Mateus Medeiros Teixeira

O Teorema de Estrutura para Anéis Primitivos

Curso de Matemática - Habilitação Licenciatura
Departamento de Matemática
Centro de Ciências Físicas e Matemáticas
Universidade Federal de Santa Catarina

Professora Orientadora: Virgínia Silva Rodrigues

Florianópolis - SC
2009

Esta Monografia foi julgada adequada como TRABALHO DE CONCLUSÃO DE CURSO no Curso de Matemática - Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº 08/CCM/09

Profª Carmem Suzane Comitre Gimenez

Professora da disciplina

Banca Examinadora:

Virgínia Silva Rodrigues

Orientadora

Daniel Gonçalves

Danilo Royer

Agradecimentos

Primeiramente agradeço a Deus pelos momentos de inspiração na realização deste trabalho.

A professora Virgínia Silva Rodrigues pela dedicação, orientação e conselhos, os quais comtribuíram muito para a realização deste trabalho.

Aos professores da banca que dispuseram-se a ler este trabalho. E aos professores que tanto me ensinaram ao longo desses 4 anos.

A meus pais, minha irmã e minha namorada pelo apoio e carinho incondicional.

Aos amigos que ao longo dessa jornada compreenderam e ajudaram sempre que possível.

Sumário

Introdução **5**

1 Módulos **7**

1.1 Módulos . . . 7
1.2 Submódulos . . . 9
1.3 Módulos Quocientes . . . 12
1.4 Homomorfismos . . . 13
1.5 Soma Direta Interna . . . 16
1.6 Sequências Exatas . . . 18

2 Anéis Semi-simples e Radical de Jacobson **22**

2.1 Condições de Cadeia . . . 22
2.2 Módulos Semi-simples . . . 24
2.3 Anéis Semi-simples . . . 25
2.4 Radical de Jacobson . . . 27

3 Anéis Primos e Semiprimos **32**

3.1 Ideais Primos . . . 32
3.2 Ideais Semiprimos, Anéis Primos e Semiprimos . . . 35

4 Teorema de Estrutura para Anéis Primitivos à Esquerda **38**

4.1 Anéis Primitivos e Semiprimitivos . . . 38
4.2 O Teorema de Estrutura . . . 40

Conclusão **48**

Referências **49**

Introdução

A teoria moderna de anéis começou quando J. H. M. Wedderburn demonstrou seu famoso teorema de estrutura para álgebras semi-simples de dimensão finita sobre corpos, em 1907. Vinte anos mais tarde, E. Noether e E. Artin introduziram as condições de cadeia ascentente e de cadeia descendente sobre ideais unilaterais, substituindo a dimensão finita, e Artin provou o análogo do teorema de Wedderburn para anéis (álgebras) semi-simples. Esta teoria passou a ser, desde então, a pedra fundamental da teoria de anéis não-comutativos.

Neste trabalho, estudamos o teorema de estrutura para anéis primitivos que é uma generalização do teorema de Wedderburn-Artin. A grosso modo, este teorema de estrutura diz que um anel primitivo à esquerda A (isto é, um anel que possui um módulo à esquerda simples e fiel), é isomorfo a um anel denso das transformações lineares sobre um A-módulo simples e fiel.

Além deste isomorfismo, o teorema garante que se A é artiniano à esquerda então $dim_k(V) = n < \infty$ e $A \cong M_n(k)$, onde k é um anel de divisão, enunciado que nos lembra o teorema de Wedderburn-Artin para anéis artinianos à esquerda simples. E se A não é artiniano à esquerda, então $dim_k(V)$ é infinita e existem um subanel A_n de A e um homomorfismo sobrejetor de A_n para $M_n(k)$.

Além da demonstração do teorema de estrutura, objetivamos estudar alguns tópicos da teoria de anéis e módulos. Dentre os tópicos estudados, estão os anéis e módulos simples e semi-simples, anéis J-semi-simples (ou Jacobson semi-simples, ou semiprimitivo), anéis e ideais primos e semiprimos e anéis primitivos à esquerda (à direita). Visamos estudar suas caracterizações e as relações existentes entre eles.

Durante o trabalho, pressupomos que o leitor esteja familiarizado com teoria de anéis. Salientamos também que em todo trabalho, A é um anel com *unidade* não *necessariamente comutativo*. Esta informação é importante pois não a repetimos durante o trabalho. Por fim, apresentamos um breve resumo desse trabalho.

Colocamos um primeiro capítulo sobre teoria geral de módulos, introduzimos definições, exemplos e resultados importantes para o desenvolvimento deste trabalho.

No segundo capítulo, estudamos as classes de anéis semi-simples e J-semi-simples. Tratamos brevemente anéis com condição de cadeia ascendente e descendente.

No terceiro capítulo, definimos anéis e ideais primos e semiprimos. Estudamos as relações existentes entre esses anéis e as relações com as estruturas já estudadas anteriormente.

No nosso último capítulo, desenvolvemos alguns resultados, como o Teorema da Densidade de Jacobson-Chevalley e alguns outros pré-requisitos para a demonstração do teorema de estrutura para anéis primitivos à esquerda.

Capítulo 1

Módulos

Neste capítulo, definimos módulos e apresentamos uma série de exemplos afim de tornar clara ao leitor essa estrutura. A grosso modo, os módulos são uma generalização de espaços vetoriais, onde ao invés de corpos, usamos anéis para o conjunto de escalares. A teoria de módulos está fortemente relacionada com a teoria de anéis e grupos, e isso se reflete, como o leitor poderá constatar, em diversos teoremas existentes para anéis e grupos, que mediante "modificações", são provados para módulos.

1.1 Módulos

Definição 1.1 *Seja M um conjunto não vazio munido de uma operação soma*

$$\begin{array}{rccc} +: & M \times M & \to & M \\ & (x, y) & \mapsto & x + y. \end{array}$$

M com a operação $+$ é dito um grupo se as propriedades a seguir são válidas:
(i) *a associatividade da soma: $(x+y)+z = x+(y+z)$, para quaisquer $x,\ y,\ z \in M$;*
(ii) *existência do elemento neutro para a soma: existe um único $0 \in M$ tal que $x + 0 = 0 + x = x$, para todo $x \in M$;*
(iii) *existência do elemento oposto: para todo $x \in M$, existe um único $y \in M$, tal que $x + y = y + x = 0$. Denotamos y por $-x$.*

M é dito grupo abeliano ou comutativo se:
(iv) *a operação $+$ é comutativa, ou seja, $x + y = y + x$, para quaisquer $x,\ y \in M$.*

Exemplo 1.2 $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *são grupos abelianos.* $(\mathbb{Z}_p - \{0\}, \cdot)$, *$p$ primo é um grupo abeliano multiplicativo.*

Definição 1.3 *Seja M um grupo abeliano. M é dito um módulo à esquerda sobre A (ou um A-módulo à esquerda) se existe uma operação de multiplicação de elementos* *de A por elementos de M tal qual a definida abaixo, satisfazendo as propriedades de* (i) - (iv) *para quaisquer $x, y \in M$ e $a, a_1 \in A$:*

$$\begin{array}{rccc} \cdot : & A \times M & \rightarrow & M \\ & (a, y) & \mapsto & a \cdot y \end{array}$$

(i) $a \cdot (a_1 \cdot x) = (a \cdot a_1) \cdot x$;

(ii) $a \cdot (x + y) = a \cdot x + a \cdot y$;

(iii) $(a + a_1) \cdot x = a \cdot x + a_1 \cdot x$;

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

De modo análogo, definimos A-módulos à direita considerando a multiplicação à direita por elementos do anel A.

Se $a \in A$ e $m \in M$, escrevemos simplesmente am para denotar o elemento $a \cdot m$.

Em todo trabalho, M é um A-módulo à esquerda. Não havendo confusão quanto a isso, escrevemos sempre M é um A-módulo. A notação ${}_AM$ (M_A) é também usada para dizer que M é um A-módulo à esquerda (à direita).

Exemplo 1.4 *O grupo trivial $\{0\}$ é um módulo sobre qualquer A-módulo.*

Exemplo 1.5 *Seja I um ideal à esquerda do anel A. Então I admite uma estrutura de A-módulo (à esquerda) com soma e multiplicação induzidos pela soma e multiplicação de A.*

De fato, dados $\alpha \in A$ e $x \in I$, temos que $\alpha x \in I$. Sendo que I é um ideal à esquerda de A, então as propriedades para que I seja um A-módulo são claramente satisfeitas.

Exemplo 1.6 *Todo grupo abeliano $(M, +)$ pode ser considerado como um módulo sobre o anel $\mathbb{Z}$ dos números inteiros definindo a multiplicação por:*

$$\begin{array}{rccl} \cdot : & \mathbb{Z} \times M & \rightarrow & M \\ & zm & \mapsto & \left\{ \begin{array}{cl} 0 & se\ z = 0 \\ \underbrace{m + \cdots + m}_{z\ vezes} & se\ z > 0 \\ \underbrace{(-m) + \cdots + (-m)}_{-z\ vezes} & se\ z < 0 \end{array} \right. \end{array}$$

para todo $z \in \mathbb{Z}$ e para todo $m \in M$.

A seguir definiremos a estrutura de bimódulo.

Definição 1.7 *Sejam R, S anéis e M um grupo abeliano (aditivo). Então, M é dito um (R, S) bimódulo se M é um R-módulo à esquerda e um S-módulo à direita.*

Aqui, cabe ressaltarmos que para quaisquer $r \in R$, $s \in S$ e $m \in M$, vale:

$$(rm)s = r(ms).$$

Exemplo 1.8 *Todo anel A é um (A, A)-bimódulo*

Exemplo 1.9 *Todo espaço vetorial sobre um corpo K é um (K, K)-bimódulo, e consequentemente, um K-módulo.*

1.2 Submódulos

Definição 1.10 *Seja M um grupo. Um subconjunto não vazio N de M é um subgrupo de M quando o conjunto N é um grupo com a operação de M.*

Proposição 1.11 *Sejam M um grupo e N um subconjunto não vazio de M. Então N é um subgrupo de M se e somente se as seguintes condições são satisfeitas:*
(i)' *$x + y \in N$, para quaisquer $x,\ y \in N$;*
(ii)' *para todo $x \in N$, existe $-x \in N$ tal que $x + (-x) = (-x) + x = 0$.*

Demonstração: De fato, se N é um subgrupo, é claro que as condições (i)' e (ii)' são válidas. Suponhamos que as condições (i)' e (ii)' sejam satisfeitas. É claro que $+$ é uma operação em N associativa. Por outro lado, dado $x \in N$, por (ii)' existe $-x \in N$ tal que $x + (-x) = (-x) + x = 0$. Por (i)', $0 \in N$. ∎

Na prática, verificamos as condições (i)' e (ii)' para mostrar que N é um submódulo de um grupo M.

Definição 1.12 *Sejam M um A-módulo e N um subconjunto não vazio de M. Então N é A-submódulo de M, ou simplesmente, um submódulo se:*
(i) *N é subgrupo aditivo de M;*
(ii) *N é fechado em relação à operação $\cdot$, isto é, dados $\alpha \in A$ e $n \in N$, tem-se que $\alpha n \in N$.*

Proposição 1.13 *Seja M um A-módulo. Um subconjunto não vazio N de M é um submódulo de M se, e somente se, as seguintes condições são satisfeitas:*
(i)' *$\forall\ n, n' \in N, n + n' \in N$;*
(ii)' *$\forall\ \alpha \in A, \forall\ n \in N$, tem-se que $\alpha n \in N$.*

Demonstração: Se N é submódulo, então (i)' e (ii)' são satisfeitas. Reciprocamente, provemos que N é submódulo de M. Claramente, $+$ é uma operação em N, pois vale (i)', que é associativa e comutativa. Como N é não vazio, existe $x \in N$. Por (ii)', $0 = 0x \in N$. Dado $y \in N$, temos que $-1 \in A$ (é o oposto de 1 em A), daí $-1y = -y \in N$. Logo, N é um subgrupo de M e por (ii)' segue que N é um submódulo de M. ■

A seguir, apresentamos alguns exemplos de submódulos de um módulo.

Exemplo 1.14 *Seja M um A-módulo. Então $\{0\}$ e M são submódulos de M chamados submódulos triviais.*

Exemplo 1.15 *Sejam N_1 e N_2 submódulos de um módulo M. Então o conjunto $N_1 + N_2 := \{n_1 + n_2 : \ n_1 \in N_1 \text{ e } n_2 \in N_2\}$ é um submódulo de M.*

De fato, $N_1 + N_2 \subset M$. Sejam $x, \ y \in N_1 + N_2$. Então, $x = x_1 + x_2$ com $x_i \in N_i$ e $y = y_1 + y_2$ com $y_i \in N_i$, para $i = 1, 2$, segue que $x + y = (x_1 + x_2) + (y_1 + y_2) = (x_1 + y_1) + (x_2 + y_2) \in N_1 + N_2$. Além disso, dado $n_1 \in N_1$ e $n_2 \in N_2$ e para todo $\alpha \in A$, segue que $\alpha n_1 \in N_1$ e $\alpha n_2 \in N_2$. Logo, $\alpha(n_1 + n_2) = \alpha n_1 + \alpha n_2 \in N_1 + N_2$.

Portanto, $N_1 + N_2$ é um submódulo de M.

Exemplo 1.16 *Sejam M um A-módulo e $\{N_i\}_{i \in I}$ é uma família de submódulos de M, onde I é um conjunto qualquer não vazio. Então $J = \bigcap\limits_{i \in I} N_i$ é submódulo de M.*

De fato, sejam n_1 e $n_2 \in J$. Então n_1 e $n_2 \in N_i$, $\forall \ i \in I$. Assim, $n_1 + n_2 \in N_i$, $\forall \ i \in I$, isto é, $n_1 + n_2 \in J$.

Sejam $\alpha \in A$ e $n \in J$. Então, $n \in N_i$, $\forall \ i \in I$, e daí, $\alpha n \in N_i$, $\forall i \in I$. Logo, $\alpha n \in J$.

Definimos agora alguns tipos de módulos que são relevantes para o trabalho.

Definição 1.17 *Um A-módulo M é dito cíclico se existe $x \in M$ tal que $M = Ax = \{ax : a \in A\}$. Neste caso, dizemos que M é gerado por x, isto é, todo elemento $y \in M$ é da forma $y = ax$ para algum $a \in A$.*

Exemplo 1.18 *Todo anel A visto como um módulo sobre si mesmo (${}_AA$ ou A_A) é cíclico gerado por 1. Trivialmente, $\{0\}$ é módulo cíclico sobre qualquer anel.*

Definição 1.19 *Um A-módulo M é dito simples se $M \neq \{0\}$ e seus únicos submódulos são os triviais.*

Proposição 1.20 *Todo A-módulo simples é cíclico.*

Demonstração: Seja M um A-módulo simples. Então existe $0 \neq x \in M$. Assim, Ax é um submódulo não nulo de M. Como M é simples, segue que $Ax = M$. ■

Definimos agora o anulador de um A-módulo. Tal definição é muito usada neste trabalho.

Sejam A um anel e M um A-módulo à esquerda, o conjunto

$$An_A(M) := \{a \in A : \ am = 0, \forall \ m \in M\}$$

é chamado de anulador à esquerda do módulo M.

Na verdade, $An_A(M)$ é um ideal de A. De fato, $0 \in An_A(M)$. Sejam x, $y \in An_A(M)$ e $\alpha \in A$. Então $0 = xm + (-y)m = (x + (-y))m = (x - y)m$, $\forall m \in M$ e portanto, $x - y \in An_A(M)$. Também, $0 = \alpha(xm) = (\alpha x)m$, $\forall m \in M$ e $(x\alpha)m = x(\alpha m) = 0$, $\forall m \in M$, pois $\alpha m \in M$. Logo, $An_A(M)$ é ideal de A.

