrm{End}_R(R_i) \cong \mathrm{End}_R(L_i^{(d_i)}) \cong M_{d_i}(\mathrm{End}_R(L_i))$$

são anéis isomorfos, e como L_i é módulo simples, segue que $\mathrm{End}_R(L_i)$ é anel de divisão, logo

$$\begin{aligned} R_i &\cong (R_i^{\mathrm{op}})^{\mathrm{op}} \\ &\cong (\mathrm{End}_R(R_i))^{\mathrm{op}} \\ &\cong (M_{d_i}(\mathrm{End}_R(L_i)))^{\mathrm{op}} \\ &\cong M_{d_i}(\mathrm{End}_R(L_i)^{\mathrm{op}}), \end{aligned}$$

onde o segundo e último isomorfismos seguem das Proposições 1.2.6 e 1.3.9, e o anel $D_i := \mathrm{End}_R(L_i)^{\mathrm{op}}$ é de divisão. Portanto o anel R_i é isomorfo à $M_{d_i}(D_i)$, para cada i, ou seja, R_i é isomorfo à um anel simples, logo também é simples. A Proposição 1.3.8 nos dá que

$$\mathrm{End}_R(R) = \mathrm{End}_R(\bigoplus_{i=1}^{m} R_i) \cong \prod_{i,j} \mathrm{Hom}_R(R_i, R_j),$$

onde os isomorfismos são de grupos abelianos, e por hipótese $L_i \ncong L_j$ se $i \neq j$, mas note que os ideais L_i, L_j são R-módulos simples e não isomorfos, portanto segue do Lema de Schur que qualquer R-homomorfismo entre L_i, L_j é identicamente nulo, ou seja, $\mathrm{Hom}_R(L_i, L_j) = \{0\}$, o que também implica que $\mathrm{Hom}_R(R_i, R_j) = \{0\}$, logo

$$\mathrm{End}_R(R) \cong \prod_{i=1}^{m} \mathrm{End}_R(R_i) \cong \prod_{i=1}^{m} M_{d_i}(\mathrm{End}_R(L_i)),$$

onde agora os isomorfismo são de anéis. Portanto, se prosseguirmos similarmente ao que foi feito para cada R_i, obtemos que

$$\begin{aligned} R &\cong (R^{\mathrm{op}})^{\mathrm{op}} \\ &\cong (\mathrm{End}_R(R))^{\mathrm{op}} \\ &\cong (\prod_{i=1}^{m} \mathrm{End}_R(R_i))^{\mathrm{op}} \\ &\cong \prod_{i=1}^{m} (\mathrm{End}_R(R_i))^{\mathrm{op}} \\ &\cong \prod_{i=1}^{m} (M_{d_i}(\mathrm{End}_R(L_i)))^{\mathrm{op}} \\ &\cong \prod_{i=1}^{m} M_{d_i}(D_i). \end{aligned}$$

Logo R é isomorfo à um produto direto de anéis de matrizes sobre anéis de divisão, onde cada termo do produto é isomorfo ao respectivo R_i da expressão de R como soma direta. Reciprocamente, se R é um produto direto de anéis de matrizes sobre anéis de divisão, sabemos do Exemplo 1.3.13 que cada elemento do produto é semissimples, e como se trata de um produto direto, cada elemento será um ideal bilateral, logo podemos identificar R também como soma direta de submódulos semissimples, e daí segue que R é semissimples. ■

O Teorema de Wedderburn tem diversas implicações relevantes para o estudo de anéis e álgebras, e dedicaremos o restante deste capítulo para discutir essas consequências em detalhes. A implicação mais imediata e talvez mais importante é justamente a garantia de que podemos identificar um anel R semissimples com um produto direto de anéis simples R_i, cada um sendo um ideal bilateral de R que é isomorfo à algum anel de matrizes sobre um anel de divisão. Essa decomposição de um anel semissimples como produto de anéis simples R_i é usualmente chamada de *decomposição de Wedderburn* do anel. Observamos também que teorema nos garante que não é necessário distinguir entre semissimplicidade à esquerda ou à direita: os anéis de matrizes sobre anéis de divisão são semissimples tanto à esquerda (com ideais minimais à esquerda dados pelas matrizes colunas C_i descritas anteriormente), quanto à direita (com ideais minimais à direita dados pelas matrizes linha definidas de maneira análoga). Ou seja, um anel é semissimples à direita se, e somente se, ele é semissimples à esquerda.

Podemos também demonstrar que a decomposição decomposição de Wedderburn é única.

Proposição 2.2.5 (Unicidade da decomposição de Wedderburn)**.** Se R é um anel semissimples com decomposição de Wedderburn dada por

$$R = \prod_{i=1}^{m} R_i,$$

onde cada R_i é anel simples, então essa decomposição é única a menos de permutação dos R_i, onde os parâmetros m, d_i são unicamente determinados por R.

Demonstração. Assuma que

$$R = \prod_{i=1}^{m} R_i = \prod_{j=1}^{m'} R'_j,$$

e note que

$$R_i \subseteq R_i R = R_i R_i \subseteq R_i,$$

logo $R_i R = R_i$ para qualquer i. Por outro lado, também temos que

$$R_i R = \prod_{j=1}^{m'} R_i R'_j,$$

mas como cada R'_j também é ideal bilateral de R, segue que $R_i R'_j$ é ideal bilateral de R_i, e sendo R_i simples, isso implica que $R_i R'_j = R_i$ ou $R_i R'_j = \{0\}$. Como $R_i R = R_i$, disso segue que existe exatamente um índice j tal que $R_i R'_j = R_i$, e se agora repetirmos o processo para j, concluímos que

$$R_i = R_i R'_j = R'_j,$$

logo para cada i existe um único j' tal que $R_i = R'_j$, e portanto a decomposição de Wedderburn de R é única a menos de permutação dos R_i's, e consequentemente os parâmetros R_i, d_i, m são unicamente determinados por R. ■

A principal consequência da decomposição de Wedderburn para este trabalho é a estrutura dos elementos idempotentes de um anel semissimples R. Se $e \in R$ é um elemento idempotente pertencente ao centro de R, dizemos que ele é um *idempotente central*, e se e_i, e_j são idempotentes distintos de R tal que $e_i e_j = 0$, dizemos que eles são *ortogonais*. Dizemos que um idempotente $e \in R$ é *primitivo* (também conhecido como *minimal*) se ele não pode ser escrito como soma de idempotentes ortogonais não-nulos de R, e um idempotente é dito

centralmente primitivo se ele é central e não pode ser escrito como soma de idempotentes centrais ortogonais não-nulos.

Com essa nova terminologia, obtemos o seguinte corolário.

Corolário 2.2.6. Seja R é um anel semissimples com decomposição de Wedderburn dada por

$$R = \prod_{i=1}^{m} R_i.$$

Então existem únicos idempotentes ortogonais centralmente primitivos $e_1, ..., e_m$ tais que

$$1 = e_1 + ... + e_m.$$

Ademais, para cada e_i, também existem únicos idempotentes ortogonais primitivos $e_{i1}, ..., e_{id_i}$ tais que

$$e_i = e_{i1} + ... + e_{id_i}.$$

Demonstração. A unicidade dos idempotentes segue da unicidade da decomposição de Wedderburn, e vimos em discussões anteriores que os idempotentes $e_1, ..., e_m$ tais que $R_i = Re_i$ são de fato ortogonais e centrais, portanto resta mostrar que são centralmente primitivos. Agora fixe i e assuma que $e_i = e_i' + e_i''$, onde e_i', e_i'' são idempotentes centrais ortogonais não-nulos, ou seja, podemos escrever o anel R_i como

$$R_i = Re_i = Re_i' \oplus Re_i'',$$

onde a soma é direta pois os idempotentes são ortogonais, mas note que como e_i' e e_i'' são centrais, os submódulos Re_i' serão ideais bilaterais próprios e não-triviais de R_i, contradizendo a simplicidade de R_i, logo cada e_i é de fato centralmente primitivo.

Lembramos que por definição cada R_i é da forma

$$R_i = \bigoplus_{L \cong_R L_i} L \cong_R L_i^{(d_i)},$$

ou seja, R_i é um anel semissimples, e seus d_i ideais à esquerda são todos isomorfos à L_i. Pela Proposição 2.2.2, segue que para cada ideal à esquerda de R é da forma Re_{ij} para algum idempotente e_{ij}, e por um argumento similar ao feito anteriormente segue esses idempotentes são ortogonais e primitivos. Portanto, como e_i é a unidade em R_i, temos que

$$e_i = e_{i1} + ... + e_{id_i},$$

como queríamos. ■

Por fim, descrevemos o caso onde R é um anel semissimples comutativo.

Corolário 2.2.7. Todo anel comutativo e semissimples R é produto direto finito de corpos. Reciprocamente, todo produto direto finito de corpos é semissimples.

Demonstração. Pelo Teorema de Wedderburn, podemos escrever

$$R \cong \prod_{i=1}^{m} M_{d_i}(D_i),$$

onde D_i é um anel de divisão. Sendo R comutativo, segue que cada $M_{d_i}(D_i)$ deve ser por sua vez comutativo, mas como se trata de um anel de matrizes, isso só é possível se $d_i = 1$. Cada $M_1(D_i)$ é naturalmente isomorfo à D_i como anel, portanto cada D_i é anel de divisão comutativo, logo é corpo. Reciprocamente, se R é um produto direto finito de corpos, note que cada corpo pode ser visto como um anel de matrizes de tamanho 1×1 com entradas no corpo, portanto é semissimples, o que implica que R por sua vez também é. ■

2.3 O Radical de Jacobson

Agora iremos realizar uma breve discussão acerca de uma importante ferramenta para o estudo de anéis e álgebras semissimples, conhecida como o radical de Jacobson de um anel. Primeiro, dado um anel R, dizemos que ele é *artiniano* à esquerda se qualquer cadeia descendente de ideais à esquerda estabiliza, isto é, dados ideais $\{L_j\}_j$ à esquerda tais que

$$L_1 \supseteq L_2 \supseteq ... \supseteq L_n \supseteq L_{n+1} \supseteq ...,$$

existe índice k tal que para qualquer $j \geq k : L_j = L_k$. Isso equivale a dizer que toda família não-vazia de ideias à esquerda de R possui um elemento minimal. Também é interessante notar que, se L é um ideal à esquerda não-nulo de R, então ele deve contem algum ideal minimal à esquerda, do contrário poderíamos construir uma família não-vazia de ideais à esquerda que não possui elemento minimal. A princípio a noção de anéis artinianos pode parecer um tanto arbitrária, no entanto, qualquer álgebra de dimensão finita é um anel artiniano. Isso segue do fato de que qualquer ideal à esquerda é um subespaço da álgebra, portanto qualquer cadeia descendente estrita de ideais à esquerda é uma cadeia de subespaços cujas dimensões estão diminuindo, e como a dimensão é finita em algum momento a cadeia deve estabilizar.

