UNIVERSIDADE FEDERAL DE VIÇOSA
CAMPUS FLORESTAL
LICENCIATURA EM MATEMÁTICA

Fábio Henrique Batista Cunha

Semissimplicidade de Anéis

Florestal
[2024]

Fábio Henrique Batista Cunha

Semissimplicidade de Anéis

Trabalho de Conclusão de Curso de Graduação em Licenciatura em Matemática do Campus Florestal da Universidade Federal de Viçosa para a obtenção do título de Licenciado(a) em Matemática.
Orientador: Luís Felipe Gonçalves Fonseca

Florestal
[2024]

F119aa Batista Cunha, Fábio Henrique

Anéis semissimples / Fábio Henrique Batista Cunha. — Brasília: Escola Superior do Ministério Público da União, 2024.

107f.

Trabalho de conclusão de curso (Licenciatura em Matemática) — Escola Superior do Ministério Público da União: Brasília, 2024.

Orientador(a): Dra. Luís Felipe Gonçalves Fonseca

1. Anéis . 2. Módulos. 3. Anéis e Módulos Semissimples. 4. Teorema de Wedderburn-Artin. 5. J-semissimplicidade. I. Título.

Ficha catalográfica elaborada automaticamente, com os dados fornecidos pelo(a) autor(a)

UNIVERSIDADE FEDERALDE VIÇOSA
CAMPUS UFV-FLORESTAL
INSTITUTO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
CURSO DE MATEMÁTICA-LICENCIATURA

ATA DE DEFESA DE TCC

Florestal, 09 de setembro de 2024

Aos 09 dias do mês de setembro de 2024 às 14 h, reuniu- se em sala virtual no Google Meet, a banca composta por **Danielle Franco Nicolau** (UFV/ IEF), **Luís Felipe Gonçalves Fonseca** (UFV/IEF) e **Monique Müller Lopes Rocha** (UFSJ), para avaliar o TCC de autoria do licenciando: Fábio Henrique Batista Cunha, matrícula 3707, intitulado: "Anéis Semissimples".

Após a apresentação do licenciando e arguição dos membros da banca, o trabalho foi aprovado, sendo feita a comunicação da aprovação. Em seguida, eu, Luís Felipe Gonçalves Fonseca (presidente, e também orientador), lavrei a presente ata que, se estiver de acordo, deverá ser assinada pelos membros da banca.

Documento assinado digitalmente
LUIS FELIPE GONCALVES FONSECA
Data: 09/09/2024 14:16:27-0300
Verifique em https://validar.iti.gov.br

Luís Felipe Gonçalves Fonseca
Presidente e Membro da Banca

Documento assinado digitalmente
DANIELLE FRANCO NICOLAU
Data: 09/09/2024 21:59:15-0300
Verifique em https://validar.iti.gov.br

Danielle Franco Nicolau
Membro da Banca

Documento assinado digitalmente
MONIQUE MULLER LOPES ROCHA
Data: 09/09/2024 22:21:48-0300
Verifique em https://validar.iti.gov.br

Monique Müller Lopes Rocha
Membro da Banca

Este trabalho é dedicado aos meus colegas de classe e aos meus queridos pais.

RESUMO

O estudo dos anéis semissimples ocupa um lugar central na teoria dos anéis e módulos devido às suas propriedades estruturais bem definidas e aplicabilidades em várias áreas da matemática, como álgebra linear, teoria de representações e teoria dos números. Este trabalho tem como objetivo explorar os conceitos fundamentais relacionados aos anéis semissimples, incluindo módulos simples e semissimples, o Teorema de Wedderburn-Artin, e as condições de Artinidade e Noetherianidade dos anéis.

Palavras-chave: Anéis Semissimples. Teorema de Wedederburn-Artin. Anéis Artinianos e Anéis Noetherianos.

ABSTRACT

The study of semisimple rings holds a central place in ring and module theory due to their well-defined structural properties and applications in various areas of mathematics such as linear algebra, representation theory, and number theory. This paper aims to explore the fundamental concepts related to semisimple rings, including simple and semisimple modules, the Wedderburn-Artin Theorem, and the Artinian and Noetherian conditions of rings.

Keywords: Semisimple ring. Wedderburn-Artin theorem. Artinian rings and Noetherian rings.

SUMÁRIO

1 INTRODUÇÃO

A ideia de semissimplicidade está associada a um certo radical. Wedderburn trabalhou com um "radical"definido como sendo o maior ideal nilpotente, o qual coincide com a soma dos ideais nilpotentes de uma álgebra finito-dimensional. Nessa pesquisa estudaremos a semissimplicidade estudada por Wedderburn, os radicais de Jacobson, que deram origem ao anéis J-semissimples na linguagem atual.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Desenvolver uma pesquisa dentro da álgebra abstrata, com o estudo de anéis semissimples a nível de graduação.

1.1.2 Objetivos Específicos

1. Pesquisar módulos sobre anéis.
2. Pesquisar sobre condições de finitudes para anéis e módulos.
3. Provar o Toerema de Wedderburn-Artin.
4. Analisar as Representações Irredutíveis de S_3 sobre $\mathbb{C}$.
5. Estudar a J-semissimplicidade.

1.2 METODOLOGIA

O estudo em pauta situa-se na área de álgebra abstrata e será dividido em duas partes. A primeira parte da pesquisa terá como foco a pesquisa bibliografica com a leitura de materiais e artigos sobre o tema. A segunda parte será a escrita do TCC.

2 DESENVOLVIMENTO

2.0.1 Definições básicas

A teoria dos anéis teve o seu ínicio do século XIX. Richard Dedekind introduziu o conceito de ideais. No século XX, matemáticos como David Hilbert, Emil Artin, Emmy Noether entre outros formalizaram a teoria dos anéis, abrangendo anéis comutativo e não comutativos, com aplicações em diversos campos do conhecimento. Nesta seção, usaremos a referência [**6**].

Definição 1. *Dizemos que um conjunto A, munido de duas operações binárias, chamada soma $(+)$ e multiplicação $(\cdot)$ é um anel, se valem as propriedades abaixo:*

(i) $(A,+)$ é um grupo abeliano, ou seja, $(+)$ é associativa, possui elemento neutro, possui elemento simétrico e é comutativa.

(ii) $(\cdot)$ é associativa $a\cdot(b\cdot c)=(a\cdot b)\cdot c, \forall a,b,c\in A$

(iii) $(+)$ e $(\cdot)$ são compatíveis, isto é, para todo a,b e $c\in A$ vale que:

$a\cdot(b+c)=a\cdot b+a\cdot c$ *e* $(a+b)\cdot c=a\cdot c+b\cdot c$.

Exemplo 1. *Os conjuntos $\mathbb{Z},\mathbb{Q},\mathbb{C},\mathbb{R}$ com operações usuais são aneis.*

Definição 2. *Sejam $(A,+,\cdot)$ um anel. Dizemos que um conjunto não vazio S é um subanel de A, se $(S,+,\cdot)$ for um anel.*

Exemplo 2. *$\mathbb{Z}$ é subanel de $(\mathbb{Q},+,\cdot)$, $\mathbb{Z}$ é subanel de $(\mathbb{R},+,\cdot)$, $\mathbb{Q}$ é subanel de $(\mathbb{C},+,\cdot)$ e $\mathbb{R}$ é subanel de $(\mathbb{C},+,\cdot)$*

Proposição 2.0.0.1. *Seja* $(A, +, \cdot)$ *um anel. Um subconjunto não vazio* S *de* A *é um subanel, se, e somente se, as seguintes condições são satisfeitas:*

$(i) a - b \in S, \forall a, b \in S$

$(ii) a \cdot b \in S, \forall a, b \in S.$

Demonstração. Suponha S um subanel de A. Pela Definição 2, temos que $(S, +, \cdot)$ é um anel. Dados $a, b \in S$, temos: $-b \in S, a + (-b) \in S$ e $a \cdot b \in S$.

De maneira recíproca, se S é fechado em relação à multiplicação e sendo S não vazio, $\exists a \in S$. Por (i) temos:

* $a - a = 0_A$. Ou seja, o zero do anel pertence a S

* $0_A - a = -a, -a \in S$. Ou seja, todo elemento de S possui inverso.

Agora, dados $a, b \in S$, (i) também nós dá $a - (-b) = a + b \in S$, garantido o fechamendo aditivo de S. Logo, $(S, +, \cdot)$ é um anel.

□

Definição 3. *Seja* $(A, +, \cdot)$ *um anel. Um subconjunto não vazio* I *de* A *é dito um* ideal *do anel* $(A, +, \cdot)$ *quando:*

$(i)(I, +)$ é um grupo abeliano.

(ii) para todos $x \in I$ e $a \in A$, temos $a \cdot x \in I$ e $x \cdot a \in I$.

Exemplo 3. *O conjunto* $8\mathbb{Z}$*, formado pelos múltiplos de 8, é um ideal do anel* $(\mathbb{Z}, +, \cdot)$.

Se $a \in \mathbb{Z}$ e $y \in 8\mathbb{Z}$, temos $y = 8z$ com $z \in \mathbb{Z}$ e $a \cdot y = a \cdot 8z = 8(a \cdot z) \in 8\mathbb{Z}$. Como $(8\mathbb{Z}, +)$ é um grupo abeliano, o conjunto $8\mathbb{Z}$ é um ideal do anel.

Corolário 2.0.0.1. *A relação* $a \equiv b \pmod{I} \Leftrightarrow a - b \in I$ *é uma relação de equivalência.*

Demonstração. Sejam a, b e $c \in A$ e I um ideal de A. Vamos mostrar que a relção dada é de equivalência.

i) **Reflexiva:** Como $a - a = 0 \in I$ implica $a \equiv a \pmod{I}$.

ii) **Simétrica:** Se $a \equiv b \pmod{I}$ temos $a - b \in I$. Então, $-(a - b) = b - a \in I$. Assim $b \equiv a \pmod{I}$.

iii) **Transitiva:** Se $a \equiv b \pmod{I}$ e $b \equiv c \pmod{I}$, então $a - b \in I$ e $b - c \in I$. Portanto, $(a - b) + (b - c) = a - c \in I$ o que mostra que $a \equiv c \pmod{I}$. □

Definição 4. *Sejam A um anel, I um ideal de A e $a \in A$. A classe de equivalência de a segundo a relação de equivalência: $a \equiv b \pmod{I} \Leftrightarrow a - b \in I$ é o conjunto:*

$$a + I = \{a + u \mid u \in I\},$$

chamado de classe lateral I em A determinada por a.

Proposição 2.0.0.2. *Sejam $(A, +, \cdot)$ um anel e I um ideal de A. As operações binárias:*

$$A/I \times A/I \to A/I$$
$$(a+I, b+I) \mapsto (a+I)+(b+I) = (a+b)+I$$

e

$$A/I \times A/I \to A/I$$
$$(a+I, b+I) \mapsto (a+I)\cdot(b+I) = a\cdot b+I,$$

com $a, b \in A$, sobre o conjunto de todas as classes laterais de I em A estão bem definidas, isto é, independem do representante da classe.

Demonstração. Suponhamos que $a+I = a_1+I$ e $b+I = b_1+I$ em que $a, a_1, b, b_1 \in A$. Desse modo, $a \equiv a_1 \pmod{I}$ e $b \equiv b_1 \pmod{I}$, de onde $a-a_1 \in I$ e $b-b_1 \in I$.

Como I é um ideal de A, temos, para a adição: $(a-a_1)+(b-b_1) = (a+b)-(a_1+b_1) \in I$, ou seja, $a+b \equiv a_1+b_1 \pmod{I}$, logo, $(a+b)+I = (a_1+b_1)+I$.

Para a multiplicação, temos:
$a-a_1 \in I, b \in A \Rightarrow (a-a_1)\cdot b = a\cdot b - a_1\cdot b \in I$;

$b-b_1 \in I, a_1 \in A \Rightarrow (b-b_1)\cdot a_1 = b\cdot a_1 - b_1\cdot a_1 \in I$.

Logo, $(a\cdot b - a_1\cdot b)+(b\cdot a_1 - b_1\cdot a_1) = a\cdot b - a_1\cdot b_1 \in I$, de onde $a\cdot b \equiv a_1\cdot b_1 \pmod{I}$. Consequentemente $(a\cdot b)+I = (a_1\cdot b_1)+I$. □

Teorema 2.0.1. *Sejam $(A, +, \cdot)$ um anel e I um ideal de A. Então o conjunto quociente $A/I = \{a+I | a \in A\}$ munido das operações de adição e multiplicação da proposição anterior é um anel.*

Demonstração. Incialmente, note que $A/I \neq \emptyset$, pois $I \in A/I$. Vamos usar a definição de anel para provarmos esse teorema.

i) **Associatividade da adição**: Dados $a+I, b+I, c+I \in A/I$ com $a, b, c \in A$ temos:

$(a+I)+[(b+I)+(c+I)] = (a+I)+[(b+c)+I] = [a+(b+c)+]I = [(a+b)+c]+I = [(a+b)+I]+(c+I) = [(a+I)+(b+I)]+(c+I)$.

ii) **Elemento neutro**: A classe $0_{A/I} = 0_A + I = I$ é o elemento neutro da adição de A/I, em outras palavras: $0_{A/I} = I$.:

Com efeito: $(a + I) + (0_A + I) = (a + 0_A) + I = a + I$ e $(0_A + I) + (a + I) = a + I$.

iii) **Elemento simétrico**: Todo $a + I \in A/I$ admite oposto e $-(a + I) = -a + I$, pois:

$(a + I) + ((-a) + I) = (a + (-a)) + I = 0_A + I = I$ e $((-a) + I) + (a + I) = I$

iv) **Distributividade da multiplicação em relação à adição:** Dados $a + I, b + I, c + I \in A/I$ temos:

$(a+I)\cdot[(b+I)+(c+I) = (a+I)\cdot[(b+c)+I] = [a\cdot(b+c)+I] = (a\cdot b+a\cdot c)+I = (a\cdot b+I)+(a\cdot c+I) = (a+I)\cdot(b+I)+(a+I)\cdot(c+I)$.

Para finalizar a demonstração, basta o leitor verificar que a comutatividade e a associativa da multiplicação são válidas.

□

2.0.2 Isomorfismo de anéis

Definição 5. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \otimes)$ dois anéis. Dizemos que a função $f : A \to B$ e um* homomorfismo *de A em B se $\forall a, b \in A$ vale:*

$$f(a + b) = f(a) \oplus f(b) \text{ e } f(a \cdot b) = f(a) \otimes f(b).$$

Exemplo 4. *Sejam os anéis $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Z}_m, \oplus, \otimes), m > 1$. Consideremos a função:*

$$f : \mathbb{Z} \to \mathbb{Z}_m$$
$$f(a) \vdash \overline{a}$$

pois para todo $a, b \in \mathbb{Z}$ temos:

$$f(a+b) = \overline{a+b} = f(a) \oplus f(b)$$
$$f(a \cdot b) = \overline{a \cdot b} = f(a) \otimes f(b).$$

Definição 6. *Um isomorfismo de anéis é um homomorfismo bijetor. Se existir um isomorfismo $A \to B$ escrevemos $A \cong B$.*

Definição 7. *Seja um homomorfismo $f : A \to B$ dizemos:*

(i) monomorfismo se f é injetora;

(ii) epimorfismo se f é sobrejetora;

Definição 8. *Seja um homomorfismo $f : A \to A$, dizemos que f é um endomorfismo de anéis.*

Exemplo 5. *Sobre o anel $(\mathbb{C}, +, \cdot)$ dos números complexos com as operações usuais, seja a função de conjugação:*

$$f : \mathbb{C} \to \mathbb{C}$$
$$f((a+bi)) \vdash a - bi$$

Note que:

$$f((a+bi)+(c+di)) = f((a+c)+(b+d)i = (a+c)-(b+d)i) = (a-bi)+(c-di) = f(a+bi)+f(c+di)$$

e

$$f((a+bi))\cdot(c+di)) = f((ac-bd)+(ad+bc)i) = (ac-bd)-(ad+bc)i = (a-bi)\cdot(c-di) = f(a+bi)\cdot f(c+di)$$

Logo, temos um homomorfismo sobre $\mathbb{C}$. Além disso, observe que f é bijetora:

Como $f(a+bi) = f(c+di) \Rightarrow a-bi = c-di$ de onde, $a=c$ e $b=d$, por definição de injetividade, f é injetora.

Dado $s = x+yi \in \mathbb{C}$, e seja $t = x-yi \in \mathbb{C}$ então $f(t) = s$, por definição de sobrejetividae, f é sobrejetiva. Portanto, temos um isomorfismo de anéis.

Exemplo 6. *Sejam os anéis* $(\mathbb{R},+,\cdot)$ *e* $(M_{2\times 2}\mathbb{R},+,\cdot)$*, consideremos a função* $f:\mathbb{R}\to M_{2\times 2}\mathbb{R}$*. Afirmamos que* f *é um homomorfismo, pois dados* $a,b\in\mathbb{R}$

$$\begin{aligned} f : \mathbb{R} &\to M_{2\times 2}\mathbb{R} \\ a &\mapsto \begin{pmatrix} 0 & 0 \\ -a & a \end{pmatrix} \end{aligned}$$

Assim, temos:

$$f(a+b) = \begin{pmatrix} 0 & 0 \\ -(a+b) & a+b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -a & a \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ -b & b \end{pmatrix} = f(a)+f(b)$$

e

$$f(a \cdot b) = \begin{pmatrix} 0 & 0 \\ -a \cdot b & a \cdot b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -a & a \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ -b & b \end{pmatrix} = f(a) \cdot f(b).$$

Além disso pode-se verificar que, f é um injetora, mas não é sobrejetora. Logo f é um monomorfismo de $\mathbb{R}$ em $M_{2\times 2}\mathbb{R}$, contudo não é um isomorfismo.

Proposição 2.0.1.1. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \otimes)$ dois anéis e $f : A \to B$ um homomorfismo de A em B. Então:*

(a) $f(0_A) = 0_B$;

(b) $f(-a) = -f(a), \forall a \in A$.

Demonstração. Provaremos o item (a). Com efeito temos que $f(0_A) = f(0_A + 0_A) = f(0_a) \oplus f(0_A)$

Como $f(0_A) \in B$ vamos adicionar o oposto desse elemento aos dois membros, obtendo:

$$f(0_A) \oplus [-f(0_A)] = [f(0_A) \oplus f(0_A)] \oplus [-f(0_A)].$$

Usando a associatividade da adição, do anel B, obtemos $0_B = f(0_A)$. Logo (a) é demonstrado.

Item (b). De fato, para todo $a \in A$, podemos escrever $a + (-a) = 0$. Aplicando f em ambos os lados concluímos $f(a + (-a)) = f(0_A)$. Como f é um homomorfismo, usando o item (a), chegamos em: $f(a) \oplus f(-a) = 0_B$ o que acarreta $f(-a) = -f(a)$. □

Definição 9. *Seja $f : A \to B$ um homomorfismo de anéis. Denotamos o núcleo como o conjunto:*

$$Ker(f) = \{a \in A : f(a) = 0_B\}.$$

Definição 10. *Seja $f : A \to B$ um homomorfismo de anéis. Denotamos imagem de f o conjunto:*

$$Im(f) = \{b \in B | \exists a \in A, f(a) = b\}$$

Proposição 2.0.1.2. *Um homomorfismo de anéis $f : A \to B$ é injetor se, e somente se, $Ker(f) = \{0\}$.*

Demonstração. $\Rightarrow$) Suponha que f é injetiva, como $f(0) = 0$ e f é injetora, segue que $Ker(f) = \{0\}$.

$\Leftarrow$) Se $Ker(f) = \{0\}$ e $f(a) = f(b)$, então $f(a - b) = 0$. Portanto, $a - b \in Ker(f) = \{0\}$ o que implica $a = b$, ou seja, f é injetiva. □

Proposição 2.0.1.3. *Seja $\varphi : A \to B$ um homomorfismo de anéis. Então $Ker(\varphi)$ é um subanel de A.*

Demonstração. Se $x, y \in Ker(\varphi)$, então $f(x) = f(y) = 0_B$. Segue que: $f(x - y) = f(x) = f(y) = 0_B$ e $f(x \cdot y) = f(x) \cdot f(y) = 0_B \cdot 0_B = 0_B$, logo $x - y, xy \in Ker(\varphi)$ □

Proposição 2.0.1.4. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \otimes)$ dois anéis:*

(i) Seja I um ideal de A. A função $\varphi : A \to A/I$ definida por: $\varphi(a) = a + I$ para todo $a \in A$ é um epimorfismo, cujo $Ker(\varphi) = I$.

(ii) Seja $f : A \to B$ um homomorfismo de anéis, então $ker(f)$ é um ideal de A.

Demonstração. (i) Dados $a, b \in A$ e, pelo fato, de A/I ser um anel, temos :

$$\varphi(a+b) = (a+b) + I = (a+I) + (b+I) = \varphi(a) + \varphi(b),$$

e

$$\varphi(a \cdot b) = (a \cdot b) + I = (a \cdot I) \cdot (b+I) = \varphi(a) \cdot \varphi(b).$$

Logo φ é um homomorfismo. Para verificar que φ é um epimorfismo, tome a classe lateral $Y \in A/I$ de modo que $Y = a + I$, com $a \in A$. Temos que $\varphi(a) = a + I = Y$. Então φ é um epimorfismo.

Agora, como I é o zero do anel A/I, temos que $Ker(\varphi) = \{a \in A \mid \varphi(a) = I\}$ .Logo $a \in A \in Ker(\varphi) \Leftrightarrow a + I = I \Leftrightarrow a \in I$. Então $Ker(\varphi) = I$.