De maneira análoga é definido anulador à direita de um A-módulo.

Para cada $m \in M$, definimos o anulador à esquerda deste elemento por $An_A(m) := \{a \in A : \ am = 0\}$ e é fácil ver que $An_A(m)$ é um ideal à esquerda de A. Se A fosse comutativo então $An_A(m)$ seria ideal de A.

Definição 1.21 *Se $An_A(M) = \{0\}$ então M é dito um A-módulo fiel.*

Proposição 1.22 *Seja M um A-módulo. Então M é um A/I-módulo, com a operação $\cdot : A/I \times M \to M$ definida por $\overline{\alpha}m = (\alpha + I)m := \alpha m$, se, e somente se, $IM = \{0\}$ (onde I é um ideal sobre A).*

Demonstração: ($\Rightarrow$) Como M é um A/I-módulo, dados $\alpha \in I$ e $m \in M$, temos que $\alpha m = (\alpha + I)m = \overline{\alpha}m = 0$, pois $\alpha + I = \overline{\alpha} = \overline{0}$. Logo, $IM = \{0\}$.
($\Leftarrow$) Definimos

$$\begin{array}{rccc} \cdot : & A/I \times M & \to & M \\ & (\overline{\alpha}, m) & \mapsto & \overline{\alpha}m := \alpha m \end{array}$$

Mostremos que $\cdot$ está bem definida. Sejam $(\overline{a}, m)$, $(\overline{a_1}, m_1) \in A/I \times M$ tais que $(\overline{a}, m) = (\overline{a_1}, m_1)$, daí $m = m_1$ e $\overline{a} = \overline{a_1}$. Isso nos diz que $a - a_1 \in I$, mas por hipótese, $(a - a_1)m = 0$. Portanto, $am = a_1m$ e isto é equivalente a dizermos que $\overline{a}m = \overline{a_1}m$. Notemos que as propriedades para que M seja um A/I-módulo decorrem do fato de que M é um A-módulo e da definição da multiplicação. ■

Corolário 1.23 *Seja M um A-módulo. Então M é um $A/An_A(M)$-módulo fiel.*

Demonstração: Como $An_A(M)M = \{0\}$, então M é um $A/An_A(M)$-módulo pela proposição acima. Provemos que M é fiel. Chamemos $R = A/An_A(M)$, temos que provar que $An_R(M) = \{\overline{0}\}$. De fato, seja $\overline{x} \in An_R(M)$. Então $\overline{x}M = 0$ e pela definição de $\cdot$ segue que $\overline{x} \cdot m = xm = 0, \forall m \in M$. Então $x \in An_A(M)$ e daí, $\overline{x} = \overline{0}$. ■

1.3 Módulos Quocientes

Sejam M um A-módulo e N um submódulo de M. Dados $x,\ y \in M$, definimos a relação

$$x \equiv y\ (mod\ N) \text{ se, e somente se, } x - y \in N.$$

Verifica-se facilmente que $\equiv\ (mod\ N)$ é uma relação de equivalência. Para cada $x \in M$, a sua respectiva classe de equivalência é dada por

$$\begin{aligned} x + N &= \{y \in M : y \equiv x\ (mod\ N)\} \\ &= \{y \in M : y - x \in N\} \\ &= \{x + n : n \in N\}. \end{aligned}$$

Notemos que por M ser um grupo abeliano, dado qualquer submódulo N (portanto, subgrupo) de M, a classe $x + N$ (chamada classe lateral à esquerda) e a classe $N + x$ (chamada classe lateral à direita) coincidem, para qualquer $x \in M$. Por isso, não fazemos menção alguma quanto à direita e à esquerda.

Podemos verificar facilmente que $x + N = y + N$ para $x,\ y \in M$ se, e somente se, $x - y \in N$, isto é, $x \equiv y\ (mod\ N)$.

Para facilitar a escrita, usamos $\overline{x}$ ao invés de $x + N$.

Consideremos o conjunto quociente $M/N = \{\overline{x} : x \in M\}$. Sendo M um grupo abeliano, não é difícil ver que $(M/N, +)$ também o é.

Definimos

$$\begin{array}{rccc} + : & M/N \times M/N & \to & M/N \\ & (\overline{x}, \overline{y}) & \mapsto & \overline{x} + \overline{y} := \overline{x + y}. \end{array}$$

Primeiramente, mostremos que $+$ está bem definida. Sejam $x, y, x', y' \in M$ tais que $(\overline{x}, \overline{y}) = (\overline{x'}, \overline{y'})$. Então $\overline{x} = \overline{x'}$ e $\overline{y} = \overline{y'}$. Daí, $x - x' \in N$ e $y - y' \in N$. Portanto, $(x + y) - (x' + y') = (x - x') + (y - y') \in N$, ou seja, $\overline{(x + y)} = \overline{(x' + y')}$. Claramente, M/N é um grupo abeliano.

Agora definimos

$$\begin{array}{rccc} \cdot : & A \times M/N & \to & M/N \\ & (a, \overline{x}) & \mapsto & a\overline{x} := \overline{ax}. \end{array}$$

Vejamos que $\cdot$ está bem definida. De fato, sejam $x, y \in M$ tais que $\overline{x} = \overline{y}$. Assim, $x - y \in N$ e portanto, $a(x - y) = ax - ay \in N$, $a \in A$. Logo, $\overline{ax} = \overline{ay}$.

Sejam $a,\ a_1 \in A$ e $m,\ m_1 \in M$. Então:
(i) $a(a_1\overline{m}) = a\overline{a_1 m} = \overline{a(a_1 m)} = \overline{(aa_1)m} = (aa_1)\overline{m}$;
(ii) $a(\overline{m} + \overline{m_1}) = a(\overline{m + m_1}) = \overline{a(m + m_1)} = \overline{am + am_1)} = \overline{am} + \overline{am_1} = a\overline{m} + a\overline{m_1}$;
(iii) $(a + a_1)\overline{m} = \overline{(a + a_1)m} = \overline{am + a_1 m} = \overline{am} + \overline{a_1 m} = a\overline{m} + a_1\overline{m}$;
(iv) $1\overline{m} = \overline{1m} = \overline{m}$.

Pelo desenvolvimento feito acima, segue que M/N é um A-módulo, chamado módulo quociente de M pelo submódulo N.

Exemplo 1.24 *Seja I um ideal à esquerda do anel R. Então R/I tem a estrutura de um R-módulo, a operação soma é a própria da estrutura do anel R/I e a operação multiplicação de elementos de R por elementos de R/I é induzida pela multiplicação do anel R.*

1.4 Homomorfismos

Nesta seção, estudamos um tópico importante dentro da teoria de módulos, que são os homomorfismos de módulos. Apresentamos as principais propriedades dos homomorfismos e introduzimos dois importantes submódulos que são o núcleo e a imagem de um homomorfismo. Tais conceitos farão toda a diferença quando estudarmos sequências exatas que culminam na caracterização de anéis semi-simples apresentados mais adiante.

Sejam M e N dois A-módulos. Uma função $f : M \to N$ diz-se um homomorfismo de A-módulos ou um A-homomorfismo se para quaisquer $m_1, m_2 \in M$ e qualquer $\alpha \in A$, verificam-se as seguintes condições:
(i) $f(m_1 + m_2) = f(m_1) + f(m_2)$;
(ii) $f(\alpha m) = \alpha f(m)$.

Se f é um homomorfismo injetor, sobrejetor ou bijetor, então f é dito um monomorfismo, epimorfismo ou um isomorfismo, respectivamente.

Um homomorfismo $f : M \to M$ é dito um endomorfismo e se f é um isomorfismo então f é chamado um automorfismo. Se $f : M \to N$ é um isomorfismo, dizemos que os módulos M e N são isomorfos e denotamos por $M \cong N$.

Determinamos por $End(M)$ o conjunto de todos os homomorfismos de M para M.

Proposição 1.25 *Sejam M e P dois A-módulos . Seja $f : M \to P$ um homomorfismo. Então as seguintes propriedades são satisfeitas:*
(i) $f(0) = 0$*;*
(ii) *para todo $x \in M$, $f(-x) = -f(x)$.*

Demonstração: (i) Temos que $f(0) = f(0+0) = f(0) + f(0)$. Daí $f(0) = 0$.
(ii) De fato, temos que $0 = f(0) = f(x + (-x))$, para todo $x \in M$. Daí, $0 = f(x) + f(-x)$ e segue que $-f(x) = f(-x)$. ■

Exemplo 1.26 *Sejam M, N dois A-módulos. Então a função $f : M \to N$ definida por $f(x) = 0$ para todo $x \in M$ é um homomorfismo, chamado homomorfismo nulo.*

Exemplo 1.27 *Seja M um A-módulo. Então a função $1_M : M \to M$ definida por $1_M(m) = m$ ($m \in M$) é chamado identidade em M e é um automorfismo.*

Exemplo 1.28 *Seja N um submódulo de um A-módulo M. Então a função inclusão canônica*

$$\begin{array}{rccc} i: & N & \hookrightarrow & M \\ & n & \mapsto & n \end{array}$$

é um monomorfismo.

Exemplo 1.29 *Seja N um submódulo de um A-módulo M. Então a função*

$$\begin{array}{rccc} \pi: & M & \to & M/N \\ & x & \mapsto & \overline{x} \end{array}$$

é um epimorfismo, chamado projeção canônica.

Seja $f : M \to N$ um A-homomorfismo, chamamos imagem de f ($Im(f)$) e núcleo de f ($(Ker(f))^*$), respectivamente aos conjuntos

$$Im(f) = \{f(x) : x \in M\};$$

$$Ker(f) = \{x \in M : \ f(x) = 0\}.$$

(*) Essa é a notação usada na literatura em que Ker abrevia a palavra núcleo em inglês, kernel.

Proposição 1.30 *Seja $f : M \to N$ um A-homomorfismo. Então $Im(f)$ e $Ker(f)$ são submódulos de N e M, respectivamente.*

Demonstração: Mostremos que $Im(f)$ é um submódulo de N.

Sejam n_1 e $n_2 \in Im(f)$. Então $n_1 = f(m_1)$ e $n_2 = f(m_2)$ para alguns m_1, $m_2 \in M$. Daí, $n_1 + n_2 = f(m_1) + f(m_2) = f(m_1 + m_2)$ e isso nos diz que $n_1 + n_2 \in Im(f)$.

Sejam $\alpha \in A$ e $n \in Im(f)$. Então $n = f(m)$, para algum $m \in M$. Daí, $\alpha n = \alpha f(m) = f(\alpha m)$, o que mostra que $\alpha n \in Im(f)$.

Mostremos que $Ker(f)$ é um submódulo de M.

Sejam m_1 e $m_2 \in Ker(f)$. Então $f(m_1 + m_2) = f(m_1) + f(m_2) = 0 + 0 = 0$. Logo, $m_1 + m_2 \in Ker(f)$.

Sejam $\alpha \in A$ e $m \in Ker(f)$. Então $f(\alpha m) = \alpha f(m) = \alpha 0 = 0$. Portanto, $\alpha m \in Ker(f)$. ■

Proposição 1.31 *Seja $f : M \to N$ um homomorfismo de A-módulos. Então f é um monomorfismo, se e somente se, $Ker(f) = \{0\}$.*

Demonstração: Seja f um monomorfismo. Provemos que $Ker(f) = \{0\}$. De fato, seja $x \in Ker(f)$. Então $f(x) = 0$. Segue que $f(x) = 0 = f(0)$, o que implica $x = 0$. Por outro lado, suponhamos $Ker(f) = 0$. Sejam x, $y \in M$ tais que $f(x) = f(y)$. Então $f(x - y) = 0$, ou seja, $x - y \in Ker(f)$. Como $Ker(f) = \{0\}$, segue que $x = y$, o que nos mostra que a função f é injetora. ■

Estando subentendido o anel A, daqui para frente, escrevemos apenas módulo(s), submódulo(s), homomorfismo(s) e isomorfismo(s) ao invés de A-módulo(s), A-submódulo(s), A-homomorfismo(s) e A-isomorfismo(s).

Teorema 1.32 (***Teorema do Homomorfismo***) *Sejam M e N módulos e $f : M \to N$ um homomorfismo. Então $M/Ker(f)$ e $Im(f)$ são módulos isomorfos.*

Demonstração: Definimos $\overline{f} : M/Ker(f) \to Im(f)$ por $\overline{f}(\overline{m}) = f(m)$. Provemos que $\overline{f}$ está bem definida.

Sejam $\overline{m}, \overline{m}' \in M/Ker(f)$ tais que $\overline{m} = \overline{m}'$. Então $m - m' \in Ker(f)$. Daí, $f(m - m') = 0$, ou seja, $f(m) = f(m')$. Logo $\overline{f}(\overline{m}) = \overline{f}(\overline{m'})$.

Provemos que $\overline{f}$ é um homomorfismo bijetor. Sejam $\overline{x}$, $\overline{y} \in M/Ker(f)$ e $a \in A$, temos que

$$\begin{aligned} \overline{f}(\overline{x} + \overline{y}) &= \overline{f}(\overline{x + y}) = f(x + y) = f(x) + f(y) = \overline{f}(\overline{x}) + \overline{f}(\overline{y}) \text{ e} \\ \overline{f}(a\overline{x}) &= \overline{f}(\overline{ax}) = f(ax) = af(x) = a\overline{f}(\overline{x}). \end{aligned}$$

Sejam $\overline{m}$ e $\overline{m}' \in M/Ker(f)$ tais que $\overline{f}(\overline{m}) = \overline{f}(\overline{m}')$. Então, $f(m) = f(m')$, o que implica $f(m - m') = 0$, ou seja, $m - m' \in Ker(f)$. Logo, $\overline{m} = \overline{m}'$.

Notemos que $Im(\overline{f}) = \{\overline{f}(\overline{x}) : x \in M\} = \{f(x) : x \in M\} = Im(f)$ e trivialmente $\overline{f}$ é sobrejetora. ■

O corolário abaixo é uma aplicação direta do teorema acima.

Corolário 1.33 *Se $f : M \to N$ é um epimorfismo, então N e $M/Ker(f)$ são isomorfos.*

Corolário 1.34 *Todo módulo cíclico é isomorfo a um módulo quociente de A por um ideal à esquerda de A.*

Demonstração: Suponhamos $M = Am$ para algum $m \in M$. Definimos $f : A \to Am$ por $f(a) = am$. Mostremos que f é um epimorfismo.

Sejam $a, b \in A$. Então $f(a+b) = (a+b)m = am + bm = f(a) + f(b)$ e $f(ab) = (ab)m = a(bm) = af(b)$.

Por outro lado, $Ker(f) = \{a \in A : f(a) = 0\} = \{a \in A : am = 0\} = An_A(m)$ e f é claramente sobrejetor. Pelo Corolário 1.33, $A/An_A(m)$ e Am são isomorfos. ■

O próximo teorema é muito importante para o nosso trabalho, vamos colocá-lo neste capítulo, porém ele será usado mais adiante. O fato de A ser um anel não-nulo garante a existência de ideal à esquerda (à direita) maximal. Isso será mostrado na Proposição 2.21.

