Elisângela Valéria de Jesus

Módulos e Grupos Abelianos Finitamente Gerados

Itabaiana

Maio de 2017

Elisângela Valéria de Jesus

Módulos e Grupos Abelianos Finitamente Gerados

Dissertação submetida ao Corpo Docente do Programa de Mestrado Profissional em Matemática da Universidade Federal de Sergipe como requisito para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Me. Aislan Leal Fontes

Universidade Federal de Sergipe

Departamento de Matemática

Programa de Pós-Graduação

Itabaiana

Maio de 2017

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA PROFESSOR ALBERTO CARVALHO
UNIVERSIDADE FEDERAL DE SERGIPE

Jesus, Elisângela Valéria de.
J58m Módulos e grupos Abelianos finitamente gerados / Elisângela Valéria de Jesus; orientador Aislan Leal Fontes. – Itabaiana, 2017.
45 f.

Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Sergipe, 2017.

1. Módulos. 2. Espaço vetorial. 3. Grupos Abelianos. I. Fontes, Aislan Leal, orient. II. Título.

CDU 511.34

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Módulos e grupos abelianos finitamente gerados

por

Elisangela Valeria de Jesus

Aprovada pela banca examinadora:

Prof. Me. Aislan Leal Fontes - UFS
Orientador

Prof. Dr. Zaqueu Alves Ramos - UFS
Primeiro Examinador

Prof. Me. Samuel Brito Silva - UFS
Segundo Examinador

São Cristóvão, 16 de Maio de 2017

Cidade Universitária "Prof. José Aloísio de Campos" – Av. Marechal Rondon, s/no - Jardim Rosa Elze – Campus de São Cristóvão. Tel. (00 55 79) 2105-6887
CEP: 49100-000 - São Cristóvão – Sergipe - Brasil – E-mail: promat.ufs@gmail.com

Resumo

O conceito de módulo M sobre um anel A pode ser visto como uma generalização do conceito de espaço vetorial V sobre um corpo K. Neste trabalho, apresentaremos definições, exemplos e resultados acerca de módulos, sendo o nosso objetivo principal demonstrar o teorema de estruturas para grupos abelianos que nos diz que todo grupo abeliano finitamente gerado é a soma direta de subgrupos cíclicos .

Palavras-chaves: Módulos, Anel, Espaço Vetorial, Corpo, Estrutura, Grupos Abelianos.

Abstract

The concept of module M on a ring A can be seen as a generalization of the concept of vector space V over a field K. In this work, we will present definitions, examples and results about modules, our main objective being to demonstrate the theorem of structures for Abelian groups that tells us that every finitely generated abelian group is the direct sum of cyclic subgroups.

Key-words: Modules, Ring, Vector Space, Field, Structure, Abelian Groups.

Sumário

Introdução

Um problema básico de álgebra linear é resolver sistema de equações lineares, e nesse caso procuramos as soluções sobre um corpo dado. Esse problema se torna mais difícil se consideramos sistemas com entradas em um anel A e procuramos por soluções nesse anel. Daí estudamos o análogo de um anel A de um espaço vetorial sobre um corpo, chamado módulo sobre A. Veremos como se resolver sistemas quando A é o anel de inteiros ou o anel de polinômios sobre um corpo. No caso de um módulo sobre um anel A tem-se resultados análogos ao de espaço vetorial sobre um corpo, no entanto existem afirmações em espaço vetorial de dimensão infinita que não são verdadeiras se consideradas em um módulo, como: não é verdade que todo conjunto gerador de um A-módulo contém uma base, também é falso, que todo subconjunto linearmente independente de um A-módulo possa ser ampliado a uma base. Essas e outras propriedades estão sendo abordadas neste trabalho e para melhor compreensão de todos, dividimos em três capítulos:

No capítulo 1, temos a teoria básica de A-módulos e dividimos em duas seções. Na primeira seção, apresentamos definições e exemplos de A-módulos e A-submódulos, da mesma forma que conceituamos espaço e subespaço vetorial em álgebra linear. Definimos também um homomorfismo de A-módulos, bem como o núcleo e a imagem de um A-homomorfismo, assim como temos em álgebra linear as transformações lineares. Para finalizarmos essa seção, apresentamos o conceito de A-módulos quociente, assim como demonstramos os principais resultados que os envolvem entre eles, o Teorema do Isomorfismo e o Teorema da Correspondência.

Iniciamos a segunda seção do Capitulo 1 exibindo os conceitos para geradores, independência linear e base de um A-módulo e módulo livre. Em seguida, provamos que se o anel é comutativo e um A módulo é livre então duas bases do A módulo tem o mesmo número de elemento, e com base nisso definimos *o posto* de A-modulo livre. Veremos, através de um exemplo, que a condição de o anel A ser comutativo é necessária, ou seja, duas bases de um A-módulo livre podem não ter a mesma cardinalidade. Além do mais, se o núcleo e a imagem do A-homomorfismo $\varphi : M \to M'$ são finitamente gerados então um A-módulo M é finitamente gerado. Depois disso, expomos o conceito de anel Noetheriano e demonstramos que todos os A-submódulos de um A-módulo finitamente gerado são finitamente gerados, se A é um anel Noetheriano. (Ver [A], [G-F], [G-L], [J], [Pe] e [Pi])

No capítulo 2, o objetivo é o teorema de diagonalização de matrizes com entradas

inteiras. O algoritmo da divisão é o principal argumento da demonstração usado nesse teorema que nos permite descrever um método sistemático para diagonalizarmos uma matriz com entradas inteiras através de uma sucessão finita de operações elementares. Encerramos esse capítulo com a demonstração de que um subgrupo de um grupo abeliano livre de posto m é um grupo abeliano livre de posto menor ou igual a m. (Ver [A], [G-L] e [Pi])

No terceiro capítulo, que foi dividido em duas seções, apresentamos o resultado mais importante do trabalho, o teorema de estrutura para grupos abelianos, onde afirma que um grupo abeliano finitamente gerado é uma soma direta de subgrupos cíclicos e um grupo abeliano livre. Na primeira seção, demonstramos esse teorema e mostramos que todo grupo abeliano finito é uma soma direta de subgrupos cíclicos de ordem de potência de um primo, bem como a unicidade do teorema de estrutura para grupos abeliano. Já na segunda seção, temos uma aplicação a operadores lineares, onde mostramos que existe uma correspondência 1-1 entre operadores lineares de um espaço vetorial V sobre um corpo K e módulos sobre o anel dos polinômios em uma indeterminada $K[t]$. E para terminamos demonstramos que ao olharmos V como um módulo sobre o anel $K[t]$, um espaço vetorial de dimensão finita V sobre um corpo K possui sua matriz de apresentação diagonal em blocos, chamada de forma racional. (Ver [A], [G-L] e [Pi])

1 Módulos

O análogo para um anel A de um espaço vetorial V sobre um corpo K é chamado de módulos. Sendo assim, neste capítulo apresentaremos algumas definições básicas de módulos bem como exemplos e alguns resultados que consideramos significativos. Neste trabalho, vamos considerar A um anel com unidade.