(ii) Vamos mostrar que dados $m, n \in ker(f)$, temos:

$m - n \in ker(f)$. De $m, n \in ker(f)$, temos $f(m) = 0_B = f(n)$, como f é um homomorfismo, vem:

$$f(m-n) = f(m + (-n)) = f(m) \oplus f(-n) = f(m) \oplus (-f(n)) = 0_B \otimes (-0_B) = 0_B \oplus 0_B = O_B$$

Portanto $m - n \in ker(f)$. Agora, vamos mostrar que $ker(f)$ absorve o produto por elementos de A. Seja $z \in ker(f)$ e $a \in A$. Assim $f(z) = 0_B$ e:

$$f(a \cdot z) = f(a) \otimes f(z) = f(a) \otimes 0_B = 0_B.$$

Logo $a \cdot z \in ker(f)$. Para $z \cdot a$ segue de maneira análoga, assim, $ker(f)$ é um ideal de A. □

Teorema 2.0.2. *(Teorema dos Homomorfismos para Anéis) Sejam R, S anéis e $f : R \to S$ um homomorfismo de anéis. Então existe um único monomorfismo de anéis $\overline{f} : R/Ker(f) \to S$ tal que $\overline{f} \circ \pi = f$.*

Demonstração. Basta definir $\overline{f}(\overline{a}) = f(a), \forall \overline{a} \in R/Ker(f)$. Vejamos que assim, $\overline{f}$ está bem definida. De fato, pois se $\overline{a} = \overline{b}$ em $R/Ker(f)$, então $(a-b) \in Kerf(f)$, ou seja $f(a-b) = 0$, de modo que $f(a) = f(b)$, pois f é um homomorfismo de anéis. Assim, temos $f(\overline{a}) = f(\overline{b})$. Por definição, temos $f(a) = \overline{f}(\overline{a}) = \overline{f}(\pi(a)) = \overline{f} \circ \pi, \forall a \in R$, ou seja, $\overline{f} \circ \pi = f$

Logo f é injetora, pois se $\overline{a} \in Ker(f)$, então $\overline{f}(\overline{a}) = 0$, ou seja, $0 = \overline{f}(\overline{a}) = f(a)$, de onde segue que $a \in Ker(f)$, o que nos diz que $\overline{a} = \overline{0}$

Agora, uma vez que mostramos a existência, basta mostra unicidade de $\overline{f}$. Suponhamos que $g : R/Ker(f) \to S$ é tal que $g \circ \pi = f$. Portanto, para cada $\overline{a} \in R/Ker(f)$, temos $g(\overline{a}) = g \circ \pi(a) = f(a) = \overline{f}(\overline{a})$, segue que $g = \overline{f}$. □

Teorema 2.0.3. *(Teorema do Isomorfismo para Anéis) Seja $f : A \to B$ um homomorfismo sobrejetor de anéis. Então $A/Ker(f) \cong B$.*

Demonstração. Denotemos $U = Ker(f)$ e definimos $\varphi : A/U \to B$ dada por $\varphi(a + U) = f(a), \forall a + U \in A/U$.

Assim, φ está bem definida, ou seja,φ independe da escolha dos representantes das classes laterais: De fato, supondo $a + U = b + U \in A/U$, temos $a - b \in U$, que implica na existência de $u \in U$ tal que $a - b = u$. Logo, $a = b + u$ e $f(a) = f(b + u) = f(b) + f(u) = f(b) + 0_B = f(b)$, o que significa que $\varphi(a + U) = \varphi(b + U)$.

Além disso, φ é um homomorfismo: Dados $a + U, b + U \in a/U$, temos:

Soma: $\varphi((a + U) + (b + U)) = \varphi((a + b) + U) = f(a + b) = f(a) + f(b) = \varphi(a + U) + \varphi(b + U)$.

Produto: $\varphi((a+U)\cdot(b+U) = \varphi((a\cdot b)+U) = f(a\cdot b) = f(a)\cdot f(b) = \varphi(a+U)\cdot\varphi(b+U)$.

φ é injetor, pois, dados $a+U, b+U \in A/U$, suponhamos $\varphi(a+U) = \varphi(b+U)$, ou seja, $f(a) = f(b)$. Com isso, $f(a-b) = 0_B$, em que $a-b \in U$. Logo $a+U = b+U$.

φ é sobrejetor, pois, por hipótese, dado $b \in B, \exists a \in A$ tal que $f(a) = b$. Considerando a classe lareal $a+U \in A/U$, temos $\varphi(a+U) = f(a) = f(b)$. □

2.0.3 Anéis de divisão e Domínios de integridade

Definição 11. *Seja $(A,+,\cdot)$ um anel. Um elemento não nulo $a \in A$ é dito invertível qunado existe b não nulo tal que $a\cdot b = b\cdot a = 1$.*

Exemplo 7. *A matriz* $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *é invertível e sua inversa é* $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

Definição 12. *Quando todos os elementos não nulos de um anel A são invertíveis, dizemos que A é um anel de divisão. Ou seja, um anel é de divisão quando $(A \setminus 0_A, \cdot)$ é um grupo.*

Definição 13. *Um elemento não nulo $a \in A$ é um divisor de zero quando existe b não nulo tal que $ab = 0$.*

Exemplo 8. *A matriz* $M = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$ *é um divisor de zero em* $M_2(\mathbb{R})$, *pois* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Definição 14. *Seja $(A, +, \cdot)$ um anel comutativo com unidade. Dizemos que A é um domínio de integridade quando, para $a, b \in A$, a igualdade $a \cdot b = 0_A$ somente é possível se $a = 0_A$ ou $b = 0_A$. Em outras palavras, um domínio de integridade é um anel comutativo com unidade sem divisores de zero.*

Exemplo 9. *O anel $(8\mathbb{Z} \cup \{1\}, +, \cdot)$ é um dominío de integridade.*

Se $a, b \in 8\mathbb{Z}$, existem z, t inteiros tais que $a = 8z$ e $b = 8t$. Logo, $a \cdot b = 0 \Leftrightarrow 64z \cdot t = 0$ se, e só se, $z = 0$ ou $t = 0$. Que por sua vez, é válido se, e somente se, $a = 0$ ou $b = 0$.

Proposição 2.0.3.1. *Seja $(A, +, \cdot)$ um anel comutativo com unidade. O anel A é um dominío de integridade se, e somente se, é válida a seguinte sentença:*

$$\textit{Se } a, b, x \in A \textit{ são tais que } a \cdot x = b \textit{ se } x \neq 0_A, \textit{ então } a = b.$$

Demonstração. $\Rightarrow$ Suponha que A seja um domínio de integridade. Adicionando o oposto $b \cdot x$ em ambos os lados da igualdade $a \cdot x = b \cdot x$ obtemos:

$$a \cdot x + (-b) \cdot x = 0_A \ (1)$$
$$(a + (-b)) \cdot x = 0_A \ (2)$$

Como $x \neq 0_A$ e A, por hipótese, é dominío de integridade por (2) temos que $a + (-b) = 0_A$, adicionando b em ambos lados, concluímos que $a = b$.

$\Leftarrow$ Suponha que a lei do cancelamento multiplicativo seja válida. Tome $a, b \in A$ tais que $a \cdot b = 0_A$ de tal maneira que $b \neq 0_A$.Provaremos que $a = 0$. Agora, caso $a \neq 0$ pela lei do cancelamento $a \cdot b = 0_A = 0_A \cdot b$,

obtemos $a = 0_A$. O que é uma contradição, logo A não admite divisores de zero.

□

Proposição 2.0.3.2. *Se $m > 1$ é um inteiro composto, então o anel $(Z_m, \oplus, \otimes)$ admite divisores próprios de zero.*

Demonstração. Sendo m composto, pelo Algoritmo da Divisão em $\mathbb{Z}$ existem $a, b \in \mathbb{Z}$ tais que:

$$0 < a, b < m \text{ e } m = a \cdot b.$$

Assim, em $\mathbb{Z}_m$, temos: $\overline{a}, \overline{b} \in \mathbb{Z}_m$, tais que $\overline{a} \neq \overline{0}, \overline{b} \neq \overline{0}$ e $\overline{m} = \overline{a} \otimes \overline{b}$. Portanto $\mathbb{Z}_m$ admite divisores de zero. □

Proposição 2.0.3.3. *O anel $(\mathbb{Z}_m, \oplus, \otimes)$ não admite divisores de zero se, e somente se, m é primo.*

Demonstração. Na Proposição 2.0.3.2, provamos que se m é composto, então $\mathbb{Z}_m$ admite divisores de zero. Suponha m primo e $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$ tais que $\overline{a} \cdot \overline{b} = \overline{0}$. Temos assim que $ab = km$, com k inteiro e m primo. Pela primalidade de m, segue que $m \mid a$ ou $m \mid b$. Logo $\overline{a} = 0$ ou $\overline{b} = 0$. Este fato mostra que $\mathbb{Z}_m$, com m primo, é um domínio de integridade. □

Exemplo 10. *Os anéis $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$ não são domínios de integridade.*

Exemplo 11. *Os anéis $\mathbb{Z}_2$, $\mathbb{Z}_5$, $\mathbb{Z}_7$ são domínios de integridade.*

Proposição 2.0.3.4. *Sejam $(A, +, \cdot)$ e $(B, \oplus, \otimes)$ dois anéis. Se $f : A \to B$ é um monomorfismo e B um domínio de integridade, então A é um domínio de integridade.*

Demonstração. Sejam $a, b \in A$ tais que $a \cdot b = 0_A$. Temos assim:

$$f(a) \otimes f(b) = f(a \cdot b) = f(0_A) = 0_B,$$

Como B é um dominío de integridade e pela Proposição 2.0.1.1, temos $f(a) = 0_B$ ou $f(b) = 0_B$. Haja visto que f é um monomorfismo temos: $f(x) = 0_B \Leftrightarrow x = 0_A$. Portanto, $a = 0_A$ ou $b = 0_A$. □

2.0.4 Corpos

Neste momento, vamos abordar algumas noções básicas sobre a teoria de corpos. Embora a noção de corpos já fosse ultilizada pelos estudiosos Richard Dedekind e Leopold Kronecker, foi o matemático Heinrich Weber que deu a primeira definição clara de um corpo abstrado. Posteriormente, Ernst Steinitz publicou o artigo Algebraische Theorie der Körper (Teria Algébrica de Corpos) e finalizamos essa introdução citando Évariste Galois que unificou a teoria de grupos e a teoria de corpos. Nesta seção, continuaremos ultilizando a referência [**6**] como base.

Definição 15. *Um conjunto matemático não vazio A munido de duas operações binárias $"+"$e $"\cdot"$é um corpo quando as seguintes propriedades são satisfeitas:*

(i) $(A, +)$ *é um grupo abeliano;*

(ii) $(A \setminus 0_A, \cdot)$ *é um grupo abeliano ;*

(iii) Propriedade distributiva da multiplicação em relação à adição: $a \cdot (b + c) = a \cdot b + a \cdot c$ *e* $(a + b) \cdot c = a \cdot c + b \cdot c$ *para quaisquer* $a, b, c \in A$.

Exemplo 12. *Os corpos canônicos* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Observação 1. *Note que todo corpo é um anel de divisão.*

Exemplo 13. *Com as operações usuais,* $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ *é um corpo.*

De fato, note que $\mathbb{Q}(\sqrt{2})$ *é um subconjunto não vazio de* $\mathbb{R}$*. A associatividade das operações de soma e multiplicação e a distributividade são preservadas.*

Para quaisquer $(a + b\sqrt{2}), (c + d\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$*, temos:*

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Além disso $(a+b\sqrt{2})(c+d\sqrt{2}) = (a+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

Os elementos 0 *e* $1 \in \mathbb{Q}[\sqrt{2}]$*. O inverso aditivo de* $a + b\sqrt{2}$ *é* $-a - b\sqrt{2}$*, um elemento de* $\mathbb{Q}[\sqrt{2}]$

Seja $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ *não nulo. Provaremos que* $(a+b\sqrt{2})^{-1} \in \mathbb{Q}[\sqrt{2}]$*. Com efeito, temos:*

$$\begin{aligned}(a + b\sqrt{2})^{-1} &= \tfrac{1}{a+b\sqrt{2}} \\ &= \tfrac{1}{a+b\sqrt{2}} \cdot \tfrac{a-b\sqrt{2}}{a-b\sqrt{2}} \\ &= \tfrac{a-b\sqrt{2}}{a^2-2b^2} \\ &= (\tfrac{a}{a^2-2b^2}) + (\tfrac{-b}{a^2-2b^2})\sqrt{2}\end{aligned}$$

e $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$*. Portanto, temos um corpo.*

Proposição 2.0.3.5. *Todo corpo é um dominío de integridade.*

Demonstração. Observe que todo corpo é um anel, logo basta mostrar a ausência de divisores próprios de zero.

Sejam $(A, +, \cdot)$ um corpo e $a, b \in A$ tais que $a \cdot b = 0_A$, mostraremos que $a = 0$ ou $b = 0$. Suponha $a \neq 0_A$ e como $(A \setminus 0_A, \cdot)$ é um grupo, existe $a^{-1} \in A - 0_A$ tal que $a^{-1} \cdot a = 1_A$.

Multiplicando ambos os membros de $a \cdot b = 0_A$ por a^{-1} pela esquerda:

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_A.$$

Recorrendo a associatividade da multiplicação e a propriedade de anéis, chegamos em:

$$(a^{-1} \cdot a) \cdot b = 0_A$$

Como $a^{-1} \cdot a = 1_A$:

$$1_A \cdot b = 0_A \text{ e } b = 0_A$$

□

Proposição 2.0.3.6. *Todo domínio de integridade finito é um corpo.*

Demonstração. Suponha A um dominío de integridade formado por n elementos, digamos $A = \{a_1, a_2, \ldots, a_n\}$. Vamos usar o fato de que A não tem divisores de zero, ou seja $a \in A \setminus \{0\}$

Seja a um desses elementos, tomamos a função:

$$f : A \to A \text{ definida por: } f(a_i) = aa_i \text{ com } i = \{1, 2, 3, ..., n\}$$

Se $f(a_i) = f(a_j)$, então $aa_i = aa_j$, cancelando a, temos $a_i = a_j$. Com isso, temos a injetividade de f, f é uma bijeção. Assim

$$Im(f) = \{aa_1, aa_2, \ldots, aa_n\}.$$

Então:

$$1 = aa_k$$

Para algum $1 \leq k \leq n$. Como $a \neq 0$, temos que A é corpo. □

Observação 2. *Claramente, existem domínios finitos que não são corpos. Um exemplo é $\mathbb{Z}$, o conjunto dos números inteiros.*

Proposição 2.0.3.7. *$\mathbb{Z}_p$, para p primo, é corpo.*

Demonstração. Por 2.0.3.3 temos que $\mathbb{Z}_p$ é um dominío de integridade. Além disso, como $\mathbb{Z}_p$ é finito, pela proposição anterior, segue que $\mathbb{Z}_p$ é um corpo. □

2.0.4.1 Anéis dos quartérnios

Nessa seção vamos introduzir um anel de divisão, que não é corpo, os quartérnios.

Seja $\mathbb{R}^4 = \{(a, b, c, d); a, b, c, d \in \mathbb{R}\}$ o conjunto das 4-úplas de $\mathbb{R}$, vamos definir a adição da seguinte maneira:

$$x = (a, b, c, d) \text{ e } y = (a', b', c', d')$$
$$x + y = (a + a', b + b', c + c', d + d')$$

e definimimos a multiplicação da seguinte forma:

$$xy = (aa' - bb' - cc' - dd', ab' + ba' + cd + c'd, ac' + a'c + db' - d'b, ad' + da' + bc' - b'c).$$

Sabemos que $(\mathbb{R}^4, +, \cdot)$ é um anel, com a $0 \setminus \mathbb{R}^4 = (0, 0, 0, 0)$. Agora, sejam $a = (a, 0, 0, 0), i = (0, 1, 0, 0), j = (0, 0, 1, 0)$ e $k = (0, 0, 0, 1)$, podemos escrever $x = (a, b, c, d) = a + bi + cj + dk$ de modo que possamos definir $\mathbb{R}^4 = \{(a + bi + cj + dk) : a, b, c, d \in \mathbb{R}\}$. Além disso, valem:

$$i^2 = j^2 = k^2 = -1$$
$$i \cdot j = k, j \cdot i = -k, j \cdot k = i, k \cdot j = -i, k \cdot i = j \text{ e } i \cdot k = -j.$$

Este anel de divisão é conhecido como Quarténios e foi construído no século XIX, pelo matemático irlandês W. R. Hamilton quando tentava construir um corpo que fosse uma extensão do corpo dos números complexos. Por não ser comutativo em relação a multiplicação, esse anel não é corpo.

2.0.4.2 Teorema de Wedderburn

Nessa seção, será apresentado o Teorema de Wedderburn, enunciado pelo matemático escocês Joseph Wedderburn (1882-1948), que relaciona anéis de divisão com corpos. Um estudo completo (com demonstração do Teorema de Wedderburn) pode ser visto no TCC de João Paulo Guardieiro Sousa, UFU 2018.

A próxima proposição é um resultado de verificação imediata.

Proposição 2.0.3.8. *Seja D um anel de divisão e F um subanel que é um corpo. Então D pode ser visto como um espaço vetorial (à esquerda) sobre F.*

Lema 2.0.4. *Seja F um corpo finito contendo um subcorpo K, isto é, um corpo contido em F, com q elementos, então F possui q^m elementos, sendo que $m = [F : K]$.*

Demonstração. Sabendo que F pode ser visto como um espaço vetorial sobre K, temos que $m = [F : K] = Dim_K F < \infty$. F tem uma base sobre K com m elementos: $a_1, a_2, ..., a_m$. Logo, todo elemento de F pode ser escrito como $b_1a_1 + b_2a_2, ..., b_ma_m$, onde $b_1, b_2, .., b_m \in K$. Para o término da demonstração, basta obeservar que, como K possui q elementos F irá possuir, exatamente, q^m elementos. □

Teorema 2.0.5. *(Teorema de Zsigmondy) Sejam a, b e n inteiros positivos, tais que $a > b > 0, n > 0, mdc(a, b) = 1$. Então existe um número primo q divisor de $a^n - b^n$ tal que $q \nmid a^k - b^k$ para todo inteiro $k, 0 < k < n$, exceto os seguintes casos:*

(i) $n = 1, a - b = 1$

(ii) $n = 2, a + b = 2^t$

(iii) $n = 6, a = 2, n = 1$.

Teorema 2.0.6. *(Teorema de Wedderburn) Todo anel de divisão finito é um corpo.*

Demonstração. A princípio vamos denotar o centralizador de um elemento x do anel de divisão D como:

$$C_D(x) = \{y \in D \mid yx = xy\}$$

Obviamente 0 e 1 são elementos de $C_D(x)$. Se y e z são elementos de $C_D(x)$, temos:

$$x(-y) = -(xy) = -(yx) = -y(x), x(y + z) = xy + zx = (y + z)x$$

e

$$x(yz) = (xy)z = (yx)z = y(xz) = y(zx) = (yz)x,$$

então $-y, y + z$ e yz são elementos de $C_D(x)$. Além disso, para $y \neq 0$ implica em $y^{-1}x = xy^{-1}y^{-1}$ é também um elemento de $C_D(x)$. Isto mostra que $C_D(x)$ é um subanel de D.

Agora vamos considerar o centro de D, que denotaremos por $Z(D)$. Este conjunto também é um subanel e a interseção de todos centralizadores.

$$Z(D) = \bigcap_{x \in D} C_D(x).$$

Note que, além de subanel, $Z(D)$ é um corpo. Adicionalmente:

$$Z(D) = \{a \in D | ab = ba \ \ \forall b \in D\}.$$

É de conhecimento que $Z(D)$ é um subgrupo abeliano de D. Podemos considerar D e cada $C_D(x)$ como espaços vetoriais sobre $Z(D)$ de dimensão n e n_x, respectivamente. Como D pode ser visto como um módulo sobre $C_D(x)$ descobrimos que n_x divide n. Se colocarmos $q := |Z(D)|$, podemos ver que $q \geq 2$ desde que $\{0, 1\} \subset Z(D)$, e $|C_D(x)| = q^{n_x}$ e $|D| = q^n$.

Provaremos que $n = 1$ e, portanto, $Z(D) = D$. Condidere o grupo multiplicativo $D^* := D - \{0\}$. Aplicaremos a equação de classes de conjugação. Para isso, consideraremos o grupo D^* e os subgrupos $Z(D^*)$ e $C_{D^*}(x)$

$$|D^*| = |Z(D^*)| + \sum_{x \notin Z(D^*)} \frac{|D^*|}{|C_{D^*}(x)|}.$$

Logo:

$$q^n - 1 = q - 1 + \sum_{x \notin Z(D^*)} \frac{q^n - 1}{q^{n_x} - 1}$$

Pelo Teorema 2.0.5, existe p primo, sendo que p é um divisor de $q^n - 1$. Contudo, p não divide qualquer $q^m - 1$ para $0 < m < n$, excepcionalmente em dois casos que serão tratados a seguir. Como p é primo e p não divide $q^{n_x} - 1$, temos $mdc(p, q^{n_x - 1}) = 1$. Com isso, p irá dividir $q^n - 1$ e cada uma das parcelas $\frac{q^n - 1}{q^{n_x} - 1}$. Então também irá dividir $q - 1$ o que só pode acontecer caso $n = 1$.

Analisaremos agora os dois casos excepcionais.

Para $n = 2$. Neste caso, D é um espaço vetorial bidimensional sobre $Z(D)$, com elementos da forma $a + b\alpha$, com $a, b \in Z(D)$. Tais

elementos claramente comutam e $D = Z(D)$. O caso $n = 2$ não pode ocorrer.

Para $n = 6$ e $q = 2$. A equação de classes de conjugação se reduz a:

$$64 - 1 = 2 - 1 + \sum_x \frac{2^6-1}{2^{n_x}-1},$$

em que n_x divide 6. Isto nos dá $62 = 63x + 21y + 9z$, com x, y, z inteiros. Isso é impossível, pois 3 não divide 62, mas 3 divide $63x + 21y + 9z$. □

2.1 CONDIÇÕES DE CADEIA

Nesta seção, estudaremos as Condições de Cadeia, trazendo algumas noções básicas. As referências para esta seção podem ser encontradas em "Anéis de Módulos"de César Polcino.

Definição 16. *Seja X um conjunto não vazio munido de uma relação $\preceq$. Dizemos que "$\preceq$"é uma relação de ordem parcial se, para todo $x, y, z \in X$, temos:*

(i) $x \preceq x$;

(ii) Se $x \preceq y$ *e* $y \preceq x$, *então* $x = y$;

(iii) Se $x \preceq y$ *e* $y \preceq z$, *então* $x \preceq z$.