Definimos o *Radical de Jacobson* $J(R)$ de um anel R como sendo a interseção de todos os ideais maximais à esquerda, isto é,

$$J(R) := \bigcap \{L \subseteq R | L \text{ ideal maximal à esquerda}\}.$$

Esse objeto será útil para nós pois é possível caracterizar a semissimplicidade de um dado anel em termos de seu radical, e veremos que em alguns casos é significativamente mais fácil demonstrar que uma álgebra é semissimples por meio do estudo de seu radical.

Primeiro observamos que se R é um anel e $y \in J(R)$ é um elemento de seu radical, então $1 + y$ deve ser invertível à esquerda, isto é, deve existir $x \in R$ tal que $x(1 + y) = 1$. De fato, se $1 + y$ não fosse invertível, então o ideal à esquerda $R(1 + y)$ é não-trivial e próprio em R, portanto está contido em algum ideal à esquerda maximal, mas $y \in J(R)$ e $J(R)$ está contido em todos os ideais maximais à esquerda, logo $1 - y + y = 1$ pertenceria a algum ideal maximal à esquerda de R, o que é um absurdo. Isso em particular também implica que qualquer elemento da forma $1 - y$ com $y \in J(R)$ é invertível à esquerda em R.

A definição do radical também nos permite concluir os seguintes fatos.

Proposição 2.3.1. Seja R um anel, e N seu radical de Jacobson. Então

(1) $J(R)$ é um ideal bilateral;

(2) Se M é R-módulo simples, então $J(R)M = \{0\}$;

(3) O radical do anel $R/J(R)$ é $\{0\}$;

(4) Se R é artiniano, o seu radical é uma interseção finita de ideais maximais à esquerda.

Demonstração.

(1) Seja $x \in J(R)$ e $r \in R$, e seja L um ideal maximal à esquerda qualquer de R, e note que por definição $x \in L$. Defina o mapa

$$\varphi : R/L \mapsto R/L,$$
$$\varphi(a + L) = ar + L,$$

e note que φ é R-endomorfismo, pois se $m \in R$, então $\varphi(ma + L) = mar + L = m(ar + L)$, e $\varphi((a + b) + L) = (a + b)r + L = (ar + L) + (br + L)$. Sabemos que qualquer R-homomorfismo mapeia o zero do domínio no zero do codomínio, portanto como $x \in L$, $x + L = 0$, logo $\varphi(x + L) = xr + L = 0$, e então $xr \in L$. Disso, segue que xr pertence à qualquer ideal maximal à esquerda de R, e portanto $xr \in J(R)$, logo o radical é ideal bilateral.

(2) Se M é R-módulo simples, sabemos pelo Teorema 1.3.11 que existe ideal maximal à esquerda L de R tal que $M \cong_R R/L$. Pelo item anterior, sabemos que $J(R)$ é ideal bilateral, portanto se $x \in J(R)$, então $xr \in J(R)$ para qualquer $r \in R$, e por definição $J(R) \subseteq L$, logo $xr \in L$, o que implica que $xr + L = 0$, e portanto

$$J(R)M = \{0\},$$

como queríamos.

(3) O Teorema de Correspondência para anéis nos diz que existe uma bijeção entre os ideais à esquerda de R que contém $J(R)$ e os ideais à esquerda de $R/J(R)$, portanto se $x + J(R)$ pertence ao radical de $R/J(R)$, vale que $x + J(R)$ pertence à todos os ideais maximais à esquerda de $R/J(R)$, e consequentemente x pertence à todos os ideais maximais à esquerda de R que contém $J(R)$ – que por definição são todos os ideais maximais à esquerda de R –, logo $x \in J(R)$. Portanto $x + J(R) = 0$, e então o radical de $R/J(R)$ é $\{0\}$.

(4) Seja R artiniano, e considere o conjunto

$$\mathcal{F} = \{\bigcap_{i=1}^{n} L_i | L_i \text{ ideal maximal à esquerda de } R, n \in \mathbb{N}\}.$$

Sendo R artiniano, $\mathcal{F}$ possui elemento minimal $L = \bigcap_{i=1}^{n} L_i$ para algum natural n. Caso $J(R) \neq L$, então existe ideal maximal à esquerda $I_j \not\subseteq L$, mas então $L_j \in \mathcal{F}$ e $L_j \cap L \subsetneq L$, contrariando a minimalidade de L. Logo $J(R)$ é uma interseção finita de ideais maximais à esquerda

■

O radical de Jacobson também está fortemente conectado com o conceito de nilpotência. Dizemos que um ideal L (unilateral ou bilateral) de um anel é *nilpotente* se existe natural r tal que $L^r = \{0\}$, em outras palavras, qualquer produto de r elementos de L é nulo. Isso nos permite demonstrar um importante resultado.

Proposição 2.3.2. Seja R um anel, então valem as seguintes:

(1) Qualquer ideal bilateral nilpotente de R está contido em $J(R)$;

(2) Se R é artiniano, então $J(R)$ é nilpotente.

Demonstração.

(1) Seja N ideal nilpotente de R, e seja L um ideal maximal à esquerda qualquer. Note então que $M = R/L$ é R-módulo simples, e portanto o R-submódulo $NM = \{0\}$ ou $NM = M$. Se $NM = \{0\}$, como $1 \in R$, significa dizer que todos os elementos da forma $a + L$, com $a \in N$ são nulos, logo $N \subseteq L$. Se $NM = M$, repetimos o processo até chegarmos em $N^r M = M$, onde r é o natural tal que $N^r = \{0\}$, e nesse caso se $N \not\subseteq L$ teríamos que $M = \{0\}$, absurdo, logo N está contido em todo ideal maximal à esquerda de R, e portanto está contido em seu radical.

(2) Denote por J o radical de Jacobson de R, e considere a seguinte cadeia descendente de ideais

$$J \supseteq J^2 \supseteq ...$$

Sendo R artiniano, existe $r \in \mathbb{N}$ tal que $J^r = J^{r+i}$, para qualquer $i \in \mathbb{N}$. Afirmamos que $J^r = \{0\}$. De fato, caso não seja, vale que $J^r J^r = J^r \neq \{0\}$, logo existem elementos não-nulos $a, b \in J^r$ tais que $ab \neq 0$, e portanto o ideal à esquerda $J^r b \neq \{0\}$. Daí, segue que $J^r J^r b = J^r b \neq 0$, portanto o conjunto dos ideais à esquerda L de J^r tal que $J^r L \neq \{0\}$ é não-vazio, e sendo R artiniano, isso implica que existe ideal à esquerda L minimal tal que $J^r L \neq \{0\}$. Certamente tal ideal é principal, pois existe elemento $x \in L$ não-nulo tal que $J^r x \neq \{0\}$, logo $L = J^r x$. Em particular, podemos então encontrar elemento $y \in J^r$ tal que $x = yx$, logo $(1 - y)x = 0$, mas como $y \in J$, segue que $1 - y$ é invertível à esquerda, e então $x = 0$. Isso implica que $L = J^r x = \{0\}$ e contradiz o fato de L ser minimal, e então de fato temos que o radical é nilpotente.

■

Note que o resultado anterior nos mostra que o radical de Jacobson é precisamente o maior ideal bilateral nilpotente de um anel artiniano, e veremos agora que um anel artiniano será semissimples precisamente quando seu radical for trivial.

Teorema 2.3.3. Seja R um anel artiniano. Então R é semissimples se, e somente se, $J(R) = \{0\}$.

Demonstração.

($\Rightarrow$) Se R é semissimples, sabemos que existem únicos idempotentes ortogonais centralmente primitivos $e_1, ..., e_m$ tais que

$$1 = e_1 + ... + e_m,$$

onde $R_i = Re_i$ correspondem aos anéis simples da decomposição de Wedderburn de R. Portanto se $a \in J(R)$, temos que

$$a = a(e_1 + ... + e_m) = ae_1 + ... + ae_m,$$

mas também vimos que cada e_i pode ser unicamente decomposto como soma de idempotentes ortogonais primitivos $e_{i1}, ..., e_{id_i}$, onde cada e_{ij} é um idempotente de um ideal à esquerda minimal de R isomorfo à L_i. Logo, obtemos que

$$ae_i = ae_{i1} + ... + ae_{id_i},$$

e da Proposição 2.3.1 sabemos que $J(R)L_i = \{0\}$ pois L_i é submódulo simples, logo $ae_{ij} = 0$ para qualquer i e j, implicando que $a = 0$ e então $J(R) = \{0\}$.

($\Leftarrow$) Da proposição anterior, sabemos que o radical de R é $\bigcap_{i=1}^{n} L_i$ para algum natural n, onde cada L_i é ideal maximal à esquerda. Portanto considere o seguinte mapa

$$\varphi : R \mapsto \bigoplus_{i=1}^{n} R/L_i,$$
$$\varphi(r) = (r + R/L_1, ..., r + R/L_n).$$

Note que tal mapa é claramente um homomorfismo de anéis, e que se $\varphi(r) = 0$, então $r \in L_i$ para qualquer i, logo $r \in J(R) = \{0\}$, implicando que o mapa é injetivo. É fácil ver que o mesmo também é sobrejetivo, e portanto φ é um isomorfismo de anéis entre R e uma soma direta finita de R-módulos, cada um sendo simples pois cada L_i é ideal à esquerda maximal, logo R é semissimples. ■

2.4 Álgebras semissimples

Dada uma álgebra $\mathcal{A}$ sobre um corpo $\mathbb{F}$, dizemos que ela é *semissimples* se ela o é como um anel, ou seja, se $\mathcal{A}$ pode ser escrita como soma direta de $\mathcal{A}$-submódulos simples. Similarmente, dizemos que uma álgebra é *simples* se ela o é como anel, isto é, se seu único ideal bilateral próprio é trivial. Como nosso estudo é focado em álgebras de matrizes, iremos considerar álgebras de dimensão finita, e nesse contexto é possível demonstrar um análogo do famoso Teorema de Cayley: se uma $\mathbb{F}$-álgebra possui dimensão d, então ela está isomorficamente imersa na álgebra das matrizes $d \times d$ sobre $\mathbb{F}$, isto é, existe um homomorfismo de álgebras injetivo de tal álgebra para a álgebra de matrizes, e esse mapa é usualmente chamada de *representação fiel*.