1.1 Conceitos básicos

Definição 1.1. Seja A um anel. Um A-módulo M é um grupo abeliano aditivo $(M, +)$ dotado de uma multiplicação escalar

$$\begin{aligned} A \times M &\longrightarrow M \\ (a, m) &\longmapsto a.m \end{aligned}$$

que satisfaz as seguintes propriedades:

(M1) $1.m = m$,

(M2) $(ab).m = a.(bm)$,

(M3) $(a + b).m = a.m + b.m$,

(M4) $a.(m_1 + m_2) = a.m_1 + a.m_2$.

para todos a, b em A e para todos m, m_1 e m_2 em M.

Vejamos alguns exemplos:

Exemplo 1.1. Todo espaço vetorial sobre um corpo K é um K-módulo.

Exemplo 1.2. Sejam $A = (\mathbb{Z}, +, \cdot)$ um anel e $(G, +)$ grupo abeliano. Definindo a multiplicação escalar por

$$\begin{aligned} * : \mathbb{Z} \times G &\longrightarrow G \\ (a, v) &\longmapsto a * v := \begin{cases} \underbrace{v + v + \cdots + v}_{a \text{ vezes}}, & \text{se } a \geq 0 \\ \underbrace{(-v) + (-v) + \cdots + (-v)}_{-a \text{ vezes}}, & \text{se } a < 0 \end{cases}, \end{aligned}$$

temos que G é um $\mathbb{Z}$-módulo.

De fato, para todo a e b em $\mathbb{Z}$ e v, v_1 e v_2 em G, temos:

(M1) Como $1 > 0$ então $1 * v = v$ (1 vez).

(M2) Como a e b são quaisquer números em $\mathbb{Z}$, analisaremos dois casos: $a.b \geq 0$ ou $a.b \leq 0$. Se $a.b \geq 0$, temos que $a \geq 0$ e $b \geq 0$ ou $a \leq 0$ e $b \leq 0$. Trataremos apenas quando $a \geq 0$ e $b \geq 0$ (para $a \leq 0$ e $b \leq 0$ é análogo). Assim,

$$\begin{aligned}(a.b) * v &= \underbrace{v + \cdots + v}_{ab \text{ vezes}} \\ &= \underbrace{\underbrace{v + \cdots + v}_{b \text{ vezes}} + \cdots + \underbrace{v + \cdots + v}_{b \text{ vezes}}}_{a \text{ vezes}} \\ &= \underbrace{b * v + \cdots + b * v}_{a \text{ vezes}} \\ &= a * (b * v)\end{aligned}$$

Se $a.b \leq 0$, temos que $-a.b \leq 0$ e segue de maneira análoga ao caso anterior.

(M3) Suponhamos, sem perda de generalidade, $\mid a \mid \geq \mid b \mid$ Como a e b são quaisquer números em $\mathbb{Z}$, analisaremos dois casos: $a + b \geq 0$ ou $a + b \leq 0$. Se $a + b \geq 0$, temos que $a \geq 0$ e $b \geq 0$ ou $a \geq 0$ e $b < 0$. Trataremos apenas quando $a \geq 0$ e $b \geq 0$ (para $a \geq 0$ e $b < 0$ é análogo). Assim,

$$\begin{aligned}(a + b) * v &= \underbrace{v + \cdots + v}_{a + b \text{ vezes}} \\ &= \underbrace{v + \cdots + v}_{a \text{ vezes}} + \underbrace{v + \cdots + v}_{b \text{ vezes}} \\ &= a * v + b * v\end{aligned}$$

Se $a + b \leq 0$, temos que $-(a + b) \leq 0$ e segue de maneira análoga ao caso anterior.

(M4) Se $a \geq 0$ então

$$\begin{aligned}a * (v_1 + v_2) &= \underbrace{(v_1 + v_2) + \cdots + (v_1 + v_2)}_{a \text{ vezes}} \\ &= \underbrace{v_1 + \cdots + v_1}_{a \text{ vezes}} + \underbrace{v_2 + \cdots + v_2}_{a \text{ vezes}} \\ &= a * v_1 + a * v_2\end{aligned}$$

Se $a < 0$, temos que $-a < 0$ e segue de maneira análoga ao caso anterior.

Logo, G é um $\mathbb{Z}$-módulo.

Note que, os grupos abelianos, munidos da multiplicação por escalar usual, são exatamente os $\mathbb{Z}$-módulos.

Exemplo 1.3. Sejam $(A, +, \cdot)$ um anel e

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A\}.$$

Definindo a operação da adição por:

$$(a_1, a_2, \ldots, a_n) \oplus (b_1, b_2, \ldots, b_n) := (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

e a multiplicação por escalar da seguinte maneira:

$$r \odot (a_1, a_2, \ldots, a_n) := (r \cdot a_1, r \cdot a_2, \ldots, r \cdot a_n),$$

temos que A^n é um A-módulo.

Exemplo 1.4. Sejam $(A, +, \cdot)$ um anel e X o conjunto não vazio. Indicaremos $\mathcal{F}(X, A)$ conjunto de todas as funções $f : X \longrightarrow A$. Podemos verificar que $\mathcal{F}(X, A)$ admite uma estrutura de A-módulo, definindo a adição e multiplicação por escalar do seguinte jeito:

$$(f + g)(x) = f(x) + g(x)$$

e

$$(af)(x) = af(x),$$

para todos f, $g \in \mathcal{F}(X, A)$, $a \in A$ e $x \in X$.