Observação 3. *Suponha que X esteja munido de uma relação de ordem parcial $\preceq$. Dizemos que X é parcialmente ordenado e escrevemos $(X, \preceq)$.*

Exemplo 14. *Sejam X um conjunto e $\mathcal{P}(X)$ o conjunto das partes de X. Então a relação:*

$$A, B \in \mathcal{P}(X), A \preceq B \Leftrightarrow A \subseteq B$$

é uma relação de ordem parcial em $\mathcal{P}(X)$.

Definição 17. *Um conjunto parcialmente ordenado* $(X, \preceq)$ *é totalmente ordenado quando quaisquer dois elementos* a *e* b *de* X *são comparáveis, Isto é* $a \leq b$ *ou* $b \leq a$.

Definição 18. *Seja* $(X, \preceq)$ *um conjunto parcialmente ordenado e* $Y \subset X$ *não vazio. Dizemos que* $Y \subset X$ *é uma cadeia se* $(Y, \preceq)$ *é totalmente ordenado.*

Definição 19. *Uma sequência* $(a_n)_{n\in\mathbb{N}}$ *de elementos de* X *diz-se uma cadeia ascendente se para todo* $n \in \mathbb{N}$ *temos:*

$$a_n \preceq a_{n+1}$$

Observação 4. *Cadeias ascendentes:*

$$a_1 \preceq a_2 \preceq ... \preceq a_n \preceq ...$$

Definição 20. *Uma cadeia ascendente diz-se estacionária se existe algum* $n_0 \in \mathbb{N}$ *tal que, para qualquer* $n \geq n_0$ *tem-se* $a_n = a_{n_0}$.

Definição 21. *Dizemos que um conjunto parcialmente ordenado* X *satisfaz a condição de cadeia ascendente (C.C.A.) se toda cadeia ascendente de* X *é estacionária.*

De modo análago, definimos a condição de cadeia descendente (C.C.D.).

Exemplo 15. *Seja U o conjunto dos subespaços de um espaço vetorial V, de dimensão finita ordenado pela inclusão. Então U satisfaz a condição de cadeia ascendente e descendente.*

Definição 22. *Seja $\mathcal{F}$ uma família parcialmente ordenada e $\mathcal{F}' \subseteq \mathcal{F}$. Chamamos cota superior (resp. cota inferior) para $\mathcal{F}'$ a todo elemento $\alpha \in \mathcal{F}$ tal que $x \preceq \alpha$ (resp. $\alpha \preceq x$), $\forall x \in \mathcal{F}'$.*

Definição 23. *Seja $(X, \preceq)$ um conjunto munido de uma relação de ordem parcial. Dizemos que um elemento $m \in X$ é maximal (resp. minimal), se valer a seguinte propriedade:*

$$\forall x \in X, m \preceq x \Rightarrow m = x \text{ (resp., } x \preceq m \Rightarrow m = x).$$

Exemplo 16. *Considere $X = \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$ munido com relação "divide". Isto, é:*

$$a, b \in X, a \preceq b \Leftrightarrow a \mid b$$

Então os elementos 6, 7, 8, 9 e 10 são elementos maximais em X e os elementos 2, 3, 5 e 7 são elementos minimais em X.

2.1.1 Lema de Zorn e aplicações

Nessa subseção, apresentaremos esse lema que garante a existência de elemento maximal em determinadas famílias de ideais e a existência de ideais maximais. Além disso, iremos apresentar algumas aplicações desse Lema, como por exemplo um resultado importante, dentro da Álgebra Linear, de que todo espaço vetorial contém uma base. Nesta seção, "Anéis e Módulos"de César Polcino continuará como referência.

Lema 2.1.1. *(Lema de Zorn) Seja $(\mathcal{F}, \preceq)$ uma família não vazia e parcialmente ordenada. Se toda cadeia $\mathcal{F}$ possui uma cota superior (respectivamente, cota inferior) em $\mathcal{F}$, então $\mathcal{F}$ possui um elemento maximal (resp. elemento minimal).*

Exemplo 17. *Seja R um anel com unidade. Então R possui ideais (resp. ideais à esquerda, ideais à direita) maximais (relação de inclusão).*

Consideramos a família $\mathcal{F}$:

$$\mathcal{F} := \{I \subseteq A : I \text{ é um ideal de } A, I \neq A\}$$

Obeservamos que $\{0\} \in \mathcal{F}$ e, consequetemente, $\mathcal{F} \neq \emptyset$. Agora, seja $\mathcal{F}'$ uma subfamília totalmente ordenada de $\mathcal{F}$. Segue que, $J = \bigcup_{I \in \mathcal{F}'} I$ será um ideal. Como $1 \notin J$, pois $1 \notin I, \forall I \in \mathcal{F}'$, toda cadeia de $\mathcal{F}$ possui uma cota superior em $\mathcal{F}$, pelo Lema de Zorn $\mathcal{F}$ possui um elemento maximal, ou seja, R possui um ideal maximal.

Teorema 2.1.2. *Um conjunto parcialmente ordenado X satisfaz a condição de cadeia ascendente (C.C.A) se, e somente se, satisfaz a condição maximal.*

Demonstração. Suponhamos que X satifaça a condição maximal, e seja $(a_n)_{n \in \mathbb{N}}$ uma cadeia ascendente de elementos de X.

O conjunto $Y = \{a_n | n \in \mathbb{N}\}$ é um subconjunto de X, portanto contém algum elemento maximal, digamos $a_{n_0} \in Y$. Agora, para todo $n \geq n_0$ pela definição de cadeia temos $a_{n_0} \preceq a_n$, assim, da maximalidade de a_{n_0}, temos:

$$a_{n_0} = a_n \text{ e a cadeia é estacionária, para todo } n \geq n_0.$$

De maneira recíproca, toda cadeia Y de elementos de X, sendo estacionária, tem um majorante que pertence a Y. Segue, imediatamente, pelo Lema de Zorn, que existe um elemento maximal em Y. □

Observação 5. *De forma análoga, mostramos que a condição de cadeia descendente (C.D.D.) é equivalente à condição minimal.*

Teorema 2.1.3. *Seja V um espaço vetorial de dimensão finita sobre um corpo F e seja $\mathcal{C}$ um conjunto L.I em V. Então existe uma base $\mathcal{B}$ de V que contém $\mathcal{C}$.*

Demonstração. Tome $\mathcal{P}$ como a classe de todos os subconjuntos L.I em V e que contenham $\mathcal{C}$. É fácil ver que $\mathcal{P}$ é não vazio, pois $\mathcal{C} \in \mathcal{P}$, além disso $\mathcal{P}$ é parcialmente ordenado pela inclusão. Agora, seja $\mathcal{D} = \{A_\alpha\}_{\alpha\in\pi}$ um subconjunto totalmente ordenado de $\mathcal{P}$. O candidato a cota superior de $\mathcal{D}$ é a união $\mathcal{A}$ de todos os conjuntos A_α em $\mathcal{D}$, isto é essencial mostrar que $\mathcal{A}$ é L.I para prosseguirmos com a prova do teorema.

De fato, seja $\mathcal{M} = \{v_1, v_2, v_3, \cdots v_n\}$ um subconjunto finito de $\mathcal{A}$. Para cada $i = 1, 2 \cdots n$, existe um $\alpha_i \in A$ tal que $v_i \in \alpha_i$. Como $\mathcal{D}$ é totalmente ordenado, reordenando os elementos de $\mathcal{M}$, se necessário, temos $A_{\alpha_i} \subseteq \cdots \subseteq A_{\alpha_n}$ e, assim, $v_i \in A_{\alpha_n}$ para cada $i = 1, 2, \cdots n$. Então $\mathcal{M}$ é linearmente independente visto que A_{α_n} é L.I, como $\mathcal{M}$ é qualquer, segue que $\mathcal{A}$ é L.I. Logo $\mathcal{D}$ tem $\mathcal{A}$ por uma cota superior. Pelo Lema 2.1.1 $\mathcal{P}$ tem elemento maximal, que denotaremos por $\mathcal{B}$. Afirmamos que $\mathcal{B}$ gera V . É claro que se existisse $v \in V$ que não fosse gerado por $\mathcal{B}$, então $\mathcal{B} \cup \{v\}$ seria L.I. Absurdo, pois $\mathcal{B}$ é maximal. Assim $\mathcal{B}$ gera V e é L.I, o que mostra que $\mathcal{B}$ é uma base de V.

□

2.2 MÓDULOS SOBRE ANÉIS

Nesta seção abordaremos a teoria de Módulos, uma teoria extensa que visa generalizar o conceito de Espaço Vetorial. Foi Richard Dedekind o primeiro a usar o termo módulo para designar uma determinada estrutura, mesmo que de forma ainda muito rudimentar.

2.2.1 Módulos e Endomorfismo

Nesta subseção introduziremos algumas noções básicas sobre módulos, uma generalização de espaços vetoriais, em que os escalares se encontram em um anel com unidade. Tendo o material "Anéis de Módulos"do matemático César Polcino como referência.

Definição 24. *Seja A um anel com unidade. Dizemos que um conjunto não vazio M é um módulo à esquerda sobre A (ou um $A-$módulo à esquerda) se M é um grupo abeliano em relação a uma operação $(+)$, e está definida uma lei de composição externa que a cada par $(\alpha, m) \in A \times M$ associa um elemento $\alpha m \in M$ e tal que, para todos $\alpha_1, \alpha_2 \in A$ e todos $m_1, m_2 \in M$ verificam:*

(i) $\alpha_1(\alpha_2 m) = (\alpha_1\alpha_2)m$;

(ii) $\alpha_1(m_1 + m_2) = \alpha_1 m_1 + \alpha_2 m_2$;

(iii) $(\alpha_1 + \alpha_2)m_1 = \alpha_1 m_1 + \alpha_2 m_1$;

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

Observação 6. *Da mesma forma, podemos definir a noção de um A-módulo a direita, desde que consideremos a multiplicação à direita por elementos do anel.*

Exemplo 18. *Todo espaço vetorial sobre um corpo K é um $K-$módulo.*

Exemplo 19. *Todo grupo abeliano G pode ser considerado um $\mathbb{Z}-$módulo, definindo o produto de $n \in \mathbb{Z}$ por um elmento $g \in G$ por:*

$$ng = \begin{cases} 0 & se\ n = 0 \\ g + \cdots + g & se\ n > 0 \\ (-g) + \cdots + (-g) & se\ n < 0. \end{cases}$$

Exemplo 20. *Sejam V um espaço vetorial sobre K e $T : V \to V$ uma transformação linear. Dado o polinômio $f \in K[x]$ da forma:*

$$f(x) = a_0 + a_1 X + \cdots a_n X^n$$

Indicaremos por $f(T)$ a transformação linear:

$$f(T) = a_o I + a_1 T + \cdots a_n T^n.$$

Podemos introduzir a V uma estrutura de $K[x]-$módulo conservando a soma de V e associando a cada par $(f, v) \in K[x] \times V$ o elemento $f(T)(v) \in V$, que indica uma função $f(T)$ aplicada em algum vetor v.

Definição 25. *Seja M um $A-$módulo. Um subconjunto $N \subset M$ é um $A-$submódulo de M, ou simplesmente, submódulo se:*

(i) N é um subgrupo aditivo de M.

(ii) N é fechado em relação à multiplicação por escalares: Dado $a \in A$ e para todo $n \in N$ temos $an \in N$.

Observação 7. *Note que um subconjunto não vazio $N \subset M$ é um submódulo se, e somente se,*

(i) $\forall n, n' \in N, n + n' \in N$.

(ii) $\forall a \in A, \forall n \in N$, *temos* $an \in N$.

Proposição 2.2.0.1. *Sejam M um A-módulo e $M_1, M_2, \cdots M_t$ submódulos de M. O conjunto:*

$$\sum_{i=1}^{t} M_i = \{\sum_{i=1}^{t} m_i : m_i \in M_i\}$$

é um submódulo de M.

Demonstração. Inicialmente, note que $\sum_{i=1}^{t} M_i$ é um subgrupo de M. Sejam $m = m_1 + m_2 + \cdots + m_t \in \sum_{i=1}^{t} M_i$ e $a \in A$. Segue que:

$$\begin{aligned} am &= a(m_1 + m_2 + \cdots + m_t) \\ &= am_1 + am_2 + \cdots am_t. \end{aligned}$$

Como M_i é um A-módulo, logo $am_i \in M_i, \forall i = 1, \cdots t$. Então:

$$am \in \sum_{i=1}^{t} M_i,$$

portanto é submódulo de M. □

Proposição 2.2.0.2. *Sejam M um A-módulo e $\mathcal{F} = \{N_i\}_{i \in I}$ um família de submódulos de M. Então $N = \bigcap_{i \in I} N_i$ é um submódulo de M.*

Demonstração. Primeiramente, note que $\bigcap_{i \in I} N_i$ é um subgrupo de M. Sejam $m \in \bigcap_{i \in I} N_i$ e $a \in A$. Temos que $am \in N_i$ para todo $i \in I$, pois N_i é um submódulo. Assim:

$$am \in \bigcap_{i \in I} N_i.$$

Logo $\bigcap_{i\in I} N_i$ é submódulo de M. □

Exemplo 21. *Os submódulos de um espaço vetorial são exatamente os seus subespaços vetoriais.*

Exemplo 22. *Os subgrupos de um grupo abeliano são, exatamente, seus $\mathbb{Z}-$submódulos.*

Definição 26. *Sejam A um anel, M um $A-$módulo à esquerda e $K \subseteq M$. Denominamos de submódulo de M gerado por K, o qual denotamos $< K >$, ao menor submódulo M que contém K.*

Exemplo 23. *Seja M um $A-$módulo e N e submódulo de M. Considerando a estrutura de grupo abeliano de M, podemos construir o grupo quociente $M/N = \{m + N \mid m \in M\}$ dado por:*

$$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N.$$

Além disso, definimos:

$$(\alpha, m + N) \in A \times M/N, \text{ com } \alpha \in A \text{ e } \alpha m + N \in M/N.$$

A operação apresentada está bem definida. Com efeito, suponha que $m_1 + N = m_2 + N$. Temos assim que $m_1 - m_2 \in N$. Como N é submódulo, $rm_1 - rm_2 \in N$. Assim $rm_1 + N = rm_2 + N$.

Definição 27. *O A-módulo M/N construído acima é chamado módulo quociente do módulo M pelo submódulo N.*

Definição 28. *Sejam M e N dois A-módulos. Uma função $f : M \to N$ é um homomorfismo de A-módulos ou um A-homomorfismo se para todo $m_1, m_2 \in M$ e todo $a \in A$ verifica-se:*

(i) $f(m_1 + m_2) = f(m_1) + f(m_2)$.

(ii) $f(am_1) = af(m_1)$.

Exemplo 24. *Se F é uma anel de divisão, então os F-homomorfismos são, exatamente, as transformações K-lineares.*

Definição 29. *Seja o A-homomorfismo $f : M \to N$:*

(i) *Dizemos que f é um monomorfismo se f é injetora;*

(ii) *Dizemos que f é um epimorfismo se f é sobrejetora.*

Definição 30. *Um $A-$ homomorfismo $f : M \to M$ é dito endomorfismo.*

Definição 31. *Dado um A-homomorfismo $f : M \to N$, denotamos imagem e núcleo (ou kernel) de f respectivamente por:*

$$Im(f) = \{n \in N | \exists m \in M \Rightarrow f(m) = n\};$$

$$Ker(f) = \{m \in M | f(m) = 0\}.$$

Observação 8. *Tendo como base 2.0.1.2. Pode-se provar que um A-homomorfismo $f : M \to N$ é injetor se, e somente se, $Ker(f) = \{0\}$.*

Definição 32. *Considere um A-homomorfismo $f : M \to N$. Dizemos que f é um A-isomorfismo se existe um A-homomorfismo $g : M \to N$ tal que:*

$$g \circ f = 1_M \ e \ f \circ g = 1_N.$$

Proposição 2.2.0.3. *Um A-homomorfismo $f : N \to N$ é um isomorfismo se, e somente se, f é simultaneamente, monomorfismo e epimorfismo.*

Demonstração. $\Rightarrow$ Seja f um isomorfismo e $g : N \to M$ um $A-$homomorfismo. Pelas definições, temos: $g \circ f = 1_M$ e, portanto, f é um monomorfismo; além disso $f \circ g = 1_N$, logo f também é um epimorfismo.

$\Leftarrow$ Suponha f seja bijetora, logo existe uma função $g : N \to M$ tal que $g \circ f = 1_M$ e $f \circ g = 1_N$. Basta verificar que g é um A-homomorfismo. Dados $y_1, y_2 \in N$, vamos verificar que:

$$g(y_1 + y_2) = g(y_1) + g(y_2).$$

Do fato, de f ser um epimorfismo, existem $x_1, x_2 \in M$ tais que:

$$f(x_1) = y_1 \text{ e } f(x_2) = y_2.$$

Agora:

$$g(y_1) + g(y_2) = g \circ f(x_1) + g \circ f(x_2) = x_1 + x_2.$$

Mas como f é um $A-$homomorfismo, $f(x_1+x_2) = y_1+y_2$. Calculando g nos dois membros da igualdade:

$$x_1 + x_2 = g(y_1 + y_2).$$

De maneira análoga, podemos provar $g(\alpha y) = \alpha g(y), \forall \alpha \in A$ e todo $y \in M$. □

Teorema 2.2.1. *(Teorema do Homomorfismo para Módulos) Sejam M e N dois A-módulos, $f : M \to N$ um $A-$homomorfismo, $\pi : M \to M/ker(f)$ a projeção canônica ao quociente e $\varphi : Im(f) \to N$ a inclusão. Existe uma única função:*

$$f' : M/Ker(f) \to Im(f)$$

tal que:

(i) $\varphi \circ f' \circ \pi$

(ii) f' *é um isomorfismo.*

Demonstração. A prova desse teorema segue essencialmente a do Teorema 2.0.2 □

Corolário 2.2.1.1. *Se $f : M \to N$ é um $A-$epimorfismo, então $M \cong N/Ker(f)$.*

Teorema 2.2.2. *(Primeiro Teorema do Isomorfismo) Seja M um $A-$módulo e sejam P e N dois submódulos tais que $P \subset N$. Então:*

$$M/N \cong \tfrac{M/P}{N/P}.$$

Demonstração. Definimos a função $f : M/P \to M/N$ por:

$$f(m + P) = m + N, \text{ para todo } m \in M.$$

Como $P \subset N$, temos que se $m_1, m_2 \in M$ e $m_1 + P = m_2 + P$, então $m_1 + N = m_2 + N$; logo f está bem definida.

De maneira trivial podemos provar que f é epimorfismo, assim pelo Corolário 2.2.1.1 temos:

$$\frac{M/P}{Ker(f)} \cong M/N.$$

Agora, a classe $m + P \in Ker(f) \Leftrightarrow m + N = N$, ou seja, se e só se $m \in N$ e $m + P \in N/P$. Portanto, $Ker(f) = N/P$. □

Teorema 2.2.3. *(Segundo Teorema do Isomorfismo) Sejam N, P dois submódulos de um A-módulo M. Então temos:*

$$\frac{N}{N \cap P} \cong \frac{N+P}{P}$$

Demonstração. Definimos $f : N \to \frac{M+N}{P}$ por $f(n) = n + P, \forall n \in N$.

De fato, f é um homomorfismo. Precisamos verificar que f é sobrejetora. Basta observar que todo elemento de $\frac{N+P}{P}$ é da forma $(n + p) + P, n \in N, p \in P$. Mas $(n + p) + P = n + P$ logo $f(n) = n + P = (n + p) + P =$ e f é epimorfismo.

Daí segue que:

$$\frac{N}{Ker(f)} \cong \frac{N+P}{P}.$$

Dado $n \in Ker(f)$, temos $n + P = P$. Assim $n \in P$. Como $n \in Ker(f) \subset N$, segue que $n \in N \cap P$. Por outro lado, se $n \in N \cap P$, então $n + P = P$, o que mostra que $n \in Ker(f)$. □

Observação 9. *O Teorema 2.2.3 é chamado às vezes de Isomorfismo de Noether.*

2.2.2 Sequências Exatas

Neste tópico, abordaremos sequências exatas, uma ferramenta muito útil em várias áreas da matemática. Usaremos as sequências exatas como uma linguagem que nos permite relacionar certos morfismos de $A-$módulos por meio de diagramas. Nesta seção, usaremos "Anéis e Módulos"do autor Polcino como maior referência.

Definição 33. *Sejam F, G e H três A-módulos, sejam $f : F \to G, g : G \to H$ dois A-homomorfismos. Dizemos que o diagrama:*

$$F \xrightarrow{f} G \xrightarrow{g} H$$

é uma sequência exata de ordem 2 em G se $Im(f) \subset Ker(g)$

Em particular, se $Im(f) = Ker(g)$ o diagrama é uma sequência exata.

Definição 34. *Seja $\{\cdots, M_{i-1}, M_i, M_{i+1}, \cdots\}$ uma família de A-módulos e seja $\{\cdots, f_i : M_i \to M_{i+1} \cdots\}$ uma família de A-homomorfismos. Dizemos que o seguinte diagrama:*

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

é uma sequência exata em M_i, para todo $i \in I$, se $Im(f_{i-1}) = Ker(f_i)$.