Teorema 1.35 *Para um anel A não-nulo, as seguintes condições são equivalentes:*
(i) *A/I é simples como um A-módulo para algum ideal à esquerda I de A;*
(ii) *I é um ideal à esquerda maximal de A.*

Demonstração: (i) $\Rightarrow$ (ii) Suponhamos que A/I é simples. Devemos mostrar que I é um ideal à esquerda maximal de A. Seja J um ideal à esquerda de A tal que $J \subsetneqq A$ e $I \subseteq J$. Então J/I é ideal à esquerda de A/I. Como A/I é simples, segue que $J/I = \{\overline{0}\}$ ou $J/I = A/I$. Se $J/I = A/I$, então $J = A$, o que contradiz a hipótese. Logo, $J/I = \{\overline{0}\}$, o que implica $J \subseteq I$, ou seja, $J = I$. Portanto, I é ideal à esquerda maximal.
(ii) $\Rightarrow$ (i) Suponhamos I um ideal à esquerda maximal. Provemos que A/I é um A-módulo simples. De fato, seja $\overline{J}$ ideal à esquerda de A/I (equivalentemente, $\overline{J}$ é um submódulo de A/I). Então existe um único ideal à esquerda J de A tal que $I \subseteq J$ e $J/I = \overline{J}$. Por hipótese, $J = I$ ou $J = A$. Assim, $\overline{J} = \{\overline{0}\}$ ou $\overline{J} = A/I$. Portanto, A/I é um A-módulo simples. ■

1.5 Soma Direta Interna

Sejam M um módulo e $\{M_\lambda\}_{\lambda \in I}$ uma família não vazia de submódulos de M. Então M é chamado soma direta interna dos submódulos M_λ, para todo $\lambda \in I$ se:
(i) $M = \sum\limits_{\lambda \in I} M_\lambda$ (lembramos que um elemento $m \in M$ é escrito como $m = \sum\limits_{i \in I} m_i$, onde $\{m_i\}_{i \in I}$ é uma família quase nula) e
(ii) $M_\lambda \cap \left(\sum\limits_{u \neq \lambda} M_u \right) = \{0\}, \forall\, \lambda \in I$.

Notamos $M = \bigoplus_{\lambda \in I} M_\lambda$ e se $I = \{1, 2, \cdots, n\}$ então $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n$. A proposição a seguir nos dá condições equivalentes para que tenhamos soma direta.

Proposição 1.36 *Seja $\{M_i\}_{i \in I}$ uma família não vazia de submódulos de um módulo M. As seguintes afirmações são equivalentes:*
(i) *todo elemento $m \in M$ se escreve de um único modo como $m = \sum_{i \in I} m_i$, onde $m_i \in M, \forall\ i \in I$ e a família $\{m_i\}_{i \in I}$ é quase nula (uma família é dita quase nula quando ela é nula exceto para um número finito de termos);*
(ii) *$M = \sum_{i \in I} M_i$ e se $\sum_{i \in I} m_i = 0$, com $m_i \in M_i$, tem-se $m_i = 0$, para todo $i \in I$;*
(iii) *$M = \sum_{i \in I} M_i$ e $M_j \cap \left(\sum_{i \neq j} M_i\right) = \{0\}, \forall\ j \in I$.*

Demonstração: (i)$\Rightarrow$ (ii) É claro que $M = \sum_{i \in I} M_i$. Suponhamos que $m = \sum_{i \in I} m_i = 0$, com $m_i \in M_i$. Mas por (i), todo elemento de M se escreve de modo único. Logo, $m_i = 0$, para todo $m_i \in M$.

(ii)$\Rightarrow$ (iii) Seja $m \in M_j \cap \sum_{i \neq j} M_i$. Então $m \in M_j$ e escrevemos $m = \sum_{i \neq j} m_i$, com $m_i \in M_i$ e $i \in I$. Portanto, $\sum_{i \neq j} m_i - m = 0$, e por (ii) todos os somandos devem ser nulos. Em particular, $m = 0$.

(iii)$\Rightarrow$(i) Como $M = \sum_{i \in I} M_i$, temos que $m = \sum_{i \in I} m_i$, com $m \in M$ onde $\{m_i\}_{i \in I}$ é uma família quase nula. Provemos que a decomposição de m é única.

Suponhamos que existam duas decomposições para m, isto é, $\sum_{i \in I} m_i = \sum_{i \in I} m_i'$. Para cada $j \in I$, temos que $m_j - m_j' = \sum_{i \neq j} m_i' - \sum_{i \neq j} m_i = \sum_{i \neq j} (m_i' - m_i)$ e portanto, $m_j' - m_j \in M_j \cap \sum_{i \neq j} M_i \overset{(iii)}{=} \{0\}$. Logo, $m_j = m_j'$. ■

Definição 1.37 *Seja N um submódulo de um módulo M. Dizemos que N é um somando direto de M se existe um submódulo P de M tal que $M = N \oplus P$.*

Exemplo 1.38 *Para qualquer módulo M, tem-se sempre que $M = M \oplus \{0\}$. Os submódulos M e $\{0\}$ são ditos somandos diretos triviais.*

Exemplo 1.39 *Sejam $k_1 = \mathbb{R}(1, 0)$, $k_2 = \mathbb{R}(0, 1)$, $k_3 = \mathbb{R}(1, 1)$, $k_4 = \mathbb{R}(3, 1)$ submódulos do $\mathbb{R}$-módulo $\mathbb{R} \times \mathbb{R}$. Então $\mathbb{R} \times \mathbb{R} = k_1 \oplus k_2 = k_1 \oplus k_3 = k_1 \oplus k_4$.*

Exemplo 1.40 *Seja R um anel. Consideremos $M_2(R)$ o anel das matrizes quadradas 2×2 com entradas no anel R. Temos que $N = \begin{pmatrix} 0 & R \\ 0 & R \end{pmatrix} = \left\{ \begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} :\ x,\ y \in R \right\}$ e $P = \begin{pmatrix} R & 0 \\ R & 0 \end{pmatrix} = \left\{ \begin{pmatrix} z & 0 \\ w & 0 \end{pmatrix} :\ z,\ w \in R \right\}$ são R-submódulos de $M_2(R)$ e $M_2(R) = N \oplus P$.*

Exemplo 1.41 *Nem todo submódulo de um módulo é um somando direto.*

De fato, tome ${}_{\mathbb{Z}}\mathbb{Z}$. Sejam N e S submódulos não-nulos de $\mathbb{Z}$. Então $N = (n)$ e $S = (s)$ para alguns $n, s \in \mathbb{Z}$. Assim, $n \cdot s \in N \cap S$. Logo, a soma não pode ser direta.

Proposição 1.42 *Sejam M um módulo e N_1, N_2 submódulos de M tais que $M = N_1 \oplus N_2$. Então $M/N_1 \cong N_2$.*

Demonstração: Como $M = N_1 \oplus N_2$, podemos escrever $m = n_1 + n_2$ onde n_1 e n_2 são unicamente determinados. Assim, definimos $\varphi : M \to N_2$ por $\varphi(m) = n_2$. É claro que φ é um homomorfismo sobrejetor. Por outro lado, $Ker(\varphi) = \{m \in M : \varphi(m) = 0\} = \{n_1 \ : \ n_1 \in N_1\} = N_1$. Logo, $M/N_1 \cong N_2$. ■

Exemplo 1.43 *Considerando o Exemplo 1.40, pela proposição acima $M_2(R)/N \cong P$ e $M_2(R)/P \cong N$.*

1.6 Sequências Exatas

A seção sobre sequências exatas desempenha papel importante no Capítulo 2, pois está totalmente relacionada com o teorema de caracterização dos anéis semi-simples.

Definição 1.44 *Sejam $\{\cdots, M_{i-1}, M_i, M_{i+1}, \cdots\}$ uma família não vazia, eventualmente infinita de módulos e $\{\cdots, f : M_i \to M_{i+1}, \cdots\}$ uma família de homomorfismos. Diz-se que o diagrama:*

$$\cdots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \cdots$$

é uma sequência exata se é exata em M_i, $\forall\, i \in I$, isto é, se $Im(f_{i-1}) = Ker(f_i), \forall\, i \in I$, onde I é um conjunto não vazio qualquer.

Definição 1.45 *Uma sequência exata de módulos da forma $0 \to F \xrightarrow{f} G \xrightarrow{g} H \to 0$ é dita uma sequência exata curta.*

Proposição 1.46 *Seja $F \xrightarrow{f} G \xrightarrow{g} H$ uma sequência exata de módulos. Então $g \circ f = 0$.*

Demonstração: Seja $x \in F$. Então $(g \circ f)(x) = g(f(x))$, mas $Im(f) = Ker(g)$ e daí, $g(f(x)) = 0$ para todo $x \in F$. Logo, $g \circ f = 0$. ■

Proposição 1.47 *Sejam M, N, P módulos. Então a sequência $0 \xrightarrow{f_o} M \xrightarrow{f} N \xrightarrow{g} P \xrightarrow{g_o} 0$ é exata se, e somente se, f é um monomorfismo, g um epimorfismo e $Im(f) = Ker(g)$ (as funções f_o, g_o são os homomorfismos nulos).*

Demonstração: ($\Rightarrow$) A sequência sendo exata, significa que é exata em M, N e P. Daí, $0 = Im(f_o) = Ker(f)$, $Im(f) = Ker(g)$ e $Im(g) = Ker(g_o) = P$, seguindo portanto que f é um monomorfismo e g é um epimorfismo.
($\Leftarrow$) Se f é um monomorfismo então $Ker(f) = 0 = Im(f_o)$. Se g é um epimorfismo, então $Im(g) = P = Ker(g_o)$ e como $Im(f) = Ker(g)$, segue que a sequência é exata. ■

Exemplo 1.48 *Seja $n \in \mathbb{Z}$, $n \geq 2$. A sequência $0 \to n\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_n \to 0$ é exata, onde i e π são respectivamente, as funções inclusão e projeção canônicas.*

O exemplo seguinte é uma generalização do anterior.

Exemplo 1.49 *Se E é um submódulo de F, então a sequência $0 \to E \xrightarrow{i} F \xrightarrow{\pi} F/E \to 0$ é exata, onde i e π são respectivamente, as funções inclusão e projeção canônicas.*

Definição 1.50 *Dada a sequência exata de módulos $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$, dizemos que a mesma cinde se $Im(f)$ é um somando direto de F.*

Proposição 1.51 *Dada uma sequência exata de A-módulos $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$, as seguintes afirmações são equivalentes:*
(i) *a sequência cinde;*
(ii) *existe um homomorfismo $\psi : F \to E$ tal que $\psi \circ f = 1_E$;*
(iii) *existe um homomorfismo $\varphi : G \to F$ tal que $g \circ \varphi = 1_G$.*

Demonstração: (i)$\Rightarrow$(ii) Temos que $Im(f)$ é um somando direto de F, ou seja, existe um submódulo P de F tal que $F = Im(f) \oplus P$. Portanto, se $x \in F$, então x é expresso de forma única como $x = y + p$ onde $y \in Im(f)$ e $p \in P$.

Como $y \in Im(f)$, segue que $y = f(v)$ para algum $v \in E$. Note que v é único, pois f é uma função injetora.

Definimos $\psi : F \to E$ por $\psi(x) = v$ (onde $x = y + p$, com $y = f(v)$, para único v). Mostremos que ψ é um homomorfismo. De fato, sejam $x, x' \in F$. Então $x = y + p$ e $x' = y' + p'$, onde $y, y' \in Im(f)$ e portanto, $y = f(v)$, $y' = f(v')$, para únicos $v, v' \in E$ e ainda, $p, p' \in P$. Temos que

$$\begin{aligned} \psi(x + x') &= \psi((y + y') + (p + p')) = \psi((f(v + v')) + (p + p')) \\ &= v + v' = \psi(x) + \psi(x') \text{ e} \\ \psi(rx) &= \psi(r(y + p)) = \psi(ry + rp) = \psi(rf(v) + rp) = \psi(f(rv) + rp) \\ &= rv = r\psi(x), \text{ para todo } r \in A. \end{aligned}$$

Agora, mostremos que $\psi \circ f = 1_E$. Seja $e \in E$. Então $(\psi \circ f)(e) = \psi(f(e)) = e$. Logo, $\psi \circ f = 1_E$.

(ii)$\Rightarrow$(i) Mostremos que $F = Im(f) \oplus Ker(\psi)$. Seja $x \in F$. Chamemos $f(\psi(x)) = y$ e $z = x - y$. Logo, $x = y + z$, e claramente $y \in Im(f)$. É suficiente mostrarmos que $z \in Ker(\psi)$. De fato,

$$\begin{aligned}\psi(z) &= \psi(x-y) = \psi(x) - \psi(y) = \psi(x) - \psi(f(\psi(x))) \\ &= \psi(x) - (\psi \circ f)(\psi(x)) \overset{(ii)}{=} \psi(x) - \psi(x) = 0.\end{aligned}$$

Provemos ainda que $Im(f) \cap Ker(\psi) = \{0\}$. Seja $y \in Im(f) \cap Ker(\psi)$. Então $y \in Im(f)$, isto é, $y = f(x)$ para algum $x \in E$ e também $\psi(y) = 0$. Logo, $0 = \psi(y) = \psi(f(x)) = (\psi \circ f)(x) = x$. Portanto, $y = f(x) = f(0) = 0$.

(i)$\Rightarrow$(iii) Sabemos que existe um submódulo P de F tal que $F = Im(f) \oplus P$.

Seja $w \in G$. Então existe $x \in F$ tal que $g(x) = w$. Como $x = y + p$, onde $y \in Im(f)$ e $p \in P$, temos que $g(x) = g(y+p) = g(y) + g(p) = g(p)$, pois $y \in Im(f) = Ker(g)$. Logo, $g(p) = w$.

Mostremos que p com esta propriedade é único. Suponhamos que exista $p' \in P$ tal que $g(p') = w$. Então $g(p) = g(p')$ e isso implica que $g(p) - g(p') = 0$, ou seja, $g(p - p') = 0$. Assim $p - p' \in Ker(g) = Im(f)$ e daí, $p - p' \in Im(f) \cap P = \{0\}$. Donde, $p = p'$.

Definimos $\varphi : G \to F$ por $\varphi(w) = p$, onde p é tal que $g(p) = w$. Mostremos que φ é um homomorfismo. Sejam $w, w' \in G$. Então $w = g(x)$ e $w' = g(x')$ para alguns $x, x' \in F$. Mas $F = Im(f) \oplus P$ e isso implica que $x = y + p$ e $x' = y' + p'$, onde $y, y' \in Im(f)$ e $p, p' \in P$. Logo,

$$\begin{aligned}\varphi(w + w') &= \varphi(g(y+p) + g(y'+p')) = \varphi(g(y + y' + p + p')) \\ &= \varphi(g(y+y') + g(p+p')) \overset{(*)}{=} \varphi(g(p+p')) = p + p' \\ &= \varphi(w) + \varphi(w') \ \text{ e} \\ \varphi(rw) &= \varphi(rg(y+p)) = \varphi(g(r(y+p))) = \varphi(g(ry + rp)) \\ &= \varphi(g(ry) + g(rp)) \overset{(*)}{=} \varphi(g(rp)) = rp = r\varphi(w), \ \forall\ r \in A.\end{aligned}$$

As igualdades $(*)$ se devem ao fato de que $y + y'$ e $ry \in Ker(g)$. Além disso, $(g \circ \varphi)(w) = g(p) = w$, $\forall\ w \in G$. Logo, $(g \circ \varphi) = 1_G$.

(iii)$\Rightarrow$(i) Mostremos que $F = Im(f) \oplus P$, onde $P = Im(\varphi)$. Se $y \in Im(f) \cap P$, então existem $z \in E$ e $w \in G$ tais que $y = f(z) = \varphi(w)$. Como $g(y) = 0$, segue que $0 = g(y) = g(f(z)) = g(\varphi(w)) = (g \circ \varphi)(w) = w$. Assim, $y = 0$ e portanto, $Im(f) \cap H = \{0\}$.