Exemplo 1.5. Sejam $(A, +, \cdot)$ um anel e $\mathcal{M}_{m\times n}(A)$ o conjunto de todas matrizes de ordem $m \times n$ com entradas em A. Definindo, $+$ a adição usual das matrizes e $\cdot$ a multiplicação usual de matrizes por escalar, temos que $\mathcal{M}_{m\times n}(A)$ é um A-módulo.

Exemplo 1.6. Seja $A = (\mathbb{Z}, +, .)$ um anel. Seja $(\mathbb{Z} \times \mathbb{Z}, +)$ um grupo munido com a operação da adição usual coordenada a coordenada. Definindo a multiplicação por escalar da seguinte maneira:

$$\begin{array}{rcl} * : \mathbb{Z} \times (\mathbb{Z} \times \mathbb{Z}) & \longrightarrow & \mathbb{Z} \times \mathbb{Z} \\ (a, (x, y)) & \longmapsto & a * (x, y) := (3ax, 3ay), \end{array}$$

temos que $(\mathbb{Z} \times \mathbb{Z}, +)$ não é um $\mathbb{Z}$-módulo.

De fato, para todos a,b em $\mathbb{Z}$ e (x, y) em $\mathbb{Z} \times \mathbb{Z}$, temos que:

$$1 * (x, y) = (3 \cdot 1x, 3 \cdot 1y) = (3x, 3y) = 3(x, y) \neq (x, y).$$

Como falhou na propriedade (M1) então $\mathbb{Z} \times \mathbb{Z}$ com essas operações não é um $\mathbb{Z}$-módulo.

Definição 1.2. Sejam A um anel, M um A-módulo e W um subconjunto não vazio de M. Dizemos que W é um submódulo do A-módulo M ou um A-submódulo de M se as seguintes condições são satisfeitas :

(i) Para todos w_1, $w_2 \in W$ tem-se $w_1 + w_2 \in W$;

(ii) Para todos $a \in A$, $w \in W$ tem-se $aw \in W$.

Observe que, essa definição implica que $0 \in W$. De fato, considere um qualquer w de W, o que é possível pois $W \neq \emptyset$. Tomando $a = 0$, pela condição (ii), segue-se que $0w = 0 \in W$.

Exemplo 1.7. Seja V um espaço vetorial sobre um corpo K. Um subconjunto $S \subseteq V$ é um K-submódulo de V se, e somente se, S é um subespaço vetorial de V.

Exemplo 1.8. Seja $(G, +)$ um grupo abeliano. Então os $\mathbb{Z}$-submódulos são exatamente os seus subgrupos.

Exemplo 1.9. Os submódulos do A-módulo A são os ideais de A.

Proposição 1.1. *Sejam S e W são submódulos do A-módulo M. Então:*

(i) *$S + W := \{s + w \mid s \in S, w \in W\}$ é um submódulo de M;*

(ii) *$S \cap W$ é um submódulo de M.*

Demonstração. **(i)** Note que, $S + W \neq \emptyset$, pois $0 \in S$ e $0 \in W$, logo $0 = 0 + 0 \in S + W$. Agora, sejam v_1, $v_2 \in S + W$, assim $v_1 = s_1 + w_1$ e $v_2 = s_2 + w_2$, onde s_1, $s_2 \in S$ e w_1, $w_2 \in W$. Daí,

$$v_1 + v_2 = s_1 + w_1 + s_2 + w_2 = (s_1 + s_2) + (w_1 + w_2) \in S + W$$

e

$$av_1 = a(s_1 + w_1) = as_1 + aw_1 \in S + W, \forall a \in A.$$

Logo, $S + W$ é um submódulo de M.

(ii) Note que, $S \cap W \neq \emptyset$, pois $0 \in S$ e $0 \in W$, já que ambos S e W são submódulos de M. Agora, sejam v_1, $v_2 \in S \cap W$. Então, $v_1 + v_2 \in S$ e $v_1 + v_2 \in W$, pois S e W são submódulos de M. Portanto, $v_1 + v_2 \in S \cap W$.

Além disso, se $a \in A$ e $v \in S \cap W$, então $v \in S$ e $v \in W$. Daí, segue que $av \in S$ e $av \in W$. Portanto, $av \in S \cap W$.

Logo, $S \cap W$ é um submódulo de M. □

Sejam $W_1, \ldots, W_k$ A-submódulos de M. Dizemos que M é a *soma direta* dos submódulos $W_1, \ldots, W_k$, e escrevemos $M = W_1 \oplus \cdots \oplus W_k$ se:

- $M = W_1 + \cdots + W_k$;

- Se $w_1 + \cdots + w_k = 0$, com w_i em W_i, então $w_i = 0$ para todo i.

Em outras palavras, M é a soma direta dos submódulos W_i, se cada elemento v em M pode ser escrito unicamente na forma $v = w_1 + \cdots + w_k$, com w_i em W_i.

Exemplo 1.10. Consideremos o $\mathbb{Z}$-módulo $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Os subconjuntos $N_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $N_2 = \{\overline{0}, \overline{3}\}$ são submódulos de $\mathbb{Z}_6$ tais que $N_1 \cap N_2 = \{\overline{0}\}$. Agora,

$$\begin{aligned} \overline{0} &= \overline{0} + \overline{0} \\ \overline{1} &= \overline{4} + \overline{3} \\ \overline{2} &= \overline{2} + \overline{0} \\ \overline{3} &= \overline{0} + \overline{3} \\ \overline{4} &= \overline{4} + \overline{0} \\ \overline{5} &= \overline{2} + \overline{3}. \end{aligned}$$

Assim, $\mathbb{Z}_6 = N_1 + N_2$, logo $\mathbb{Z}_6 = N_1 \oplus N_2$.

Definição 1.3. Sejam $(M, +)$ e $(M', \uplus)$ dois A-módulos. Uma aplicação $\varphi : M \to M'$ é homomorfismo de A-módulos ou um A-homomorfismo se satisfaz as seguintes condições:

(i) $\varphi(v_1 + v_2) = \varphi(v_1) \uplus \varphi(v_2)$, para todos v_1, v_2 em M;

(ii) $\varphi(a \cdot v) = a \odot \varphi(v)$, para todos a em A, v em M.

Observação 1.1. A fim de evitar futuras confusões, denotaremos as operações de adição e multiplicação por escalar no A-módulo M da seguinte maneira: $+$ e $\cdot$, respectivamente. Já as operações de adição e multiplicação por escalar no A-módulo M' denotaremos do seguinte modo: $\uplus$ e $\odot$, respectivamente.