Exemplo 25. *Sejam A um anel e $f : N \to M$ um A-homomorfismo à esquerda. São fatos bem conhecidos:*

1. *A sequência $0 \to N \xrightarrow{f} M$ é exata se, e somente se, f é um monomorfismo.*

2. *A sequência* $N \xrightarrow{f} M \to 0$ *é exata se, e somente se,* f *é um epimorfismo.*

3. *A sequência* $0 \to N \xrightarrow{f} M \to 0$ *é exata se, e somente se,* f *é um isomorfismo.*

Definição 35. *Uma sequência do tipo* $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ *é dita uma sequência exata curta.*

Exemplo 26. *A sequência* $0 \to 2\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\omega} \mathbb{Z}_2 \to 0$*, onde* $i : 2\mathbb{Z} \to \mathbb{Z}$ *é a inclusão e* $\omega : \mathbb{Z} \to \mathbb{Z}_2$ *a função que associa cada inteiro a sua classe em* $\mathbb{Z}_2$*, é uma sequência exata curta.*

Exemplo 27. *Sejam* A *um anel,* M *um* A*-módulo à esquerda e* N *um submódulo de* M*. Então a sequência*

$$0 \to N \to M \xrightarrow{\pi} M/N \to 0$$

é uma sequêcia exata curta, em que π *é a projeção canônica.*

Proposição 2.2.3.1. *Se a sequência* $M \xrightarrow{f} N \xrightarrow{g} R \xrightarrow{h} S$ *é exata, são equivalentes:*

(i) f *é epimorfismo.*

(ii) $Im(g) = \{0\}$*.*

(iii) h *é monomorfismo.*

Demonstração. $(i) \Rightarrow (ii)$

Como a sequência é exata, $Im(f) = Ker(g)$ e $Im(g) = Ker(h)$. Como f é epimorfismo, então $Im(f) = N = Ker(g)$. Assim temos $Ker(g) = N$, o que mostra que $Im(g) = \{0\}$

$(ii) \Rightarrow (iii)$

Seja a sequência $N \xrightarrow{g} R \xrightarrow{h} S$ e $Im(g) = 0$. Como a sequência é exata $Im(g) = Ker(h)$ implica $\{0\} = Ker(h)$ temos que h é injetiva, logo é um monomorfismo.

$(iii) \Rightarrow (i)$

Por hipótese h é monomorfismo, ou seja, h é injetiva e $Ker(h) = \{0\}$. Seja a sequência $M \xrightarrow{f} N \xrightarrow{g} R \xrightarrow{h} S$. Como $Ker(h) = \{0\} = Im(g)$, temos $Im(g) = \{0\}$, assim $Ker(g) = N$. Daí segue que $Ker(g) = Im(f)$, o que acarreta $Im(f) = N$. Logo f é sobrejetiva e f é epimorfismo. □

2.2.3 Soma direta e produto direto

Seja $\{M_i\}_{i\in I}$ uma família de $A-$módulos e seja $M = \prod_{i\in I} M_i$ o produto cartesiano dos membros da família. Em M podemos introduzir uma estrutura de A-módulo, desde que:

$$(m_i)_{i\in I} + (m'_i)_{i\in I} = (m_i + m'_i)_{i\in I},$$
$$\lambda(m_i)_{i\in I} = (\lambda m_i)_{i\in I}.$$

Definição 36. *O $A-$módulo construído acima é definido como produto direto da família $\{M_i\}_{i\in I}$.*

$$\prod_{i\in I} M_i = M_1 \times \cdots M_n.$$

Definição 37. *Seja $\{M_i\}_{i\in I}$ uma família A-módulos e considere $M = \prod_{i\in I} M_i$. Uma família $(m_i)_{i\in I} \in M$ é dita uma família quase nula se $m_i = 0$, exceto para um número finito de índices.*

Proposição 2.2.3.2. *Seja $\{M_i\}_{i\in I}$ uma família de submódulos do A-módulo M. Então, as seguintes afirmações são equivalentes:*

(i) Todo elemento $m \in M$ se escreve de uma única maneira, na forma $m = \sum_{i\in I} m_i$ em que $m_i \in M, \forall i \in I$ a família $(m_i)_{i\in I}$ é quase nula.

(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 $m_i = 0, \forall i \in I$.

(iii) $M = \sum_{i\in I} M_i$ e $M_j \cap \sum_{i\neq j} M_i = (0), \forall j \in I$.

Demonstração. $(i) \Rightarrow (ii)$: É imediato.

$(ii) \Rightarrow (iii)$: Seja m um elemento $M_j \cap \sum_{i\neq j} M_i$. Logo, $m \in M_j$ pode ser escrito na forma $m = \sum_{i\neq j} m_i$, com $m_i \in M_i, i \in I$. Temos assim:

$$\sum_{i\neq j} m_i - m = 0.$$

De (ii) os somandos devem ser nulos, em particular $m = 0$.

$(iii) \Rightarrow (i)$: Do fato de $M = \sum_{i\in I} M_i$ temos que todo elemento $m \in M$ é da forma $m = \sum_{i\in I} m_i$ em que $m_i \in M_i, \forall i \in I$ e a família $(m_i)_{i\in I}$ é quase nula. Suponhamos $\sum_{i\in I} m_i = \sum_{i\in I} m'_i$. Para todo $j \in I$, pode-se escrever:

$$m_j - m'_j = \sum_{i\neq j}(m'_i - m_i).$$

Portanto $m_j - m'_j \in M_j \cap \sum_{i\neq j} M_i$ e $m_j = m'_j$. □

Definição 38. *Seja M um A-módulo, definimos a soma direta de uma família $\{M_i\}_{i\in I}$ de submódulos se forem validas as condições de equivalência da Proposição 2.2.3.2.*

Observação 10. *Indicaremos que M é soma direta dos submódulos $\{M_i\}_{i\in I}$ como:*

$$M = \bigoplus_{i\in I} M_i.$$

Se $I = \{1, 2, \cdots n\}$, denotaremos

$$M = M_1 \oplus M_2 \oplus \cdots M_n.$$

Exemplo 28. *Para que seja um A-módulo M, temos sempre que $M = M \oplus \{0\}$. Os submódulos M e $\{0\}$ são ditos somando diretos triviais.*

Exemplo 29. *O $\mathbb{Z}$-módulo $\mathbb{Z}_6$ e seus submódulos $M_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $M_2 = \{\overline{0}, \overline{3}\}$ são tais que $M_1 \cap M_2 = (0)$. O $\mathbb{Z}-$módulo $\mathbb{Z}_6$ pode ser escrito como uma soma direta de submódulos da forma:*

$$\mathbb{Z}_6 = M_1 \oplus M_2.$$

2.2.4 Base e dimensão de módulos

Definição 39. *Seja $\{x_i\}_{i\in I}$ uma família de elementos de um A-módulo M. Dizemos que um elemento $x \in M$ é uma combinação linear dos elementos da família se existe $(\lambda_i)_{i\in I} \in A^{(I)}$ tal que:*

$$x = \sum_{i\in I} \lambda_i x_i.$$

Note que a soma acima está bem definida, devido ao fato de só um número finito de somandos ser diferente de zero.

Pode-se verificar que dado um subcojunto S de M, o submódulo gerado por S é o cojunto de todas as combinações lineares dos elementos de S.

Definição 40. *Seja M um $A-$ módulo. Dizemos que M é finitamente gerado quando existe uma família $\{x_1, x_2, \cdots, x_n\}$ de elementos de M tal que todo outro $x \in M$ é da forma:*

$$x = \sum_{i=1}^{n} \lambda_i x_i$$

com $\lambda_i \in A, 1 \leq i \leq n$.

Definição 41. *Um família $\{x_i\}_{i\in I}$ de elementos de um A-módulo M é linearmente independente (L.I) ou livre se para todo $(\lambda_i)_{i\in I} \in A^{(I)}$ temos:*

$$\sum_{i\in I} \lambda_i x_i = 0 \text{ implica em } \lambda_i = 0, \forall i \in I.$$

Definição 42. *Um família $\{x_i\}_{i\in I}$ de elementos de um A-módulo M é uma base de M se é uma famiília L.I e gera M.*

Observação 11. *Note que se $\{x_i\}_{x\in I}$ é uma base de um A-módulo M, então:*

$$M = \bigoplus_{i\in I} Ax_i.$$

Definição 43. *Um $A-$módulo M é dito livre se ele contém uma base.*

É bem conhecido que se β e β' são duas bases de um A-módulo livre M, sendo A um anel comutativo com unidade, então a cardinalidade de β é igual a cardinalidade de β'. Nestas condições, então o posto de um A-módulo livre M é a cardinalidade de uma base de M.

Exemplo 30. *Todo espaço vetorial sobre um corpo K é um $K-$módulo livre.*

2.3 CONDIÇÕES DE FINITUDE PARA ANÉIS E MÓDULOS

Nesta seção, abordaremos o conceito de Módulos Simples e Condições de Cadeias, apresentaremos o Teorema de Jordan Hölder, sendo o principal resultado desse capítulo. Nesta seção do trabalho, usaremos "Uma introdução ao Estudo de Anéis Semissimples"do matemático Alveri Sant'Ana.

2.3.1 Módulos e Anéis Simples

Definição 44. (i) *Dizemos que um A-módulo à esquerda M é simples, se $M \neq \{0\}$ e M não possui nenhum submódulo além do submódulo M e o submódulo trivial $\{0\}$*

(ii) *Dizemos que um anel A é simples se $A \neq \{0\}$ e A não possui ideais bilaterais além do ideal nulo e do próprio A.*

Observação 12. *Note que anéis de divisão são anéis simples.*

Exemplo 31. *Os espaços vetoriais unidimensionais são módulos simples à esquerda.*

Exemplo 32. *Para verificarmos que $M_n(K)$ é um anel simples, vamos considerar o conjunto $\overline{n} = \{1, 2, \dots n\}$ e um ideal bilateral J em $M_n(K)$. Sejam o conjunto $X = \{(i,j) \in \overline{n} \times \overline{n}\}$ e, para cada $(i,g) \in X$ o seguinte ideal bilateral de K:*

$$I_{i,j} = \{x \in K \mid \exists A \in J \mid a_{ij=x}\}.$$

Como K é corpo, só temos duas possibilidades:

$$I_{i,j} = \{0\} \text{ ou } I_{i,j} = K$$

Caso $I_{i,j}\{0\}$ para todo par $(i,j) \in X$, então $J = \{0\}$ tal que $I_{i_1,j_1} = K$, existe uma matriz $B \in J$ tal que $b_{i_1,j_1} = 1$. Como J é ideal bilateral, temos que $E_{i_1,j_1} = E_{i_1,i_1} B E_{j_1,j_1}$ e $E_{kl} = E_{ki_1} E_{j_1 l}$ são elementos de J. Como as matrizes elementares geram $M_n(K)$ como espaço vetorial, segue que $J = M_n(K)$. Assim o anel $M_n(K)$ é simples.

Definição 45. *Seja M um $A-$módulo à esquerda. Seja $m \in K$ o conjunto $An_A(m) = \{r \in A \mid rm = 0\}$ é um ideal à esquerda de A. O conjunto $An_A(m)$ é denominado anulador de m.*

Exemplo 33. *Seja A um anel com unidade e seja M um $A-$módulo simples. Tomando $0 \neq m \in M$, considere o $A-$homomorfismo:*

$$f : A \to M$$
$$f(r) = rm$$

Como M é simples, logo $Im(f) = 0$ ou $Im(f) = M$. Haja visto que A tem unidade, f não pode ser o homomorfismo nulo, pois $0 \neq m = 1m = f(1)$. Então $Im(f) = M$ e, assim, $M \cong A/An_A(m)$.

Assim podemos enunciar a seguinte proposição que nos diz a respeito da classificação de módulos simples.

Proposição 2.3.0.1. *Sejam A um anel com unidade e M um A-módulo. Então M é simples se, e somente se, existe um ideal à esquerda maximal I de A tal que $M \cong A/I$.*

Demonstração. Suponha M simples. Considere $m \in M$ não nulo. Temos $A/An_A(m)$ é um ideal à esquerda maximal de A. Por outro lado, se existe um ideal maximal à esquerda J, então A/J é um $A-$módulo simples. Como $A/J \cong M$, segue que M é simples.

□

2.3.2 Séries de Composição

Definição 46. *Sejam A um anel e M um A-módulo. Consideremos*

$$\mathcal{C} : M = M_0 \supset M_1 \supset M_2 \supset \cdots M_r = \{0\}$$

e

$$\mathcal{C}' : M = M'_0 \supset M'_1 \supset M'_2 \supset \cdots M'_t = \{0\}$$

duas cadeias finitas e estritamente decrescentes de submódulos de M. Então dizemos que:

(i) $\mathcal{C}'$ é um refinamento de $\mathcal{C}$, se todo membro de $\mathcal{C}$ aparece em $\mathcal{C}'$ (usamos a notação $\mathcal{C} \subseteq \mathcal{C}'$);

(ii) A cadeia $\mathcal{C}$ é uma série de composição de M, se cada módulo quociente

$$\frac{M_i}{M_{i+1}},\ (0 \leq i \leq r-1)$$

é simples, ou seja, $\mathcal{C}$ não pode ser refinada;

(iii) O módulo M tem um comprimento r e denotamos $\ell(M) = r$, se M possui uma série de composição com r inclusões estritas. No Teorema de Jordan-Hölder, verificaremos que r está bem definido, independe da série de composição. Se M não possui nehuma série de composição, então M tem comprimento infinito: $\ell(M) = \infty$;

(iv) As cadeias $\mathcal{C}$ e $\mathcal{C}'$ são equivalentes, e denominamos por $\mathcal{C} \cong \mathcal{C}'$, se $r = t$ e, após uma reodenação nos índices, se necessário, temos:

$$\frac{M_i}{M_{i+1}} \cong \frac{M'_i}{M'_{i+1}} \ .$$

Exemplo 34. *Se K é um corpo (ou anel de divisão) e V é um $K-$espaço vetorial de dimensão n com base $\mathcal{B} = \{v_1, v_2, \cdots, v_n\}$, temos:*

$$V = V_0 = \sum_{i=1}^{n} Kv_i \supset V_1 = \sum_{i=2}^{n} Kv_i \supset \cdots \supset V_{n-1} = Kv_n \supset V_n = 0$$

é uma série de composição de V, com $\ell(V) = n$.

Proposição 2.3.0.2. *A série*

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_r = 0$$

é uma série de composição se, e somente se, cada quociente $M_i/M_{i+1}, 0 \leq i \leq r-1$, é um módulo simples.

Demonstração. Basta observer que M_i/M_{i+1} é simples se, e somente se, não existe nenhum submódulo N_1 de M tal que:

$$M_i \supsetneq N_i \supsetneq M_{i+1}.$$

□

Agora, vamos apresentar alguns lemas essencias para a demonstração de um dos teoremas mais importantes da seção: O Teorema de Jordan-Hölder.

Lema 2.3.1. *(Lema de Zassenhaus) Sejam A um anel e M um A-módulo. Se $N \subset P$ e $N' \subset P'$ são submódulos de M, então:*

$$\frac{N+(P\cap P')}{N+(P\cap N')} \cong \frac{P\cap P'}{(N\cap P')+(N'\cap P)} \cong \frac{N'+(P'\cap P)}{N'+(P'\cap N)}$$

Demonstração. Para provar o lema, basta assegurar o primeiro isomorfismo, consequentemente teremos o segundo por simetria.

Consideremos a aplicação:

$$\varphi : N + (P + P') \longrightarrow \frac{P\cap P'}{(N\cap P')+(N'\cap P)}$$
$$n + q \mapsto q + [(N \cap P') + (N' + P)]$$

com $n \in N$ e $q \in P \cap P'$.

Primeiro, vejamos se φ está bem definida. Seja $x = n + q = n_1 + q_1$. Assim $n - n_1 = q_1 - q \in N \cap P'$. Então as classes q e q_1 módulo $[(N \cap P' + (N' \cap P)]$ são iguais. Além disso, note que φ é um $A-$epimorfismo, um homomorfismo sobrejetor.

Vamos mostrar que $Ker(\varphi) = N + (P \cap N')$. Observe que $N + (P \cap N') \subseteq Ker(\varphi)$. Por outro lado, se $n \in N$ e $q \in P \cap P'$ são tais que $\varphi(n+q) = \overline{0}$, temos $q \in (N\cap P')+(N'\cap P)$, ou seja $q = q_1+q_2$ de modo que $q_1 \in N\cap P'$ e $q_2 \in N'\cap P$. Logo, $n+q = n+q_1+q_2$, de tal forma que $n+q_1 \in N$ e $q_2 \in P\cap P'$, quer dizer, $N+(P\cap N') \subseteq Ker(\varphi)$. Portanto φ é isomorfismo. □

Lema 2.3.2. *(Lema do refinamento de Schreier) Sejam $\mathcal{C}$ e $\mathcal{C}'$ duas cadeias finitas e estritamente decrescentes de submódulos de um A-módulo M. Então existem refinamentos $\mathcal{C}_1$ de $\mathcal{C}$ e $\mathcal{C}'_1$ de $\mathcal{C}'$, os quais são equivalentes.*

Demonstração. Sejam as cadeias finitas estritamentes decrescentes dos submódulos de um A-módulo M.

$$\mathcal{C} : M = M_0 \supset M_1 \supset M_2 \supset \cdots \supset M_r = \{0\}$$

e

$$\mathcal{C}' : M = M'_0 \supset M'_1 \supset M'_2 \supset \cdots \supset M'_s = \{0\}$$

Para cada $i \in \{1, 2, \ldots r\}$ e $j \in \{1, 2, \ldots s\}$, definimos os A-módulos:

$$M_{i,j} := M_i + (M_{i-1} \cap M'_j) \subseteq M_i$$

e

$$M'_{j,i} := M'_j + (M'_{j-1} \cap M_i) \subseteq M'_j.$$

Consideremos agora as seguintes cadeias decrescentes dos submódulos do A-módulo M :

$$\overline{\mathcal{C}_1} := M \supseteq M_{1,1} \supseteq \cdots \supseteq M_{1,s} = M_1 \supseteq M_{2,1} \supseteq \cdots \subseteq M_{2,s} = M_2 \supseteq \cdots \supseteq M'_{r,s} = \{0\}$$

e

$$\overline{\mathcal{C}'_1} := M \supseteq M'_{1,1} \supseteq \cdots \supseteq M'_{1,r} = M'_1 \supseteq M'_{2,1} \supseteq \cdots \subseteq M'_{2,r} = M'_2 \supseteq \cdots \supseteq M_{s,r} = \{0\}$$

Desta forma, temos $\mathcal{C} \subseteq \mathcal{C}'_1$ e $\mathcal{C}' \subseteq \overline{\mathcal{C}'_1}$. Pelo Lema 2.3.1 temos que:

$$\frac{M_{i,j-1}}{M_{i,j}} = \frac{M_i+(M_{i-1}\cap M'_{j-1})}{M_i+(M_{i-1}\cap M'_j)} \cong \frac{M'_j+(M'_{j-1}\cap M_{i-1})}{M'_j+(M'_{j-1}\cap M_i)} = \frac{M'_{j,i-1}}{M'_{j,i}}.$$

Ou seja, $\frac{M_{i,j-1}}{M_{i,j}} \cong \frac{M'_{i,j-1}}{M'_{j,i}}$. Isto mostra que $M_{i,j-1} = M_{i,j}$ se, e só se, $M'_{i,j-1} = M'_{j,i}$. Portanto $\overline{\mathcal{C}_1}$ e $\overline{\mathcal{C}'_1}$ são equivalentes a $\mathcal{C}_1$. □

Teorema 2.3.3. *(Teorema de Jordan Holder)*

Seja M um A-módulo à esquerda que possui uma séria de composição $\mathcal{C}$. Então

(i) Toda cadeia estritamente decrescente de submódulos M é finita e admite um refinamento que é uma série de composição;

(ii) Duas séries de composição são equivalentes.

Demonstração. (i) Sejam $\mathcal{C}$ uma série de composição de M com comprimento r e $\mathcal{C}'$ uma cadeia estritamente decrescente de A-submódulos de M. Então, pelo Lema 2.3.2, existem refinamentos $\mathcal{C}'_1$ de $\mathcal{C}'$ e $\mathcal{C}_1$ de $\mathcal{C}$ de modo que $\mathcal{C}'_1$ seja equivalente. Como $\mathcal{C}_1 = \mathcal{C}$, pois $\mathcal{C}$ é um série de composição, segue que $\overline{\mathcal{C}'_1}$, é uma série de composição, com o mesmo comprimento r.

(ii) Este item segue diretamente pelo Lema 2.3.2. □

Proposição 2.3.3.1. *Sejam A um anel, M um $A-$módulo e N um submódulo de M. Então $\ell(M) < \infty$ se, e somente se, $\ell(N), \ell(M/N) < \infty$. Além disso, $\ell(M) = \ell(N) + \ell(M/N)$.*

Demonstração. $(\Rightarrow)$ Se $N = 0$ ou $N = M$, não há nada para mostrar.

Suponha que N é um submódulo próprio de M. Consideremos a cadeia:

$$\{0\} \subset N \subset M.$$

Sabemos que essa cadeia pode ser refinada a uma série de composição, digamos:

$$N_0 \subset \cdots \subset N_n = N = M_0 \subset \cdots \subset M_m = M,$$

De onde concluímos que $\ell(N) = n < \infty$. Tomando $P_i = M_i/N$ temos a cadeia:

$$\subset P_0 \cdots \subset P_m = M/N.$$

De modo que:

$$\frac{P_i}{P_{i-1}} = \frac{M_i/N}{M_{i-1}/N} \cong \frac{M_i}{M_{i-1}},$$

em que todos os módulos descritos são simples. Então $\ell(M/N) = m \neq \infty$, portanto $\ell(M) = m + n = \ell(N) + \ell(M/N)$.

($\Leftarrow$) Suponha $\ell(N) = n$ e $\ell(M/N) = m$ e tome as seguintes séries de composição:

$$N_0 \subset N_1 \subset \cdots \subset N_n = N$$

e

$$P_1 \subset \cdots \subset P_m = M/N,$$

em que π é projeção canônica de M em M/N, sendo $1 \leq i \leq m$.

Agora, seja $M_i = \pi^{-1}(P_i)$. Segue que $P_i = M_i/N$ e:

$$\frac{M_i}{M_{i-1}} \cong \frac{P_i}{P_{i-1}} \text{ com } 1 \leq i \leq m,$$

em que todos são módulos simples.

$$\text{Assim } N_0 \subset \cdots \subset N_n = N = M \subset \cdots \subset M_m = M$$

é, de fato, uma série de composição de M, segue então que $\ell(M) = \ell(N) + \ell(M/N) < \infty$. □

Teorema 2.3.4. *Sejam A um anel e M um A-módulo. Então M tem comprimento finito se, e somente se, toda cadeia estritamente decrescente e toda cadeia estritamente crescente de A-submódulos de M é finita. Em particular, todo A-módulo finito possui comprimento finito.*

Demonstração. ($\Rightarrow$) Suponhamos que $\ell(M) = r$. Se $\mathcal{C} := M = M_0 \supset M_1 \supset \cdots M_k \supset \cdots$ é uma cadeia estritamente decrescente de submódulos de M; pelo Teorema 2.3.3, $\mathcal{C}$ é finita.