Agora, seja $y \in F$. Então é claro que $t = y - \varphi(g(y)) \in Ker(g) = Im(f)$. Portanto, $y = t + \varphi(g(y)) \in Im(f) + Im(\varphi)$. Assim, $F = Im(f) \oplus H$ e a condição (i) é satisfeita. ■

Corolário 1.52 *Se a sequência exata curta* $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$ *cinde, então* $F \cong E \oplus G$.

Demonstração: Como a sequência cinde, então $F = Im(f) \oplus Im(\varphi)$, por $(iii) \Rightarrow (i)$ do teorema acima. Além disso, φ é injetor (pois $g \circ \varphi = 1_G$, isto é, φ tem inversa à esquerda) daí, $G \cong Im(\varphi)$.

Por f ser injetor, $Im(f) \cong E$. Logo, $F = Im(f) \oplus Im(\varphi) \cong E \oplus G$. ■

Exemplo 1.53 *Sejam A um anel e $R = M_2(A)$ o anel das matrizes de ordem 2 sobre A. É fácil verificar que os conjuntos*

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a,\ b \in A \right\} e\ J = \left\{ \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} : c,\ d \in A \right\}$$

são ideais à esquerda de R e portanto R-submódulos (à esquerda) de R. Claramente ${}_RR = I \oplus J$ e portanto, a sequência exata curta $0 \to I \xrightarrow{i} R \xrightarrow{\pi} R/I \to 0$ cinde. Na sequência dada i é a inclusão e π a projeção canônicas. Notemos que $R/I \cong J$.

Capítulo 2

Anéis Semi-simples e Radical de Jacobson

Nesse capítulo trabalhamos com duas classes importantes de anéis, a saber, a dos anéis semi-simples e dos anéis J-semi-simples. Estudamos as caracterizações destes anéis, assim como, a relação entre eles. Enunciamos, sem demonstrar, o teorema de Wedderburn-Artin, um caso particular do teorema da estrutura para anéis primitivos.

2.1 Condições de Cadeia

Nesta seção, definimos módulos e anéis noetherianos (artinianos). Para isso, falamos brevemente sobre condições de cadeia. Nosso objetivo é apenas lembrar definições e resultados relacionados, sem demonstrá-los.

Dado um conjunto C, dizemos que uma família de subconjuntos $F = \{C_i \,:\, i \in I\}$ de C satisfaz a condição de cadeia ascendente (CCA) se F não contém uma subfamília estritamente crescente $C_{i_1} \subsetneqq C_{i_2} \subsetneqq \cdots$, ou seja, para qualquer cadeia ascendente $C_{i_1} \subseteq C_{i_2} \subseteq \cdots$ de elementos de F, existe um inteiro n tal que $C_{i_n} = C_{i_{n+1}} = C_{i_{n+2}} = \cdots$.

A condição de cadeia descendente (CCD) é formulada de maneira semelhante, invertendo o sentido das inclusões.

Definição 2.1 *Seja M um A-módulo à esquerda. Dizemos que o módulo M é noetheriano (respectivamente artiniano) se a família de todos os submódulos de M satisfaz CCA (respectivamente CCD).*

Para o caso em que $M = A$ temos as definições para anéis noetherianos e artinianos.

Dizemos que o anel A é noetheriano à esquerda (respectivamente à direita) se A é noetheriano quando visto como um A-módulo à esquerda (respectivamente à direita) e artiniano à esquerda (respectivamente à direita) se A é artiniano quando visto como um A-módulo à esquerda (respectivamente à direita). Se o anel A é noetheriano à esquerda e à direita, A diz-se simplesmente noetheriano. O mesmo vale para o caso artiniano.

Apresentamos agora um resultado bem conhecido e muito útil para encontramos exemplos de módulos noetherianos. Ao leitor interessado, indicamos ([4], Theorem 1.9, p. 375).

Proposição 2.2 *Um módulo M é noetheriano se, e somente se, cada submódulo de M é finitamente gerado (M é um A-módulo finitamente gerado se existem $m_1, \cdots, m_s \in M$ tais que $M = Am_1 + Am_2 + \cdots + Am_s$).*

Exemplo 2.3 *O $\mathbb{Z}$-módulo $\mathbb{Z}$ é noetheriano, pois todo submódulo de $\mathbb{Z}$ é cíclico e portanto finitamente gerado. Entretanto, o $\mathbb{Z}$-módulo $\mathbb{Z}$ não é artiniano, pois obtemos a cadeia estritamente crescente de ideais de $\mathbb{Z}$*

$$2\mathbb{Z} \supsetneqq 4\mathbb{Z} \supsetneqq 8\mathbb{Z} \supsetneqq \cdots \supsetneqq 2^n\mathbb{Z} \supsetneqq \cdots .$$

Exemplo 2.4 *Corpos e anéis de divisão são anéis noetherianos e artinianos.*

Para finalizar esta seção, gostaríamos de lembrar um resultado útil para o trabalho. Primeiramente apresentamos duas definições.

Definição 2.5 *Dado um A-módulo à esquerda M, uma série normal para M é uma cadeia de submódulos*

$$M = M_0 \supset M_1 \supset \cdots \supset M_s.$$

Os fatores da série são os módulos quocientes M_i/M_{i+1} ($i = 0, 1, \cdots, s-1$).

Definição 2.6 *Uma série de composição (finita) para um A-módulo M é uma série normal $M = M_0 \supset M_1 \supset \cdots \supset M_s$ tal que cada fator da série, isto é, M_i/M_{i+1} é um A-módulo simples para todo $i \in \{1, 2, \cdots, s-1\}$.*

Para maiores detalhes, veja ([4], p. 375)

Teorema 2.7 *Um A-módulo à esquerda M é noetheriano e artiniano se, e somente se, M possui um série de composição finita.*

Ao leitor interessado, indicamos ([4], Theorem 1.11, p. 376).

2.2 Módulos Semi-simples

Definição 2.8 *Um A-módulo M é dito semi-simples se todo submódulo de M é um somando direto de M.*

Proposição 2.9 *Todo submódulo de um módulo semi-simples é semi-simples.*

Demonstração: Sejam M um módulo semi-simples e N um submódulo de M. Seja H um submódulo de N. Provemos que existe um submódulo P de N tal que $N = P \oplus H$.

Sendo M semi-simples, existe um submódulo J de M tal que $M = J \oplus H$, pois H é um submódulo de M. Mostremos que $N = (J \cap N) \oplus H$.

É claro que $(J \cap N) \cap H = \{0\}$, pois $J \cap N \cap H \subset J \cap H = \{0\}$. Como $(J \cap N) \oplus H$ é um submódulo de N, resta provarmos que $N \subset (J \cap N) \oplus H$.

Seja $n \in N$. Então $n \in M$ e portanto, $n = u + v$ onde $u \in J$ e $v \in H$. Daí, $u \in J \cap N$, pois $u = n - v$. Portanto $n = u + v \in (J \cap N) \oplus H$ e então $N = (J \cap N) \oplus H$. Logo, N é semi-simples. ■

Exemplo 2.10 *Seja K um corpo. Então todo K-espaço vetorial é um K-módulo semi-simples. Em particular, K é um K-módulo semi-simples.*

De fato, sua única decomposição é a trivial, isto é, $K = K \oplus \{0\}$

Exemplo 2.11 *Todo módulo simples é semi-simples.*

De fato, seja M um módulo simples. Então seus únicos submódulos são $\{0\}$ e M e obviamente $M = \{0\} \oplus M$.

Consideremos D um anel de divisão. Notemos que D não possui ideais à esquerda e nem à direita que não sejam os triviais. Portanto, ${}_DD$ e D_D são simples e consequentemente semi-simples.

O seguinte resultado é interessante, pois garante que todo módulo semi-simples não-nulo possui submódulo simples. Este resultado é fortemente usado na demonstração do Teorema 2.13 a seguir.

Proposição 2.12 *Todo A-módulo semi-simples não-nulo contém um submódulo simples.*

Demonstração: Seja M um A-módulo semi-simples não-nulo. Seja $0 \neq m \in M$. Então Am é um submódulo não-nulo de M e, pela Proposição 2.9, temos que Am é semi-simples. Mostremos que Am contém um submódulo simples. Pelo Lema de Zorn, existe N um submódulo de Am que é maximal com respeito a propriedade de que $m \notin N$. Sendo Am semi-simples, existe N' submódulo de Am tal que $Am = N \oplus N'$.

É claro que N' é não-nulo, pois caso contrário, $Am = N$ e teríamos um absurdo, pois m não pertenceria a Am.

Mostremos que N' é simples. Seja N'' um submódulo não-nulo de N'. Então $N \oplus N''$ deve conter m (pela maximidade de N). Logo, $Am = N \oplus N''$ e isso implica que $N'' = N'$. ■

O teorema abaixo não é demonstrado aqui. Ao leitor interessado, indicamos ([5], p. 26).

Teorema 2.13 *Seja M um A-módulo. São equivalentes:*
(i) *M é semi-simples;*
(ii) *M é soma direta de uma família de submódulos simples;*
(iii) *M é soma de uma família de submódulos simples.*

2.3 Anéis Semi-simples

Um anel A é dito semi-simples à esquerda se A, como A-módulo à esquerda, é semi-simples, isto é, ${}_AA$ é semi-simples. Analogamente, definimos anel semi-simples à direita considerando A como A-módulo à direita.

O teorema abaixo caracteriza anéis semi-simples à esquerda. O análogo do mesmo caracteriza anéis semi-simples à direita.

Teorema 2.14 *Seja A um anel. Então são equivalentes:*
(i) *A é semi-simples à esquerda;*
(ii) *toda sequência exata curta de A-módulos à esquerda cinde;*
(iii) *todo A-módulo à esquerda é semi-simples.*

Demonstração: (ii) $\Rightarrow$ (iii) Seja M um A-módulo e N um submódulo de M. Sabemos que a sequência $0 \rightarrow N \xrightarrow{i} M \xrightarrow{\pi} M/N \rightarrow 0$ cinde. Portanto, N é um somando direto de M.
(iii) $\Rightarrow$ (ii) Seja M um A-módulo à esquerda semi-simples. Consideremos a sequência exata curta $0 \rightarrow P \xrightarrow{f} M \xrightarrow{g} G \rightarrow 0$. Como $Im(f)$ e $Ker(g)$ são submódulos de M, segue que $Im(f)$ e $Ker(g)$ são somandos diretos de M, pois M é semi-simples. Logo, a sequência cinde.
(iii) $\Rightarrow$ (i) Como todo A-módulo à esquerda é semi-simples, segue que A é semi-simples à esquerda.

(i) $\Rightarrow$ (iii) Seja M um A-módulo à esquerda. Se $M = \{0\}$, claramente M é semi-simples à esquerda.

Suponhamos $M \neq \{0\}$. Então existe $0 \neq m \in M$. Consideremos o A-submódulo cíclico Am de M.

Seja o epimorfismo de módulos $\varphi : A \to Am$ dado por $\varphi(a) = am$. Claramente $A/Ker(\varphi) \cong Am$. Como A é semi-simples à esquerda, podemos escrever $A = Ker(\varphi) \oplus I$, onde I é um submódulo semi-simples de A.

Portanto, $Am \cong (Ker(\varphi) \oplus I)/Ker(\varphi) \cong I$ (veja Proposição 1.42).

Logo, Am é um A-módulo semi-simples e, pelo Teorema 2.13, Am é uma soma de módulos simples. Agora, $M = \sum\limits_{m \in M} Am$ e segue novamente do Teorema 2.13 que M é semi-simples. ■

Exemplo 2.15 *Corpos e anéis de divisão são anéis semi-simples à esquerda.*

Definição 2.16 *Dizemos que I é um ideal à esquerda minimal de A se $I \neq \{0\}$ e se J é um ideal à esquerda de A tal que $\{0\} \subset J \subset I$ então $J = \{0\}$ ou $J = I$.*

Corolário 2.17 *Todo anel semi-simples à esquerda é noetheriano à esquerda e artiniano à esquerda.*

Demonstração: Seja A um anel semi-simples à esquerda. Podemos escrever ${}_AA = \bigoplus\limits_{i \in I} U_i$, onde os $U_i's$ são A-submódulos simples de A (de fato, cada U_i é um ideal à esquerda minimal de A).

Temos que $1 \in A$ e é escrito como $1 = u_{i_1} + \cdots + u_{i_t}$ onde $u_{i_j} \in U_{i_j}$ para $j \in \{1, 2, \cdots, t\}$. Logo, $A \subset \bigoplus\limits_{j=1}^{t} U_{i_j} \subset A$ e assim, $A = \bigoplus\limits_{j=1}^{t} U_{i_j}$.

Reindexando e reordenando os índices ${i_j}'s$, chamamos $J = \{1, \cdots, t\}$. Logo, $A = \bigoplus\limits_{i \in J} U_i$ é uma soma direta finita. Daí,

$$A = \bigoplus_{i \in J} U_i \supset \bigoplus_{i=1}^{t-1} U_i \supset \bigoplus_{i=1}^{t-2} U_i \supset \cdots \supset \bigoplus_{i=1}^{2} U_i \supset U_1 \supset 0$$

e isso nos diz que ${}_AA$ possui uma série de composição.

Pelo Teorema 2.7, ${}_AA$ é artiniano e noetheriano, isto é, A como um anel é noetheriano à esquerda e artiniano à esquerda. ■

Os resultados a seguir são utilizados no capítulo 4, porém vamos apresentá-los (sem demonstração) agora em virtude do contexto em que estamos.

Lembramos que um anel A é simples se, e somente se, seus únicos ideais são os triviais ($\{0\}$ e A).

Teorema 2.18 *Seja A um anel simples. Então são equivalentes:*

(i) *A é artiniano à esquerda;*

(ii) *A é semi-simples à esquerda;*

(iii) *A tem um ideal minimal à esquerda;*

(iv) *$A \cong M_n(D)$ para algum número natural n e algum anel de divisão D.*

O teorema acima nos diz que um anel simples satisfazendo CCD é semi-simples à esquerda. A hipótese de satisfazer CCD é essencial, pois abaixo exibimos um exemplo de anel simples (este não satisfaz CCD) que não é semi-simples. Ao leitor interessado, indicamos ([5], p. 40).

Exemplo 2.19 *Sejam D um anel de divisão e $V_D = \bigoplus_{i \geqslant 1} e_i D$ um D-espaço vetorial à direita de dimensão infinita. Consideremos $E = End(V_D)$ e I um ideal de E consistindo de posto finito. Então o quociente $A = E/I$ é anel simples mas não é semi-simples.*

Finalizamos esta seção com o teorema de Wedderburn-Artin que como dissemos no início deste capítulo, é um caso particular do teorema de estrutura para anéis primitivos, teorema este que originou nosso trabalho. O teorema de Wedderburn-Artin é muito importante, pois a maneira como os anéis semi-simples à esquerda (à direita) são caracterizados (produto de matrizes quadradas sobre anéis de divisão) nos traz, como corolário, que anéis semi-simples à esquerda são semi-simples à direita (e reciprocamente), ou seja, podemos dizer apenas anéis semi-simples.

Teorema 2.20 ***(Teorema de Wedderburn-Artin)*** *Seja A um anel semi-simples à esquerda. Então $A \cong M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_r}(D_r)$ para anéis de divisão $D_1, \cdots, D_r$ e inteiros positivos $n_1, \cdots, n_r$ convenientes. O número r é unicamente determinado, assim como os pares $(n_1, D_1), \cdots, (n_r, D_r)$. Então há exatamente r módulos simples à esquerda mutuamente não isomorfos.*

2.4 Radical de Jacobson

O radical de Jacobson de um anel A é denotado por $rad\ A$ e é definido como a intersecção de todos os ideais à esquerda maximais de A.

De acordo com esta definição, $rad\ A$ deveria ser chamado radical à esquerda de A. Similarmente, definimos radical à direita de A como sendo a intersecção de ideais à direita maximais. De fato, o radical à direita e à esquerda coincidem e essa distinção é portanto desnecessária.