Exemplo 1.11. Se K é um corpo, os homomorfismos de K-módulos são as transformações lineares entre espaços vetoriais sobre K.

Definição 1.4. Dizemos que um homomorfismo de A-módulos é isomorfismo de A-módulos se ele é bijetivo.

Observação 1.2. Quando existe um isomorfismo entre dois A-módulos M e M', dizemos que M é isomorfo à M', e denotamos por $M \simeq M'$.

Definição 1.5. Dado um homomorfismo de A-módulos $\varphi : M \to M'$, definimos o núcleo de φ e a imagem de φ, respectivamente, como os seguinte conjuntos:

$$\ker(\varphi) = \{v \in M \mid \varphi(v) = 0\}$$

e

$$\mathrm{Im}(\varphi) = \{\varphi(v) \in M' \mid v \in M\}.$$

Dado $\varphi : M \to M'$ um homomorfismo de A - módulos, temos que se φ é injetivo então $\ker\varphi = \{0\}$. A recíproca também é válida. De fato, sejam v_1, $v_2 \in M$ tais que $\varphi(v_1) = \varphi(v_2)$. Assim, $\varphi(v_1) - \varphi(v_2) = 0$. Daí, segue que $\varphi(v_1 - v_2) = 0 \in Ker(\varphi)$. Como $Ker(\varphi) = \{0\}$, temos que $v_1 - v_2 = 0$. Donde segue que $v_1 = v_2$. Logo, φ é injetivo.

Proposição 1.2. *Se $\varphi : M \to M'$ é um homomorfismo de A-módulos, então:*

(i) *O* $\ker(\varphi)$ *é um submódulo de M;*

(ii) *A* $\mathrm{Im}\,(\varphi)$ *é um submódulo de M'.*

Demonstração. **(i)** Observe que, $0 \in \ker(\varphi)$. De fato,

$$\varphi(0) = \varphi(0+0) = \varphi(0) \uplus \varphi(0), \text{ então}$$

$$\varphi(0) - \varphi(0) = \varphi(0), \text{ então}$$

$$\varphi(0) = 0.$$

Portanto, $\ker(\varphi)$ é um subconjunto não vazio de M.

Agora,sejam v_1, $v_2 \in \ker(\varphi)$. Então, $\varphi(v_1) = 0$ e $\varphi(v_2) = 0$. Assim, $\varphi(v_1 + v_2) = \varphi(v_1) \uplus \varphi(v_2) = 0 \uplus 0 = 0$. Portanto, $v_1 + v_2 \in \ker(\varphi)$. Além disso, se $a \in A$ e $v \in \ker(\varphi)$, então $\varphi(a \cdot v) = a \odot \varphi(v) = a \odot 0 = 0$. Portanto, $a \cdot v \in \ker(\varphi)$, mostrando que o $Ker(\varphi)$ é um submódulo de M.

(ii) Note que $\mathrm{Im}(\varphi)$ é um subconjunto não vazio de M, pois $\varphi(0) = 0 \in \mathrm{Im}(\varphi)$. Sejam w_1, $w_2 \in \mathrm{Im}(\varphi) \subseteq M'$. Tomemos v_1, $v_2 \in M$ tais que $\varphi(v_1) = w_1$ e $\varphi(v_2) = w_2$. Assim, $w_1 \uplus w_2 = \varphi(v_1) \uplus \varphi(v_2) = \varphi(v_1 + v_2)$. Sendo assim, $w_1 \uplus w_2 \in \mathrm{Im}(\varphi)$. Além disso, se $a \in A$ então $a \odot w_1 = a \odot \varphi(v_1) = \varphi(a \cdot v_1)$. Portanto, $a \odot w_1 \in \mathrm{Im}(\varphi)$. Logo, o $\mathrm{Im}(\varphi)$ é um submódulo de M'. □

Seja M um A-módulo e N um submódulo de M. Então, o grupo quociente $(M/N, +)$, isto é, o conjunto de $\{m + N \mid m \in M\}$ das classes laterais de N em M, munido de uma multiplicação por escalar de A

$$r.\overline{v} = r.(v + N) = rv + N = \overline{rv},\ \forall r \in A,\ \forall v \in M$$

herda uma estrutura de A-módulo de M. O A-módulo M/N chamado de *A-módulo quociente* de M por N.

Os principais resultados sobre módulo quociente estão reunidos no teorema a seguir:

Teorema 1.1. *Sejam M e M' dois A-módulos e N um submódulo de M.*

(i) *Considere a projeção canônica*

$$\begin{aligned} \pi : M &\longrightarrow M/N \\ v &\longmapsto v+N. \end{aligned}$$

Então π *é um homomorfismo sobrejetor cujo* $\ker(\pi) = N$.

(ii) *Seja* $\varphi : M \to M'$ *um homomorfismo de* A*-módulos cujo* $\ker(\varphi)$ *contém* N. *Então existe um único homomorfismo de* A*-módulos* $\psi : M/N \to M'$ *tal que* $\varphi = \psi \circ \pi$.

(iii) (Teorema do Isomorfismo) *Seja* $\varphi : M \to M'$ *um homomorfismo sobrejetor de* A*-módulos cujo* $\ker(\varphi) = N$. *Então* ψ *é um isomorfismo de* A*-módulos entre o quociente* M/N *e a imagem do homomorfismo* φ.

(iv) (Teorema da Correspondência) *Seja* $\pi : M \to M/N$ *o homomorfismo projeção. Então existe uma correspondência bijetiva entre os submódulos de* M/N *e os submódulos de* M *que contém* N.

Demonstração. **(i)** De imediato, temos que π é homomorfismo, pois

$$\pi(v+w) = (v+w)+N = (v+N)+(w+N) = \pi(v)+\pi(w)$$

e

$$\pi(rv) = rv+N = r(v+N) = r\pi(v),$$

para todo v, w em M e r em A. Além disso, pela definição A-módulo quociente, para todo $\overline{v} \in M/N$, tem-se que $v \in M$. Assim, existe um $v \in M$ tal que $\pi(v) = \overline{v}$. Logo, π é sobrejetor.

Agora, seja $w \in M$ tal que $\pi(w) = 0$. Então, para todo w em $\ker(\pi)$ temos que $w+N = 0+N$. Daí, segue que $w \in N$. Portanto, $\ker(\pi) = N$.