Agora, seja $N_0 \subset N_1 \subset \cdots \subset N_k \subset \cdots$ uma cadeia estritamente crescente de submódulos de M. Portanto, para cada $t \in \mathbb{N}$ podemos tomar a cadeia $\mathcal{C}' := M \supset N_t \supset N_{t-1} \supset \cdots \supset N_0 \supseteq \{0\}$, pelo Teorema 2.3.3 esta cadeia pode ser refinada até uma série de composição de comprimento r. Logo $t \leq r = \ell(M)$, como t foi tomado de maneira arbtitrária, a cadeia $N_0 \supset N_1 \supset \cdots \supset N_k \supset \ldots$ tem comprimento finito.

($\Leftarrow$) Caso $M = 0$ a prova é imediata. Agora, seja $M \neq \{0\}$. Tomemos um submódulo maximal de M, digamos M_1 que, por hipótese, existe, a existência é assegurada pelo Lema 2.1.1. Se $M_1 = \{0\}$, então $M \supset M_1 = \{0\}$ é uma série de composição de M. Caso $M_1 \neq \{0\}$ escolhemos um submódulo maximal de M , digamos M_2. Se $M_2 = 0$, logo $M = M_0 \supset M_1 \supset M_2 = \{0\}$ é uma série de composição. Continuando o processo, de maneia induzida, obtemos a cadeia:

$$M = M_0 \supset M_1 \supset \cdots \supset M_k = \{0\}.$$

devido ao fato de toda cadeia estritamente decrescente ser finita. Como para todo $0 \leq j \leq k-1$ o módulo $\frac{M_j}{M_{j+1}}$ é simples, pela escolha de M_{j+1}. Assim, a cadeia acima é uma séria de composição de M com comprimento finito. $\square$

Exemplo 35. *Sejam M um grupo cíclico de quatro elementos e K o grupo de Klein, então $\ell(_{\mathbb{Z}}M) = \ell(_{\mathbb{Z}}K)$, mas M e K não são isomorfos, visto como $\mathbb{Z}-$módulo.*

2.3.3 Anéis e módulos noetherianos e artinianos

Definição 47. *Sejam A um anel e M um A-módulo. Então dizemos que:*

(i) M é um módulo artiniano, se toda cadeia estritamente decrescente de submódulos de M é finita;

(ii) M é um módulo noetheriano, se toda cadeia estritamente crescente de submódulos de M é finita.

Observação 13. *Podemos definir módulos noetherianos e artinianos de outra maneira, usando condições de cadeia ascedentes e descendentes.*

Definição 48. *Um A-módulo M diz-se noetheriano (respectivamente artiniano) se o conjunto de seus submódulos, ordenados pela inclusão, satizfas a C.C.A (respectivamente C.C.D).*

Exemplo 36. *Seja V um F-espaço vetorial de dimensaõ finita. Então V é um F-módulo artiniano e noetheriano.*

Exemplo 37. *Seja I um conjunto infinito de índices e seja $\{M_i\}_{i\in I}$ uma família de A-módulos. Logo $M = \bigoplus_{i\in I} M_i$ não é artiniano e nem noetheriano.*

Para mostrar que M não é notheriano, consideremos a família de subconjuntos de $J_1, J_2, \ldots, J_n, \ldots$, tais que $J_n \subsetneq J_m$, sempre que

$n < m$. Agora, seja a cadeia estritamente crescente $P_1 \subset P_2 \subset \cdots \subset P_k \subset \cdots$, em que $P_k = \oplus_{i \in J_k} M_i$. Logo a cadeia não é estacionária.

Para mostrar que M é não artiniano, basta construir a família $K_1, K_2, , K_n, \ldots$ de subconjuntos de J, definida por:

$$(i)\ K_0 = I,$$

$$(ii)\ K_1 = I \setminus \{i_1\} \in I,$$

$$(iii)\ K_2 = I \setminus \{i_1, i_2\},\ \text{em que } i_2 \in I \setminus \{i_1\};$$

E assim, sucessivamente, por indução. Observe que a cadeia $Q_0 \supset Q_1 \supset \cdots \supset Q_k \supset \cdots$, em que $Q_t = \oplus_{I \in K_i} M_i$ que é infinita, logo não é estacionária.

Exemplo 38. *$\mathbb{Z}$, visto como um $\mathbb{Z}$-módulo é noetheriano, contudo não é artiniano.*

Note que todos os $\mathbb{Z}$-submódulos de $\mathbb{Z}$ são seus ideais da forma $n\mathbb{Z}$. O $\mathbb{Z}-$módulo não é artiniano, pois, por exemplo, a cadeia estritamente decresente a seguir é infinita, não estaciona:

$$2\mathbb{Z} \supset 4\mathbb{Z} \supset \cdots \supset 2^n\mathbb{Z} \supset \cdots$$

não é finita. Em contrapartida, $n\mathbb{Z} \subseteq m\mathbb{Z}$ se, e somente se, $m \mid n$. Como o conjunto de divisores de um inteiro é finito, toda cadeia ascendentes de submódulos de $\mathbb{Z}$ estaciona.

Proposição 2.3.4.1. *Um A-módulo M é noetheriano se, e somente se, todo submódulo de M é finitamente gerado. Em particular, todo módulo noetheriano é finitamente gerado.*

Demonstração. ($\Rightarrow$) Suponha M um módulo noetheriano e seja N um submódulo de M. Consideremos a família $\mathcal{F}$ de todos os submódulos fintamente gerados de N. Pelo Lema de Zorn, pode-se verificar que $\mathcal{F}$ tem um elemento maximal, digamos K. Se $K \neq N$, então $\exists x \in N \setminus K$. Pode-se considerar o A-submódulo $K + Ax$ que é fintamente gerado. Logo $K + Ax \in \mathcal{F}$, absurdo, pois contradiz a maximilidade de K, devido ao fato de $K \subsetneq K + Ax$. Portanto $K = N$ e N é finitamente gerado.

($\Leftarrow$) Seja $N_1 \subseteq N_2 \subseteq \cdots \subseteq N_k \subseteq \cdots$ uma cadeia estritamente crescente de submódulos de M. Tome $N = \cup_{i \geq 1} N_i$. Visto que, N é submódulo de M, então N é finitamente gerado, portanto, $N = Ax_1 + Ax_2 + \cdots + Ax_t$ com $x_1 \in N_i$ para $i = 1, \ldots, t$. Assim, existe um $j \in \mathbb{N}$ tal que $N_j = N_{j+1} = \cdots = N_{j+k} = \cdots$, logo M é noetheriano. □

Proposição 2.3.4.2. *Seja* $0 \longrightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \longrightarrow 0$ *uma sequência exata curta de A-módulos. Então M é noetheriano (respectivamente artiniano) se, e somente se,* M_1 *e* M_2 *são noetherianos (respectivamente artinianos).*

Demonstração. ($\Rightarrow$) Suponha M um A-módulo noetheriano e considere as cadeias $N_1 \subseteq N_2 \subseteq \cdots N_k \subseteq \cdots$ e $L_1 \subseteq L_2 \subseteq \cdots \subseteq L_k \subseteq \cdots$ de submódulos de M_1 e M_2, respectivamente. Dessa maneira, $f(N_1) \subseteq f(N_2) \subseteq \cdots \subseteq f(N_k) \subseteq \cdots$ e $g^{-1}(L_1) \subseteq g^{-1}(L_2) \subseteq \cdots \subseteq g^{-1}(L_k) \subseteq \cdots$ são cadeias crescentes dos submódulos de M. Obtemos, da noetherianidade de M, que existe um índice $n \in \mathbb{N}$ tal que $f(N_n) = f(N_{n+j})$ e $g^{-1}(L_n) = g^{-1}(L_{n+j}), \forall j \geq 1$.

Como f é injetora, temos $N_n = N_{n+j}, \forall j \geq 1$, da sobrejetividade de g, segue que $L_n = L_{n+j}, \forall j \geq 1$. Assim M_1 e M_2 são noetherianos.

($\Leftarrow$) Agora, suponha que M_1 e M_2 sejam noetherianos. Considere a cadeia $P_1 \subseteq P_2 \subseteq \cdots \subseteq P_k \subseteq \cdots$ de submódulos de M. Vamos induzir as seguintes cadeias:

$$f^{-1}(P_1) \subseteq f^{-1}(P_2) \subseteq \cdots \subseteq f^{-1}(P_k) \subseteq \cdots$$

e

$$g(P_1) \subseteq g(P_2) \subseteq \cdots g(P_k) \subseteq \cdots.$$

Da noetherianidade de M_1 e M_2, existem índices n_1 e n_2 tais que $f^{-1}(P_{n_1}) = f^{-1}(P_{n_1+j})$ e $g(P_{n_2}) = g(P_{n_2+j}), \forall j > 0$. Tomando $n = max\{n_1, n_2\}$. Concluímos $f^{-1}(P_n) = f^{-1}(P_{n+j})$ e $g(P_n) = g(P_{n+j}), \forall j > 0$.

Dado $j > 0$, pelo axioma da escolha, escolhemos um $x \in P_{n+j}$. Portanto, $g(x) \in g(P_n)$, ou seja, existe $y \in P_n$ tais que $g(x) = g(y)$, de maneira que $y - x \in Ker(g) = Im(f)$. Então existe $z \in f^{-1}(P_{n+j})$ tais que $f(z) = y - x$. Como $f^{-1}(P_n) = f^{-1}(P_{n+j})$, temos $f(z) = y - x \in P_n$, segue então que $x = y - f(z) \in P_n$, ou seja, $P_{n+j} = P_n$, para todo $j > 0$. Iso mostra que M é noetheriano. □

Observação 14. *A demonstração para o caso artiniano pode ser demonstrada de maneira completamente análoga.*

Dois resultados interessantse da proposição acima são os seguintes corolários.

Corolário 2.3.4.1. *Sejam A um anel, M um A-módulo e N um submódulo de M. Então M é noetheriano (respectivamente artiniano) se, e somente se, N e M/N são noetherianos (respectivamente artinianos).*

Corolário 2.3.4.2. *Sejam A um anel e $M_1, M_2, \ldots, M_r$ A-módulos noetherianos (respectivamente artinianos). Então $M = \bigoplus_{i=1}^{r} M_i$ é noetheriano (respectivamente artiniano).*

Definição 49. *Seja A um anel. Então dizemos que A é um:*

(i) Anel artiniano à esquerda se o módulo regular ${}_AA$ é artiniano.

(ii) Anel noetheriano à esquerda se o módulo regular ${}_AA$ é notheriano.

Observação 15. *Caso o módulo regular seja noetheriano (respectivamente artiniano) à direita e a esquerda, ao mesmo tempo, denominamos anel notheriano (respectivamente artiniano).*

Teorema 2.3.5. *(Teorema da base de Hilbert) Seja A um anel noetheriano. Então o anel de polinômios $A[x]$ também é noetheriano.*

Demonstração. Suponha, por absurdo, que $A[x]$ não seja noetheriano. Então existe um ideal $J \subseteq A[x]$ tal que J não é finitamente gerado. Agora, seja $f_1(x) \in J$ de menor grau possível e seja $f_2(x)$ de menor grau possível em $J \setminus \langle f_1 \rangle$. Da mesma forma, seja

$$f_n(x) \in J \setminus (f_1, f_2, \ldots f_{n-1})$$

de menor grau possível. Observe que as escolhas dos f_i sempre é possível devido ao Princípio da Boa Ordem e pelo fato de J não ser finitamente gerado. Para todo i inteiro positivo podemos definir $gr(f_i) = m_i \neq 0$ e o termo líder (associado a maior potência) de f_i por $a_i x^{m_i}$, vamos tomar a seguinte cadeia:

$$\langle a_1 \rangle \subseteq \langle a_1, a_2 \rangle \subseteq \langle a_1, a_2, a_2 \rangle \subseteq \cdots \subseteq \langle a_1, \ldots a \rangle \subseteq \cdots$$

Como A é noetheriano, existe $n \in \mathbb{N}$ tal que:

$$\langle a_1, \ldots, a_n \rangle = \langle a_1, \ldots, a_n, a_{n+1} \rangle = \cdots = \ldots$$

Portanto $a_{n+1} \in \langle a_1, a_2, \ldots, a_n \rangle$. Em outras palavras, $a_{n+1} = \sum_{i=1}^{n} \beta_i a_1$ em que $\beta_i \in A$. Considere

$$g(x) = f_{n+1} - \sum_{i=1}^{n} \beta_i x^{m_{n+1}-m_i} f_i(x),$$

Provaremos a seguir três fatos sobre $g(x)$.

(i) $g(x) \neq 0$;

(ii) $g(x) \notin \langle f_1, f_2, \ldots, f_n \rangle$;

(iii) $gr(g(x)) < gr(f_{n+1}(x))$;,

Com efeito, ao provar $(i), (ii)$ e (iii), recaíremos em uma contradição com a minimalidade do grau de $f(n)$

(i) Se $g(x) = 0$, então $f_{n+1}(x) \in \langle f_1, f_2, \ldots, f_n \rangle$. Daí segue que $g(x) \neq 0$. Contradição.

(ii) Suponha por contradição que $g(x) \in \langle f_1, f_2, \ldots, f_n \rangle$. Como $g(x) = f_{n+1} - \sum_{i=1}^{n} \beta_i x^{m_{n+1}-m_i} f_i(x)$, segue que:

$$f_{n+1} = g(x) - \sum_{i=1}^{n} \beta_i x^{m_{n+1}-m_i} f_i(x) \in \langle f_1, f_2, \ldots, f_n \rangle$$

o que é um absurdo. Logo $g(x) \notin (f_1, f_2, \ldots, f_n)$;

(iii) Basta analisarmos os graus dos f_i's o desenvolvimento do somatório e usaremos a hipotése de que $f_{n+1}(x) \in J \setminus \langle f_1, f_2, \ldots, f_n \rangle$ é de menor grau possível.

Assim, f_{n+1} não é de menor grau possível em $J \setminus (f_1, f_2, \ldots, f_n)$. Consequetemente $A[x]$ é noetheriano.

□

Exemplo 39. *Pelo Teorema da Base de Hilbert, temos que o anel* $\mathbb{Z}[x]$ *é um anel noetheriano, pois* $\mathbb{Z}$ *é noetheriano.*

Exemplo 40. *Sejam* p *um primo e* $\mathbb{Z}_{(p)} := \{\frac{a}{p^m} : a \in \mathbb{Z} \text{ e } m \geq 0\}$. *Então* $\mathbb{Z}_{(p)}$ *é um grupo abeliano aditivo e, assim, um* $\mathbb{Z}$*-módulo. Vamos considerar, agora,* $M = \mathbb{Z}_{(p)}/\mathbb{Z}$. *Afirmamos que* M *é artiniano e não é noetheriano.*

Para verificar que M *não é noetheriano, tome a cadeira estritamente crescente:*

$$\mathbb{Z} \subsetneq \tfrac{1}{p}\mathbb{Z} \subsetneq \tfrac{1}{p^2}\mathbb{Z} \subsetneq \cdots$$

Pode-se verififcar que $1/p^{i+1}$ *pertence a* $1/p^{i+1}\mathbb{Z}$, *mas* $1/p^{i+1}$ *não pertence a* $1/p^i\mathbb{Z}$, *isto mostra a inclusão estrita e o fato da cadeia não ser estacionária. A cadeia induzida no módulo quociente* $M = \mathbb{Z}_p/\mathbb{Z}$ *também não será estacionária.*

Para finalizar esse exemplo, é preciso mostrar a artinianidade de M. *Para tal, provaremos que todo submódulo próprio de* M *é finito. Observe que, caso* N *é um submódulo próprio de* M *e* $\frac{a}{p^m} + \mathbb{Z} \in M$, *com* $mdc(a, p) = 1$ *implica* $\frac{b}{p^n} + \mathbb{Z} \in N, \forall b \in \mathbb{Z}$ *e* $n \leq m$. *Realmente, pois existem* $r, s \in \mathbb{Z}$ *tais que* $ra + sp^m = 1$ *e:*

$$b = b1 = b(ra + sp^m) = bra + bsp^m, \forall b \in \mathbb{Z}$$

agora, vamos analisar se $n \neq m$, *temos:*

$$\tfrac{b}{p^n} = \tfrac{bra}{p^n} + \tfrac{bsp^m}{p^n} = (p^{m-n})\tfrac{bra}{p^m} + p^{m-n}bs$$

devido ao fato da última parcela estar em $\mathbb{Z}$ *podemos passar o quociente, resultando em:*

$$\tfrac{b}{p^n} + \mathbb{Z} = (p^{m-n})br(\tfrac{a}{p^m} + \mathbb{Z}) \in N.$$

Para finalizar, como N é um submódulo próprio de M, deve existir um número maximal natural t_N de forma que:

$$N := \{\tfrac{a}{p^m} + \mathbb{Z} : a \in \mathbb{Z}, m \leq t_N\}$$

Assim, devido a existência de finitas classes de equivalências da forma $\frac{a}{p^m} + \mathbb{Z}$, com $m \leq t_N$, resulta em N ser finito.

2.3.4 Semissimplicidade

Definição 50. *Sejam A um anel e M um $A-$módulo. Dizemos que M é um módulo:*

(i) Simples, se $M \neq 0$ e os únicos submódulos de M são os trivias, a saber, 0 e M;

(ii) Semissimples, se todo submódulos de M é um somando direto de M, isto é, se N é um submódulo de M, existe um submódulo P de M tal que $M = N \oplus P$.

Exemplo 41. *Os $\mathbb{Z}-$módulos simples são isomorfos a $\mathbb{Z}/p\mathbb{Z}$, sendo que p é um número primo.*

Exemplo 42. *Todo ideal minimal de um anel A é um módulo simples.*

Exemplo 43. *Sejam F um corpo (ou anel de divisão) e V um $F-$espaço vetorial. Consideremos $S = End_F(V)$ o anel das transformações lineares de V em V. Então V torna-se um S-módulo via ação:*

$$f \cdot v = f(v), \forall f \in S, v \in V.$$

É bem conhecido que V é um $S-$módulo simples.

Exemplo 44. *Todo módulo simples é semissimples. O módulo trivial $M = \{0\}$ é semissimples, mas não é simples.*

Exemplo 45. *Se F é um corpo, ou um anel de divisão, então todo F-espaço vetorial é um módulo semissimples.*

De fato, se W é subespaço de V, tomamos uma base de W. Após complementarmos a base de W até obter uma base para V. Deste modo, concluímos que W é somando direto de V.

Definição 51. *Sejam A um anel e M um A-módulo. Dizemos que M é indecomponível, se $M \neq 0$ e M não pode ser escrito como uma soma direta de quaisquer dois de seus submódulos não triviais, ou seja, se $M = N \oplus L$, então $N = 0$ ou $L = 0$.*

Observação 16. *Se F é um corpo, ou anel de divisão, então um F-espaço vetorial V é indecomponível se, e somente se, V é unidimensional.*

Observação 17. *Todo módulo simples é indecomponível. Mas nem todo módulo indecomponível é simples.*

Exemplo 46. *$\mathbb{Z}$, visto como um $\mathbb{Z}-$módulo, é indecomponível. Contudo é não simples, pois seus submódulos são da forma $n\mathbb{Z}$, para $n \in \mathbb{Z}$, mas se $m, n \in \mathbb{Z}$, então $n\mathbb{Z} \cap m\mathbb{Z} = mmc(m, n)\mathbb{Z}$.*

Exemplo 47. *$\mathbb{Z}$, visto como um $\mathbb{Z}$-módulo, não é semissimples.*

Lema 2.3.6. *Seja M um A-módulo semissimples. Então:*

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

(ii) Toda imagem homomórfica de M é um A-módulo semissimples. Isto é, se $\varphi : M \to N$ é um $A-$epimorfismo, então $\varphi(M) = N$ é semidssimples.

Demonstração. (i) Seja L um submódulo de M, vamos considerar N um submódulo de L, então N é um submódulo de M e temos que existe um submódulo K de N tal que $M = N \oplus K$. Assim, $L = M \cap L = (N \oplus K) \cap L = (N \cap L) + (K \cap L) = N + (K \cap L) = N \oplus (K \cap L)$.

(ii) Sejam $\varphi : M \to L$ um A-epimorfismo e N um submódulo de L. Então $\varphi^{-1}(N)$ é um submódulo de M e, consequentemente, $M = \varphi^{-1}(N) \oplus K$ para algum submódulo K de M. Logo, dado $y \in L$ existe $x \in M$ tal que $y = \varphi(x)$. Portanto, existem $x \in \varphi^{-1}(N)$ e $x_2 \in K$ tais que $x = x_1 + x_2$, de onde segue que $y = \varphi(x) = \varphi(x_1) + \varphi(x_2) \in N + \varphi(K)$, em outras palavras, $L = N + \varphi(K)$. Em contrapartida, se $z \in N \cap \varphi(K)$, então existe $a \in K$ tal que $z = \varphi(a)$. Mas como $a \in \varphi^{-1}(N) \cap K = 0$ temos $z = \varphi(a) = \varphi(0) = 0$, e segue que $L = N \oplus \varphi(K)$. Logo L é semissimples. □

Lema 2.3.7. *Todo módulo semissimples contém um submódulo simples.*

Demonstração. Sejam A um anel e M um $A-$módulo semissimples. Consideremos $m \in M$ e $m \neq 0$, Am é um submódulo de M. Vamos mostrar que Am contém um submódulo simples. Para isso, considere a família $\mathcal{F}$ de todos os submódulos de Am que não contém m. É não vazia, pois $0 \in \mathcal{F}$. Pelo Lema de Zorn é possível verificar que existe

um elemento maximal em $\mathcal{F}$, o qual chamaremos de N. Pelo Lema 2.3.6, $Am = N \oplus N'$. Mostraremos que N' é um módulo simples. Note que $N' \neq \{0\}$, devido ao fato de $m = n + n'$, com $n \in N$ e $n' \in N'$ como $m \notin N$, implica $n' \neq 0$. Além disso, se $0 \neq N"$ é um submódulo de N', temos $N' = N" \oplus P$, para algum submódulo de P de N'. Pela maximalidade de N, devemos ter $m \in N \oplus N"$, de modo que $N \oplus N" = Am$, portanto:

$$N \oplus N" = Am = N \oplus N' = N \oplus (N" \oplus P).$$

Concluímos assim que $P = \{0\}$ e $N" = N'$. Logo N' é simples. □

Teorema 2.3.8. *Sejam A um anel e M um A-módulo. As seguintes afirmações são equivalentes:*

(i) M é semissimples;

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

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

Demonstração. Se considerarmos $M = \{0\}$, não há nada para mostrarmos. Para a demonstração, vamos assumir $M \neq \{0\}$.