Proposição 2.4.1. Seja $\mathcal{A}$ uma $\mathbb{F}$-álgebra. Então $\mathcal{A}$ está isomorficamente imersa em $\mathrm{End}_{\mathbb{F}}(\mathcal{A})$. Em particular, se $\mathcal{A}$ possui dimensão finita d, então $\mathcal{A}$ está isomorficamente imersa em $M_d(\mathbb{F})$.

Demonstração. Similarmente ao que é feito na demonstração usual do Teorema de Cayley, podemos tomar um elemento A em $\mathcal{A}$ e definir o $\mathbb{F}$-endomorfismo $f_A(B) = AB$, para qualquer B em $\mathcal{A}$, isto é, consideramos o mapa que multiplica elementos de $\mathcal{A}$ por A pela esquerda. Daí definimos a seguinte função:

$$\varphi : \mathcal{A} \mapsto \mathrm{End}_{\mathbb{F}}(\mathcal{A});$$
$$\varphi(A) = f_A.$$

Note que sendo $\mathbb{F}$ corpo, $\mathrm{End}_{\mathbb{F}}(\mathcal{A})$ é $\mathbb{F}$-álgebra, e é imediato verificar que φ é homomorfismo de $\mathbb{F}$-espaços vetoriais. Dados $A, B \in \mathcal{A}$, vale que $\varphi(AB) = f_{AB}$, e para qualquer $C \in \mathcal{A}$, temos que $f_{AB}(C) = ABC = (f_A \circ f_B)(C)$, logo de fato φ é homomorfismo de $\mathbb{F}$-álgebras.

Ademais, note que se $\varphi(A) = 0$, então $A = AE = f_A(E) = 0$, implicando que $A = 0$, logo segue que φ é um monomorfismo de $\mathbb{F}$-álgebras. Com isso, vale que $\mathcal{A}$ é isomorfo à imagem de φ, i.e., está isomorficamente imerso em $\mathrm{End}_{\mathbb{F}}(\mathcal{A})$. Se a dimensão de $\mathcal{A}$ é finita com valor d, vale que, se fixarmos uma base de $\mathcal{A}$, $\mathrm{End}_{\mathbb{F}}(\mathcal{A})$ e $M_d(\mathbb{F})$ são $\mathbb{F}$-álgebras isomorfas, e portanto segue o resultado. ■

O resultado acima nos permite identificar cada elemento de $\mathcal{A}$ com uma matriz $d \times d$ de maneira única. Se agora considerarmos álgebras de dimensão finita sobre corpos algebricamente fechados, como $\mathbb{C}$ por exemplo, podemos concluir uma versão mais forte do Lema de Schur.

Lema 2.4.2. Seja $\mathcal{A}$ uma álgebra de dimensão finita sobre um corpo algebricamente fechado $\mathbb{F}$, e seja $\mathcal{L}$ um $\mathcal{A}$-submódulo simples. Então $\mathrm{End}_{\mathcal{A}}(\mathcal{L})$ e $\mathbb{F}$ são corpos isomorfos.

Demonstração. Primeiro, note que foi previamente observado que todo $\mathcal{A}$-submódulo também é um subespaço vetorial, ou seja, também possui dimensão finita. Ademais, dado elemento $f \in \mathrm{End}_{\mathcal{A}}(\mathcal{L})$, note que f também é $\mathbb{F}$-endomorfismo, pois para qualquer α em $\mathbb{F}$, e para qualquer A em $\mathcal{L}$, vale que

$$f(\alpha A) = f(\alpha EA) = f((\alpha E)A) = \alpha E f(A) = \alpha f(A),$$

portanto $\mathrm{End}_{\mathcal{A}}(\mathcal{L}) \subseteq \mathrm{End}_{\mathbb{F}}(\mathcal{L})$. Sendo $\mathbb{F}$ algebricamente fechado, vale então que existe autovalor $\lambda \in \mathbb{F}$ de f com autovetor não-nulo $X \in \mathcal{L}$ tal que

$$f(X) = \lambda X.$$

Portanto a função $f - \lambda E$ é um $\mathbb{F}$-endomorfismo com núcleo não-trivial que pertence à $\mathrm{End}_{\mathcal{A}}(\mathcal{L})$. No entanto, sendo $\mathcal{L}$ um $\mathcal{A}$-módulo simples, segue o Lema de Schur que $\mathrm{End}_{\mathcal{A}}(\mathcal{L})$ é anel de divisão, ou seja, $f - \lambda E$ deve ser identicamente nula, portanto $f = \lambda E$. Considere então o seguinte homomorfismo de anéis

$$\begin{aligned} &\varphi : \mathbb{F} \mapsto \mathrm{End}_{\mathcal{A}}(\mathcal{L}), \\ &\varphi(\lambda) = \lambda E. \end{aligned}$$

Note que φ é claramente injetivo, tendo em vista que $\lambda E = 0$ implica que que $\lambda = 0$. As observações anteriores acerca de $\mathrm{End}_{\mathcal{A}}(\mathcal{L})$ nos mostram que φ é sobrejetiva, portanto segue o resultado. ■

Similarmente ao que foi feito para o caso de anéis, podemos escrever uma álgebra semissimples $\mathcal{A}$ como

$$\mathcal{A} = \bigoplus_{i=1}^{l} \mathcal{L}_i,$$

onde cada $\mathcal{L}_i$ é $\mathcal{A}$-submódulo simples, e então podemos considerar os submódulos

$$\mathcal{A}_i := \bigoplus_{\mathcal{L} \cong_{\mathcal{A}} \mathcal{L}_i} \mathcal{L} \cong_{\mathcal{A}} \mathcal{L}_i^{(d_i)}$$

que agrupam todos os d_i somandos isomorfos à $\mathcal{L}_i$ na soma direta de $\mathcal{A}$, para algum d_i inteiro não-negativo. Dessa forma, podemos escrever

$$\mathcal{A} = \bigoplus_{i=1}^{m} \mathcal{A}_i \cong_{\mathcal{A}} \bigoplus_{i=1}^{m} \mathcal{L}_i^{(d_i)},$$

onde $\mathcal{L}_i \ncong_{\mathcal{A}} \mathcal{L}_j$ se $i \neq j$. Disso segue que cada $\mathcal{A}_i$ é uma álgebra simples e um um ideal bilateral de $\mathcal{A}$ da forma $\mathcal{A}_i = \mathcal{A}E_i$, onde cada E_i é um idempotente central de $\mathcal{A}$ que também é a unidade da álgebra $\mathcal{A}_i$. Isso implica imediatamente que se $i \neq j$, então $\mathcal{A}_i\mathcal{A}_j = \{0\}$, e portanto podemos identificar $\mathcal{A}$ com o produto direto das álgebras $\mathcal{A}_i$

$$\mathcal{A} = \prod_{i=1}^{m} \mathcal{A}_i.$$

Note que o Teorema de Wedderburn nos garante que cada $\mathcal{A}_i$ é isomorfa como anel à $M_{d_i}(\mathrm{End}_R(\mathcal{L}_i)^{\mathrm{op}})$, e deixamos ao leitor verificar que esse isomorfismo também é de álgebras. Como cada $\mathcal{L}_i$ é submódulo simples de $\mathcal{A}$, o Lema 2.4.2 nos garante que $\mathrm{End}_R(\mathcal{L}_i)$ é um corpo isomorfo à $\mathbb{F}$, e portanto

$$\mathcal{A}_i \cong M_{d_i}(\mathbb{F})$$

são $\mathbb{F}$-álgebras isomorfas. Essas observações nos permitem concluir versões análogas par álgebras dos resultados discutidos nas seções anteriores.

Teorema 2.4.3 (Teoremas de Wedderburn para Álgebras)**.** Seja $\mathcal{A}$ uma álgebra semissimples de dimensão finita sobre um corpo algebricamente fechado $\mathbb{F}$, escrita como

$$\mathcal{A} = \bigoplus_{i=1}^{m} \mathcal{A}_i,$$

onde $\mathcal{A}_i \cong_{\mathcal{A}} \mathcal{L}_i^{(d_i)}$, cada $\mathcal{L}_i$ é submódulo simples, e $\mathcal{L}_i \ncong_{\mathcal{A}} \mathcal{L}_j$ se $i \neq j$. Então valem as seguintes:

(1) Cada $\mathcal{A}_i$ é isomorfo como $\mathbb{F}$-álgebra à álgebra completa de matrizes $M_{d_i}(\mathbb{F})$, e portanto

$$\mathcal{A} \cong \prod_{i=1}^{m} M_{d_i}(\mathbb{F})$$

é um isomorfismo de $\mathbb{F}$-álgebras. Reciprocamente, qualquer produto direto finito de álgebras completas de matrizes é semissimples;

(2) A decomposição de Wedderburn da álgebra $\mathcal{A}$ é única a menos de permutação das $\mathcal{A}_i$, e os parâmetros m, d_i são unicamente determinados por $\mathcal{A}$;

(3) Existem únicos idempotentes ortogonais centralmente primitivos $E_1, ..., E_m$ tais que

$$E = E_1 + ... + E_m,$$

onde E é a unidade da álgebra $\mathcal{A}$. Ademais, para cada E_i, também existem únicos idempotentes ortogonais primitivos $E_{i1}, ..., E_{id_i}$ tais que

$$E_i = E_{i1} + ... + E_{id_i};$$

(4) Se $\mathcal{A}$ também é comutativa, então

$$\mathcal{A} \cong \prod_{i=1}^{m} \mathbb{F},$$

e em particular os idempotentes ortogonais centralmente primitivos formam uma base para $\mathcal{A}$ como $\mathbb{F}$-espaço vetorial.