(ii) (Existência) Note que,

$$\varphi(v) = \psi \circ \pi(v) = \psi(\pi(v)) = \psi(\overline{v}) = \psi(v+N),\ \forall v \in M.$$

Assim, definimos a função $\psi : M/N \to M'$ por $\psi(v+N) = \varphi(v)$. Observe que, ψ está bem definida, pois dados v_1, $v_2 \in M$, obtemos

$$v_1+N = v_2+N \Rightarrow v_1 - v_2 \in N \subseteq \ker(\varphi) \Rightarrow \varphi(v_1-v_2) = 0 \Rightarrow$$

$$\Rightarrow \varphi(v_1) - \varphi(v_2) = 0 \Rightarrow \varphi(v_1) = \varphi(v_2) \Rightarrow \psi(v_1) = \psi(v_2).$$

Além disso, ψ é um homomorfismo. De fato, dados v_1, $v_2 \in M$, temos que

$$\begin{aligned} \psi((v_1+N)+(v_2+N)) &= \psi((v_1+v_2)+N) = \varphi(v_1+v_2) \\ &= \varphi(v_1) \uplus \varphi(v_2) = \psi(v_1+N) \uplus \psi(v_2+N) \end{aligned}$$

e

$$\begin{aligned}\psi(a\cdot(v+N)) &= \psi(av+N)=\varphi(av)\\ &= a\odot\varphi(v)=a\odot\psi(v),\end{aligned}$$

para todo $a\in A$ e $v\in M$.

(Unicidade) Seja $\varphi':M/N\to M'$ tal que $\varphi'\circ\pi=\varphi$. Então,

$$\varphi'(v+N)=\varphi(v)=\psi(v+N),\ \forall v\in M.$$

Logo, $\varphi'=\psi$.

(iii) Observe que, pelo item (ii), $\psi:M/N\to \mathrm{Im}(\varphi)$ é um A-homomorfismo. Para mostrarmos que ψ é um isomorfismo de A-módulos entre o quociente M/N e a imagem do homomorfismo φ, bastamos mostrar que ψ é sobrejetor e injetor. De fato, dado $s\in\mathrm{Im}(\varphi)$, desde que φ é sobrejetor, existe $v\in M$ tal que $\varphi(v)=s$. Portanto, $\psi(v+N)=\varphi(v)=s$, mostrando que ψ é sobrejetor.

Agora, dado v_1, $v_2\in M$, se $\varphi(v_1)=\varphi(v_2)$, então $\varphi(v_1-v_2)=0$, ou seja, $(v_1-v_2)\in\ker(\varphi)=N$. Assim, $v_1+N=v_2+N$, mostrando que ψ é injetor.

(iv) Seja S um submódulo de M/N e W um submódulo de M que contém N. Para mostrar que existe uma correspondência bijetiva entre os submódulos de M/N e os submódulos de M que contém N, basta mostrar que:

- $\pi(W)=S$ é um submódulo correspondente de N, se W é um submódulo de M que contém N;
- $\pi^{-1}(S)=W$ é um submódulo de M, se S é um submódulo de M/N;
- Se $\pi(W)=S$ e $\pi^{-1}(S)=W$, então $S\simeq W$.

Primeiramente, vamos mostrar que se W é um submódulo de M que contém N, então o submódulo correspondente de N é $\pi(W)=S$. Se v_1, $v_2\in S$, existem w_1, $w_2\in W$, respectivamente, tais que $\pi(w_1)=v_1$ e $\pi(w_2)=v_2$. Como W é submódulo de M que contém N, temos que $w_1+w_2\in W$. Assim,

$$\pi(w_1+w_2)=\pi(w_1)+\pi(w_2)=v_1+v_2\in S=\pi(W).$$

Além disso, se $v\in S$, existe $w\in W$ tal que $\pi(w)=v$. Então, dado $r\in A$, temos que $rw\in W$ e, daí segue que $\pi(rw)=rv\in S$. Portanto, $\pi(W)=S$ é um submódulo de N.

Agora, mostraremos que se S é um submódulo de M/N, então o submódulo de M é $\pi^{-1}(S)=W$. Dados w_1, $w_2\in W$, temos que $\pi(w_1)$, $\pi(w_2)\in S$. Assim, $\pi(w_1)+\pi(w_2)=\pi(v_1+v_2)\in S$ e, daí $v_1+v_2\in W$. Além do mais, se $r\in A$ e $w\in W$ então $\pi(rw)=r\pi(w)$.

Como $\pi(w) \in S$, segue que $\pi(rw) \in S$ e consequentemente, $rw \in W = \pi^{-1}(S)$. Logo, $\pi^{-1}(S) = W$ é um submódulo de M.

Finalmente, suponhamos que $\pi(W) = S$ e $\pi^{-1}(S) = W$ e seja o homomorfismo projeção $\tilde{\pi} : M \to S$. Considere o homomorfismo $\varphi : M \to W$ pelo item (ii), existe um único homomorfismo $\overline{\varphi} : S \to W$ tal que $\varphi = \overline{\varphi} \circ \tilde{\pi}$. Além disso, o núcleo de φ é um elemento $x \in M$ tal que $\varphi(x) = \overline{\varphi}(\tilde{\pi}(x)) = 0$. Como $\tilde{\pi}(x) \in S$, temos que $x \in \tilde{\pi}^{-1}(S) = W$. Daí segue que $\ker(\varphi) = W$ e φ é um homomorfismo sobrejetor. Pelo teorema do Isomorfismo, os submódulos de M/N são isomorfos aos submódulos de M que contém N. □

1.2 Módulos livres

Nesta seção, apresentaremos o conceito de módulo livre bem como alguns resultados que são de grande valia para o estudo de módulos. E para isso, iniciaremos definindo geradores, independência linear e base.

Seja β um conjunto de elementos de um A-módulo M.

Definição 1.6. Dizemos que β é um conjunto de geradores de M, ou simplesmente, que β gera M se qualquer elemento $v \in M$ pode ser escrito como combinação linear finita (em geral, não única) de elementos de β, isto é, existem $a_i, \ldots, a_{i+j} \in A$ e $v_i, \ldots, v_{i+j} \in \beta$ tais que

$$v = a_i v_i + \cdots + a_{i+j} v_{i+j}.$$

Um A-módulos M é dito *finitamente gerado* se existe um conjunto finito de elementos que gera M.