(i) $\Rightarrow$ (ii) Inicialmente, vamos tomar $N = \sum_{i \in I} S_i$, em que $\{S_i\}_{i \in I}$ é a família de todos os A-módulos simples de M que não é vazia. Assim existe um submódulo P de M de maneira que $M = N \oplus P$. Caso $P \neq \{0\}$ pelo Lema 2.3.7, existe um submódulo simples T de P. Mas, como P deve ser semissimples, pelo fato de ser um submódulo de um módulo semissimples. Logo $P \cap N \neq \{0\}$, absurdo. Assim, só podemos ter $P = \{0\}$. Como consequência $M = N$.

$(ii) \Rightarrow (iii)$ Suponha $M = \sum_{i\in I} S_i$, em que $\{S_i\}$ é uma família de submódulos simples de S. Considere a família $\mathcal{F} := \{J \subseteq I : \sum_{j\in J} M_j\}$ tal que $\sum_{j\in I} M_j$ é um soma direta cujos elementos são somas diretas. Vamos assumir que $\mathcal{F} \neq \{0\}$. Como toda cadeia de $\mathcal{F}$ possui uma cota superior, pelo Lema de Zorn (2.1.1) existe $I' \subset J$. Agora, seja $M' = \oplus_{j\in I'} M_j$ temos $M' = M$, pois para cada $i \in I, M_i$ é um módulo simples e $M_i \cap M' = M_i$ ou $M_i \cap M' = 0$. Caso $M_i \cap M' = \{0\}$ ocorra, então $I' \cup \{i\} \supsetneq I'$, o que é um absurdo, pois contradiz a maximilidade de I'. Assim, $M_i \cap M' = M_i$ para todo $i \in I$.

$(iii) \Rightarrow (i)$ Suponha que M seja uma soma direta de submódulos simples: $M = \oplus_{i\in I} M_i$, em que M_i é um módulo simples, para todo $i \in I$. Agora, seja N um submódulo de M. Pela argumentação realizada anteriormente, temos: $N \cap M = M_i$ ou $N \cap M_i = 0$, note que $N = \oplus_{j\in J} M_j$, sendo que $J = \{I \in I : M_i \cap N = M_i\}$. Portanto $M = (\oplus_{j\in J} M_j) \oplus (\oplus_{j\in I\setminus J} M_j) = N \oplus K$, com $K = \oplus_{j\in I\setminus J} M_j$. Assim, M é semissimples, pois N foi tomado arbitrariamente, determinamos um submódulo K tal que $M = N \oplus K$. □

2.4 CAPÍTULO 4: TEOREMA DE WEDDERBURN-ARTIN

Neste capítulo, abordaremos o Teorema de Wedderburn-Artin, um dos resultados centrais no estudo de anéis semissimples. Este teorema fornece uma caracterização dos anéis semissimples como sendo uma soma direta de anéis de matrizes sobre corpos, o que desempenha um papel fundamental na álgebra moderna. A compreensão deste teorema não só ilumina a estrutura dos anéis, mas também tem implicações profundas em áreas como teoria de representações e álgebra linear. Para fundamentar nossa análise, utilizamos como principal referência a obra "Uma Introdução ao Estudo de Anéis Semissimples", que oferece uma base sólida e detalhada sobre o tema.

Teorema 2.4.1. *Seja A um anel. Então as seguintes afirmações são equivalentes:*

(i) O módulo regular A_A é semissimples;

(ii) Todos os A-módulos à esquerda são semissimples;

(iii) Todos os A-módulos à esquerda finitamente gerados são semissimples.

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

Demonstração. Vamos demostrar as afirmações $(i) \Rightarrow (ii)$, uma vez que a implicações $(ii) \Rightarrow (iii) \Rightarrow (iv)$ são de verificação imediata.

Para a demonstração, vamos supor que o módulo regular A_A seja semissimples e seja M um A-módulo. Como $M = \sum_{m \in M} Am$, basta verificarmos que Am é semissimples, para todo $m \in M$. Realmente, se $A_A = \oplus_{i=1}^{K} I_i$, onde I_i é um ideal à esquerda minimal de A, então temos:

$$Am = (I_1 \oplus I_2 \oplus I_3 \oplus \cdots \oplus I_k)m = I_1m + I_2m + \ldots I_km.$$

Precismos mostrar que cada um dos módulos I_im é uma A-submódulo simples de Am. Para isso, vamos fixar um $i \in \{1, 2, 3, \ldots k\}$ e considere L um A-submódulo de I_im. Caso $L \neq 0$, existe $0 \neq x \in L$ de forma que obtemos $x = a_im$, para algum $a_i \in I$. Assim $(L : m)_i = \{a \in I_i : am \in L\}$ é um submódulo de I, com isto $(L : m)_i = I_i$, uma vez que $0 \neq a_i \in (L : m)_i$ e I_i é simples. Logo $L = I_m$ e I_im é simples. □

Observação 18. *Para prosseguirmos na classificação de anéis semissimples, vamos introduzir uma nova notação. Seja A um anel semissimples e I um ideial à esquerda minimal de A, denotaremos A_I como o seguinte conjunto:*

$$A_I := \sum\{J \lhd_l R : J \simeq I\}.$$

Lema 2.4.2. *Com as notações acima, valem as seguintes afirmações:*

(i) A_I é um ideal (bilateral) de A

(ii) Se I e J são ideais à esquerda minimais de A tais que $I \ncong J$, então $A_I A_J = 0$.

Demonstração. $(i) \Rightarrow$ Basta mostrar que A_I absorve a multiplicação à direta. Para isso, mostraremos que $J \lhd_l A$ é tal que $J \simeq I \Rightarrow Ja \subseteq A_I, \forall a \in A$. Agora, dado $a \in A$, consideremos a aplicação:

$$f_a : J \to R \text{ definida por } f_a(x) = xa, \text{ para cada } x \in J.$$

Desse modo, f_a é um A-homomorfismo, pois se $b \in A, x \in J$, logo $f_a(bx) = (bx)a = b(xa) = bf_a(x)$. Então $Ker(f_a) = \{0\}$ ou $Ker(f_a) = J$, dado que J é um ideal minimal à esquerda de A

Do primero caso, temos $Ja = Im(f_a) \simeq J \simeq I$ e no segundo, temos $Ja = 0$. Portanto, nos dois casos, devemos ter $Ja \subseteq A_I$.

$(ii) \Rightarrow$ Sejam I, J ideias minimais à esquerda de A, de modo que $I \ncong J$. Temos que provar que $A_I A_J = 0$. Para isso, temos que verificar se L e K são submódulos à esquerda de A, tais que $L \cong I$ e $K \cong J$, então $LK = \{0\}$. Devido ao fato de todo elemento $x \in A_I$ ser da forma $x = \sum_{i=1}^{n} b_i$ com $b_i \in L \simeq I_i, (1 \leq i \leq n)$ e todo elemento $y \in A_J$ é da forma $y = \sum_{j=1}^{m} c_j$, com $c_j \in K_j \simeq J (1 \leq j \leq m)$. Note que, se $L \simeq I$ e $y \in K \simeq J$ implica $Ly = 0$, caso contrário, teríamos $Ly = K$, devido à minimalidade de K, Então, teríamos:

$$I \simeq L \simeq Ly = K \simeq J$$

o que é um absurdo, logo só podemos ter $A_I A_J = 0$. A prova está concluída. □

Observação 19. *Se A um anel semissimples, então o módulo regular A_A é semissimples e pode ser escrito como:*

$$_AA = I_{11} \oplus \ldots \oplus I_{In_1} \oplus \ldots \oplus I_{r1} \oplus \ldots \oplus I_{rn_r}$$

$$A_{I_k} = \sum\{J \lhd_l R : J \simeq I_k\}, \text{ em que } J \text{ é minimal.}$$

Definição 52. *Dizemos que os ideais A_{I_l} na representação descrita são chamados componentes homogêneas.*

Definição 53. *Seja A um anel com unidade 1. Um elemento $a \in A$ é idempotente quando $a^2 = a$. Dois elementos idempotentes b e c são ditos ortogonais quando $b \cdot c = c \cdot b = 0$.*

Exemplo 48. *A matriz* $\begin{pmatrix} 2 & -1 & 1 \\ -3 & 4 & -3 \\ -5 & 5 & -4 \end{pmatrix}$ *é um elemento idempotente de $M_3(\mathbb{R})$.*

Exemplo 49. *As matrizes* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *são idempotente ortogonais de $M_2(\mathbb{R})$.*

Observação 20. *Para prosseguirmos, note que se* $A = I_1 \oplus I_2 \oplus \cdots \oplus I_n$, *com* $I_j \lhd A, 1 \leq j \leq n$ *e* $J \lhd A$, $J = J_1 \oplus J_2 \oplus \cdots \oplus J_n$, *em que* $J_k \lhd I_k (1 \leq k \leq n)$. *Isso é válido, pois estamos assumindo que* A *tem unidade. Então obtemos* $1_A = e_1 + e_2 + e_3 + \cdots + e_n$, *com* $e_i \in I_i, (1 \leq i \leq n)$. *Portanto,* $1 = 1^2 = \sum_{ij} e_i e_j = \sum_{i=1}^{n} e_i^2, (1 \leq i \leq n)$ *e* $(1 \leq j \leq n)$, *devido ao fato de* $e_i e_j \in I_i I_j \subseteq I_i \cap I_j = 0$ *para* $i \neq j$. *Da unicidade da escrita em uma soma direta, temos que* $e_i^2 = e_i$, *em outras palavras,* $\{e_i\}_{i=1}^{n}$ *é uma família de elementos idempotentes ortogonais de* A. *Indo além, como* $a = 1a = a1$ *os elemntos comutam com todos elementos de* A. *Portanto* $J = AJ = (I_1 \oplus I_2 \oplus \cdots \oplus I_n)J = J_{e_1} \oplus J_{e_2} \oplus \cdots \oplus J_{e_n}$, *onde* $J_{e_i} \lhd A_{e_i} = I_i$ *para* $(1 \leq i \leq n)$.

Lema 2.4.3. *Sejam* A *um anel e* $I_1, I_2, \ldots, I_r$ *e* $J_1, J_2, \ldots, J_s$ *ideias bilaterais indecomponíveis de* A *isto é, todos estes ideais não podem ser expressos como a soma direta de outros ideais diferentes do ideal* $\{0\}$ *tais que* $A = I_1 \oplus I_2 \oplus \cdots I_r = J_1 \oplus J_2 \oplus \cdots \oplus J_s$. *Então,* $r = s$ *e, após uma permutação nos índices, se necessário,* $I_i = J_i, 1 \leq i \leq r$.

Demonstração. Suponha $A = I_1 \oplus I_2 \oplus \cdots I_r = J_1 \oplus J_2 \oplus \cdots \oplus J_s$, assim obtemos que $J_1 \lhd A$, pela argumentação realizada acima, temos que $J_1 = I_1' \oplus \cdots I_r'$, com $I_i' \lhd I_i, 1 \leq i \leq r$. Contudo, J_1 é indecomponível como ideal, assim existe $k \in \{1, 2, \ldots, r\}$ tal que $J_1 = I_k'$. Realizando as permutações nos índices, se necessário, é possível escrever $J_1 = I_1'$. Logo, temos $J_1 \subseteq I_1$. Se argumentarmos de forma similar, mas trocando I_1 de lugar com J_1, provaremos a outra inclusão, ou seja, $J_1 = I_1$. Repetindo sucessivamente, demostramos o lema.

□

Lema 2.4.4. *Seja* A *um anel semissimples. Então* $A = A_1 \oplus A_2 \oplus \cdots \oplus A_r$, *em que cada* $A_i, 1 \leq i \leq r$, *é um anel simples com unidade, que possui um único idela minimal à esquerda, a menos de isomorfismo.*

Demonstração. Como A é semissimples, podemos escrever A como:

$$A = A_1 \oplus A_2 \oplus \cdots \oplus A_r$$

em que cada $A_i, 1 \leq i \leq r$ é um ideal bilateral, e portanto, subanel de A que contém um único ideal minimal à esquerda, a menos de isomorfismo. Pela argumentação anterior, se $1_A = e_1 + e_2 + \cdots + e_r$, temos $e_1^2 = e_i, A_i = e_iA = Ae_i$ e A_i é um anel com unidade $e_1 (1 \leq i \leq r)$.

Para demonstrarmos por completo o lema, é necessário mostrar que os anéis A_i são simples, para cada $i \in \{1, 2, 3, \ldots, r\}$. De fato, pois se fixarmos $i \in \{1, 2, 3, \ldots, r\}$ e tomando $0 \neq I \lhd A_i$ temos que I é um ideal de A. Mas como todo ideal de A é também um ideal à esquerda, concluímos que I é um submódulo de ${}_AA$, em outras palavras, I é um módulo simples. Para obter esta conclusão usamos o fato que todo módulo de um anel semissimples é semissimples. Portanto I possui um ideal minimal à esquerda, digamos I_0. Segundo a linha de raciocínio da prova do Lema 2.4.3 temos $I_0 = Ae$, para um certo idempotente $e \in A$. Agora, consideremos a componente homogênea de A correspondente a este ideal minimal de I_0, sendo assim $A_{I_0} = A_j$ para $j \in \{1, 2, 3, \ldots, j\}$. Pela construção dos $A_j's$, só vale $A_{I_0} = A_j$. Caso contrário, se $J \lhd_l A$ for um ideal à esquerda minimal de A tal que $J \subseteq A_i$, portanto existe um isomorfismo $\varphi : I_0 \to J$, daí:

$$J \cong \varphi(I_0) = \varphi(Ae) = \varphi(Aee) = \varphi(I_0e) = I_0\varphi(e) \subseteq I$$

De onde, obtemos que $I = A_i$, ou seja, A_i é um anel simples. □

Lema 2.4.5. *(Lema de Schur) Sejam A um anel e M um $A-$módulo simples. Então, $End_{(A)}(M)$ é um anel de divisão.*

Demonstração. Seja um f endomorfismo de M:

$$f : M \to M$$

Deste modo, $Ker(f)$ e $Im(f)$ são submódulos de M. Como M é um módulo simples, temos que $Ker(f) = \{0\}$ e $Im(f) = M$ ou $Ker(f) = M$ e $Im(f) = \{0\}$. No primeiro caso, f é um isomorfismo. No segundo caso, um homomorfismo nulo. Assim, $End_A(M)$ é um anel de divisão. □

Proposição 2.4.5.1. *(Proposição de Rieffel) Seja A um anel simples. Suponhamos que A contenha um ideal à esquerda não nulo I e seja $D = End_{(A)}(I)$. Então, $A \cong End_{(A)}(I_D)$ como anéis.*

Demonstração. Seja φ a aplicação:

$$\begin{gathered} \varphi : A \to End_A(I_D) \\ r \mapsto \varphi_r : I \to I \\ a \mapsto ra \end{gathered}$$

φ é um homomorfismo, pois se $r, s \in A$ e $a \in I$, temos:

$$\varphi(r+s)(a) = \varphi_{r+s}(a) = (r+s)a = ra + sa = \varphi_r(a) + \varphi_r(a) = (\varphi(r) + \varphi(s))(a)$$

e

$$\varphi(rs)(a) = \varphi_{(rs)}(a) = (rs)a = r(sa) = \varphi_r(sa) = \varphi_r(\varphi_s(a)) = (\varphi(r) \circ \varphi(s))(a),$$

Além disso, como A é um anel simples: $Ker(\varphi) = \{0\}$ ou $Ker(\varphi) = A$. Visto que $\varphi(1_A) = id_I \in End_A(I_D)$, só podemos ter $Ker(\varphi) = \{0\}$ e φ é injetora. Para verficarmos a sobrejetividade de φ vamos mostrar, primeiro, que $\varphi(I)$ é um ideal à esquerda de $End_A(I_D)$.

A princípio, observe que se $a \in I$, existe um homomorfismo definido por: $g_a : I \to I, g_a(x) = xa, \forall x \in I$. De fato, é um homomorfismo, pois:

$x, y \in I$ e $r \in A$ então $g_a(x+y) = (x+y)a = xa + ya = g_a(x) + g_a(y)$

e

$$g_a(rx) = (rx)a = r(xa) = rg_a(x)$$

Logo $g_a \in D$. Tomando $a, b \in I$ e $h \in End_A(I_D)$, temos

$$h \cdot (\varphi_a(b)) = h(ab) = h(a)b = \varphi_{h(a)}(b).$$

Em outras palavras, $h \circ \varphi_a = \varphi_{h(a)} \in End_A(I_D)$, para todos $a \in I, h \in End_A(I_D)$. Segue que $End_A(I_D)\varphi(I) \subseteq \varphi(I)$, ou seja, $\varphi(I) \lhd_l End_A(I_D)$.

Agora, pelo fato de A ser simples e $I \neq 0$ concluímos que $IA = A$, devido ao fato de $IA \lhd A$. Assim, $\varphi(A) = \varphi(IA) = \varphi(I)\varphi(A)$. Sendo assim:

$$End_A(I_D)\varphi(A) = End_A(I_D)\varphi(I)\varphi(A) \subseteq \varphi(I)\varphi(A) = \varphi(A).$$

Em síntese, $\varphi(A)$ é um ideal à esquerda de $End_{(A)}(I_D)$. Para completarmos a demonstração, note que $1_{End_A(I_D)} = id_I = \varphi(1_A) \in \varphi(A)$, dai concluímos que $\varphi(A) = End_A(I_D)$. Isto é, φ é sobrejetora. □

Corolário 2.4.5.1. *Seja A um anel simples que contém um ideal à esquerda minimal. Então $R \cong \mathcal{M}_n(D)$, para algum $n \geq 1$ e D um anel de divisão.*

Demonstração. Tome I um ideal minimal à esquerda de A. Pelo Lema 2.4.5 (Lema de Schur), temos que $D = End({}_AI)$ é um anel de divisão. Logo I possui uma estrutura de $(A, D)-$ bimódulo, isto é, é um $A-$módulo à esquerda e um $D-$módulo a direita. Além disso, $(ai)d =$

$a(id)$, para todos $a \in A, i \in I$ e $d \in D$. Pela Proposição 2.4.5.1, temos que $End_A(I_D)$ é um anel simples, pois $A \cong End_A(I_D)$ como anéis.

Agora, afirmamos que $dim_D I < \infty$. Com efeito, se $dim_D I = \infty, K = \{f \in End_A(I_D) : dim_D Im(f) < \infty\}$ seria um ideal próprio de $End_A(I_D)$, o que é um absurdo, devido ao fato de contradizer a simplicidade do anel $End_A(I_D)$. Assim, só podemos ter $dim_D I = n$, com $n \in \mathbb{N}$. Nesse caso, $End_A(I_D)$ é o anel das transformações lineares de I em I, em outras palavras, $End_A(I_D) \cong \mathcal{M}_n(D)$. □

Definição 54. *Seja A um anel e seja I um ideal à esquerda de A. O anulador de I, o qual denotamos por $An_A(I)$, é o seguinte subconjunto de A:*

$$An_A(I) = \{a \in A \mid ai = 0, \forall i \in I\}.$$

Dizemos que I é fiel quando $An_A(I) = \{0\}$.

Lema 2.4.6. *Seja A um anel simples que possui um ideal à esquerda minimal I. Então A possui, a menos de isomorfismo, um único módulo simples e fiel isomorfo a I. Além disso, nestas condições $A \cong I^{(n)}$, em que $I^{(n)}$ significa a soma direta de n cópias de I.*

Demonstração. Como A é simples, $An_A(I) \lhd A$ (ideal bilateral) e A tem unidade, então $An_A(I) = \{0\}$, ou seja, I é um A-módulo simples e fiel. Agora, seja M um A-módulo simples e fiel qualquer, como $An_A(M) = 0$. Existe $m \in M$ tal que $Im \neq \{0\}$ o que implica $Im = M$, pela simplicidade de M. Considere o epimorfismo:

$$\varphi : I \to M \text{ definido por } \varphi(x) = xm.$$

Como $Ker(\varphi) \lhd_l I$, então $Ker(\varphi) = 0$ e φ é um isomorfismo, ou seja, $M \cong I$. Assim, a menos de isomorfismo, A possui um único módulo simples e fiel.

Para finalizar, se $R \cong \mathcal{M}_n(D)$, em que $End_A(I_D), n = dim_D I$. Logo $R \cong \mathcal{M}_n(D) \cong I^{(n)}$, onde $I = \{(a_{ij}) \in \mathcal{M}_n(D) : a_{ij} = 0, j \neq 1\}$ □

Exemplo 50. *$M_2(\mathbb{R})$ é um anel simples $I_1 = \left\{ \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \middle| a, c \in \mathbb{R} \right\}$ e $I_2 = \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \middle| b, d \in \mathbb{R} \right\}$ são ideais à esquerda minimais. O homomorfismo:*

$$\begin{gathered} \varphi : I_1 \to I_2 \\ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \end{gathered}$$

é um isomorfismo. Por fim, note que $M_2(F) = I_1 \oplus I_2 \cong I_1 \times J_1$.

Teorema 2.4.7. *(Teorema de Wedderburn-Artin) Seja A um anel semissimples. Então*

$$A \cong \mathcal{M}_{n_1}(D_1) \times \mathcal{M}_{n_2}(D_2) \times \cdots \times \mathcal{M}_{n_t}(D_t)$$

onde $D_1, D_2, \ldots D_t$ são anéis de divisão e $n_1, n_2, \ldots, n_t$ são inteiros positivos. O número t e os pares ordenados (D_i, n_i) são unicamente determinados a menos de permutações. Além disso, existem exatamente t A-módulos simples e fiéis, dois a dois não isomorfos.