■

A afirmativa (1) nada mais é que a versão análoga do Teorema 2.2.4, (2) é o análogo da Proposição 2.2.5, e (3), (4) são os análogos dos Corolários 2.2.6 e 2.2.7, respectivamente, notando que no caso de álgebras comutativas semissimples, teremos que $\mathcal{A}$ será isomorfo à $\prod_{i=1}^{m} \mathbb{F}$, que é um espaço vetorial de dimensão m, e notando também que o conjunto dos idempotentes $E_1, ..., E_m$ é linearmente independente, segue que eles formam uma base para $\mathcal{A}$.

As discussões ao longo deste capítulo foram um tanto abstratas, mas agora iremos mostrar como aplicar estes resultados de uma forma um tanto concreta. Quando dizemos que uma álgebra é isomorfa à um produto direto de matrizes, uma boa forma de visualizar isso é com matrizes diagonais por blocos. Podemos identificar o produto direto de álgebras completas de de matrizes com dimensões $d_1, ..., d_m$ como um conjunto de matrizes quadradas diagonais por blocos de tamanho $d_1 + ... + d_m$, onde cada bloco é uma matriz quadrada

de tamanho d_i. As operações de soma e multiplicação se comportam da mesma maneira que se comportariam para elementos do produto direto direta, em especial a multiplicação de duas matrizes diagonais em blocos – com blocos do mesmo tamanho – é uma matriz diagonal dos respectivos produtos entre os blocos. Portanto, o Teorema de Wedderburn nos mostra que qualquer álgebra semissimples de dimensão finita sobre um corpo algebricamente fechado será da forma

$$\mathcal{A} \cong \{ \begin{pmatrix} M_1 & & \\ & \ddots & \\ & & M_m \end{pmatrix} | M_i \in M_{d_i}(\mathbb{F}) \}$$

isto é, um conjunto de matrizes diagonais por blocos, onde cada bloco equivale à um ideal minimal à esquerda com multiplicidade d_i na expansão de $\mathcal{A}$ como soma direta, e se a dimensão de $\mathcal{A}$ é d, devemos ter que $d = d_1^2 + ... + d_m^2$, pois se tratam de álgebras isomorfas onde cada $M_{d_i}(\mathbb{F})$ tem dimensão d_i^2.

Agora iremos responder a pergunta motivadora feita no início deste capítulo: quando é possível bloco-diagonalizar um conjunto de matrizes de forma simultânea, ou seja, quando é possível encontrar uma matriz invertível P tal que todas as matrizes A_i de um dado conjunto estejam numa forma bloco-diagonal quando fazemos a mudança de base $P^{-1}A_iP$? Tendo em vista os resultados discutidos neste capítulo, a resposta pode parecer óbvia: as álgebras de matrizes semissimples são precisamente aquelas que podem ser simultaneamente bloco-diagonalizadas, mas essa conclusão não é de forma alguma imediata a partir dos teoremas. O isomorfismo do Teorema de Wedderburn só nos garante que podemos identificar matrizes da álgebra original com matrizes bloco-diagonais em uma outra álgebra que não necessariamente possui matrizes do mesmo tamanho que as originais, portanto nossa pergunta agora se torna: como obter uma matriz de mudança de base a partir do isomorfismo do Teorema de Wedderburn?

Para responder essa nova pergunta, iremos considerar subconjuntos da álgebra completa de matrizes $M_n(\mathbb{F})$ que formam álgebras, isto é, subespaços vetoriais que são fechados para produto matricial e possuam alguma unidade E, onde $\mathbb{F}$ é algebricamente fechado. Tais álgebras são chamadas de *álgebras de matrizes*, e vale notar que elas não são necessariamente subálgebras de $M_n(\mathbb{F})$, pois não precisam conter a matriz identidade I. Nosso objetivo agora é encontrar uma decomposição do espaço vetorial $\mathbb{F}^{(n)}$ como soma direta de subespaços que sejam invariantes por $\mathcal{A}$.

Começamos escrevendo nossa álgebra semissimples $\mathcal{A}$ como

$$\mathcal{A} \cong_{\mathcal{A}} \bigoplus_{i=1}^{m} \mathcal{L}_i^{(d_i)},$$

onde cada $\mathcal{L}_i$ é $\mathcal{A}$-módulo simples, e $\mathcal{L}_i \ncong \mathcal{L}_j$ se $i \neq j$. O Teorema de Wedderburn nos diz que cada $\mathcal{L}_i^{(d_i)}$ é isomorfo à $M_{d_i}(\mathbb{F})$, e portanto seus submódulos simples também devem ser isomorfos, ou seja, $\mathcal{L}_i$ é isomorfo como $\mathcal{A}$-módulo à $\mathbb{F}^{(d_i)}$, mas vimos também que qualquer $\mathcal{A}$-homomorfismo é um F-homomorfismo, ou seja, a dimensão de $\mathcal{L}_i$ como F-espaço é precisamente d_i. Agora note que a matriz identidade I pode ser escrita como

$$I = E + (I - E),$$

onde

$$(I - E)^2 = I - E \qquad \text{e} \qquad E(I - E) = 0,$$

ou seja, E e $I - E$ são duas projeções ortogonais que somam para I, implicando que podemos decompor o espaço $\mathbb{F}^{(n)}$ como soma direta de suas imagens, isto é,

$$\mathbb{F}^{(n)} = E\mathbb{F}^{(n)} \oplus (I - E)\mathbb{F}^{(n)}.$$

Como E é a unidade de $\mathcal{A}$, segue que $E\mathbb{F}^{(n)}$ é um $\mathcal{A}$-módulo, e que $\mathcal{A}(I - E)\mathbb{F}^{(n)} = \{0\}$, ou seja, ambos os somandos são $\mathcal{A}$-invariantes, o que significa que se considerarmos uma base para $\mathbb{F}^{(n)}$ formada pela união das bases para os somandos, obtemos uma base onde todas as matrizes de $\mathcal{A}$ são blocos-diagonais, com um bloco correspondendo à $E\mathbb{F}^{(n)}$, e um bloco com todas entradas iguais à zero correspondendo à $(I - E)\mathbb{F}^{(n)}$.

Podemos dizer bem mais sobre o primeiro bloco em questão. Como $E\mathbb{F}^{(n)}$ é $\mathcal{A}$-módulo, segue da Proposição 2.2.1 que ele é semissimples, ou seja, podemos decompor $E\mathbb{F}^{(n)}$ como soma direta de $\mathcal{A}$-submódulos simples (que também são subespaços), e da Proposição 2.2.3 segue que cada somando será isomorfo à algum dos $\mathcal{L}_i$ como $\mathcal{A}$-módulo, e consequentemente como F-espaço. Ou seja, existem inteiros não-negativos e_i para todo $i \in \{1, ..., m\}$ tal que

$$E\mathbb{F}^{(n)} \cong_{\mathcal{A}} \bigoplus_{i=1}^{m} \mathcal{L}_i^{(e_i)},$$

e como cada $\mathcal{L}_i$ é um F-subespaço de dimensão d_i que também é um $\mathcal{A}$-módulo, se considerarmos uma base para $E\mathbb{F}^{(n)}$ composta pela união de bases para cada um dos subespaços isomorfos à algum $\mathcal{L}_i$, obtemos que o bloco correspondente à $E\mathbb{F}^{(n)}$ estará em uma forma bloco-diagonal, com e_i blocos de tamanho $d_i \times d_i$ para cada i. Isso nos permite concluir que sempre podemos encontrar uma matriz invertível P tal que $P^{-1}\mathcal{A}P$ seja uma álgebra de matrizes bloco-diagonais, ou seja, as álgebras de matrizes semissimples são de fato aquelas para as quais é possível encontrar uma bloco-diagonalização simultânea de todos seus elementos.

3 Álgebras de Matrizes sobre $\mathbb{C}$

Este capítulo tem como objetivo principal demonstrar que certas álgebras de matrizes são semissimples, e a partir disso obter um conjunto de resultados úteis para as aplicações que serão discutidas em capítulos futuros. Alguns resultados deste capítulo serão demonstrados de mais de uma forma, e nosso objetivo é contrastar métodos elementares de demonstração com as técnicas algébricas que desenvolvemos nos últimos capítulos para ilustrar as vantagens e desvantagens destes, e como em muitos casos diferentes demonstrações servem propósitos distintos.

Denotamos a matriz identidade em $M_n(\mathbb{C})$ por I, e a matriz com todos elementos igual à 1 como J. Se n é um número natural, iremos definir o conjunto $[n] := \{1, ..., n\}$ como todos os naturais até n. Lembramos ao leitor que se V é um espaço vetorial sobre $\mathbb{C}$, e se existe função

$$\langle \cdot, \cdot \rangle : V \times V \mapsto \mathbb{C}$$

que é linear na primeira variável, satisfaz $\langle v, w \rangle = \overline{\langle w, v \rangle}$ para quaisquer v, w em V, e $\langle v, v \rangle$ é real e positivo se $v \neq 0$, então dizemos que V é um *espaço de produto interno*. Tal função determina uma *norma induzida* $||v|| := \langle v, v \rangle^{1/2}$ que mapeia elementos de V nos números reais. Se V, W são dois espaços vetoriais sobre $\mathbb{C}$ com produtos internos $\langle \cdot, \cdot \rangle_1, \langle \cdot, \cdot \rangle_2$, respectivamente, e se φ é um $\mathbb{C}$-homomorfismo entre V e W, definimos o *adjunto* φ^* de φ como o $\mathbb{C}$-homomorfismo entre W e V tal que para quaisquer v em V e u em W vale que

$$\langle v, \varphi^*(u) \rangle_1 = \langle \varphi(v), u \rangle_2.$$

No caso de matrizes, o adjunto de uma matriz A em $M_n(\mathbb{C})$ nada mais é que a matriz conjugada-transposta $A^* = (\overline{A})^T$. Podemos definir um produto interno para a álgebra de matrizes $M_n(\mathbb{C})$ da seguinte forma:

$$\langle A, B \rangle := \mathrm{tr}(AB^*),$$

onde tr denota o *traço* de uma matriz. Deixamos para o leitor verificar que a função acima é de fato um produto interno, e vale notar também que para qualquer matriz $A \in M_n(\mathbb{C})$, a matriz AA^* é hermitiana, ou seja, possui autovalores reais, e portanto seu traço também é um número real. Dado um subespaço W de $M_n(\mathbb{C})$, definimos

$$W^\perp := \{A \in M_n(\mathbb{C}) | \forall B \in W : \langle A, B \rangle = 0\}$$

como o subespaço ortogonal de W, e nesse caso, sempre podemos decompor

$$M_n(\mathbb{C}) = W \oplus W^\perp$$

como soma direta de espaços vetoriais, onde existem únicos operadores $P_W, P_{W^\perp}$ autoadjuntos e idempotentes – ditos projeções ortogonais – que mapeiam uma dada matriz X em sua respectiva componente em W ou $W^\perp$.