Definição 1.7. Dizemos que β é linearmente independente se, para todo subconjunto $\{v_i, \ldots, v_{i+j}\}$ finito de β, sempre que

$$a_i v_i + \cdots + a_{i+j} v_{i+j} = 0,$$

implica $a_i = \ldots = a_{i+j} = 0$, para todo $a_i, \ldots, a_{i+j} \in A$.

Definição 1.8. Um conjunto β de elementos de um A-módulos M é uma base de M se as seguintes condições são satisfeitas:

(i) β gera M;

(ii) β é linearmente independente.

Dado um conjunto ordenado $\beta = \{v_1, v_2, \ldots, v_n\}$ de M, podemos definir um homomorfismo de módulos de A^n e M:

$$\begin{array}{rcl} \varphi : A^n & \longrightarrow & M \\ X & \longmapsto & BX := (v_1, v_2, \ldots, v_n) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = x_1 v_1 + \cdots + x_n v_n, \end{array}$$

onde B é a matriz das coordenadas dos elementos de β na base canônica de A^n.

Proposição 1.3. *Seja o homomorfismo $\varphi : A^n \longrightarrow M$ definido por $\varphi(X) = BX$. Então:*

(i) *φ é injetiva se, e somente se, β é linearmente independente;*

(ii) *φ é sobrejetiva se, e somente se, β gera M;*

(iii) *φ é bijetiva se, e somente se, β é uma base de M.*

Demonstração. **(i)** Sejam $X = (x_1, \ldots, x_n)$, $X' = (x'_1, \ldots, x'_n) \in A^n$.

Se $\varphi(X) = \varphi(X')$, temos que $BX = BX'$, ou seja,

$$x_1 v_1 + \cdots + x_n v_n = x'_1 v_1 + \cdots + x'_n v_n.$$

Daí, segue que

$$(x_1 - x'_1)v_1 + \cdots + (x_n - x'_n)v_n = 0.$$

Como β é linearmente independente, temos que $x_i - x'_i = 0$, para todo $1 \leq i \leq n$. Logo φ é injetiva.

Reciprocamente, dado a equação

$$x_1 v_1 + \cdots + x_n v_n = 0,$$

com $X = (x_1, \ldots, x_n) \in A^n$, temos

$$\varphi(X) = BX = x_1 v_1 + \cdots + x_n v_n = \varphi(0).$$

Como φ é injetiva, temos que $X = 0$. Logo, β é linearmente independente.

(ii) Se φ é sobrejetiva, para todo v em M, existe X em A^n tal que $\varphi(X) = v$. Assim,

$$v = \varphi(X) = BX = v_1 x_1 + \cdots + v_n x_n.$$

Portanto, β gera M.

Reciprocamente, se β gera M então qualquer v em M pode ser escrito da seguinte maneira

$$v = v_1 x_1 + \cdots + v_n x_n,$$

com $X = (x_1, \ldots, x_n) \in A^n$. Assim,

$$\varphi(X) = BX = v_1x_1 + \cdots + v_nx_n = v.$$

Logo, φ é sobrejetiva.

(iii) Decorre dos itens (i) e (ii).

□

Definição 1.9. Um A-módulo M é dito livre se ele admite uma base. Se o A-módulo livre M é finitamente gerado então o módulo M é isomorfo a A^n para algum n.

Exemplo 1.12. Todo espaço vetorial não nulo de dimensão finita é um módulo livre.

Exemplo 1.13. No $\mathbb{Z}$-módulo $\mathbb{Z} \times \mathbb{Z}$, o conjunto $\{(1,0),(0,1)\}$ é uma base de $\mathbb{Z} \times \mathbb{Z}$.

Em seguida, apresentamos alguns exemplos para mostrar que nem sempre os módulos se comportam como um espaço vetorial.

Exemplo 1.14. Não é verdade que todo subconjunto linearmente independente de um módulo livre possa ser ampliado a uma base. De fato, o $\mathbb{Z}$-módulo $\mathbb{Z}$ é livre e o conjunto $\{2\}$ é linearmente independente. Entretanto, esse conjunto não é e não pode ser ampliado a uma base pois todo conjunto com dois ou mais elementos do $\mathbb{Z}$-módulo $\mathbb{Z}$ é linearmente dependente (Ver [Pe], Exemplo 1.5.8.).

Exemplo 1.15. Não é verdade que todo conjunto de gerador pode ser reduzido a uma base. Novamente, considerando o $\mathbb{Z}$-módulo $\mathbb{Z}$ temos o conjunto gerador $\{2,3\}$ que não é e nem pode ser reduzido a uma base.

Teorema 1.2. *Se A é um anel comutativo e M é um A-módulo livre com bases $\{v_1, \ldots, v_n\}$ e $\{w_1, \ldots, w_m\}$ então $m = n$.*

Demonstração. Se $\{v_1, \ldots, v_n\}$ e $\{w_1, \ldots, w_m\}$ são bases de um A-módulo livre M, então existem $b_{ij}, c_{ks} \in A$, $1 \leq i,k \leq n$, $1 \leq j,s \leq m$, tais que

$$v_i = \sum_{j=1}^{m} b_{ij}w_j \text{ e } w_k = \sum_{s=1}^{n} c_{ks}v_s,$$

temos que

$$v_i = \sum_{j=1}^{m}\sum_{s=1}^{n} b_{ij}c_{js}v_s \text{ e } w_k = \sum_{s=1}^{n}\sum_{j=1}^{m} c_{ks}b_{sj}w_j.$$

Sejam as matrizes $B = (b_{ij})_{n\times m}$ e $C = (c_{ji})_{m\times n}$. Então, $BC = I_n$ e $CB = I_m$. Como A é um anel comutativo então $n = m$ (Ver [Pi], Exercício 3.10.). □

Considerando o teorema (1.2), podemos definir *o posto* de um módulo livre M como sendo o número de elementos de uma base de M.

O seguinte exemplo mostra que para anéis não comutativos, as bases de um módulo livre M podem não ter o mesmo número de elementos.

Exemplo 1.16. Seja $\mathbb{Z}[X]$ o $\mathbb{Z}$-módulo dos polinômios na indeterminada X com coeficientes inteiros. Considere o anel de endomorfismos $A := \mathrm{End}_{\mathbb{Z}}\,\mathbb{Z}[X]$. O anel não comutativo A, considerado como um A-módulo, possui duas bases finitas com diferente cardinalidade.