Demonstração. Suponha A um anel semissimples, de modo que $A \cong \mathcal{M}_{n_1}(D_1) \times \mathcal{M}_{n_2}(D_2) \times \cdots \times \mathcal{M}_{n_t}(D_t)$ e $A \cong \mathcal{M}_{l_1}(D_1)' \times \mathcal{M}_{l_2}(D_2)' \times \cdots \times \mathcal{M}_{l_s}(D_s)'$, em que D_i, D_l' são anéis de divisão com $1 \leq i \leq t, 1 \leq l \leq s$. Agora, seja V_i o único módulo simples e fiel sobre $A_i = \mathcal{M}_{n_j}(D_i)$, logo V_i se torna um A-módulo, definindo-se $A_i \cdot V_j = \{0\}$, caso $i \neq j$, assim V_i é um A-módulo simples.

Mas ainda, se $i \neq j$, então $V_i \ncong V_j$. Realmente, pois se $\beta : V_i \to V_j$ é um A-isomorfismo, então, para todo $a \in A$, temos $\phi(av) = a\phi(v), \forall v \in V_i$, contudo tomando $b = (0, \ldots, 1_{A_j}, 0, \ldots, 0) \in A$ obtemos $b\phi(v) = \phi(bv) = \phi(0) = 0$, ou seja, $b \in An_A(V_j)$, uma vez que $v \in V_i$ foi tomado de maneira abitrária e $\phi(V_i) = V_j$. Então $V_i \ncong V_j$.

Para concluir, basta repertimos o mesmo argumento para a outra decomposição de A.

$$V_1^{(n_1)} \oplus \cdots \oplus V_t^{(n_t)} \cong_A A \cong V_1'^{(l_1)} \oplus \cdots \oplus V_s'^{(l_s)}.$$

Concluindo, pelo Teorema 2.3.3 (Teorema de Jordan-Hölder), segue que $s = t, n_i = l_i$ e ${}_AV_i \cong_A V_i', 1 \leq i \leq t$. Agora, bastar observar que:

$$D_i' \cong End_{A_i'}(V_i') \cong End_A(V_i') \cong End_A(V_i) \cong End_{A_i}(V_i) \cong D_i.$$

Com isso, a demostração está finalizada, note que foi preciso mostrar apenas a unicidade, uma vez que a existência foi resultada do Lema 2.4.4 e do Corolário 2.4.5.1. □

Uma consequência imediata do Teorema de Wedderburn-Artin é que um anel é semissimples à esquerda se, e somente se, é semissimples à direita.

Corolário 2.4.7.1. *Um anel artiniano é simples se, e somente se, é isomorfo a um anel de matrizes sobre um anel de divisão.*

Demonstração. Seja A um anel artiniano e simples. Como A tem unidade, então todo ideal à esquerda é um A-módulo fiel. Esta conclusão vem do Lema 2.4.6. Pela artinianidade de A, todo A-módulo à esquerda possui um A-submódulo simples. Assim, ou A é um anel de

divisão ou A é um anel simples que possui um ideal à esquerda minimal. Portanto, $R \cong \mathcal{M}_n(D)$, para algum $n \geq 1$ e D um anel de divisão. A recíproca é obvia. □

Exemplo 51. *Se n é livre de quadrados, então $\mathbb{Z}/_n\mathbb{Z}$ é semissimples*

De fato, se $n = p_1 p_2 \dots p_k$, com p_i e p_j primos distintos, temos:

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{k} /p_i\mathbb{Z}$$

e cada uma dos anéis $\mathbb{Z}/p_i\mathbb{Z}$ é um corpo, logo um anel simples e artiniano.

Exemplo 52. *Sejam $A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n \subseteq \cdots$ uma cadeia de anéis simples com a mesma unidade e consideremos $A = \cup A_i$. Então A é simples.*

De fato, pois se I é um ideal de $A, I = \{0\}$, então $I \cap A_j$ é um ideal não nulo de A_j, para algum $j \geq 1$. Pórem como A_j é simples temos que $I \cap A_j = A_j$ e $1_A = 1_{A_j} \in I \cap A_j \subseteq I$, logo $I = A$.

Observação 21. *Considere $A_i = M_{2^i}(D)$, sendo D um anel de divisão. O anel A_i é simples e pode ser "mergulhado"em $M_{2^{i+1}}(D)$ via o homomorfismo $\varphi M_{2^i}(D) \to M_{2^{i+1}}(D)$ tal que $f(m) = \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}$. O anel $A = \prod_{i=0}^{\infty} M_{2^i}$ é simples, entretanto não é semissimples.*

2.5 CAPÍTULO 5: ANÉIS DE GRUPO

Sejam G um grupo e X um conjunto. Dizemos que G age em X se existir uma aplicação

$$\begin{aligned} \alpha : G \times X &\to X \\ (g, y) &\mapsto g \cdot x \end{aligned}$$

satisfazendo as seguintes condições:

(i) $1_G \cdot x = x, \forall x \in X$

(ii) $g \cdot (h \cdot x) = gh \cdot x, \forall g, h \in G, x \in X$

Exemplo 53. *Sejam G um grupo e X um conjunto, então a ação trivial de G em X é definida por $g \cdot x = x, \forall x \in X$.*

Exemplo 54. *Sejam F um corpo e V um espaço vetorial. Então a ação F sobre V determina uma ação do grupo multiplicação $F^{\times} := F \setminus \{0\}$ no conjunto V.*

Observação 22. *Em nosso estudo, o que de fato nos interessa são as chamadas representações lineares de um grupo.*

Definição 55. *Seja G um grupo finito, F um corpo e V um espaço vetorial de dimensão n. Chamamos de representação linear de G em V a todo homomorfismo:*

$$\psi : G \to GL_{(n)}(V).$$

Em que $GL_{(n)}(V)$ denota o grupo das transformações lineares sobrejetivas de V em V. A dimensão de V sobre F é denominada grau desta representação.

Observação 23. *As representações lineares de um grupo finito G em um K-espaço vetorial de dimensão n originam as chamadas ações lineares de G em V.*

Definição 56. *Dizemos que ação G em V é linear se ρ_g é um transformção linear, para cada $g \in G$. Em outras palavras, a ação de G em V é linear, se:*

(i) $1_G \cdot v = v, \forall v \in V$;

(ii) $g \cdot (h \cdot v) = gh \cdot v, \forall g, h \in G, \forall v \in V$;

(iii) $g \cdot (\lambda u + \beta v) = \lambda(g \cdot u) + \beta(g \cdot v), \forall g \in G, \forall \lambda, \beta \in F, \forall u, v \in V$.

Para continuarmos nossos estudos, precisamos introduzir o conceito de um G-módulo. Para isso, consideramos o anel de grupo de G sobre K.

Definição 57. *Dados um grupo G, tal que $G = \{g_1, g_2, \dots g_n\}$, e um corpo F, definimos o anel de grupos de G sobre F como sendo o F-espaço vetorial com base $\{g_1, g_2, g_3, \dots g_n\}$, ou seja:*

$$F[G] := \{\textstyle\sum_{i=1}^{n} \lambda_i g_i \mid \lambda_i \in F, g \in G\},$$

com a soma usual de vetores e com a multiplicação induzida por

$$(\lambda_i g_i)(\lambda_j g_j) = (\lambda_i \lambda_j g_i g_j)$$

e estendida por linearidade.

Observação 24. *É fácil ver que $F[G]$ é um anel com unidade $1_F 1_G$. Além disso, a aplicação $\varphi : G \to F[G]$, dada por $\varphi(x) = 1_F x$ é um imersão de G em $F[G]$, $\theta : F \to F[G]$, dada por $\theta(a) = a1_G$ é uma imersão de F em $F[G]$*

Proposição 2.5.0.1. *Sejam G um grupo, F um corpo e V um espaço vetorial sobre F. Então G age linearmente em V se, e somente se, Vé um $F[G]$-módulo.*

Demonstração. Suponha que G age linearmente em V via ρ. Assim, definimos uma ação $F[G]$ em V: para $x = \sum \lambda_i g_i \in F[G]$ e $v \in V$, tomamos $x \cdot v := \sum \lambda_i (g_i \cdot v)$. Assim V se torna um $F[G]$-módulo. Pela linearidade de ρ_g, as propriedades aditivas seguem facilmente para cada $g \in G$. Além disso, dados $x = \sum \lambda_i g_i$ e $y = \sum \beta_j h_j, \in F[G], v \in V$, temos $x \cdot (y \cdot v) = \sum_i \lambda_i g_i \cdot (\sum_j \beta_j h_j \cdot v) = (xy \cdot v)$. De maneira recíproca, se V é um $F[G]-$módulo, logo definimos $\rho : G \times V \to V$, por $\rho_g(v) = (1_{F[G]} g) \cdot v$. Por raciocínios algébricos usuais, verificamos que a aplicação ρ uma ação linear de G em V. □

Definição 58. *Seja G um grupo finito que age linearmente em um F-espaço vetorial V. Então dizemos que a representação associada a esta ação linear é:*

(i) irredutível, se V é um $F[G]$-módulo simples,

(ii) semissimples, se V é um $F[G]$-módulo semissimples,

(iii) regular, se $V = F[G]$ e a ação de G é induzida pela multiplicação de G.

Exemplo 55. *Sejam $G = \{e, g, g^2\}$ o grupo cíclico de ordem 3, $F = \mathbb{C}$ e ρ a representação regular de G em $\mathbb{C}$.Portanto, as transformações lineares ρ_g possuem as matrizes na base $\mathcal{B} = \{e, g, g^2\}$, dadas por:*

$$[\rho_e]_{\mathcal{B}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, [\rho_g]_{\mathcal{B}} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}. [\rho_{g^2}]_{\mathcal{B}} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

2.5.1 Teorema de Maschke

Neste capítulo, exploraremos o Teorema de Maschke, um resultado fundamental na teoria de representações de grupos. O teorema afirma que, para um grupo finito G e um corpo K cuja característica não divide a ordem de G, toda representação de G é completamente redutível. Esse resultado garante que qualquer módulo de representação pode ser decomposto em uma soma direta de submódulos simples, facilitando o estudo das representações de grupos finitos. A nossa análise será apoiada pela obra *"Uma Introdução ao Estudo de Anéis Semissimples"*, que nos fornece uma base teórica abrangente para entender este teorema e suas aplicações.

Teorema 2.5.1. *(Teorema de Maschke) Sejam G um grupo finito, F um corpo de caracterísica zero ou tal que $car(F)$ não divide $|G|$. Então, $F[G]$ é uma anel semissimples.*

Demonstração. Tome $n =\mid G \mid$ e considere V um $F[G]$-módulo. Agora, para mostrarmos que $F[G]$ é semissimples é necessário provar que $F[G] = V \oplus W$ para um certo $F[G]$-submódulo W. Mas, como todo $F[G]$-módulo tem uma estrutra de espaço vetorial, podemos escrever $F[G] = V \oplus U$, sendo que U é um F-espaço vetorial. Agora considere a projeção linear: $\pi : F[G] \to V$ com núcleo U, isto é, se $w = u + v$,

sendo que $u \in U, v \in V$, então $\pi(u+v) = u$. É um aplicação F-linear, embora não necessariamente seja $F[G]$-linear. Para obter a decomposição que desejamos, vamos definir $\pi^* : F[G] \to F[G]$ por

$$\pi^*(x) = \frac{1}{n} \sum_{g \in G} g^{-1}\pi(gx).$$

Mostraremos que $\pi^*(F[G]) = V$ e que $F[G] = V \oplus (id - \pi^*)(F[G])$, com $F[G]$-módulos. Para isso, considere $y \in F[G]$ e $g \in G$, então $\pi(gy) \in V$, e deduzimos que:

$$\pi^*(gy) = \frac{1}{n} \sum_{h \in G} h^{-1}\pi(hgy) \in V.$$

Ademais, caso $x \in V$, temos:

$$\pi^*(x) = \frac{1}{n} \sum_{g \in G} g^{-1}\pi(gx) = \frac{1}{n} \sum_{g \in G} g^{-1}gx = \frac{1}{n}nx = x$$

ou seja, $Im(\pi^*) = V$. Mais ainda, $(\pi^*)^2 = \pi^*$. Logo π^* é uma projeção e segue que

$$F[G] = \pi^*(F[G]) \oplus (id - \pi^*)(F[G]) = V \oplus (id - \pi^*)(F[G]).$$

Para finalizar, basta mostrar que o F-espaço vetorial $W = (id - \pi^*)(F[G])$ é um $F[G]$-submódulo, em outras palavras, π^* deve ser um $F[G]$-homomorfismo. Consideramos $h \in G, x \in F[G]$. Então temos

$$h^{-1}\pi^*(hx) = \frac{1}{n} \sum_{g \in G} h^{-1}g^{-1}\pi(ghx) = \frac{1}{n} \sum_{y \in G} y^{-1}\pi(yx) = \pi^*(x).$$

Deste modo $\pi^*(hx) = h\pi^*(x), \forall h \in G, x \in K[G]$. Assim, tomando um elemento arbitrário de W, da forma $(id - \pi^*)(x)$, obtemos:

$$h[(id - \pi^*)(x)] = hx - \pi^*(x) = hx = \pi^*(hx) = (id - \pi^*)(h(x)) \in W.$$

Com isso, terminamos a argumentação da demostração. □

Observação 25. *Observe que o fato de usar $n =\mid G \mid$ ser um elemento invertível em F foi nesse momento que assumimos a hipótese de $car(F)$ não dividir $|G|$.*

Observação 26. *Quando F é um corpo algebricamente fechado e de caractéristica zero, A um anel semissimples sobre F de dimensão finita, é bem conhecido que $A \cong \mathcal{M}_n(F) \oplus \cdots \oplus M_{n_t}(F)$.*

Corolário 2.5.1.1. *Sejam G um grupo finito de ordem n, F um corpo algebricamente fechado de característica zero. Então:*

$$F[G] \cong \mathcal{M}_{n_1}(F) \oplus \mathcal{M}_{n_2}(F) \oplus \cdots \oplus \mathcal{M}_{n_r}(F)$$

em que $n = n_1^2 + n_2^2 + \cdots + n_r^2$. Além disso, $F[G]$ possui exatamente r módulos simples não isomorfos de dimensão respectivamentes iguais a $n_1, n_2, \ldots n_r$ sobre F e r coincide com o número de classes de conjugação de G.

Demonstração. Pelo Teorema de Maschke, $F[G]$ é um anel semissimples e do Teorema de Wedderburn-Artin, temos que:

$$F[G] \cong \mathcal{M}_{n_1}(F) \oplus \mathcal{M}_{n_2}(F) \oplus \cdots \oplus \mathcal{M}_{n_r}(F)$$

Além disso, se computarmos dimensões sobre F, obtemos do isomorfismo acima que: $n = n_1^2 + n_2^2 \dots n_r^2$. Agora, basta mostrar que que o número de classes de conjugação de G é igual a r. Iniciamos obeservando que $dim_F Z(F[G]) = r$. Realmente, pois o centro do anel $\mathcal{M}_n(F)$ é o conjunto das matrizes escalares αI_n, um espaço vetorial unidimensional. Pelo isomorfismo apresentado $dim_F Z(F[G]) = r$.

Agora, note que para cada classe de conjugação C_i de G, podemos considerar o elemento $c_i = \sum_{x \in C_i} x \in GF[G]$. Portanto, se $g \in G$, então $g^{-1}c_i g = c_i$. Segue daí que todos elementos c_i pertecem ao centro de $F[G]$. Ao mesmo tempo, podemos considerar $\{c_i\}$ um subconjunto de G, então $\{c_i\}$ é um conjunto L.I sobre F, assim para cada $h \in G$, obtemos:

$$\sum_{g \in G} \alpha_g g = h^{-1}(\sum_{g \in G} \alpha_g g)h = \sum_{g \in G} \alpha_g h^{-1} g h$$

ou seja, da escrita única de $F[G]$ ($F[G]$ é um espaço vetorial sobre F), segue que $\alpha_g = \alpha_{h^{-1}gh}$ implica que $\sum_{g \in G} \alpha_g$ é uma combinação linear dos elementos do conjunto $\{c_i\}$. Portanto $\{c_i\}$ é uma F-base de $Z(F[G])$ e consequentemente:

$r = dim_F Z(F[G])$, o número de classes de conjugação de G.

□

2.5.2 Decomposição de $\mathbb{C}_{S_3}$ em irredutíveis

Nessa subseção, iremos classificar as representações irredutíveis de S_3 sobre $\mathbb{C}$.

Inicialmente, vamos relembrar alguns tópicos importantes relacionados à esse grupo. Consideremos o grupo das permutações S_3,

com $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ e $\mid S_3 \mid = 6$. Além disso, S_3 é gerado por dois elementos, digamos a e b, de modo que $a^2 = (1)$ e $b^3 = (1)$ e $ba = ab^2$, por exemplo, podemos tomar $a = (12)$ e $b = (123)$. Também sabemos que S_3 possui um subgrupo normal de ordem 3, $N =< b >$, S_3 possui três classes de conjugação. A classe do elemento neutro $\{(1)\}$, a classe das transposições $\{(12), (13), (23)\}$ e a classe dos três ciclos $\{(123), (132)\}$.

Observação 27. *Pelo Corolário 2.5.1.1, temos que:*

$$\mathbb{C}S_3 \cong \mathcal{M}_{n_1}(\mathbb{C}) \oplus \mathcal{M}_{n_2}(\mathbb{C}) \oplus \mathcal{M}_{n_3}(\mathbb{C})$$

com $6 = n_1^2 + n_2^2 + n_3^2$. *Note que como* S_3 *não é abeliano, então pelo menos um dos índices* $n_j \neq 1$. *Logo,* $n_1 = n_2 = 1$ *e* $n_3 = 2$, *em outras palavras,* S_3 *possui duas representações irredutíveis unidimensionais e uma bidimensional. Melhorando a decomposição de* $\mathbb{C}S_3$ *para a seguinte forma:*

$$\mathbb{C}S_3 \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathcal{M}_2(\mathbb{C})$$

Nesse momento, vamos encontrar as representações de grau 1 de S_3 sobre $\mathbb{C}$. Para tal, seja V um $\mathbb{C}$-espaço vetorial unidimensional e digamos que $V = \mathbb{C}v$, com $v \in V$. Note que a ação trivial $\rho : G \to GL_1(V), \rho_g = id_V, \forall g \in S_3$ é uma representação linear de S_3 sobre o corpo dos complexos.

Agora, considere $N = \{(1), (123), (132)\}$ e defina $\rho : S_3 \to GL_1(V)$, $\rho_g = id_V$, se $g \in N, \rho_g = id_V$ se $g \notin N$. Então se $g, h \in S_3$, com $gh \in N$, temos: $g, h \in N$ ou $g, h \notin N$ e, consequentemente, $\rho_{gh} = id_V = \rho_g \circ \rho_h$. O mesmo acontece para $gh \notin N$. Com isso, ρ é uma representação linear de grau 1 de S_3 sobre $\mathbb{C}$.

Encontraremos, agora, a representação irredutível de grau dois de S_3 sobre $\mathbb{C}$, note que se ω é uma raíz cúbica primitiva da unidade, isto é $\omega = \frac{1-\sqrt{3}i}{2}$, então:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

e

$$\begin{bmatrix} \omega & 0 \\ 0 & \omega^3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \omega & 0 \\ 0 & \omega^3 \end{bmatrix}.$$

Assim, a aplicação $\varphi : S_3 \to GL_2(\mathbb{C})$ induzida por:

$$a \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ e } b \mapsto \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$$

é, nitidamente, um isomorfismo de grupos. Então tome V um $\mathbb{C}$-espaço vetorial com dimensão 2 sobre V e com base $\mathcal{B} = \{e_1, e_2\}$. Logo, podemos definir $\rho : S_3 \to GL_2(V)$, induzida por:

$$\rho_x : e_1 \mapsto e_2, \rho_x : e_2 \mapsto e_1, \rho_y : e_1 \mapsto \omega e_1 \text{ e } \rho_y : e_2 \mapsto \omega^2 e_2.$$

Para obtermos uma representação linear de S_3 sobre os complexos. Agora, é preciso verificar que a representação acima é irredutível. Para tal fato, não deve haver nenhum subespaço unidimensional de V que seja invariante pela ação linear de S_3 dada por:

$$x \cdot e_1 = e + 2, x \cdot e_2 = e_1, y \cdot e_1 = \omega e_1 \text{ e } y \cdot e_2 = \omega^2 e_2.$$

De fato, o subespço $\mathbb{C}e_1$ não é fixado por x. Agora, dado W um subespaço undimensional de V, então existe um número complexo λ tal que $\omega = \mathbb{C}(e + \lambda e_2)$. Nesse momento, suponha que W seja invariante por esta ação de S_3. Logo temos:

$$x \cdot (e_1 + \lambda e_2) = e_2 + \lambda e_1 \in \mathbb{C}(e_1 + \lambda e_2)$$

ora, existe $\alpha \in \mathbb{C}$ tal que $\lambda e_1 + e_2 = \alpha e_1 + \lambda e_2$, ou seja, só podemos ter $\alpha = \lambda = 1$ ou $\alpha = \lambda = -1$. Por outro lado, temos: $y \cdot (e_1 + e_2) = \omega e_1 + \omega^2 e_2 \notin \mathbb{C}(e_1 + e_2)$ e $y \cdot (e_1 - e_2) = \omega e_1 - \omega^2 e_2 \notin \mathbb{C}(e_1 + e_2)$, o que é um absurdo. Então V é uma representação irredutível de grau 2 sobre $\mathbb{C}$.

2.6 CAPÍTULO 6: RADICAL DE JACOBSON

Definição 59. *Seja A um anel e seja V um $A-$módulo. O anulador de V em A, o qual denotamos por $An_A V$, é definido por:*

$$An_A V = \{a \in V \mid av = 0\}$$

Definição 60. *Sejam A um anel e $\mathcal{S}$ a família dos A-módulos simples. O radical de Jacobson de A é definido como sendo o conjunto*

$$J(A) := \cap_{V \in \mathcal{S}} An_A V$$

Observe que $An_A V$ é um ideal bilateral de A. Deste modo, $J(A) := \cap_{V \in S} An_V$ é um ideal bilateral. Ademais $1_a \notin J(A)$, ou seja, $J(A) \neq A$.