Com essa linguagem, podemos formalizar duas operações que a partir de agora serão bastante comuns: a operação de mapear um vetor $v = (v_1, ..., v_n)$ em uma matriz diagonal $\mathrm{Diag}(v)$ com entradas diagonais dadas por $v_1, ..., v_n$, e a operação de mapear uma matriz qualquer A no vetor $\mathrm{diag}(A) = (A_{11}, ..., A_{nn})$ das suas entradas diagonais. Formalmente, definimos a função

$$\mathrm{Diag} : \mathbb{C}^{(n)} \mapsto M_n(\mathbb{C}),$$

onde

$$\mathrm{Diag}(v) = \begin{pmatrix} v_1 & 0 & \dots & 0 \\ 0 & v_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & v_n \end{pmatrix},$$

e similarmente definimos a função

$$\begin{aligned} \mathrm{diag} : M_n(\mathbb{C}) &\mapsto \mathbb{C}^{(n)}, \\ \mathrm{diag}(A) &= (A_{11}, ..., A_{nn}). \end{aligned}$$

Observe que ambas são funções $\mathbb{C}$-lineares, e que $\text{Diag}^* = \text{diag}$, ou seja, uma é o adjunto da outra.

Lembramos que uma matriz hermitiana $X \in M_n(\mathbb{C})$ é dita *positiva semidefinida* (PSD) se, para qualquer vetor v em $\mathbb{C}^{(n)}$, vale que $v^*Xv \geq 0$. Equivalentemente, X possui apenas autovalores reais não-negativos, e portanto se escrevermos a diagonalização $X = U\Lambda U^*$, onde $\Lambda = \text{Diag}(\lambda_1, ..., \lambda_n)$ é matriz diagonal de autovalores e U é matriz unitária de autovetores, podemos definir

$$X^{1/2} := U\text{Diag}(\lambda_1^{1/2}, ..., \lambda_n^{1/2})U^*.$$

Note que $X^{1/2}$ é claramente hermitiana, e nesse caso segue facilmente que X é PSD se, e somente se, existe matriz B tal que $X = BB^*$, pois basta tomar $B = U\text{Diag}(\lambda_1^{1/2}, ..., \lambda_n^{1/2})$. Iremos denotar o conjunto das matrizes simétricas $n \times n$ por $\mathbb{S}^n$, e note que esse conjunto é um subespaço vetorial de $M_n(\mathbb{C})$, apesar de não ser uma álgebra, o subconjunto de $\mathbb{S}^n$ formado pelas matrizes PSD será denotado por $\mathbb{S}^n_+$, e o subconjunto das matrizes positivas definidas será denotado por $\mathbb{S}^n_{++}$. O conjunto $\mathbb{S}^n_+ \subseteq \mathbb{S}^n$ não é um subespaço vetorial pois, apesar de ser fechado para soma, não é fechado para produto por escalar, mas é um *cone*, isto é, é um subconjunto fechado para produto por escalares não-negativos, e também é um conjunto *convexo*.

3.1 $*$-Álgebras

Seja $\mathcal{A}$ uma $\mathbb{C}$-subálgebra de $M_n(\mathbb{C})$, isto é, um $\mathbb{C}$-subespaço fechado para produto matricial que possui um elemento neutro multiplicativo. Dizemos que $\mathcal{A}$ é uma *$*$-álgebra* – ou *álgebra autoadjunta* – se dado qualquer elemento A de $\mathcal{A}$, o seu conjugado-transposto A^* também pertece a $\mathcal{A}$. Uma subálgebra $\mathcal{B}$ de $\mathcal{A}$ que também é fechada para o conjugado transposto é dita *$*$-subálgebra*, e um homomorfismo ϕ de álgebras é dito *$*$-homomorfismo* se $\phi(A^*) = \phi(A)^*$.

Exemplo 3.1.1. A álgebra $M_n(\mathbb{C})$ é claramente uma $*$-álgebra. Se considerarmos uma matriz $A \in M_n(\mathbb{C})$ hermitiana qualquer, o conjunto de todos os polinômios em A, isto é, expressões do tipo

$$a_0I + a_1A + a_2A^2 + ... + a_kA^k,$$

também é uma $*$-álgebra. De forma geral, se considerarmos qualquer matriz A, o conjunto de todos os polinômios em A e A^* é uma $*$-álgebra, que no caso possui elemento neutro igual à matriz identidade.

Exemplo 3.1.2. Um exemplo importante se $*$-álgebras são os centralizadores de grupos de permutação. Formalmente, um grupo de permutação nada mais é que um subgrupo do grupo formado por todas as possíveis permutações de n elementos, e existe uma correspondência natural entre os grupos de permutação e os subgrupos de $GL_n(\mathbb{C})$ formados por matrizes de permutação. Seja $G \subseteq GL_n(\mathbb{C})$ um subgrupo formado por matrizes de permutação, e considere seu centralizador $C = C_{M_n(\mathbb{C})}(G)$. Sabemos que o centralizador é um subanel de $M_n(\mathbb{C})$, e certamente também será um subespaço, ou seja, é uma subálgebra, logo resta checar se ele é fechado para conjugado-transposto. De fato, tome $A \in C$ e $P \in G$, e note que

$$A^*P = (P^*A)^* = (AP^T)^* = PA^*,$$

logo de fato C é $*$-álgebra. Um caso que será especialmente interessante nos capítulos futuros é quando consideramos o centralizador do grupo de automorfismos de um grafo G, isto é, do subgrupo de $GL_n(\mathbb{C})$ formado pelas matrizes de permutação P tal que $PAP^T = A$, onde A é a matriz de adjacência de G. O fato de que esse conjunto forma uma $*$-álgebra será útil para inferir propriedades combinatórias de certos grafos que apresentam alta regularidade.

As próximas três seções serão dedicadas à demonstração do seguinte fato: toda $*$-álgebra é semissimples, ou seja, sempre podemos bloco-diagonalizar todos os elementos de uma $*$-álgebra de forma simultânea. Iremos fornecer duas demonstrações desse fato: a primeira sendo elementar e construtiva, mas no entanto significativamente mais trabalhosa, e a segunda sendo imediata a partir dos resultados vistos no capítulo anterior, no entanto requerendo uma teoria mais intricada. Queremos justamente contrastar as diferentes demonstrações para ressaltar a utilidade da teoria desenvolvida até então: os métodos de álgebra abstrata podem parecer um tanto confusos e excessivamente gerais a primeira vista, mas muitas vezes essa compreensão abrangente da teoria nos permite demonstrar facilmente resultados cujas demonstrações elementares são significativamente mais complicadas.

3.2 Triangularização e diagonalização de álgebras comutativas

Nesta seção, iremos demonstrar alguns resultados sobre álgebras comutativas que serão uteis nas próximas seções. As demonstrações utilizarão somente conceitos de álgebra linear básica, mas em muitos casos os resultados também irão seguir imediatamente dos fatos vistos no capítulos anterior. Primeiro, iremos mostrar que toda álgebra comutativa de matrizes em $M_n(\mathbb{C})$ pode ser simultaneamente triangularizada, isto é, existe base ortogonal onde todas as matrizes da álgebra estão na forma triangular superior. Daí, iremos concluir que toda $*$-álgebra comutativa pode ser simultaneamente diagonalizada, ou seja, existe base comum de autovetores para todas as matrizes da álgebra.

Proposição 3.2.1. Se A é um matriz em $M_n(\mathbb{C})$, então existe base ortogonal tal que A é triangular superior.

Demonstração. Iremos demonstrar o resultado por indução em n. O caso com $n = 1$ é imediato, portanto assuma como hipótese que para qualquer $k < n$, existe base ortogonal $\{v_1, ..., v_k\}$ tal que

$$Av_i \in \text{span}_{\mathbb{C}}(v_1, ..., v_i),$$

para todo $i \in [k]$ – note que tal hipótese é naturalmente equivalente à existência de uma base em que A é triangular superior. Agora para o caso geral, como $\mathbb{C}$ é algebricamente fechado, existe autovetor v_1 com autovalor λ_1 de A, portanto podemos escrever

$$\mathbb{C}^{(n)} = \mathbb{C}v_1 \oplus W,$$

onde $W = (\mathbb{C}v_1)^{\perp}$. Daí consideramos a projeção ortogonal P_W de $\mathbb{C}^{(n)}$ em W, e notamos que $P_W A$ é endomorfismo em W, logo aplicamos indução para obter uma base ortogonal $\{v_2, ..., v_n\}$ tal que

$$(P_W A)v_i \in \text{span}_{\mathbb{C}}(v_2, ..., v_i),$$

para qualquer $i \in \{2, ..., n\}$. Em conjunto com a projeção ortogonal P em $\mathbb{C}v_1$, obtemos que para qualquer $v_i \in \{v_1, ..., v_n\}$,

$$Av_i = ((P + P_W)A)v_i = PAv_i + P_W Av_i,$$

onde $PAv_i \in \mathbb{C}v_1$ e $P_W Av_i \in \text{span}_{\mathbb{C}}(v_2, ..., v_i)$, logo

$$Av_i \in \text{span}_{\mathbb{C}}(v_1, v_2, ..., v_i),$$

como queríamos. ■

Isto nos mostra que sempre podemos encontrar uma base onde uma dada matriz de $M_n(\mathbb{C})$ está na forma triangular superior. Em outras palavras, isso nos diz que para qualquer matriz $A \in M_n(\mathbb{C})$ existe uma matriz unitária U tal que U^*AU está em uma forma triangular superior.