De fato, A como um A-módulo é finitamente gerado por apenas um elemento, tendo o endomorfismo identidade como base. Definamos agora $f_1, f_2 \in A$ da seguinte forma: para todo o $n \in \mathbb{N}_0$, tomamos

$$\begin{cases} f_1(X^{2n+1}) = X^n \\ f_1(X^{2n}) = 0 \end{cases} \quad \text{e} \quad \begin{cases} f_2(X^{2n+1}) = 0 \\ f_2(X^{2n}) = X^n \end{cases} .$$

Estendendo linearmente, temos que cada elemento $f \in A$ fica definido pelas suas imagens nos monômios X^n, pois estes elementos formam uma base de $\mathbb{Z}[X]$. Assim, expandimos as aplicações linearmente a todos os elementos de $\mathbb{Z}[X]$. Verifiquemos que $\{f_1, f_2\}$ é uma base de A.

Sejam $\alpha_1, \alpha_2 \in A$ e considere $\alpha_1 f_1 + \alpha_2 f_2 \equiv 0$. Então, para todo $n \in \mathbb{N}_0$, temos que

$$\begin{aligned} 0 &= (\alpha_1 f_1 + \alpha_2 f_2)(X^{2n+1}) \\ &= \alpha_1(f_1(X^{2n+1})) + \alpha_2(f_2(X^{2n+1})) \\ &= \alpha_1(X^n). \end{aligned}$$

Assim, $\alpha_1(p) = 0$ para todo $p \in \mathbb{Z}[X]$. Portanto, $\alpha_1 \equiv 0$. Fazendo o mesmo cálculo para cada X^{2n} temos $\alpha_2 \equiv 0$. Logo, $\{f_1, f_2\}$ é linearmente independente.

Agora, seja $f \in A$. Consideremos $\beta_1, \beta_2 \in A$ definidos da seguinte maneira: para todo $n \in \mathbb{N}_0$, temos que

$$\begin{cases} \beta_1(X^n) := f(X^{2n+1}) \\ \beta_2(X^n) := f(X^{2n}), \end{cases}$$

e estendemos por linearidade. Temos que, para todo $n \in \mathbb{N}_0$,

$$\begin{aligned} (\beta_1 f_1 + \beta_2 f_2)(X^{2n+1}) &= \beta_1(f_1(X^{2n+1})) + \beta_2(f_2(X^{2n+1})) \\ &= \beta_1(X^n) \\ &= f(X^{2n+1}). \end{aligned}$$

Do mesmo modo, calculando $(\beta_1 f_1 + \beta_2 f_2)(X^{2n})$ vemos que coincide com $f(X^{2n})$. Assim, por linearidade, temos que $f = \beta_1 f_1 + \beta_2 f_2$. Portanto, $\{f_1, f_2\}$ gera A. Logo, $\{f_1, f_2\}$ é uma base de A.

Teorema 1.3. *Seja $\varphi : M \to M'$ um A-homomorfismo. Se $\ker(\varphi)$ e $\mathrm{Im}(\varphi)$ são A-módulos finitamente gerados, então M é finitamente gerado.*

Demonstração. Considere $\{u_1, \ldots, u_m\}$ um conjunto de geradores para o $\ker(\varphi)$ e $\{w_1, \ldots, w_n\}$ um conjunto de geradores para a $\mathrm{Im}(\varphi)$. Além disso, existem elementos v_i de M tais que $\varphi(v_i) = w_i$, com $1 \leq i \leq n$. Agora, tome um elemento qualquer v de M. Temos que $\varphi(v) \in \mathrm{Im}(\varphi)$. Assim, existem a_i em A, com $1 \leq i \leq n$, tais que

$$\varphi(v) = a_1\varphi(v_1) + \cdots + a_n\varphi(v_n),$$

ou seja,

$$\varphi(v - (a_1 v_1 + \cdots + a_n v_n)) = 0.$$

Daí, temos que $\alpha = v - (a_1 v_1 + \cdots + a_n v_n) \in \ker(\varphi)$. Então, existem $r_j \in A$, com$1 \leq j \leq m$, tais que

$$\alpha = r_1 u_1 + \cdots + r_m u_m.$$

Portanto,

$$v = a_1 v_1 + \cdots + a_n v_n + r_1 u_1 + \cdots + r_m u_m.$$

Logo, M é finitamente gerado por $\{v_1, \ldots, v_n, u_1, \ldots, u_m\}$. □

Neste momento, introduziremos o conceito assim como alguns resultado envolvendo anel Noetheriano.

Definição 1.10. Um anel A é dito Noetheriano se todos os seus ideais são finitamente gerados.

Teorema 1.4. *Se A é um anel Noetheriano e M é um A-módulo finitamente gerado então todos os A-submódulos de M são finitamente gerados.*

Demonstração. A demonstração será dividida em dois casos. O primeiro caso é quando $M = A^m$ e o faremos por indução sobre m. Se $m = 1$, um A-submódulo de A é um ideal de A e portanto, é finitamente gerado, por definição de A ser Noetheriano. Suponhamos que $m > 1$ e que qualquer A-submódulo de A^{m-1} seja finitamente gerado. Consideremos a projeção

$$\pi : A^m \to A^{m-1}.$$

Notemos que π é um A-homomorfismo sobrejetor e seu núcleo é o conjunto de vetores de A^m cujas primeiras $m - 1$ coordenadas são zeros.

Seja N um A-submódulo de A^m e considere $\varphi : N \to A^{m-1}$ uma restrição de π a N. Assim, a imagem $\varphi(N)$ é um A-submódulo de A^{m-1} e, por hipótese de indução, é finitamente gerado. Além disso, $\ker(\varphi) = N \cap \ker(\pi)$ é um submódulo de $\ker(\pi)$, que é um módulo isomorfo a A. Portanto, $\ker(\varphi)$ é finitamente gerado. Logo, pelo teorema (1.3), N é finitamente gerado.