Observação 28. *Seja A um anel, denominamos:*

(i) $\mathcal{M}ax_l(A)$, como a família de todos ideais à esquerda maximais de A.

(ii) $\mathcal{M}ax_r(A)$, como a família de todos ideais à direita maximais de A.

Note que se $x \in J(A)$ e $\mathfrak{M} \in \mathcal{M}ax_l(A)$, então $A/\mathfrak{M}$ é um A-módulo simples à esquerda. Ou seja, $xA \subseteq \mathfrak{M}$ e temos que $x \in \mathfrak{M}$ para todo $\mathfrak{M} \in \mathfrak{M}ax_l(A)$.

De maneira recíproca, se $x \in \cap\{\mathfrak{M} : \mathfrak{M} \in \mathcal{M}ax_l(A)\}$ e V é um A-módulo simples, então $V = Av$, para todo elemento não nulo $v \in V$ e que $An_A(v) \in \mathcal{M}ax_l(A)$, pois V é simples. Portanto $xv = 0, \forall v \in V \setminus \{0\}$. Sendo assim $xV = \{0\}$ e que $x \in An_R(V)$. Tendo em mente que V é qualquer $A-$módulo simples, segue que $x \in J(A)$.

Proposição 2.6.0.1. *Seja A um anel, então $J(A) = \cup I$, em que I percorre a família dos ideais à esquerda maximais de A.*

Proposição 2.6.0.2. *Seja A um anel. As seguintes afirmações são equivalentes:*

(i) $x \in J(A)$;

(ii) $1 - ax$ possui um inverso à esquerda, para todo $a \in A$;

(iii) $1 - axt$ é um elemento invertível em A, para todos $a, t \in A$

Demonstração. $(i) \Rightarrow (ii)$ Suponhamos que exista $a \in A$ tal que $1 - ax$ não possua inverso à esquerda em A. Desse modo, $A(1 - ax)$ é um ideal à esquerda próprio de A, pois $1 \notin A(1 - ax)$. Então existe $\mathfrak{M} \in \mathcal{M}ax_l(A)$ tal que $R(1 - ax) \subseteq \mathfrak{M}$. Mas então, como $1 - ax \in \mathfrak{M}$

e $x \in J(A) = \bigcap\{\mathfrak{N} : \mathfrak{N} \in \mathcal{M}ax_l(A)\}$ segue que $1 - ax, ax, 1 \in \mathfrak{M}$. O fato de $1 \in \mathfrak{M}$ é uma contradição.

$(ii) \Rightarrow (i)$ Seja $x \in A$ e suponha $1 - ax$ possui um inverso à esquerda em A para qualquer escolha de $a \in A$. É necessário provar que $x \in \bigcap\{\mathfrak{M} : \mathfrak{M} \in \mathcal{M}\mathrm{ax}_l(A)\}$. De fato, e se existir $\mathfrak{M} \in \mathcal{M}ax_l(A)$ tal que $x \notin \mathfrak{M}, \mathfrak{M} + Ax = A$ pela maximalidade de $\mathfrak{M}$. Existem elementos $b \in \mathfrak{M}, a \in A$ tal que $b + ax = 1$, em outras palavras, $1 - ax = b \in \mathfrak{M}$, o que é um absurdo. Ja que m não possui invertíveis.

$(i) \Rightarrow (iii)$ Sejam $x \in J(A), a, t \in A$. Assim $xt \in J(A)$ tal que $1 - a(xt)$ tem inverso pelo item anterior. De tal forma, existe $s \in A$ tal que $s(1 - axt) = 1$, mas como $-axt \in J(A)$, $1 - s(axt)$ possui inverso à esquerda, ou seja, existe $u \in A$ tal que $u(1 - s(-axt)) = 1$. Recorde-se que $s = 1 + saxt$, logo $1 = u(1 - s(-axt)) = u(1 + saxt) = us$ daí segue que s é um elemento invertível em A. Logo, $1 - axt$ é um elemento invertível em A.

$(iii) \Rightarrow (i)$ Caso $1 - axt$ seja invertível à esquerda em A, para toda escolha de $r, t \in A$, escolhendo $t = 1\mathrm{d}$ esta forma $1 - ax$ tem inverso à esquerda $\forall a \in A$, sendo assim $x \in J(A)$ pelo argumento feito em $(ii) \Rightarrow (i)$.

□

Vejamos um resultado importante da proposição vista acima.

Corolário 2.6.0.1. *Seja A um anel, então:*

$$J(A) = \bigcap\{\mathfrak{M} : \mathfrak{M} \in \mathcal{M}ax_l(A)\} = \bigcap\{\mathfrak{N} : \mathfrak{N} \in \mathcal{M}ax_r(A)\}.$$

Enunciaremos, agora, um resultado importante deste capítulo.

Proposição 2.6.0.3. *(Lema de Nakayama) Sejam A um anel e M um A-módulo finitamente gerado. Se $J(A)M = M$, então $M = \{0\}$.*

Demonstração. Seja $M = Am_1 + \cdots + Am_s$ um A-módulo não nulo, em que $\{m_1, m_2, \ldots m_s\}$ é um conjunto minimal de geradores. Logo $m_1 \neq 0$. Assim podemos tomar um submódulo maximal de M que contém m_1, o qual existe pelo Lema de Zorn (Lema 2.1.1). Denomine este módulo maximal por N. Assim $V = M/N$ é um A-módulo simples desta forma $J(A)V = \{0\}$. Portanto $J(A)M \supseteq Ker(\pi)$, em que $\pi : M \to M/N$ é a projeção canônica. Logo $J(A)M \neq M$, assim o Lema de Nakayama está demostrado. □

Definição 61. *Sejam A um anel e I um ideal bilateral de A. Dizemos que I é nilpotente, se existir $n \leq 1$ tal que $I^n = 0$, onde $I^n := \{\sum_{finita} a_1 a_2 \ldots a_n : a_i \in I\}$. O menor inteiro positivo n tal que $I^n = 0$ é chamado índice de nilpotência de I.*

Proposição 2.6.0.4. *Seja A um anel artiniano. Então $J(A)$ é um ideal nilpotente.*

Demonstração. Vamos partir do fato que todo ideal bilateral é um ideal à esquerda. Haja vista que A é artiniano, a cadeia descendente a seguir é estacionária.

$$J(A) \supseteq J(A)^2 \supseteq \cdots \supseteq J(A)^n \supseteq \cdots$$

Em outras palavras, existe um m de forma que $J(A)^n = J(A)^{m+1}$. Seja $I = J(A)^m$. Afirmamos que $I = 0$. De fato, pois caso contrário, como $I^2 = I$ a família de ideias à esquerda K de A tais que $IK \neq \{0\}$ seria não vazia, assim existiria um elemento minimal, pela artinianidade de A. Denominaremos tal elemento de W. Então para todo

$y \in A \setminus \{0\}$. Contudo, $IW = IAy = Iy = W$, pois Iy é um A-submódulo não nulo de W tal que $I(Iy) = I^2y = Iy \neq 0$. Logo

$$J(A)W = J(A)IW = IW = W.$$

Mas, como $W = Ay$ é finitamente gerado, segue do Lema de Nakayama, $W = 0$. Contradição. □

Observação 29. *$UT_3(\mathbb{R})$ tem dimensão finita sobre $\mathbb{R}$, assim o anel é artiniano. Temos $J(UT_3(F)) = I$, em que I foi definido no exemplo anterior.*

É importante salientar que o resultado acima não vale sem o presuposto de A ser artiniano. O conceito de nilpotência pode ser feito para elementos, como definido abaixo.

Definição 62. *Seja A um anel e seja $a \in A$. Dizemos que a é um elemento nilpotente se existir $n \geq 1$ tal que $a^n = 0$. O menor inteiro n tal que $a^n = 0$ é chamado de índice de nilpotência de a. Um ideal I de A é denominado nil ideal se todo elemento de I é nilpotente.*

Observação 30. *Note que todo ideal nilpotente é um nil ideal, mas nem todo nil ideal é um ideal nilpotente.*

Por exemplo, tome $A = \frac{\mathbb{Z}[x_1,x_2,\dots]}{<x_1^2,x_2^2,\cdots>}$ e I o ideal gerado pelos elementos $\overline{x_1}, \overline{x_2}, \dots$. Então I, nitidamente, é um nil ideal, mas não é nilpotente.

Lema 2.6.1. *Sejam A um anel e I um nil ideal de A. Então $I \subseteq J(A)$.*

Demonstração. Sejam $m \in I, a \in A$. Como I é um nil ideal, temos que ma é um elemento nilpotente, uma vez que $am \in I$. Agora seja n o índice de nilpotência de am. Logo:

$$(1 + am + (am)^2 + (am)^3 + \cdots + (am)^{n-1})(1 - am) = 1$$

Isto mostra que $1 - am$ possui inverso. Segue da Proposição 6.0.2 que $m \in J(A)$. □

2.6.1 Noções, exemplos e resultados básicos

Neste capítulo, discutiremos as noções fundamentais, exemplos e resultados básicos relacionados à semissimplicidade. O conceito de semissimplicidade é crucial na teoria de anéis e módulos, fornecendo uma estrutura que permite a decomposição em componentes mais simples e a compreensão profunda da estrutura dos anéis e módulos.

Teorema 2.6.2. *Seja A um anel. Se A é semissimples, então $J(A) = \{0\}$. A recíproca é verdadeira se A for artiniano à esquerda.*

Demonstração. Dada a semissimplicidade de A, temos ${}_AA$ semissimples. Deste modo, A é soma direta de ideais à esquerda minimais . Considere $x \in J(A)$. Por definição, x anula todos os $A-$ módulos simples. Logo $xA = \{0\}$. Tal fato implica que $x = 0$

Para a recíproca, vamos assumir, por hipótese, a artinianidade de A e $J(A) = \{0\}$. Tomemos I_1 um ideal à esquerda minimal de A. É necessário provar que I_1 é uma soma direta de ${}_AA$. Realmente, pois como $J(A) = 0$, existe $\mathfrak{M} \in Max_l(A)$ que contém I. Este fato é uma consequência da Proposição 2.6.0.1. Então deveríamos ter $\mathfrak{M} \cap I_1 = \{0\}$, pela simplicidade de I_1, ademais, pelo fato da maximilidade de $\mathfrak{M}$ segue que $\mathfrak{M} + I_1 = A$, em outras palavras, $A = \mathfrak{M} \oplus I_1$. Agora, bastar

observar que $\mathfrak{M}$ é artiniano, e fazer a repetição da argumentação com $\mathfrak{M}$ no lugar de ${}_AA$, para obtermos ${}_AA = I_1 \oplus I_2 \oplus \cdots \oplus I_r$, em que cada I é um ideal à esquerda minimal para $j = 1, 2, \ldots, r$. Assim, A é semissimples. □

No teorema acima, usamos o fato de A ser artiniano para assegurar a existência de ideiais maximais.

Exemplo 56. *Os ideais maximais de $\mathbb{Z}$ são da forma $p\mathbb{Z}$, com p primo. $\mathbb{Z}$ é noetheriano, mas não é artiniano e semissimples. Além disso, $J(\mathbb{Z}) = \cup\{p\mathbb{Z}\} = \{0\}$ com p primo.*

Definição 63. *Seja A um anel, dizemos que A é jacobson semissimples (ou J-semissimples) se $J(A) = 0$*

A partir da definição, obtemos uma nova forma de escrever o Teorema 2.6.2.

Corolário 2.6.2.1. *Seja A um anel. Então as seguintes afirmações são equivalentes:*

(i) A é semissimples;

(ii) A é artiniano à esquerda e J-semissimples.

Exemplo 57. *O anel $\mathbb{Z}_9$ é Noetheriano e Artiniano, mas não é semissimples. Considere o submódulo $V = \{\overline{0}, \overline{3}, \overline{6}\}$ de $\mathbb{Z}_9$. Não existe um submódulo W tal que $\mathbb{Z}_9 = V \oplus W$.*

2.6.2 Versão fraca do Teorema de Hopkins-Levitski

Nessa seção, vamos enunciar e provar a versão fraca do Teorema de Hopkins-Levitski que relaciona anéis artinianos com anéis noetherianos.

Teorema 2.6.3. *(Teorema de Hopkins-Levitski) Seja A um anel. Se A é artiniano à esquerda, então A é noetheriano à esquerda.*

Demonstração. Suponhamos A um anel artiniano à esquerda. Logo $J(A)$ é nilpotente com n e seja n seu índice de nilpotência. Logo, $J(A)^n = \{0\}$. Além disso, temos a segunte cadeia estacionária:

$$A = J(A)^0 \supset J(A)^2 \supset \cdots \supset J(A)^n = \{0\}.$$

Para a prova desse teorema, deveremos mostrar que cada um dos A-módulos $N_i = J(A)^i/J(A)^{i+1}$ tem comprimento finito. Isto ocorre por que um $A-$módulo à esquerda M é artiniano e noetheriano se, e só se $\ell(N) < \infty$. De fato, pois quocientes de um anel artiniano, N_i é artiniano para cada índice i. Note que N_i é anulado por $J(A)$. Assim N_i é um $A/J(A)$-módulo. Como $A/J(A)$ é semissimples temos que N_i é semissimples como um $A/J(A)$-módulo. Como as estruturas de módulos de N_i (como $A-$módulo e $A/J(A)-$módulo) se coincidem, segue que cada um dos A-módulos de N_i é semissimples e artinianos, o que resulta em comprimentos finitos, por meio de resultados já demonstrados no Capítulo 4. Isto mostra que o módulo regular ${}_AA$ possui uma série de composição. □

Observação 31. *Observe que a recíproca desse teorema não é válida, pois já é de conhecimento que o anel dos inteiros ($\mathbb{Z}$) é noetheriano , mas não é artiniano. Logo condição de cadeia ascendente não implica em condição de cadeia descendente. Além disso, para anéis com unidade, a artinianidade é uma condição mais forte que a noetheriano.*

Teorema 2.6.4. *(Generalização do Pequeno Teorema de Wedderburn-Teorema de Jacobson) Seja A um anel tal que para todo $x \in A$ existe um inteiro positivo $n(x) \geq 2$ tal que $x^{n(x)} = x$. Então A é um anel comutativo.*

Teorema 2.6.5. *(Teorema de Hopekens-Levitzki-Azikuki) Seja A um anel com unidade tal que $A/J(A)$ é semissimples e $J(A)$ é um ideal nilpotente. Seja M um $A-$módulo à esquerda. As seguintes condições são equivalentes:*

(i) M é Noetheriano à esquerda;

(ii) M é Artiniano à esquerda;

(iii) M possui uma série de composição

Observação 32. *É possível encontrar as demonstrações dos Teoremas 2.6.4 e 2.6.5 em:*

(i) Canad.Math.Bull.Vol 19(1), 1976 S.W. Dollan;

(ii) Jakob Levitzki. On rings with satisfy the minimum for right-hand ideals Composition Math, 7 214-222, 1939;

(iii) Charles Hopkins. Rings whith minimal conditions for left ideals. Ann of Math. 40:712-130, 1939.

BIBLIOGRAFIA

[1] Sant'Ana, Alveri Alves. *Uma Introdução ao Estudo dos Anéis Semissimples*. Sociedade Brasileira de Matemática, 2016.

[2] Beachy, John A. *Introductory Lectures on Rings and Modules*. Cambridge University Press, 1999.

[3] Coutinho, Mariana de Almeida Nery. *Corpos Finitos e Códigos Corretores de Erros*. Trabalho de Conclusão de Curso (TCC), UFJF — Juiz de Fora, 2019.

[4] Polcino Milies, Francisco César. *Anéis e Módulos*. Editora, 1972.

[5] Da Silva, Ewellyn Carolaine Rodrigues. *Introdução à Álgebra Comutativa: Um Estudo sobre Tensores e Sequências Exatas*. Trabalho de Conclusão de Curso (TCC), Universidade Federal Rural de Pernambuco (UFRPE), Recife, 2019.

[6] Silva, Jhone Caldeira e Gomes, Olimpio Ribeiro. *Estruturas Algébricas para Licenciatura*. Elementos de Aritmética Superior, Volume 2, Editora, 2020.

[7] Guardieiro Sousa, João Paulo. *O Teorema de Wedderburn.*Trabalho de Conclusão de Curso (TCC), Universidade Federal de Uberlândia (UFU), Uberlândia, 2018.

3 CONCLUSÃO

O estudo dos anéis semissimples, noetherianos e artinianos, juntamente com o Teorema de Wedderburn-Artin, revela-se uma área rica e profunda da álgebra abstrata. Esses conceitos são fundamentais para a compreensão da estrutura dos anéis e dos módulos, e possuem aplicações significativas tanto na teoria quanto na matemática aplicada. O Teorema de Wedderburn-Artin, em particular, fornece uma caracterização poderosa dos anéis semissimples, mostrando que eles são isomorfos a produtos diretos de anéis de matrizes sobre corpos.

Durante a realização desta pesquisa, uma lacuna importante foi identificada: a escassez de materiais e recursos disponíveis, especificamente voltados para estudantes de graduação. A maioria dos textos e artigos sobre esses tópicos assume um nível de conhecimento avançado, muitas vezes direcionado a estudantes de pós-graduação ou pesquisadores. Isso pode dificultar o aprendizado e a compreensão dos alunos de graduação. Estes podem se beneficiar imensamente de uma introdução mais acessível e didática destes conceitos. Este é o objetivo principal deste texto.

APÊNDICE A – DESCRIÇÃO 1

DEFINIÇÕES

Grupo

Um **grupo** é um conjunto G equipado com uma operação binária $\cdot : G \times G \to G$ satisfazendo três propriedades fundamentais:

1. **Associatividade**: Para todos $a, b, c \in G$, temos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

2. **Elemento neutro**: Existe um elemento $e \in G$ tal que, para todo elemento $a \in G$, $e \cdot a = a \cdot e = a$.

3. **Inverso**: Para cada elemento $a \in G$, existe um elemento $b \in G$ tal que $a \cdot b = b \cdot a = e$, sendo que e é o elemento neutro.

Grupo Abeliano

Um **grupo abeliano** G (ou comutativo) é um grupo tal que para todos
$a, b \in G$, tem-se que $a \cdot b = b \cdot a$.

Subgrupo

Um **subgrupo** é um subconjunto H de um grupo G que por si só é um grupo com a operação herdada de G. Para que H seja um subgrupo, ele deve satisfazer as seguintes condições:

1. **Fechamento**: Para todos $a, b \in H$, $a \cdot b \in H$.

2. **Elemento neutro**: O elemento neutro de G está em H.

3. **Inverso**: Para cada elemento $a \in H$, o inverso de a em G está em H.

EXEMPLOS

1. **Grupo**: O conjunto dos números inteiros $\mathbb{Z}$ com a operação de adição $+$.

$$(\mathbb{Z}, +)$$

2. **Grupo Abeliano**: O mesmo conjunto $\mathbb{Z}$ com a operação de adição $+$ é também um grupo abeliano, porque a adição de inteiros é comutativa.

$$(\mathbb{Z}, +)$$

3. **Subgrupo**: O conjunto dos números inteiros pares $2\mathbb{Z}$ com a operação de adição $+$ é um subgrupo de $(\mathbb{Z}, +)$.

$$(2\mathbb{Z}, +)$$

4. **Grupo** O conjunto dos números inteiros módulo 2 com a operação $+$:

$$(\mathbf{Z}_2, +)$$

5. **Grupo**: O conjunto dos números inteiros módulo 3 com a operação $+$

$$(\mathbf{Z}_3, +)$$

6. **Grupo**: O conjunto das matrizes invertíveis $m \times n$ sobre um corpo F

$$(gl_n(F), \cdot)$$

7. **Grupo**: O conjunto das transformações lineares invertíveis de um espaço vetorial V de dimensão n em si mesmo é conhecido como o grupo linear geral de ordem n, denotado por $\mathrm{GL}(n, \mathbb{F})$. Aqui, $\mathbb{F}$ representa o corpo sobre o qual o espaço vetorial V está definido.

   As transformações lineares invertíveis são aquelas que possuem uma inversa. O conjunto de todas essas transformações forma um grupo sob a operação de composição de funções. Formalmente, o grupo linear geral pode ser descrito como:

$$\mathrm{GL}(n, \mathbb{F}) = \{T \in \mathrm{End}(V) \mid T \text{ é invertível}\},$$

   onde $\mathrm{End}(V)$ denota o conjunto de todas as transformações lineares de V em V.

$$(Gl_n(F), \circ)$$

8. **Grupo De Klein**: O grupo com quatro elementos não-cíclico

$$(K, +)$$

9. **Grupo de permutações**: O grupo das permutações de ordem 6

$$(S_3, \circ)$$

Ordem de um Grupo e um elemento

A **ordem de um grupo** é denotada por $|G|$ é dada pelo números de elementos de G.

A **ordem de um elemento do grupo** é denotada por $ord(g), g \in G$ é dada pelo menor inteiro positivo, tal que $g^n = e$.

Centro de um grupo e Centralizador de um grupo

Seja G um grupo. Definimos o **centro de um grupo** da seguinte forma:

$$C_D(x) = \{y \in D \mid yx = xy\}$$

O **centralizador de** x **em** G é definido da seguinte maneira:

$$C_D(x) = \{y \in D \mid yx = xy\}$$

Classes de conjugação

Sejam G um grupo e $x \in G$. A classe de conjugação (C_x) de x é o cojunto dos elementos de G que são conjugados de x, em outras palavras:

$$C_x = \{g \cdot x \cdot g^{-1} : g \in G\}$$

Equação de classes de conjugação

Se G é um grupo finito e existem n classes de conjugação (em G). Podemos chegar na **equação de classes de conjugação**:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)_{1 \leq i \leq n}} \frac{|G|}{|C_x(G)|}$$

Referência: GONÇALVES, Adílson. Introdução à Álgebra. Projeto Euclides. Editora SBM.