Proposição 2.21 *Seja A um anel não-nulo. Então A possui ideais à esquerda maximais.*

Demonstração: Seja $F = \{I : I$ é ideal à esquerda próprio de $A\}$. Claramente, $F \neq \emptyset$ pois $0 \in F$ e consideremos F parcialmente ordenado pela inclusão.

Seja F' um subconjunto não vazio de F e totalmente ordenado. Consideremos $J = \bigcup_{I' \in F'} I'$. Claramente, J é um ideal à esquerda de A, pois F' é totalmente ordenado. Por outro lado, $J \neq A$, pois caso contrário, $1 \in J$. Logo, $1 \in I'$ para algum $I' \in F'$ e isso nos dá que $I' = A$, absurdo.

Logo, $J \in F$ e é uma cota superior para F' em F. Pelo Lema de Zorn, existe I um elemento maximal em F, isto é, I é um ideal à esquerda próprio de A tal que se K é ideal à esquerda próprio de A tal que $I \subset K \subsetneqq A$ então $K = I$, ou seja, I é ideal à esquerda maximal de A. ■

Do exposto acima, $rad\ A \neq A$. Se $A = 0$, não há ideais à esquerda maximais e definimos $rad\ A = 0$.

O lema abaixo, cuja demonstração pode ser encontrada em ([5], p. 50) nos dá uma caracterização dos elementos do $rad\ A$.

Lema 2.22 *Seja $y \in A$. Então são equivalentes:*
(i) *$y \in rad\ A$;*
(ii) *$1 - xy$ é invertível à esquerda para qualquer $x \in A$;*
(iii) *$yM = 0$ para qualquer A-módulo à esquerda simples M.*

Lembramos que o anulador de um módulo M é dado por $An_A(M) := \{a \in A : am = 0, \forall\ m \in M\}$.

Observemos que no caso em que $A \neq 0$, a existência de ideais à esquerda maximais de A nos dá trivialmente a existência de A-módulos simples (veja Teorema 1.35), sendo que no caso $A = 0$, $rad\ A = 0$. Podemos enunciar o seguinte

Corolário 2.23 *$rad\ A = \bigcap An_A(M)$, interseção dos anuladores de todos os A-módulos simples. Em particular, $rad\ A$ é um ideal de A.*

Demonstração: Provemos que $rad\ A \subseteq \bigcap An_A(M)$. Seja $y \in rad\ A$. Pelo Lema 2.22, $yN = 0$ para qualquer A-módulo simples N. Logo, $y \in An_A(N)$, para qualquer A-módulo simples N, isto é, $y \in \bigcap An_A(M)$ (interseção dos anuladores de todos os A-módulos simples).

Agora, seja $y \in \bigcap An_A(M)$, para todo M simples. Então, $yM = 0$ para todo A-módulo simples M. Pelo Lema 2.22, $y \in rad\ A$.

É claro que $rad\ A$ é um ideal de A, pois é a interseção de ideais de A. ■

Definição 2.24 *Seja A um anel. Dizemos que A é Jacobson semi-simples (ou J-semi-simples) se $rad\ A = 0$.*

Mais adiante, veremos que a noção de J-semisimplicidade é bem relacionada com a noção de simplicidade.

Exemplo 2.25 *$\mathbb{Z}$ é um anel J-semi-simles, pois $rad\ \mathbb{Z} = \bigcap\limits_{p\ primo} p\mathbb{Z} = 0$, mas $\mathbb{Z}$ não é semi-simples ($\mathbb{Z}$ não é artiniano).*

Lema 2.26 *Seja A um anel não-nulo. Então todo ideal à esquerda próprio de A está contido em um ideal à esquerda maximal.*

Demonstração: Seja B um ideal à esquerda próprio de A. Consideremos $F = \{I \subsetneqq A : I$ é ideal à esquerda de A e $B \subset I\}$. Temos que $F \neq \emptyset$, pois $B \in F$. Suponhamos que F seja parcialmente ordenado pela inclusão.

Seja F' um subconjunto não vazio de F e totalmente ordenado. Claramente, $J = \bigcup\limits_{I' \in F'} I'$ é um ideal à esquerda de A, pois F' é totalmente ordenado e $J \neq A$. Por outro lado, $B \subset J$ pois $B \subset K$ para algum $K \in F' \subset F$ (na verdade, $B \subset I'$, para todo $I' \in F'$). Assim, $J \in F$ e é uma cota superior para F' em F. Pelo Lema de Zorn, F possui um elemento maximal, existe I ideal à esquerda próprio de A tal que $B \subset I$ e se K é um elemento de F tal que $I \subset K \subsetneqq A$ então $K = I$, isto é, I é ideal à esquerda maximal. ■

Teorema 2.27 *Seja A um anel. Então são equivalentes:*

(i) *A é semi-simples;*

(ii) *A é J-semi-simples e artiniano à esquerda.*

Demonstração: (i) $\Rightarrow$ (ii) Seja A um anel semi-simples e $U = rad\ A$. Então podemos escrever $A = U \oplus B$ para algum ideal à esquerda B de A. Suponhamos $U \neq 0$. Isto implica que $A \neq 0$ e daí, $U \neq A$. Logo, $B \neq 0$. Pelo Lema 2.26, existe M um ideal à esquerda maximal de A tal que $B \subset M$. Por definição, $U = rad\ A \subset M$ e assim, $U + B \subset M$. Portanto, $M = A$ e isso é um absurdo.

Sendo A semi-simples, segue, pelo Corolário 2.17, que A é artiniano à esquerda.

(ii) $\Rightarrow$ (i) Observemos primeiro que todo ideal à esquerda minimal I de A é um somando direto de ${}_AA$. Como $rad\ A = 0$, segue que existe um ideal à esquerda maximal M de A tal que $I \not\subset M$, pois caso contrário, isto é, se I estivesse contido em qualquer ideal à esquerda maximal de A então $I \subset rad\ A = 0$, absurdo pois $I \neq \{0\}$. Sendo que I é minimal, M é maximal e $I \not\subset M$, segue que $I \cap M = \{0\}$ e $I + M = A$. Logo, $I \oplus M =_A A$.

Agora, A é artiniano à esquerda então é claro que A possui um ideal à esquerda minimal A_1 e, pelo que observamos acima, ${}_AA = A_1 \oplus B_1$ para algum ideal à esquerda B_1 de A. Aplicando novamente CCD, existe um ideal à esquerda minimal $A_2 \subset B_1$ de A. Além disso, ${}_AA = A_2 \oplus B_2$ para algum ideal à esquerda B_2 de A. Segue que $A = A_1 \oplus A_2 \oplus (B_1 \cap B_2)$. Repetindo o procedimento, obtemos

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_n \oplus (B_1 \cap B_2 \cap \cdots \cap B_n),$$

onde $B_1 \supset B_1 \cap B_2 \supset \cdots \supset B_1 \cap B_2 \cap \cdots \cap B_n$ e os ideais à esquerda $A_i's$ são minimais. Por hipótese, existe um inteiro m tal que $B_1 \cap B_2 \cap \cdots \cap B_m = 0$. Assim, $A = A_1 \oplus A_2 \oplus \cdots \oplus A_m$ e A é semi-simples, os $A_i's$ sendo ideais à esquerda minimais equivalem a A-submódulos simples. ■

Finalizamos esta seção com uma relação entre ideais nil e $rad\ A$ do anel A.

Definição 2.28 *Um ideal U de A é dito nil se U é constituído por elementos nilpotentes do anel A (lembrando que um elemento $x \in A$ é dito nilpotente se $x^n = 0$, para algum $n \geqslant 1$).*

Exemplo 2.29 *Considere o anel $A = \mathbb{Z}[x_1, x_2, x_3, \cdots]/(x_1^2, x_2^3, x_3^4, \cdots)$ (onde $(x_1^2, x_2^3, x_3^4, \cdots)$ é o ideal gerado por $x_1^2, x_2^3, x_3^4, \cdots$) e o ideal U gerado por $\overline{x_1}, \overline{x_2}, \overline{x_3}, \cdots$. Portanto, U é um ideal nil.*

Temos que $U = (\overline{x_1}, \overline{x_2}, \cdots)$ e claramente $\overline{x_i}^{\,i+1} = \overline{0}$, para todo $i \in \{1, 2, \cdots\}$. Seja $\overline{x} \in U$. Então $\overline{x} = \sum_{i \in F} \overline{a_i}\,\overline{x_i}$, onde F é um subconjunto finito de $\{1, 2, \cdots\}$ e $\overline{a_i} \in A$, para todo $i \in F$. Devemos mostrar que $\overline{x}$ é nilpotente. Para isto, observamos que

(i) como A é anel comutativo, então para qualquer $\overline{a} \in A$, se $\overline{y} \in A$ é nilpotente, então $\overline{a}\,\overline{y}$ é nilpotente. De fato, suponhamos $\overline{y}^n = \overline{0}$, para algum $n \geqslant 1$. Daí, $(\overline{a}\,\overline{y})^n = \overline{a}^n \overline{y}^n = \overline{0}$;

(ii) se $\overline{x}$ e $\overline{y}$ são elementos nilpotentes de A, como $\overline{x}\,\overline{y} = \overline{y}\,\overline{x}$ (A é comutativo), segue que $\overline{x} + \overline{y} = \overline{x+y}$ é um elemento nilpotente. Basta desenvolvermos $(\overline{x+y})^{n+m}$, onde $\overline{x}^n = 0 = \overline{y}^m$ e chegaremos que $(\overline{x} + \overline{y})^{n+m} = (\overline{x+y})^{n+m} = \overline{0}$. Por indução, não é difícil mostrar que se $\overline{y_1}, \overline{y_2}, \cdots, \overline{y_k}$ são elementos nilpotentes de A então também o é $\overline{y_1} + \overline{y_2} + \cdots + \overline{y_k}$.

Agora, de (i) e (ii) é fácil ver que $\overline{x}$ acima é nilpotente.

Teorema 2.30 *Seja U um ideal nil de A. Então $U \subset rad\ A$.*

Demonstração: Seja $y \in U$. Então para qualquer $x \in A$, $xy \in U$ e portanto, xy é nilpotente. Daí, existe $n \in \mathbb{N}$, $n \geqslant 1$ tal que $(xy)^n = 0$.

Verificamos que $\sum\limits_{i=0}^{n-1} (xy)^i$ é o inverso de $1 - xy$. De fato,

$$\begin{aligned}
(1-xy)\sum_{i=0}^{n-1}(xy)^i &= (1-xy)(1+xy+(xy)^2+\cdots+(xy)^{n-1}) \\
&= 1+xy+(xy)^2+\cdots+(xy)^{n-1}-xy-(xy)^2-\cdots-(xy)^{n-1} \\
&= 1.
\end{aligned}$$

Analogamente, $(\sum\limits_{i=0}^{n-1} (xy)^i)(1-xy) = 1$. Logo, pelo Lema 2.22, $y \in rad\ A$. ■

Capítulo 3

Anéis Primos e Semiprimos

Nesse capítulo, nos dedicamos a estudar a estrutura dos anéis primos e semiprimos. Veremos a relação entre essas duas estruturas e além disso, a relação que essas estruturas possuem com as estruturas de anéis já vistas até agora.

3.1 Ideais Primos

Seja I um ideal de um anel A. Dizemos que I é um ideal completamente primo se para $x, y \in A$ tais que $xy \in I$, então $x \in I$ ou $y \in I$.

Dizemos que I é um ideal primo se para quaisquer ideais U e V de A tais que $UV \subseteq I$ então $U \subseteq I$ ou $V \subseteq I$.

Quando A é um anel comutativo, temos o seguinte resultado

Proposição 3.1 *Um ideal I é completamente primo se, e somente se, I é ideal primo.*

Demonstração: ($\Rightarrow$) Consideremos U e V dois ideais não-nulos de A tais que $UV \subseteq I$ (os casos em que U ou V são nulos são triviais). Suponhamos que $V \not\subseteq I$. Mostremos que $U \subseteq I$.

De fato, sejam $v \in V \backslash I$ e $u \in U$ tais que $uv \in I$. Por hipótese, $u \in I$ ou $v \in I$. Como $v \in V \backslash I$, segue que $u \in I$. Portanto $U \subseteq I$.

($\Leftarrow$) Sejam $x, y \in A$ tais que $xy \in I$. Consideremos os ideais Ax e Ay. Então $AxAy \overset{(*)}{=} Axy \subseteq I$.

A igualdade $(*)$ vale, pois A é comutativo. Se $Ax \subseteq I$ então $x \in I$. Se $Ay \subseteq I$ então $y \in I$. $\blacksquare$

Vemos assim que as definições de ideais completamente primo e primo são equivalentes no contexto comutativo.

A proposição a seguir nos dá outras formas de caracterizar ideais primos em anéis arbitrários. Lembramos que $(u) = AuA$ denota o ideal gerado por $u \in A$, para qualquer $u \in A$.

Proposição 3.2 *Para um ideal I de A são equivalentes:*
(i) *I é primo;*
(ii) *dados $u, v \in A$ tais que $(u)(v) \subseteq I$ então $u \in I$ ou $v \in I$;*
(iii) *dados $u, v \in A$ tais que $uAv \subseteq I$ então $u \in I$ ou $v \in I$;*
(iv) *dados U e V ideais à esquerda de A tais que $UV \subseteq I$ então $U \subseteq I$ ou $V \subseteq I$;*
(iv)' *dados U e V ideais à direita de A tais que $UV \subseteq I$ então $U \subseteq I$ ou $V \subseteq I$;*

Demonstração: (i) $\Rightarrow$ (ii) Se $(u)(v) \subseteq I$ para $u, v \in A$, então segue por (i) que $(u) \subseteq I$ ou $(v) \subseteq I$. Logo, $u \in I$ ou $v \in I$
(ii) $\Rightarrow$ (iii) Notemos que $(u)(v) = AuAAvA \subseteq AuAvA$. Como $uAv \subseteq I$ por hipótese, segue que $AuAvA \subseteq AIA \subseteq I$, pois I é ideal de A. Logo, $(u)(v) \subseteq I$ e por (ii) segue que $u \in I$ ou $v \in I$.
(iii) $\Rightarrow$ (iv) Sejam U e V ideais à esquerda de A tais que $UV \subseteq I$. Suponhamos que $U \not\subset I$. Devemos provar que $V \subseteq I$.

Sejam $u \in U \backslash I$ e $v \in V$. Como V é ideal à esquerda de A, vem que $uAv \subseteq UV \subseteq I$. Por (iii) segue que $u \in I$ ou $v \in I$. Como $u \notin I$, segue que $v \in I$ e daí $V \subseteq I$.
(iv) $\Rightarrow$ (i) Sejam U e V ideais de A tais que $UV \subseteq I$. Claramente U e V são ideais à esquerda de A e portanto, $U \subseteq I$ ou $V \subseteq I$.

As implicações (iii) $\Rightarrow$ (iv)' e (iv)' $\Rightarrow$ (i) são análogas, considerando ideais à direita. ■

Observamos que todo ideal maximal de A é primo, sendo falsa a recíproca.

De fato, sejam I, J ideais de A tais que $IJ \subset M$. Queremos mostrar que $I \subset M$ ou $J \subset M$.

Suponhamos que $I \not\subset M$. Como M é maximal, segue que $I + M = A$. Por outro lado, $J + M = A(J + M) = (I + M)(J + M) \overset{(*)}{\subset} IJ + M \subset M$, pois $IJ \subset M$. Assim, $J + M \subset M$ e portanto, $J \subset M$.