Antes de provarmos o resultado geral, iremos precisar de dois resultados auxiliares que são provados a seguir.

Lema 3.2.2. Seja A uma matriz em $M_n(\mathbb{C})$, e W um subespaço A-invariante de $\mathbb{C}^{(n)}$. Então existe autovetor de A em W.

Demonstração. Seja $B = (v_1 \quad v_2 \quad \dots \quad v_k)$ matriz $n \times k$ com uma base para W em suas colunas, onde k é a dimensão de W. O fato de W ser A invariante equivale a dizer que

$$AB = BC,$$

onde C é alguma matriz $k \times k$ com os coeficientes da aplicação de A em cada um dos elementos da base de W. A matriz C pode ser vista como um endomorfismo em $\mathbb{C}^k$, logo existe autovetor $v \in \mathbb{C}^k$ com autovalor λ para C, portanto

$$ABv = BCv = \lambda Bv,$$

logo Bv é autovetor de A com autovalor λ. ■

Lema 3.2.3. Se $\{A_1, ..., A_d\}$ é um conjunto de matrizes em $M_n(\mathbb{C})$ que comutam entre si, então existe vetor v que é autovetor comum de todas as matrizes.

Demonstração. Faremos indução em d. No caso base, note que como A_1 e A_2 comutam, temos que se v é autovetor de A_1 com autovalor λ, então para qualquer k

$$A_1(A_2^k v) = A_2^k(A_1 v) = \lambda(A_2^k v),$$

logo $A_2^k v$ é autovetor de A_1. Portanto, consideramos o espaço

$$W = \text{span}_{\mathbb{C}}(v, A_2 v, A_2^2 v, ...),$$

que por construção é A_2-invariante, logo pelo lema anterior contém autovetor de A_2, mas como todo elemento de W também é autovetor de A_1, obtemos um autovetor em comum. Para o caso geral, basta usar indução para encontrar um autovetor comum de $A_1, ..., A_{d-1}$, e então aplicar o mesmo raciocínio em

$$W = \text{span}_{\mathbb{C}}(v, A_d v, A_d^2 v, ...),$$

assim obtendo um autovetor comum para $A_1, ..., A_d$. ■

Agora estamos prontos para demonstrar o resultado principal desta seção:

Teorema 3.2.4. Toda álgebra comutativa $\mathcal{A}$ de matrizes em $M_n(\mathbb{C})$ pode ser simultâneamente triangularizada por uma base ortogonal. Em outras palavras, existe matriz unitária U tal que as matrizes de $U^*\mathcal{A}U$ estão todas na forma triangular superior.

Demonstração. Seja $\{A_1, ..., A_d\}$ uma base para $\mathcal{A}$. Iremos fazer indução na dimensão n de $M_n(\mathbb{C})$. O caso base é imediato, e para o caso geral nós primeiro encontramos um autovetor v_1 comum para $A_1, ..., A_d$ utilizando o lema anterior, e daí decompomos o espaço como

$$\mathbb{C}^{(n)} = \mathbb{C}v_1 \oplus W,$$

onde $W = (\mathbb{C}v_1)^{\perp}$. Note então que cada matriz A_i pode ser escrita com respeito à uma base formada por v_1 e uma base para W, e tal matriz será da forma

$$A_i = \begin{pmatrix} \lambda_i & a_i \\ 0 & A_i' \end{pmatrix},$$

onde λ_i é o autovalor de A_i associado à v_1, a_i é um vetor linha de dimensão $n-1$, e 0 é o vetor de dimensão $n-1$ com todas as entradas iguais à zero. Como cada A_i comuta com cada A_j, segue que cada A_i' comuta com cada A_j', e daí podemos aplicar indução para encontrarmos uma base ortogonal $\{v_2, ..., v_k\}$ para W tal que para quaisquer i, j em $[d]$,

$$A_i' v_j \in \text{span}_{\mathbb{C}}(v_2, ..., v_j),$$

logo aplicando o mesmo raciocínio da demonstração da Proposição 3.2.1 – e notando que os A_i' serão precisamente a projeção ortogonal de A_i em W –, obtemos que

$$A_i v_j \in \text{span}_{\mathbb{C}}(v_1, ..., v_j),$$

para quaisquer i, j em $[d]$. Ou seja, existe uma base ortogonal para as matrizes $A_1, ..., A_d$ onde todas estão na forma triangular superior, como queríamos. ■

Também é comum encontrar versões do resultado anterior enunciadas em termos de uma família comutativa de matrizes, isto é, um conjunto $\{A_i\}$ arbitrário de matrizes em $M_n(\mathbb{C})$, mas note que o resultado em questão implica essas outras versões imediatamente: basta considerar a álgebra gerada pela família, que será uma subálgebra de $M_n(\mathbb{C})$ de dimensão finita, e daí basta aplicar o nosso resultado em uma base. No caso particular de $*$-álgebras comutativas, obtemos o seguinte corolário.

Corolário 3.2.5. Toda $*$-álgebra comutativa $\mathcal{A}$ de matrizes em $M_n(\mathbb{C})$ possui base ortogonal comum de autovetores. Em outras palavras, existe matriz unitária U tal que as matrizes de $U^*\mathcal{A}U$ estão todas na forma diagonal.

Demonstração. Basta observar que a base ortogonal que obtemos que coloca uma matriz normal A na forma triangular superior é precisamente uma base de autovetores para a mesma, isto é, ela se encontra em sua forma diagonal. Isso se deve ao fato de que, se um subespaço W qualquer é A-invariante, então $W^\perp$ é também A^*-invariante, mas em especial o subespaço gerado por um autovetor de A será invariante tanto por A quanto por A^* pois A é normal, logo $W^\perp$ será A-invariante. Portanto, a demonstração da existência da base que triangulariza a matriz se torna precisamente a demonstração do Teorema Espectral para matrizes normais sobre $\mathbb{C}$, e como o teorema anterior nos garante a existência de uma base comum que triangulariza todas as matrizes da família, segue que todas estão em sua forma diagonal. ■

3.3 Semissimplicidade de $*$-álgebras

Agora estamos prontos para exibir a demonstração elementar do resultado principal deste capítulo: toda $*$-álgebra é semissimples. Para isso, primeiro vamos exibir duas demonstrações diferentes para um resultado geral sobre álgebras de matrizes com respeito ao produto de Schur, e daí concluíremos que toda $*$-álgebra comutativa é semissimples, e isso por sua vez implicará o resultado desejado. A primeira demonstração é quase imediata, mas requer um conhecimento adicional acerca das caracterizações de semissimplicidade e sobre o radical de Jacobson, já a demonstração 2, apesar de um pouco mais trabalhosa, nos permite construir de maneira mais explícita os elementos da base de matrizes 01 para a álgebra em questão.

Lema 3.3.1. Se $\mathcal{A} \subseteq M_n(\mathbb{C})$ é uma álgebra de matrizes com respeito ao produto de Schur, isto é, ao produto termo a termo de matrizes, então existe única base de matrizes 01 para $\mathcal{A}$. Em particular, toda álgebra de matrizes diagonais possui uma única base de matrizes diagonais 01.

Demonstração 1. Seja $\mathcal{A}$ uma álgebra de matrizes com respeito ao produto de Schur, isto é, para quaisquer $A, B \in \mathcal{A}$, o produto $A \circ B \in \mathcal{A}$, onde $(A \circ B)_{ij} = A_{ij}B_{ij}$. Denote por $A^{\circ k}$ o produto de Schur de uma matriz A consigo mesma k vezes, e note que $A_{ij}^{\circ k} = A_{ij}^k$, logo se $A \in \mathcal{A}$ é um elemento nilpotente, segue que $A = 0$, logo $J(\mathcal{A}) = \{0\}$, implicando que $\mathcal{A}$ é semissimples. Isso mostra que toda álgebra de matrizes com respeito ao produto de Schur é semissimples, e portanto podemos considerar seus idempotentes centralmente primitivos $A_1, ..., A_d$ tais que

$$E = A_1 + \ldots + A_d,$$

mas note que as matrizes A_i são idempotentes com respeito ao produto de Schur, logo $A_i \circ A_i = A_i$, implicando que as matrizes A_i são 01. Toda álgebra de matrizes com respeito ao produto de Schur é comutativa, logo pelo Teorema 2.4.3 segue que os idempotentes $A_1, ..., A_d$ formam uma base para $\mathcal{A}$, e a unicidade de tal base também segue da unicidade dos idempotentes. ■

Demonstração 2. Seja $A_1, ..., A_d$ uma base para a álgebra $\mathcal{A}$. Por definição, $\mathcal{A}$ é fechada para o produto de Schur e para somas de seus elementos, portanto se $p(x) = a_0 + a_1x + ... + a_nx^n$ é um polinômio com coeficientes em $\mathbb{C}$, a expressão

$$p(A) = a_0E + a_1A + ... + a_nA^{\circ n}$$

será elemento de $\mathcal{A}$ para qualquer elemento A pertencente à álgebra, e note que $p(A)_{ij} = p(A_{ij})$ pois se trata do produto de Schur. Logo podemos definir para qualquer entrada A_{ij} de A um polinômio p_{ij} que leva A_{ij} em 1, e as demais entradas em 0, de modo que $p_{ij}(A)$ é uma matriz 01. Aplicando esse procedimento nas matrizes $A_1, ..., A_d$, obtemos um conjunto de matrizes 01 que geram $\mathcal{A}$ como espaço vetorial, e portanto podemos obter disso uma base de matrizes 01. Como toda matriz 01 é idempotente com respeito ao produto de Schur, a unicidade dessa base segue de quando consideramos uma base de matrizes 01 formada por idempotentes primitivos. ■

As matrizes $A_1, ..., A_d$ da demonstração anterior formam a *base de Schur* de uma álgebra fechada para o produto de Schur, e elas serão extremamente úteis para demonstrar diversos resultados na próxima parte deste trabalho. O resultado anterior também nos garante que toda $*$-álgebra comutativa é semissimples.