Provando $(*)$: seja $z \in (I + M)(J + M)$. Então $z = \sum_{i \in F} x_i y_i$, onde $x_i \in I + M$ e $y_i \in J + M$, para todo $i \in F$, onde F é um conjunto finito. Assim, para cada $i \in F$, temos $x_i = a_i + b_i$ e $y_i = c_i + d_i$ com $a_i \in I$, $c_i \in J$ e $b_i, d_i \in M$.

Portanto, $z = \sum_{i \in F} (a_i + b_i)(c_i + d_i) = \sum_{i \in F} a_i c_i + \sum_{i \in F} (a_i d_i + b_i c_i + b_i d_i) \in IJ + M$.

Exemplo 3.3 *$\{0\}$ é um ideal primo em $\mathbb{Z}$ e não é maximal.*

Exemplo 3.4 *Considerando A um anel simples, então o anel $M_n(A)$ (anel das matrizes $n \times n$ com entradas em A) é um anel simples. Este fato é devido ao seguinte resultado que pode ser visto em ([5], Theorem 3.1, p. 31): Seja A um anel. Então todo ideal I de $M_n(A)$ é da forma $M_n(J)$ para um ideal unicamente determinado J de A. Em particular, se A é simples o é $M_n(A)$.*

Mostraremos no capítulo 4 que todo anel simples é primo. Assim, o anel $M_n(A)$ é simples se A é simples e portanto, um anel primo.

Definição 3.5 *Um conjunto não vazio $S \subseteq A$ é chamado m-sistema se para quaisquer $u, v \in S$, existe $a \in A$ tal que $uav \in S$.*

Exemplo 3.6 *Todo conjunto não vazio multiplicativamente fechado é um m-sistema.*

Exemplo 3.7 *Sejam A um anel e $a \in A$. O conjunto $\{a, a^2, a^4, a^8, \cdots\}$ é um m-sistema.*

Corolário 3.8 *Um ideal I de A é primo se, e somente se, $A \setminus I$ é um m-sistema.*

Demonstração: ($\Rightarrow$) Sejam $u, v \in A \setminus I$. Como I é primo, temos que se $uAv \subseteq I$ então $u \in I$ ou $v \in I$ o que é um absurdo visto que tomamos $u, v \in A \setminus I$. Assim, existe $a \in A$ tal que $uav \notin I$, isto é, $uav \in A \setminus I$. Logo, $A \setminus I$ é um m-sistema.
($\Leftarrow$) Suponhamos $u, v \in A$ tais que $uAv \subseteq I$, mas $u \notin I$ e $v \notin I$. Daí, $u, v \in A \setminus I$ e por ser $A \setminus I$ um m-sistema, existe $a \in A$ tal que $uav \in A \setminus I$, o que é um absurdo, pois $uAv \subseteq I$. ■

Proposição 3.9 *Sejam $S \subseteq A$ um m-sistema e I um ideal maximal com respeito à propriedade de que I não intercepta S. Então I é um ideal primo.*

Demonstração: Suponhamos que I não seja um ideal primo. Daí, existem $u, v \in A$ tais que $(u)(v) \subseteq I$, mas $u \notin I$ e $v \notin I$. Sendo que $I \subsetneqq I + (u)$ e $I \subsetneqq I + (v)$ segue, pela maximalidade da propriedade de I, que existem $s, s' \in S$ tais que $s \in I + (u)$ e $s' \in I + (v)$. Sendo S um m-sistema, existe $a \in A$ tal que $sas' \in S$. Então $sas' \in (I+(u))A(I+(v)) \subseteq I+(u)(v) \subseteq I$ e isso é uma contradição, pois $sas' \in S \cap I$. Logo, I é ideal primo. ■

Definição 3.10 *Para um ideal U em um anel A, definimos o radical de U por $\sqrt{U} = \{s \in A :$ todo m-sistema contendo s intercepta $U\}$.*

Observação 3.11 *Na verdade, $\sqrt{U} \subseteq \{s \in A : s^n \in U$ para algum $n \geqslant 1\}$.*

De fato, seja $x \in \sqrt{U}$ e consideremos o m-sistema $S = \{x, x^2, \cdots, x^n, \cdots\}$. Por hipótese, $S \cap U \neq \emptyset$. Assim, existe $n_0 \in \mathbb{N}$, $n_0 \geqslant 1$ tal que $x^{n_0} \in S \cap U$ e portanto, $x^{n_0} \in U$. Logo, $x \in \{s \in A : s^n \in U \text{ para algum } n \geqslant 1\}$.

Teorema 3.12 *Para qualquer ideal U de A, $\sqrt{U}$ é igual a interseção de todos os ideais primos que contêm o ideal U. Em particular, $\sqrt{U}$ é um ideal de A.*

Demonstração: Sejam $s \in \sqrt{U}$ e P um ideal primo de A tal que $U \subseteq P$. Assim, $A \setminus P$ é um m-sistema e notemos que $s \notin A \setminus P$, pois se $s \in A \setminus P$ então $(A \setminus P) \cap U \neq \emptyset$ o que implicaria $(A \setminus P) \cap P \neq \emptyset$, o que é um absurdo. Logo, $s \in P$, para todo ideal primo P que contém U.

Reciprocamente, mostremos que $\bigcap\limits_{\substack{P \text{ primo} \\ U \subseteq P}} P \subset \sqrt{U}$. Suponhamos que exista $s \in \bigcap\limits_{\substack{P \text{ primo} \\ U \subseteq P}} P$ tal que $s \notin \sqrt{U}$. Daí, existe um m-sistema S que contém s e é tal que $S \cap U = \emptyset$. Pelo Lema de Zorn, existe um ideal P de A que contém U e que é maximal com respeito à propriedade de ser disjunto de S. Pela Proposição 3.9, P é ideal primo e portanto, $s \notin P$, o que é um absurdo. ■

3.2 Ideais Semiprimos, Anéis Primos e Semiprimos

Nesta seção, introduzimos a noção de ideal semiprimo, vímos a relação entre um ideal semiprimo e seu radical, para então definirmos os anéis primos (anéis semiprimos).

Definição 3.13 *Um ideal C de um anel A é dito um ideal semiprimo se para todo ideal U de A tal que $U^2 \subseteq C$ então $U \subseteq C$.*

Notemos que todo ideal primo é semiprimo.

A proposição abaixo nos dá definições equivalentes de um ideal semiprimo.

Proposição 3.14 *Para um ideal C de A são equivalentes:*

(i) *C é semiprimo;*

(ii) *dado $r \in A$ tal que $(r)^2 \subseteq C$ então $r \in C$;*

(iii) *dado $r \in A$ tal que $rAr \subseteq C$ então $r \in C$;*

(iv) *dado U um ideal à esquerda A tal que $U^2 \subseteq C$ então $U \subseteq C$;*

(iv)' *dado U um ideal à direita A tal que $U^2 \subseteq C$ então $U \subseteq C$.*

Demonstração: (i) $\Rightarrow$ (ii) Temos que $(r)^2 \subseteq C$ e como C é um ideal semiprimo, segue que $(r) \subseteq C$, ou seja, $r \in C$.

(ii) $\Rightarrow$ (iii) Notemos que $(r)(r) = ArAArA \subseteq ArArA$. Como $rAr \subseteq C$ por hipótese, segue que $ArArA \subseteq ACA \subseteq C$. Logo, $(r)^2 \subseteq C$ e por (ii), $r \in C$.
(iii) $\Rightarrow$ (iv) Seja U ideal à esquerda de A tal que $U^2 \subseteq C$. Suponhamos que $U \not\subset C$. Tomemos $u \in U \backslash C$. Como U é ideal à esquerda de A, segue que $uAu \subseteq U^2 \subseteq C$. Logo, $u \in C$ por (iii) e isso é um absurdo.
(iv) $\Rightarrow$ (i) Seja U ideal de A tal que $U^2 \subseteq C$. Claramente U é ideal à esquerda de A e portanto, $U \subseteq C$.

As implicações (iii) $\Rightarrow$ (iv)' e (iv)' $\Rightarrow$ (i) são análogas, considerando ideais à direita. ■

Definição 3.15 *Um conjunto não vazio S de A é chamado n-sistema se para qualquer $u \in S$, existe $a \in A$ tal que $uau \in S$.*

Notemos que todo m-sistema é um n-sistema.

Corolário 3.16 *Um ideal C é semiprimo se, e somente se, $A \backslash C$ é um n-sistema*

Demonstração: A demonstração é análoga à demonstração do Corolário 3.8. ■

Lema 3.17 *Sejam N um n-sistema e $v \in N$. Então existe um m-sistema $M \subseteq N$ tal que $v \in M$.*

Demonstração: Definimos $M = \{m_1, m_2, m_3, \cdots\}$, onde $m_1 = v \in N$, $m_2 = m_1 a_1 m_1 \in N$ (para algum $a_1 \in A$), $m_3 = m_2 a_2 m_2 \in N$ (para algum $a_2 \in A$), e assim sucessivamente para todos os elementos de M. Provemos que M é um m-sistema, ou seja, para quaisquer $i, j \in \mathbb{N}$, $m_i A m_j$ contém elementos de M. De fato, sejam $i, j \in \mathbb{N}$. Então se $i \leqslant j$ temos que $m_{j+1} \in m_j A m_j \subset m_i A m_j$ e se $i \geqslant j$ então $m_{i+1} \in m_i A m_i \subset m_i A m_j$. ■

Teorema 3.18 *Para um ideal C de A, as seguintes afirmações são equivalentes:*
(i) *C é um ideal semiprimo;*
(ii) *C é uma interseção de ideais primos;*
(iii) *$C = \sqrt{C}$.*

Demonstração: (iii) $\Rightarrow$ (ii) Segue do Teorema 3.12.
(ii) $\Rightarrow$ (i) Sendo C uma interseção de ideais primos então C é um ideal semiprimo.
(i) $\Rightarrow$ (iii) Devemos mostrar que $\sqrt{C} \subseteq C$. Suponhamos o contrário, então existe $a \in \sqrt{C}$ tal que $a \notin C$. Definimos o n-sistema $N = A \backslash C$ e claramente $a \in N$. Pelo Lema 3.17 existe um m-sistema $M \subseteq N$ tal que $a \in M$. Logo, M não intercepta C e pela Definição 3.10, $a \notin \sqrt{C}$, o que é um absurdo. ■

Definição 3.19 *Para qualquer anel A, definimos $Nil_*A = \sqrt{\{0\}}$. Nil_*A é o menor ideal semiprimo de A (e é igual a interseção de todos os ideais primos de A). Na literatura, Nil_*A é chamado radical de Baer-McCoy de A ou radical primo de A.*

Definição 3.20 *Um anel A é dito anel primo (respectivamente semiprimo) se $\{0\}$ é um ideal primo (respectivamente semiprimo).*

É claro que todo anel primo é semiprimo.

Proposição 3.21 *Para um anel A, são equivalentes:*
(i) *A é anel semiprimo;*
(ii) *$Nil_*A = \{0\}$;*
(iii) *A não tem ideal nilpotente diferente de zero (isto é, não existe I ideal não-nulo de A tal que $I^n = \{0\}$ para algum número natural n);*
(iv) *A não tem ideal à esquerda nilpotente diferente de zero.*

Demonstração: (i) $\Leftrightarrow$ (ii) Sendo A é anel semiprimo, $\{0\}$ é ideal semiprimo e, pelo Teorema 3.18, $Nil_*A = \sqrt{\{0\}} = \{0\}$. Reciprocamente, se $Nil_*A = \{0\}$ então $\sqrt{\{0\}} = \{0\}$ é um ideal semiprimo e novamente pelo Teorema 3.18 A é anel semiprimo.
(iv) $\Rightarrow$ (iii) Seja U um ideal nilpotente de A, logo U é ideal à esquerda nilpotente de A. Assim, $U^n = \{0\}$ e isto implica que $U = \{0\}$.
(iii) $\Rightarrow$ (i) Seja U um ideal de A tal que $U^2 \subseteq \{0\}$, ou seja, $U^2 = \{0\}$. Como A não tem ideal nilpotente não-nulo, segue que $U = \{0\}$. Logo, A é semiprimo.
(i) $\Rightarrow$ (iv) Suponhamos A um anel semiprimo e seja U um ideal à esquerda nilpotente. Assim, existe $n \in \mathbb{N}$ mínimo tal que $U^n = \{0\}$.

Se $n > 1$ então $(U^{n-1})^2 = U^{2n-2} \subseteq U^n = \{0\}$. Por (i), $U^{n-1} = \{0\}$, o que é um absurdo visto que n é o menor elemento tal que $U^n = \{0\}$. Portanto, $n = 1$ e $U = \{0\}$. ■

Exemplo 3.22 *Um anel A é primo (respectivamente semiprimo) se, e só se, o anel $M_n(A)$ é primo (respectivamente semiprimo). O leitor interessado pode consultar ([5], Proposition 10.20, p. 160).*

O teorema abaixo é o análogo do Teorema 2.27 só que ao invés de anéis J-semi-simples trataremos anéis semiprimos. Sua demonstração pode ser vista em ([5], p. 162).

Teorema 3.23 *Seja A um anel. Então são equivalentes:*
(i) *A é semi-simples;*
(ii) *A é semiprimo e artiniano à esquerda.*

Capítulo 4

Teorema de Estrutura para Anéis Primitivos à Esquerda

Neste capítulo, mostraremos a relação entre todos os anéis já estudados até agora, incluindo os anéis primitivos que serão estudados efetivamente aqui. O objetivo principal deste capítulo que, na verdade, é o objetivo principal deste trabalho, é demonstrar o teorema da estrutura para anéis primitivos à esquerda (à direita) e, para isso, desenvolvemos alguns outros resultados como, por exemplo, o teorema da Densidade de Jacobson-Chevalley.

4.1 Anéis Primitivos e Semiprimitivos

Afim de definirmos anéis primitivos à esquerda, chamamos a atenção para a seguinte caracterização de anéis semiprimitivos (ou anéis J-semi-simples).

Proposição 4.1 *Um anel A é semiprimitivo se, e somente se, A possui um módulo à esquerda M semi-simples e fiel.*

Demonstração: ($\Rightarrow$) Seja A um anel semiprimitivo. Então $rad\ A = 0$.

Seja $\{M_i\}$ a família de todos os A-módulos à esquerda simples. Logo, pelo Teorema 2.13, $\bigoplus\limits_i M_i = M$ é um módulo semi-simples. Como $An_A(M) = \bigcap\limits_i An_A(M_i)$, segue do Corolário 2.23 que $An_A(M) = rad\ A = 0$. Assim, M é um A-módulo à esquerda semi-simples e fiel.

($\Leftarrow$) Seja M um A-módulo à esquerda semi-simples e fiel. Pelo Lema 2.22, sabemos que $rad\ A$ anula todos os A-módulos à esquerda simples e sendo que $An_A(M) = 0$ segue que $rad\ A = 0$. Portanto, A é semiprimitivo. ■

Esta proposição motiva a seguinte definição

Definição 4.2 *Um anel não-nulo A é dito primitivo à esquerda (respectivamente à direita) se A possui um A-módulo à esquerda (respectivamente à direita) simples e fiel. Notemos que A é necessariamente não-nulo.*

A noção de semiprimitividade independe dos adjetivos esquerda-direita, o que não ocorre com a primitividade de um anel. Um dos primeiros exemplos que retrata esta situação foi construído por G. Bergman em 1965.

Proposição 4.3 *Todo anel simples é primitivo à esquerda (respectivamente à direita).*

Demonstração: Seja A um anel simples. Devido a este fato, A age fielmente em qualquer A-módulo M não-nulo, pois $An_A(M)$ é um ideal de A. Sendo A não-nulo, a existência de A-módulos simples já foi garantida pelo Teorema 1.35. Assim, A é anel primitivo à esquerda. ■

Proposição 4.4 *Todo anel primitivo à esquerda é semiprimitivo.*

Demonstração: Seja A um anel primitivo à esquerda. Então A possui um A-módulo à esquerda simples e fiel M. Logo, M é semi-simples e portanto, A é semiprimitivo. ■

Proposição 4.5 *Todo anel primitivo à esquerda é primo.*

Demonstração: Sejam A um anel primitivo à esquerda e M um A-módulo à esquerda simples e fiel. Provemos que A é anel primo. Seja U um ideal não-nulo de A.

Então, UM é um A-submódulo de M e como M é fiel, segue que UM é um submódulo não-nulo de M, o que implica $UM = M$. Se V é um ideal qualquer não-nulo de A, então

$(VU)M = V(UM) = VM = M$, o que implica $VU \neq 0$ e portanto A é um anel primo. ■

Proposição 4.6 *Todo anel semiprimitivo é semiprimo.*

Demonstração: Pela Observação 3.11, $Nil_*A = \sqrt{\{0\}}$ é um ideal nil de A. Pelo Teorema 2.30, $Nil_*A \subset rad\ A$ e, por hipótese, $rad\ A = \{0\}$. Logo, $Nil_*A = \{0\}$. Pela Proposição 3.21, A é anel semiprimo.

Com base nos Teoremas 2.18, 2.27 e nas proposições acima, vemos que a cadeia de implicações a seguir é verdadeira

$$\begin{array}{ccccc}
A \text{ é semi-simples} & \Rightarrow & A \text{ é semiprimitivo (ou } J\text{-semi-simples)} & \Rightarrow & A \text{ é semiprimo} \\
\Uparrow \text{(se CCD)} & & \Uparrow & & \Uparrow \\
A \text{ é simples} & \Rightarrow & A \text{ é primitivo à esquerda} & \Rightarrow & A \text{ é primo}
\end{array}$$

4.2 O Teorema de Estrutura

Sejam A, k dois anéis, $V = {}_AV_k$ um (A,k)-bimódulo e $E = End(V_k)$, o qual age à esquerda em V. Dizemos que A *age densamente sobre* V_k se para qualquer $f \in E$ e quaisquer $v_1, v_2, \cdots, v_n \in V$, existe $a \in A$ tal que $av_i = f(v_i)$ para $i = 1, 2, \cdots, n$.

Lema 4.7 *Com a notação acima, consideremos ${}_AV$ um A-módulo semi-simples e $k = End({}_AV)$. Então qualquer A-submódulo W de V é um E-submódulo de V.*

Demonstração: Como V é semi-simples, existe W' um A-submódulo de V tal que $V = W \oplus W'$.

Seja $p : V \to V$ a projeção de $V = W \oplus W'$ sobre W, isto é, para $v = w + w' \in V$, $(v)p = w$, $p \in k$.

Queremos mostrar que $f(W) \subset W$, para todo $f \in E$. Seja $w \in W$. Então

$$f(w) = f((w+0)p) = (f(w))p \in W.$$

Logo, $f(W) \subset W$. ■

Lema 4.8 *Sejam A um anel, V um A-módulo à esquerda e $k = End({}_AV)$. Definimos $\tilde{V} = V^n = \bigoplus_{i=1}^{n} V_i$, onde $V_i = V$ e $\tilde{k} = End({}_A\tilde{V})$. Então $\tilde{k} \cong M_n(k)$.*

Demonstração: Seja $f \in End({}_A\tilde{V})$. Consideremos $g_{ij} = p_i \circ f \circ i_j$, onde i_j é a j-ésima inclusão e p_i é a i-ésima projeção, para quaisquer $1 \leqslant i, j \leqslant n$. Afim de evitarmos repetição, dado $x \in V$, x pode ser escrito como $(0, \cdots, x_j, \cdots, 0)$, onde $x_j = x$, isso é possível devido às inclusões i_j.

Claramente, $g_{ij} : V \to V$ e $g_{ij} \in k$, pois g_{ij} é uma composição de A-homomorfismos. Portanto, a matriz $(g_{ij})_{1 \leqslant i,j \leqslant n} \in M_n(k)$. Definimos

$$\begin{array}{rccc} \varphi : & End({}_A\tilde{V}) & \to & M_n(k) \\ & f & \mapsto & (p_i \circ f \circ i_j)_{1 \leqslant i,j \leqslant n} \end{array}$$

Provemos que φ é um isomorfismo de anéis. De fato, sejam $x \in V$ e $f, g \in End({}_A\tilde{V})$. Para $1 \leqslant i, j \leqslant n$ fixados, temos

$$\begin{aligned} (p_i \circ (f+g) \circ i_j)(x) &= p_i((f+g)(i_j(x))) \\ &= p_i(f(i_j(x)) + g(i_j(x))) \\ &= p_i(f(i_j(x))) + p_i(g(i_j(x))) \\ &= (p_i \circ f \circ i_j)(x) + (p_i \circ g \circ i_j)(x) \\ &= (p_i \circ f \circ i_j + p_i \circ g \circ i_j)(x). \end{aligned}$$

Logo, $p_i \circ (f+g) \circ i_j \ = p_i \circ f \circ i_j + p_i \circ g \circ i_j$, para quaisquer $1 \leq i,j \leq n$ e portanto, $\varphi(f+g) = \varphi(f) + \varphi(g)$.

Agora, mostremos que $\varphi(f \circ g) = \varphi(f)\,\varphi(g)$. Para $1 \leq i,j \leq n$ fixados e $x \in V$, suponhamos que $g(0,\cdots,x_j,\cdots,0) = (y_1,\cdots,y_n)$ e que $f(y_1,y_2,\cdots,y_n) = (z_1,z_2,\cdots,z_n)$. Então, para todo $x \in V$, temos

$$\begin{aligned}(p_i \circ (f \circ g) \circ i_j)(x) &= p_i(f(g(x))) = p_i(f(y_1,\cdots,y_n)) \\ &= p_i(z_1,\cdots,z_n) = z_i.\end{aligned}$$

Observamos que $p_i \circ (f \circ g) \circ i_j$ é o elemento na posição (i,j) da matriz $\varphi(f \circ g)$.

Por outro lado, $\sum_{k=1}^{n} (p_i \circ f \circ i_k \circ p_k \circ g \circ i_j)$ é o elemento na posição $\varphi(f)\varphi(g)$. E para todo $x \in V$, temos

$$\begin{aligned}(\sum_{k=1}^{n}(p_i \circ f \circ i_k \circ p_k \circ g \circ i_j))(x) &= \sum_{k=1}^{n}(p_i \circ f \circ i_k \circ p_k \circ g \circ i_j)(x) \\ &= \sum_{k=1}^{n}(p_i \circ f)(0,\cdots,y_k,\cdots,0) \\ &= p_i(\sum_{k=1}^{n} f(0,\cdots,y_k,\cdots,0)) \\ &= p_i(f(y_1,\cdots,y_n)) \\ &= p_i(z_1,\cdots,z_n) = z_i.\end{aligned}$$

Logo, $p_i \circ (f \circ g) \circ i_j = \sum_{k=1}^{n} (p_i \circ f \circ i_k \circ p_k \circ g \circ i_j)$ para quaisquer $1 \leq i,j \leq n$ e portanto, $\varphi(f \circ g) = \varphi(f)\varphi(g)$. Assim, φ é um homomorfismo de anéis.

Mostremos que φ é sobrejetor. Seja $X \in M_n(k)$. Então $X = (g_{ij})_{1 \leqslant i,j \leqslant n}$ onde $g_{ij} : V \to V$ são A-homomorfismos. Mostremos que existe $g \in End({}_A\tilde{V})$ tal que $\varphi(f) = X$. Tomemos $g \in End({}_A\tilde{V})$ assim

$$g(x_1 + \cdots + x_n) = (g_{11}(x_1) + \cdots + g_{1n}(x_n), \cdots, g_{n1}(x_1) + \cdots + g_{nn}(x_n)).$$

Para i,j fixados e para qualquer $x \in V$, temos que

$$\begin{aligned}(p_i \circ g \circ i_j)(x) &= p_i(g(0,\cdots,x_j,\cdots,0)) \\ &= p_i(g_{1j}(x_j), g_{2j}(x_j), \cdots, g_{ij}(x_j), \cdots, g_{nj}(x_j)) \\ &= g_{ij}(x).\end{aligned}$$

Portanto, φ é sobrejetor, pois $p_i \circ g \circ i_j = g_{ij}$ para quaisquer $1 \leqslant i,j \leqslant n$. Assim, $\varphi(g) = X$.

Resta mostrarmos que φ é injetor. De fato, seja $f \in Ker(\varphi)$. Então $\varphi(f) = (p_i \circ f \circ i_j)_{1 \leqslant i,j \leqslant n} = 0$ (matriz nula).

Seja $(x_1, \cdots, x_n) \in \tilde{V}$. Então $f(x_1, \cdots, x_n) = (y_1, \cdots, y_n)$. Mostremos que $y_i = 0$, para todo $i \in \{1, 2, \cdots, n\}$.

Para i fixo, temos

$$\begin{aligned} y_i &= p_i(y_1, \cdots, y_i, \cdots, y_n) \\ &= p_i(\sum_{j=1}^{n} f(0, \cdots, x_j, \cdots, 0)) \\ &= p_i(\sum_{j=1}^{n} (f \circ i_j)(x)) \\ &= \sum_{j=1}^{n} (p_i \circ f \circ i_j)(x) \;=\; 0, \end{aligned}$$

pois $p_i \circ f \circ i_j = 0$ para quaisquer $i, j \in \{1, 2, \cdots, n\}$. Logo, $y_i = 0$ para qualquer $1 \leqslant i \leqslant n$ e portanto f é a função nula. ■

Teorema 4.9 ***(Teorema da densidade de Jacobson-Chevalley)*** *Sejam A um anel e V um A-módulo à esquerda semi-simples. Então para $k = End({}_AV)$, A age densamente sobre V_k.*

Demonstração: Seja $\tilde{V} = V^n = \bigoplus_{i=1}^{n} V_i$, onde $V_i = V$. Notemos que $\tilde{V}$ é um A-módulo semi-simples, pois cada $V_i = V$ é semi-simples, e daí, V é uma soma de módulos simples.

Definimos $\tilde{k} = End({}_A\tilde{V})$. Pelo lema acima $End({}_A\tilde{V}) \cong M_n(End({}_AV))$.

Seja $f \in E = End(V_k)$. Consideremos $\tilde{f} = (f, f, \cdots, f)$ uma função de $\tilde{V} \to \tilde{V}$, definida por $\tilde{f}((v_1, v_2, \cdots, v_n)) = (f(v_1), f(v_2), \cdots, f(v_n))$.

Provemos que $\tilde{f} \in End(\tilde{V}_{\tilde{k}})$. De fato, sejam $(w_1, w_2, \cdots, w_n), (w'_1, w'_2, \cdots, w'_n) \in \tilde{V}$ e $\tilde{e} \in \tilde{k}$. Então

$$\begin{aligned} \tilde{f}((w_1, \cdots, w_n) + (w'_1, \cdots, w'_n)) &= \tilde{f}((w_1 + w'_1, \cdots, w_n + w'_n)) \\ &= (f(w_1 + w'_1), \cdots, f(w_n + w'_n)) \\ &= (f(w_1) + f(w'_1), \cdots, f(w_n) + f(w'_n)) \\ &= (f(w_1), \cdots, f(w_n)) + (f(w'_1), \cdots, f(w'_n)) \\ &= \tilde{f}(w_1, \cdots, w_n) + \tilde{f}(w'_1, \cdots, w'_n); \end{aligned}$$

$$\begin{aligned} \tilde{f}((w_1, w_2, \cdots, w_n)\tilde{e}) &\overset{(*)}{=} \tilde{f}(\sum w_i e_{i1}, \cdots, \sum w_i e_{in}) \\ &= (f(\sum w_i e_{i1}), \cdots, f(\sum w_i e_{in})) \\ &\overset{(**)}{=} (\sum f(w_i) e_{i1}, \cdots, \sum f(w_i) e_{in}) \\ &= (f(w_1), \cdots, f(w_n))\tilde{e} \\ &= \tilde{f}((w_1, \cdots, w_n))\tilde{e}, \end{aligned}$$

onde a igualdade $(*)$ segue do fato de que $\tilde{k} \cong M_n(k)$ com $e_{ij} \in k$ e a igualdade $(**)$ ocorre pois $f \in End(V_k)$.

Sejam $v_1, v_2, \cdots, v_n \in V$. Consideremos $\tilde{W}$ um A-submódulo cíclico de V^n gerado por $(v_1, v_2, \cdots, v_n) \in V_n = \tilde{V}$, isto é, $\tilde{W} = A(v_1, v_2, \cdots, v_n)$. Sendo $\tilde{V}$ um A-módulo semi-simples e $\tilde{k} = End({}_A\tilde{V})$, segue do Lema 4.7 (aplicado a $\tilde{W}$), que $\tilde{W}$ é um $\tilde{E}$-submódulo de $\tilde{V}$, onde $\tilde{E} = End(\tilde{V}_{\tilde{k}})$.

Portanto, $\tilde{f}(v_1, v_2, \cdots, v_n) \in \tilde{W}$. Logo, existe $a \in A$ tal que $\tilde{f}(v_1, v_2, \cdots, v_n) = a(v_1, v_2, \cdots, v_n)$ e isto é equivalente a dizermos que $(f(v_1), f(v_2), \cdots, f(v_n)) = a(v_1, v_2, \cdots, v_n)$. Assim, $f(v_i) = av_i$ para $i \in \{1, 2, \cdots, n\}$ e A age densamente sobre V_k. ■

Corolário 4.10 *Sejam A, V, k e E como no teorema anterior. Se V_k é finitamente gerado como um k-módulo (à direita), então $\rho : A \to E$ é um homomorfismo sobrejetor de anéis.*

Demonstração: Seja $\rho : A \to E$ definida por $\rho(a)(v) = av$, para $a \in A$, e $v \in V$.

Vejamos que ρ é um homomorfismo de anéis. De fato, sejam $a_1, a_2 \in A$ e $v \in V$, temos que

$$\begin{aligned} \rho(a_1 + a_2)(v) &= (a_1 + a_2)v = a_1 v + a_2 v \\ &= \rho(a_1)(v) + \rho(a_2)(v) = (\rho(a_1) + \rho(a_2))(v); \end{aligned}$$

$$\begin{aligned} \rho(a_1 a_2)(v) &= (a_1 a_2)v = a_1(a_2 v) \\ &= \rho(a_1)(a_2 v) = \rho(a_1)(\rho(a_2)(v)) \\ &= (\rho(a_1) \circ \rho(a_2))(v). \end{aligned}$$

Provemos que ρ é sobrejetor. Por hipótese, V é um k-módulo finitamente gerado, isto é, existem $v_1, \cdots, v_n \in V$ tais que $V = \sum_{i=1}^{n} v_i k$.