Teorema 3.3.2. Toda $*$-álgebra comutativa é semissimples. Em particular, se $\mathcal{A}$ é uma $*$-álgebra comutativa de dimensão d, então existe uma matriz unitária U e uma partição $[n] = S_0 \sqcup S_1 \sqcup ... \sqcup S_d$, com $S_1, ..., S_d$ não-vazios, tal que

$$\mathcal{A} = U\{\lambda_1 I_1 + ... + \lambda_d I_d | \lambda_i \in \mathbb{C}\}U^*,$$

onde cada I_i é a matriz diagonal com uns nas posições de S_i e zeros nas demais.

Demonstração. Note que se $A \in \mathcal{A}$, então $A^* \in \mathcal{A}$ por definição, e como a álgebra é comutativa, segue que A é normal. Se fixarmos uma base para $\mathcal{A}$, isso implica que tal base é composta por matrizes normais que comutam, logo o Corolário 3.2.5 nos garante que existe matriz U que simultaneamente diagonaliza todas as matrizes da base, e consequentemente todas as matrizes de $\mathcal{A}$. O Lema 3.3.1 nos diz que podemos tomar uma base $I_1, ..., I_d$ de matrizes diagonais 01 com suporte disjunto, portanto basta definir S_i como o conjunto de índices das respectivas entradas não-nulas de I_i, e S_0 como o conjunto dos índices de $[n]$ que correspondem à entradas nulas em todos os elementos da base, ou seja, $I_0 = I - (I_1 + ... + I_d)$. Assim obtemos uma partição $[n] = S_0 \sqcup S_1 \sqcup ... \sqcup S_d$, e todo elemento de $\mathcal{A}$ será combinação linear de $I_1, ..., I_d$. ■

Note que as matrizes $E_1, ..., E_d$, onde $E_i = UI_iU^*$, obtidas a partir das matrizes do teorema anterior são os idempotentes centralmente primitivos de $\mathcal{A}$, pois $E_iE_j = \delta_{ij}E_i$, $E_1 + ... + E_d$ é a sua unidade, e a dimensão da álgebra é precisamente d. Além disso, a construção nos garante que cada E_i é uma matriz PSD, pois cada I_i também é e os E_i's são obtidos a partir de uma mudança de base ortogonal. Note também que $S_0 = \emptyset$ implica que $I \in \mathcal{A}$, e nesse caso a álgebra $\mathcal{A}$ será uma subálgebra de $M_n(\mathbb{C})$.

Com isso, estamos prontos para demonstrar o teorema principal desta seção. Primeiro iremos exibir uma demonstração construtiva e elementar devido à Bachoc et al. (2012), e então exibiremos duas demonstrações que dependem fortemente dos conceitos desenvolvidos no capítulo anterior acerca de álgebras semissimples e suas diversas caracterizações.

Teorema 3.3.3. Toda $*$-álgebra $\mathcal{A}$ de $M_n(\mathbb{C})$ é semissimples. Em particular, podemos escrever

$$\mathcal{A} = \bigoplus_{i=1}^{m} \mathcal{A}E_i,$$

onde as matrizes E_i são os idempotentes centralmente primitivos de $\mathcal{A}$.

Demonstração 1 (Teorema 9.1, Bachoc et al. (2012)). Para mostrarmos o resultado iremos seguir a seguinte estratégia: primeiro vamos considerar uma $*$-subálgebra maximal contida em $\mathcal{A}$ e obter seus idempotentes minimais, depois vamos construir uma relação de equivalência a partir desse conjunto de idempotentes, e então finalmente vamos obter os idempotentes centralmente primitivos de $\mathcal{A}$ a partir das classes de equivalência dessa relação.

Começamos com $\mathcal{B} \subseteq \mathcal{A}$ uma $*$-subálgebra comutativa maximal – e note que $Z(\mathcal{A}) \subseteq \mathcal{B}$. Primeiro mostramos que $C_{\mathcal{A}}(\mathcal{B}) \subseteq \mathcal{B}$, isto é, $\mathcal{B}$ contém todas as matrizes que comutam com todos os seus elementos. De fato, seja $A \in C_{\mathcal{A}}(\mathcal{B})$ uma matriz no centralizador da subálgebra, e considere as seguintes possibilidades:

(i) Se A é normal, note que caso $A \notin \mathcal{B}$ então a álgebra gerada por $\mathcal{B} \cup \{A, A^*\}$ é uma $*$-subálgebra comutativa que contém estritamente $\mathcal{B}$, contrairando sua maximalidade

(ii) Se A não é normal, podemos considerar a matriz $A + A^*$, que certamente é normal, e portanto pelo mesmo argumento feito no item anterior vale que $A + A^*$ pertence à $\mathcal{B}$. Mas então como $A \in C_{\mathcal{A}}(\mathcal{B})$, teríamos que $A(A + A^*) = (A + A^*)A$, implicando que A é normal e nos levando à uma contradição

Portanto concluímos que $\mathcal{B}$ contém seu centralizador. Utilizando o Teorema 3.3.2, podemos obter uma matriz unitária U que, após substituir $\mathcal{A}$ por $U^*\mathcal{A}U$, nos permite assumir sem perda de generalidade que $\mathcal{B}$ está na forma diagonal, com idempotentes minimais dados pelas matrizes $I_0, I_1, ..., I_d$ com entradas 01 que formam uma base ortogonal para $\mathcal{B}$, e com partição $[n] = S_0 \sqcup S_1 \sqcup ... \sqcup S_d$. Como a unidade em $\mathcal{B}$ é a mesma que em $\mathcal{A}$, segue que $I_1 + ... + I_d$ é a unidade de $\mathcal{A}$, mas vale notar que em geral as matrizes I_i não precisam pertencer

ao centro de $\mathcal{A}$, simplesmente pois $Z(\mathcal{A}) \subseteq Z(\mathcal{B})$, ou seja, as matrizes I_i ainda não são os idempotentes centralmente primitivos de $\mathcal{A}$, e para obtê-los precisaremos de um pouco mais de esforço.

Agora iremos fixar $A \in \mathcal{A}$, e definir as matrizes A_{ij}, com $i, j \in \{0, ..., d\}$ e de tamanho $|S_i| \times |S_j|$, dadas pelas restrições de $I_i A I_j$ nas linhas de S_i e nas colunas de S_j. Observamos que:

(i) $A_{00} = 0$, e A_{ii} é um múltiplo da matriz identidade em $M_{|S_i|}(\mathbb{C})$. Para ver isso, primeiro notamos que a matriz $I_i A I_i$ é uma matriz diagonal com entradas não-nulas dadas pelas entradas diagonais de A indexadas por S_i, e também que, se $i \neq j$,

$$(I_i A I_i) I_j = 0 = I_j (I_i A I_i),$$

logo $I_i A I_i$ comuta com a base de $\mathcal{B}$, e daí segue que $I_i A I_i \in C_{\mathcal{A}}(\mathcal{B}) \subseteq \mathcal{B}$. No caso de $I_0 A I_0$, como $I_0 \mathcal{B} I_0 = \{0\}$, obtemos que $I_0 A I_0 = 0$. Para os demais i, como a base é formada por matrizes diagonais com suporte disjunto, temos que os coeficientes de $I_i A I_i$ com respeito à base $I_1, ..., I_d$ serão nulos para quaisquer $j \neq i$, ou seja, $I_i A I_i$ é de fato múltiplo de I_i, e sua restrição em $M_{|S_i|}(\mathbb{C})$ será um múltiplo da matriz identidade.

(ii) A_{ij} é igual à zero ou é um múltiplo positivo de uma matriz unitária, e nesse caso as cardinalidades dos S_i são iguais. De fato, tome A_{ij} não-nulo e assuma sem perda de generalidade que $|S_i| \geq |S_j|$, e note que

$$(I_i A I_j)(I_i A I_j)^* = I_i (A I_j A^*) I_i,$$

logo por (i) segue que $(A I_j A^*)_{ii}$ é múltiplo da identidade $M_{|S_i|}(\mathbb{C})$, implicando que $A_{ij} A_{ij}^*$ também é, portanto $\mathrm{rk}(A_{ij}) = |S_i|$, mas por outro lado, $\mathrm{rk}(A_{ij}) \leq |S_j|$, logo $|S_i| = |S_j|$ e então as matrizes A_{ij} são quadradas para quaisquer i, j. Isso implica que $A_{ij} A_{ij}^*$ é uma matriz PSD, e então deve ser um múltiplo real positivo – que chamaremos de α – da identidade em $M_{|S_i|}(\mathbb{C})$, e então $\sqrt{\alpha} A_{ij}$ é uma matriz unitária, fazendo com que A_{ij} seja claramente um múltiplo positivo de uma matriz unitária.

Com essas observações, avançaremos para a parte final da demonstração. Iremos definir uma relação $\sim$ no conjunto $[d]$ da seguinte forma: $i \sim j$ se e somente se $I_i \mathcal{A} I_j \neq \{0\}$, ou seja, o índice i é relacionado com o índice j se e somente se existe alguma matriz A de $\mathcal{A}$ tal que a matriz formada pelas linhas de A indexadas por S_i e as colunas de A indexadas por S_j não seja toda nula. A relação é reflexiva devido à observação (i), e também é simétrica pois $\mathcal{A}$ é $*$-álgebra logo $I_i \mathcal{A} I_j = (I_j \mathcal{A} I_i)^*$. A transitividade é consequência da observação (ii): se $i \sim j$ e $j \sim k$, segue que existem matrizes $A, B \in \mathcal{A}$ tais que $I_i A I_j$ e $I_j B I_k$ são não-nulas, e portanto A_{ij}, B_{jk} são múltiplos positivos de matrizes unitárias de mesmo tamanho (pois $|S_i| = |S_j| = |S_k|$), e então o produto $A_{ij} B_{jk}$ é uma matriz unitária, fazendo com que

$$0 \neq (I_i A I_j)(I_j B I_k) = I_i (A I_j B) I_k \in I_i \mathcal{A} I_k,$$

logo $i \sim k$.

Agora considere $\{E_1, ..., E_m\} = \{\sum_{j \sim i} I_j | i \in [d]\}$ como as matrizes diagonais 01 induzidas pela relação de equivalência $\sim$ nos idempotentes minimais de $\mathcal{B}$. Afirmamos que as matrizes E_i são os idempotentes centralmente primitivos de $\mathcal{A}$. De fato, primeiro temos por construção que $E_1 + ... + E_m$ é a unidade em $\mathcal{A}$, e que se $i \neq j$, então $E_i \mathcal{A} E_j = \{0\}$ – em particular $E_i E_j = 0$ –, logo se $A \in \mathcal{A}$, temos

$$\begin{aligned} AE_i &= (\sum_j E_j)AE_i \\ &= \sum_j E_j AE_i \\ &= E_i AE_i \\ &= E_i AE_i + \sum_{j\neq i} E_i AE_j \\ &= \sum_j E_i AE_j \\ &= E_i A(\sum_j E_j) \\ &= E_i A, \end{aligned}$$

implicando que cada $E_i \in Z(\mathcal{A})$, e como cada E_i é uma soma de idempotentes minimais de $\mathcal{B}$, isso nos da que eles são idempotentes e primitivos, e também obtemos que cada E_i é uma matriz hermitiana. Obtemos então a seguinte decomposição de $\mathcal{A}$

$$\mathcal{A} = \bigoplus_{i=1}^{m} \mathcal{A}E_i.$$

Os conjuntos $\mathcal{A}E_i$ são $\mathcal{A}$-submódulos por construção, a soma é direta pois os submódulos são escritos em termos de idempotentes ortogonais, e os submódulos são simples pois cada E_i é primitivo, logo $\mathcal{A}$ é semissimples, como queríamos. ■

A demonstração em questão interessante por diversos motivos, mas talvez o principal deles é o fato de se tratar de uma demonstração construtiva, onde os idempotentes centralmente primitivos da álgebras são construídos a partir de uma subálgebra comutativa maximal, e isso implica que os idempotentes em questão serão matrizes hermitianas. É possível encontrar uma $*$-subálgebra comutativa maximal em tempo linear na dimensão da álgebra $\mathcal{A}$, ou seja, a demonstração nos dá um algoritmo eficiente para encontrar os idempotentes da álgebra, e a partir destes idempotentes é possível se obter uma base bloco-diagonal para todas a matrizes da álgebra, algo que será particularmente útil para alguns problemas de otimização que veremos em próximos capítulos. Agora prosseguimos com as demais demonstrações.

Demonstração 2. Seja $\mathcal{A}$ uma $*$-álgebra, e seja $\mathcal{B} \subseteq \mathcal{A}$ um $\mathcal{A}$-submódulo. Sabemos que $\mathcal{B}$ também é um subespaço vetorial de $\mathcal{A}$, portanto podemos decompor

$$\mathcal{A} = \mathcal{B} \oplus \mathcal{B}^{\perp},$$

onde $\mathcal{B}^{\perp}$ é o complemento ortogonal de $\mathcal{B}$ em $\mathcal{A}$. Fixe $X \in \mathcal{B}^{\perp}$, e tome um elemento $A \in \mathcal{A}$ qualquer, logo para qualquer $B \in \mathcal{B}$

$$\begin{aligned} \langle AX, B\rangle &= \operatorname{tr}(AXB^*) \\ &= \operatorname{tr}(XB^*A) \\ &= \operatorname{tr}(X(A^*B)^*) \\ &= \langle X, A^*B\rangle. \end{aligned}$$

Como $A \in \mathcal{A}$, segue que $A^* \in \mathcal{A}$, e como $\mathcal{B}$ é $\mathcal{A}$-submódulo, segue que $A^*B \in \mathcal{B}$. Portanto $\langle X, A^*B\rangle = 0$, e disso temos que $\langle AX, B\rangle = 0$, ou seja, $\mathcal{B}^{\perp}$ também é $\mathcal{A}$-submódulo. Logo, concluímos que todo $\mathcal{A}$-submódulo de $\mathcal{A}$ é somando direto, e então pela Proposição 2.1.2 segue que $\mathcal{A}$ é semissimples. ■

Demonstração 3. Seja $\mathcal{A}$ uma $*$-álgebra, e tome um elemento $A \in J(\mathcal{A})$ em seu radical de Jacobson. Como o radical é um ideal, vale que $A^*A \in J(\mathcal{A})$, e da Proposição 2.3.2 sabemos que isso implica que existe um

natural r tal que $(A^*A)^r = 0$. Por outro lado, note que A^*A é matriz hermitiana, logo existem projetores ortogonais E_θ para todo θ autovalor de A^*A tais que

$$A^*A = \sum_\theta \theta E_\theta$$

logo

$$(A^*A)^r = \sum_\theta \theta^r E_\theta.$$

Em particular, se tomarmos um autovetor v não-nulo associado a um autovalor θ qualquer, vale que

$$0 = (A^*A)^r v = \theta^r v,$$

mas isso ocorre se, e somente se, $\theta = 0$, implicando que $A^*A = 0$. Tome então um vetor v não-nulo, e note que $(Av)^*(Av) = 0$ se, e somente se, $Av = 0$, mas $(Av)^*(Av) = v^*(A^*A)v = 0$, logo $Av = 0$ para qualquer vetor do espaço, e portanto $A = 0$. Isso implica que o radical de Jacobson de $\mathcal{A}$ é trivial, e portanto pelo Teorema 2.3.3 segue que $\mathcal{A}$ é semissimples. ■

As duas últimas demonstrações, quando vistas de forma isoladas, são concisas e simples, mas implicitamente escondem uma teoria extremamente rica e complexa que foi parcialmente discutida no capítulo anterior. Por outro lado, elas não nos fornecem uma construção tão explícita dos submódulos simples e dos idempotentes minimais da álgebra em questão, algo que é essencial para quaisquer aplicações algorítmicas destes tipos de problemas. As diferenças entre as três demonstrações em questão são justamente o motivo pelo qual decidimos as exibir: cada uma ilustra uma faceta diferente da teoria de álgebras de matrizes, e em conjunto a compreensão de todas essas técnicas enriquece o entendimento de problemas deste tipo, tanto do ponto de vista matemático quanto computacional.

Referências bibliográficas

S. Axler. *Linear Algebra Done Right*. Undergraduate Texts in Mathematics. Springer International Publishing, 2014. ISBN 9783319110806. URL https://books.google.com.br/books?id=5qYxBQAAQBAJ.

Christine Bachoc, Dion C. Gijswijt, Alexander Schrijver, and Frank Vallentin. *Invariant Semidefinite Programs*, pages 219–269. Springer US, New York, NY, 2012. ISBN 978-1-4614-0769-0. doi: 10.1007/978-1-4614-0769-0_9. URL https://doi.org/10.1007/978-1-4614-0769-0_9.

R. Bailey. *Association Schemes: Designed Experiments, Algebra, and Combinatorics*. Cambridge studies in advanced mathematics. Cambridge University Press, 2004. ISBN 9780521824460. URL https://books.google.com.br/books?id=CSxwnQEACAAJ.

G. Chen and I. Ponomarenko. Lectures on coherent configurations, October 2023. URL https://www.pdmi.ras.ru/~inp/ccNOTES%20(13.12.23).pdf.

P.M. Cohn. *Basic Algebra: Groups, Rings and Fields*. Springer London, 2012. ISBN 9781447110606. URL https://books.google.com.br/books?id=OrSrngEACAAJ.

C.W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras*. AMS Chelsea Publishing Series. Interscience Publishers, 1966. ISBN 9780821869451. URL https://books.google.com.br/books?id=RKwjeZKMr8oC.

Marcel K. de Carli Silva, Gabriel Coutinho, Chris Godsil, and David E. Roberson. Algebras, graphs and thetas. *Electronic Notes in Theoretical Computer Science*, 346:275–283, August 2019. ISSN 1571-0661. doi: 10.1016/j.entcs.2019.08.025. URL http://dx.doi.org/10.1016/j.entcs.2019.08.025.

B. Farb and R.K. Dennis. *Noncommutative Algebra*. Graduate Texts in Mathematics. Springer New York, 2012. ISBN 9781461208891. URL https://books.google.com.br/books?id=sELhBwAAQBAJ.

C. Godsil. *Algebraic Combinatorics*. Chapman Hall/CRC Mathematics Series. Taylor & Francis, 1993. ISBN 9780412041310. URL https://books.google.com.br/books?id=eADtlNCkkIMC.

C. Godsil. Association schemes, June 2010. URL https://www.math.uwaterloo.ca/~cgodsil/pdfs/assoc2.pdf.

Richard M. Karp. *Reducibility among Combinatorial Problems*, pages 85–103. Springer US, Boston, MA, 1972. ISBN 978-1-4684-2001-2. doi: 10.1007/978-1-4684-2001-2_9. URL https://doi.org/10.1007/978-1-4684-2001-2_9.

T.Y. Lam. *A First Course in Noncommutative Rings*. Graduate Texts in Mathematics. Springer New York, 2013. ISBN 9781441986160. URL https://books.google.com.br/books?id=2T5DAAAAQBAJ.

S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005. ISBN 9780387953854. URL https://books.google.com.br/books?id=Fge-BwqhqIYC.

L. Mendonça. Notas de aula em Álgebra não-comutativa, Novembro 2023. URL https://drive.google.com/file/d/1LptQLQFRXwTWsqxDMRk8ReSHNkFZhucO/view.

D.S. Passman. *A Course in Ring Theory*. AMS Chelsea Publishing Series. AMS Chelsea Pub., 2004. ISBN 9780821836804. URL https://books.google.com.br/books?id=OKvQDgAAQBAJ.

Nathan Benedetto Proença, Marcel K. de Carli Silva, Cristiane M. Sato, and Levent Tunçel. A primal-dual extension of the goemans–williamson algorithm for the weighted fractional cut-covering problem, 2023.

A.C. Vieira and R.B. Santos. *PI-álgebras: uma introdução à PI-teoria*. 33º Colóquio Brasileiro de Matemática. IMPA, 2021. ISBN 9786589124375. URL https://coloquio33.impa.br/pdf/33CBM11-eBook-preview.pdf.