Seja $f \in E$. Pelo Teorema da Densidade, existe $a \in A$ tal que $av_i = f(v_i)$ para $i = 1, 2, \cdots, n$. Portanto, para qualquer $v \in V$, $v = \sum_{i=1}^{n} v_i k_i$ para alguns $k_1, \cdots, k_n \in k$. Logo,

$$f(v) = f(\sum_{i=1}^{n} v_i k_i) \overset{(*)}{=} \sum_{i=1}^{n} f(v_i)k_i = \sum_{i=1}^{n} (av_i)k_i = a \sum_{i=1}^{n} v_i k_i = av = \rho(a)(v)$$

para todo $v \in V$ e isto nos diz que $f = \rho(a)$ e ρ é sobrejetor. Só para finalizar, a igualdade $(*)$ é devida ao fato de que $f \in E = End(V_k)$. ■

Um caso importante do Teorema da Densidade é quando V é um A-módulo à esquerda simples. Neste caso, o anel dos endomorfismos $k = End({}_AV)$ é um anel de divisão, pelo Lema de Schur, e então, V é um espaço vetorial à direita sobre k, o que nos sugere algumas relações importantes. Para tanto, definimos

Definição 4.11 *Sejam V um espaço vetorial à direita sobre o anel de divisão k e $E = End(V_k)$. Dizemos que um subconjunto $S \subset E$ é m-transitivo sobre V se* *para quaisquer vetores linearmente independentes $v_1, v_2, \cdots, v_n$, $n \leqslant m$ e quaisquer n vetores $v'_1, v'_2, \cdots, v'_n$ em V, existe $s \in S$ tal que $s(v_i) = v'_i$ para todo $i \in \{1, 2, \cdots, n\}$.*

Definição 4.12 *Dizemos que S é um conjunto denso das transformações lineares sobre V_k se S é m-transitivo para todo m (finito).*

Proposição 4.13 *Sejam V um (A, k)-bimódulo, sendo k é um anel de divisão, $E = End(V_k)$ e $\rho : A \to E$ a aplicação dada por $\rho(a)(v) = av$, para quaisquer $a \in A$ e $v \in V$. Então A age densamente sobre V_k se, e somente se, $\rho(A)$ é um anel denso de transformações lineares sobre V.*

Demonstração: $(\Rightarrow)$ Suponhamos que A age densamente sobre V_k. Sejam $v_1, v_2, \cdots, v_n \in V$ um conjunto linearmente independente de n vetores $(n \leqslant m)$ e $v'_1, v'_2, \cdots, v'_n \in V$ um outro conjunto de n vetores. Devemos provar que existe $a \in A$ tal que $\rho(a)(v_i) = v'_i$ para todo $i \in \{1, 2, \cdots, n\}$.

De fato, existe uma transformação linear f de $V \to V$ tal que $f(v_i) = v'_i$, o leitor interessado deve consultar ([3], Teorema 1, p. 69). Mas então, $f \in E$, e como A age densamente sobre V_k, existe $a \in A$ tal que $f(v_i) = av_i$.

Portanto, existe $s = \rho(a) \in \rho(A)$ tal que $s(v_i) = \rho(a)(v_i) = av_i = f(v_i) = v'_i$ e então $\rho(A)$ é um anel denso de transformações lineares.

$(\Leftarrow)$ Suponhamos agora que $\rho(A)$ é um anel denso de transformações lineares. Provemos que A age densamente sobre V_k.

Sejam $f \in E$ e $v_1, v_2, \cdots, v_n \in V$. Do conjunto $\{v_1, v_2, \cdots, v_n\}$, após uma reindexação, se necessário, extraímos o conjunto $\{v_1, v_2, \cdots, v_m\}$ k-linearmente independente, com $m \leqslant n$. Consideremos $f(v_1) = v'_1, \cdots, f(v_m) = v'_m$.

Como $\rho(A)$ é m-transitivo, então existe $a \in A$ tal que $av_i = \rho(a)(v_i) = v'_i = f(v_i)$. Daí, $f(v_i) = av_i$, para todo $i \leqslant m$.

Resta mostrarmos que $f(v_i) = av_i$ para todo $i \leqslant n$. Seja $i > m$ $(m + 1 \leqslant i \leqslant n)$. Como $v_1, v_2, \cdots, v_m$ são linearmente independentes, podemos escrever $v_i = \sum_{j=1}^{m} v_j \alpha_j$, $\alpha_j \in k$, logo

$$f(v_i) = f(\sum_{j=1}^{m} v_j \alpha_j) = \sum_{j=1}^{m} f(v_j)\alpha_j = \sum_{j=1}^{m} (av_j)\alpha_j = a \sum_{j=1}^{m} v_j \alpha_j = av_i.$$

Portanto, A age densamente sobre V_k. ■

Apesar de ser um resultado básico, optamos por demonstrar o seguinte lema.

Lema 4.14 *Sejam V um k-espaço vetorial à direita de dimensão n e $E = End(V_k)$. Então $E \cong M_n(k)$.*

Demonstração: Seja $\beta = \{v_1, \cdots, v_n\}$ uma base de V como k-espaço vetorial à direita. Então, para qualquer $j \in \{1, 2, \cdots, n\}$ e $f \in E$,

$$f(v_j) = \sum_{i=1}^{n} v_i \alpha_{ij}, \text{ com } \alpha'_{ij}s \in k.$$

Definimos $\psi : E \to M_n(k)$ por $\psi(f) = [f]_\beta = (\alpha_{ij})_{1 \leqslant i,j \leqslant n}$.

Provemos que ψ é um homomorfismo de anéis. De fato, sejam $f, g \in E$. Então

$$\psi(f + g) = [f + g]_\beta = [f]_\beta + [g]_\beta = \psi(f) + \psi(g);$$

$$\psi(f \circ g) = [f \circ g]_\beta = [f]_\beta[g]_\beta = \psi(f)\psi(g).$$

Mostremos que ψ é bijetor. Suponhamos $\psi(f) = \psi(g)$. Então $(\alpha_{ij})_{1 \leqslant i,j \leqslant n} = (\beta_{ij})_{1 \leqslant i,j \leqslant n}$ e isto equivale a dizermos que $\alpha_{ij} = \beta_{ij}$, para quaisquer $i, j \in \{1, 2, \cdots, n\}$. Portanto, $f = g$.

Mostremos que ψ é sobrejetora. De fato, dada $(a_{ij})_{1 \leqslant i,j \leqslant n} \in M_n(k)$. Consideremos $f \in E$ tal que $f(v_j) = \sum\limits_{i=1}^{n} v_i a_{ij}$, para todo $j \in \{1, 2, \cdots, n\}$. Daí, $\psi(f) = [f]_\beta = (a_{ij})_{1 \leqslant i,j \leqslant n}$ ■

Combinando os resultados 4.9, 4.10 e 4.13 finalizamos nosso trabalho com o principal resultado do mesmo.

Teorema 4.15 ***(Teorema de estrutura para anéis primitivos à esquerda)*** *Sejam A um anel primitivo à esquerda, V um A-módulo simples e fiel e $k = End(_AV)$ um anel de divisão. Então A é isomorfo a um anel denso de transformações lineares sobre V_k, e, além disso,*

(i) *se A é um anel artiniano à esquerda, então $dim_k(V) = n$ é finita e $A \cong M_n(k)$;*

(ii) *se A não é artiniano à esquerda, então $dim_k(V)$ é infinita e para qualquer inteiro $n > 0$, existe um subanel A_n de A que admite um homomorfismo sobrejetor $\varphi : A_n \to M_n(k)$.*

Demonstração: Seja $E = End(V_k)$. Definimos $\rho : A \to E$ por $\rho(a)(v) = av$, para quaisquer $a \in A$ e $v \in V$. Como antes, ρ é um homomorfismo de anéis.

Mostremos que ρ é injetor. De fato, seja $a \in Ker(\rho)$. Então $\rho(a) = 0$, ou seja, $\rho(a)(v) = av = 0$, para todo $v \in V$. Logo, $a \in An_A(V)$ e como V é um A-módulo fiel, segue que $a = 0$. Assim, $Ker(\rho) = \{0\}$, ou seja, ρ é injetor.

Daí, $A \cong \rho(A)$. Pelo Teorema 4.9, A age densamente sobre V_k e pela Proposição 4.13, $\rho(A)$ é um anel denso de transformações lineares.

Portanto, A é isomorfo ao anel denso de transformações lineares sobre V_k, a saber, $\rho(A)$.

Provemos agora (i) e (ii).

Suponhamos $dim_k(V) = n < \infty$. Assim, pelo Corolário 4.10 temos que ρ é sobrejetor, e como provamos acima que ρ é um homomorfismo injetor, segue que $A \cong \rho(A) = E$.

Pelo Lema 4.14, temos que $E \cong M_n(k)$ e sendo k um anel de divisão (anel simples), temos que $M_n(k)$ é simples. Logo, $A \cong E \cong M_n(k)$ é simples e segue do Teorema 2.18 que A é artiniano à esquerda.

Suponhamos $dim_k(V)$ infinita. Fixemos uma sequência $v_1, v_2, \cdots \in V$ de vetores linearmente independentes e consideremos os conjuntos

$$V_n = \sum_{i=1}^{n} v_i k \text{ com } 1 \leqslant n < \infty,$$

$$A_n = \{a \in A : a(V_n) \subseteq V_n\} \text{ e } U_n = \{a \in A : a(V_n) = 0\}.$$

Não é difícil ver que A_n é um subanel de A e que U_n é ideal de A_n e ideal à esquerda de A.

Para cada $1 \leqslant n < \infty$, temos que V_n é um módulo sobre o anel A_n/U_n, pois $U_n V_n = 0$ e a ação é dada por $\overline{a}v := av \in V_n$, para quaisquer $a \in A_n$ e $v \in V_n$.

Além disso, A_n/U_n age fielmente sobre V_n. De fato, se $\overline{a} \in A_n/U_n$ é tal que $\overline{a}v = 0$, para todo $v \in V_n$, então $0 = \overline{a}v = av$, para todo $v \in V_n$ e isto implica que $a \in U_n$. Logo, $\overline{a} = \overline{0}$.

Lembrando que, pela n-transitividade de $\rho(A)$ sobre V, para qualquer conjunto de vetores linearmente independentes $\{v_1, v_2, \cdots, v_n\} \subseteq V_n \subseteq V$ e qualquer outro conjunto de vetores $\{v'_1, v'_2, \cdots, v'_n\} \subset V$, existe $a \in A$ tal que $\rho(a)(v_i) = v'_i$, isto é, $av_i = v'_i$ para $i \in \{1, 2, \cdots, n\}$.

Consideremos $\phi : A_n \to End((V_n)_k)$ definida por $\phi(a)(v) = av$, para quaisquer $a \in A_n$ e $v \in V_n$.

Vejamos que $\phi(a) \in End((V_n)_k)$, para todo $a \in V_n$. De fato,

$$\phi(a)(v_1 + v_2) = a(v_1 + v_2) = av_1 + av_2 = \phi(a)(v_1) + \phi(a)(v_2)$$

e isto ocorre, pois v_1, v_2 estão em $V_n \subseteq V$ e V é um A-módulo à esquerda.

Também, para todo $v \in V_n$ e $\alpha \in k$, temos que

$$\phi(a)(v\alpha) = a(v\alpha) = (av)\alpha = (\phi(a)(v))\alpha$$

e isto ocorre, pois $v \in V_n \subseteq V$ e V é (A, k)-bimódulo.

Mostremos que ϕ é um homomorfismo de anéis, isto decorre do fato de que V é um A-módulo à esquerda. Sejam $a, b \in A_n$ e $v \in V_n$. Então

$$\phi(a+b)(v) = (a+b)v = av + bv = \phi(a)(v) + \phi(b)(v) = (\phi(a) + \phi(b))(v).$$

Donde $\phi(a+b) = \phi(a) + \phi(b)$. Por outro lado,

$$\phi(ab)(v) = (ab)v = a(bv) = \phi(a)(bv) = \phi(a)(\phi(b)(v)) = (\phi(a) \circ \phi(b))(v).$$

Daí, $\phi(ab) = \phi(a) \circ \phi(b)$.

Provemos que ϕ é sobrejetor. Seja $f \in End((V_n)_k)$. Como $\{f(v_1), \cdots, f(v_n)\} \subseteq V_n \subset V$ e pela n-transitividade de $\rho(A)$ sobre V, existe $a \in A$ tal que $\rho(a)(v_i) = f(v_i)$, ou seja, $av_i = f(v_i)$ para $i \in \{1, 2, \cdots, n\}$.

Por linearidade, para todo $v \in V_n$, temos

$$f(v) = f(\sum_{i=1}^{n} v_i\alpha_i) = \sum_{i=1}^{n} f(v_i)\alpha_i = \sum_{i=1}^{n} (av_i)\alpha_i = a \sum_{i=1}^{n} v_i\alpha_i = av \in V_n.$$

Logo, $aV_n \subseteq V_n$ e isto nos diz que $a \in A_n$. Portanto, $\phi(a)(v) = av = f(v)$, para todo $v \in V_n$ e assim, $\phi(a) = f$ e por conseguinte, ϕ é sobrejetor.

Provemos que $Ker(\phi) = U_n$. De fato, seja $a \in Ker(\phi)$. Então $0 = \phi(a)(v) = av$, para todo $v \in V_n$ e então $a \in U_n$. Por outro lado, seja $a \in U_n$. Então $0 = av = \phi(a)(v)$, para todo $v \in V_n$. Portanto, $a \in Ker(\phi)$. Assim, $A_n/U_n \cong End((V_n)_k) \cong M_n(k)$, onde o último isomorfismo é devido ao Lema 4.14.

Sabemos que $\rho(A)$ é m-transitivo para todo m, em particular, $\rho(A)$ é $(n+1)$-transitivo. Logo, para o conjunto de vetores linearmente independentes $\{v_1, v_2, \cdots, v_{n+1}\}$ e qualquer outro conjunto de vetores $\{v'_1, v'_2, \cdots, v'_{n+1}\}$, existe $a \in A$ tal que $av_i = \rho(a)(v_i) = v'_i$.

Em particular, consideremos $v'_i = 0$, $1 \leqslant i \leqslant n$ e assim, $av_i = 0$ e $av_{n+1} \neq 0$. Logo, existe $a \in U_n$ tal que $a \notin U_{n+1}$ e é claro que $U_n \supsetneqq U_{n+1}$ para todo n. Portanto, $U_1 \supsetneqq U_2 \supsetneqq \cdots$ é uma cadeia estritamente decrescente de ideais à esquerda de A e deste modo A não é artiniano à esquerda. ■

Conclusão

Este trabalho possibilitou uma formalização matemática até então não obtida com as disciplinas de graduação. Por intermeio dele, obteve-se uma evolução na pesquisa e no modo de pensar Matemática, principalmente o conteúdo de Álgebra.

Durante a graduação, tive muito contato com áreas como cálculo e álgebra linear, e pouca aproximação com a álgebra. Todavia esse pouco bastou para gerar meu interesse. E foi assim que iniciou-se essa pesquisa e graças a ela meu entusiasmo pela álgebra só aumentou, me levando ao desejo de prosseguir meus estudos num mestrado em matemática.

O estudo do teorema de estrutura para anéis primitivos é extremamente valioso, uma vez que permite a comunhão de conteúdos matemáticos como Álgebra e Álgebra Linear (mesmo que não tenhamos explorado muito esta relação aqui) assim como permite a fabricação de exemplos.

Por fim, esperamos que esse trabalho possa ser útil como objeto de consulta e/ou estudo.

Referências Bibliográficas

[1] AZEVEDO, A.; COLÓQUIO BRASILEIRO DE MATEMÁTICA : (8.: 1971. Poços de Caldas). "Módulos sobre domínios principais". IMPA, Rio de Janeiro, 1971.

[2] FERRERO, M., "XVI Escola de Álgebra", UnB, 2000.

[3] HOFFMAN, K.; KUNZE, R. A., "Álgebra linear", LTC, Rio de Janeiro - São Paulo, 1979.

[4] HUNGERFORD, T. W.; "Algebra, Graduate Texts in Mathematics 73", Springer, New York, 1974.

[5] LAM, T.Y.; "A First Course in Noncommutative Rings", Graduate Texts in Mathematics, 131, Springer-Verlag, Second Edition, New York - Berlin - Heidelberg, 2001.

[6] MILIES, F. C. P.; "Anéis e Módulos", publicações do Instituto de Matemática da Universidade de São Paulo, 1972.