Agora faremos a demonstração do segundo caso que é para qualquer A-módulo M. Seja N um A-submódulo de M. Desde que M é finitamente gerado, existe um homomorfismo sobrejetor $\varphi : A^m \to M$. Pelo teorema (1.1), temos que $S = \varphi^{-1}(N)$ é submódulo de A^m e que $N = \varphi(S)$. Assim, S é finitamente gerado pelo caso anterior. Agora, considere $\widetilde{\varphi} : S \to N$ uma retrição de φ para S. Como $\widetilde{\varphi}$ é sobrejetiva, segue que N é finitamente gerado. □

Ainda considerando A um anel Noetheriano, seja M um A-módulo finitamente gerado por $\{v_1, \ldots, v_m\}$. Então, existe um A-homomorfismo sobrejetor

$$\pi : A^m \to M.$$

Temos que $\ker(\pi) = N$ é um submódulo de A^m e portanto, finitamente gerado. Seja $\{w_1, \ldots, w_n\}$ um conjunto de geradores de N. Assim, temos um A-homomorfismo sobrejetor

$$\varphi : A^n \to N.$$

Entretanto, os geradores w_j, com $1 \leq j \leq n$, são elementos de A^m. Desta maneira criamos um A-homomorfismo

$$\psi : A^n \to A^m.$$

Como todo A-homomorfismo entre A-módulos livres A^n e A^m é dado por B uma matriz $m \times n$:

$$\begin{aligned} \psi : A^n &\to A^m \\ X &\mapsto BX, \end{aligned}$$

temos que $\mathrm{Im}(\psi) = BA^n = N = \ker(\pi)$. Pelo teorema do Isomorfismo, segue que A^m/BA^n é isomorfo a M. Neste caso, dizemos que a matriz B é uma *matriz de apresentação* de M.

Agora, definiremos relação entre geradores:

Definição 1.11. Seja M um A-módulo finitamente gerado por um conjunto $B = \{v_1, \ldots, v_m\}$. Chamamos um elemento $Y = (y_1, \ldots, v_m)^t$ em A^m, tal que $y_1v_1 + \cdots + y_mv_m = 0$, um vetor relação ou uma relação entre geradores de M.

Definição 1.12. Um conjunto S de relações de M é um conjunto maximal de M se cada relação de M é uma combinação linear de elementos de S com coeficientes em A.

Exemplo 1.17. O $\mathbb{Z}$-módulo que é gerado por três elementos v_1, v_2 e v_3 com o conjunto completo de relações

$$\begin{aligned} 3v_1 + 2v_2 + v_3 &= 0 \\ 8v_1 + 4v_2 + 2v_3 &= 0 \\ 7v_1 + 6v_2 + 2v_3 &= 0 \\ 9v_1 + 6v_2 + v_3 &= 0 \end{aligned}$$

é apresentado pela matriz

$$B = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix}.$$

Uma vez que várias matrizes apresentam o mesmo módulo ou módulos isomorfos, exibiremos, a seguir, algumas regras para manipular uma matriz B sem alterar a classe do isomorfismo do módulo que essa matriz apresenta:

Propriedade 1.1. Seja B uma matriz de apresentação $m \times n$ de um A-módulo M. As seguintes regras não modifica o módulo em que B apresenta:

- Multiplicar à esquerda de B por Q^{-1}, com Q em $\mathrm{GL}_m(A)$;
- Multiplicar à direita de B por P, com P em $\mathrm{GL}_n(A)$;
- Exclusão de uma coluna de zeros da matriz B;
- Exclusão da linha i e da coluna j, caso a j-ésima coluna de B seja e_i.

As matrizes P e Q usadas na propriedade anterior são matrizes elementares, de tamanho adequado, de modo que $Q^{-1}BP$ é diagonal da forma descrita pelo teorema (2.1) (Ver capítulo 2).

Utilizando essas regras com a matriz de apresentação B do exemplo (1.17), podemos reduzi-la a matriz

$$B = \begin{bmatrix} 4 \end{bmatrix}$$

e isso significa $M \simeq \mathbb{Z}_4$.

2 Diagonalização de Matrizes com Entradas Inteiras

Seja $B = (b_{ij})$ uma matriz com entradas b_{ij} nos inteiros. Neste capítulo mostraremos que qualquer matriz B, pode ser "diagonalizada" através de uma sucessão finita das seguintes operações elementares em suas linhas e colunas:

1. Permutação de duas linhas (respectivamente de duas colunas).
2. Substituição de uma linha (respectivamente de uma coluna) pela soma desta linha com um múltiplo inteiro de uma outra linha (respectivamente pela soma desta coluna com um múltiplo inteiro de uma outra coluna.
3. Multiplicar uma linha ou coluna por -1.

Vejamos, através de exemplos, que as operações elementares (1), (2) e (3) são obtidas por multiplicação, à direita ou à esquerda, da matriz B por certas matrizes invertíveis.

Exemplo 2.1. Seja $B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}$:

a) Permutação de linhas ou colunas.

$$\begin{pmatrix} b_{11} & b_{13} & b_{12} \\ b_{21} & b_{23} & b_{22} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix};$$

note que a permutação entre a segunda e a terceira coluna foi obtida pela multiplicação à direita de B pela matriz quadrada $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, cujo o determinante é 1.

Analogamente em relação a permutação de linhas, temos

$$\begin{pmatrix} b_{21} & b_{23} & b_{22} \\ b_{11} & b_{13} & b_{12} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}.$$

b) Substituição de linha ou coluna.

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} + db_{11} \\ b_{21} & b_{22} & b_{23} + db_{21} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix} \begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

vemos que a substituição da terceira coluna pelo resultado de (terceira coluna)+d.(primeira coluna), onde d é um inteiro, foi obtida pela multiplicação à direita de B pela matriz quadrada $\begin{pmatrix} 1 & 0 & d \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, cujo o determinante é 1. Analogamente em relação a substituição de linhas, temos

$$\begin{pmatrix} b_{11}+db_{21} & b_{12}+db_{22} & b_{13}+db_{23} \\ b_{21} & b_{22} & b_{23} \end{pmatrix} = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}.$$

c) Multiplicar uma linha ou coluna por -1. Esta operação também é obtida pela multiplicação, à direita ou à esquerda de B pela certas matrizes inteiras invertíveis.

$$\begin{pmatrix} b_{11} & -b_{12} & b_{13} \\ b_{21} & -b_{22} & b_{23} \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

$$\begin{pmatrix} b_{11} & b_{12} & b_{13} \\ -b_{21} & -b_{22} & -b_{23} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{pmatrix}.$$

Exemplo 2.2. Seja $B=\begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 6 \end{bmatrix}$. Determinemos as matrizes B', Q^{-1} e P, tal que $B' = Q^{-1}BP$, onde Q e P são invertíveis.

$$\begin{bmatrix} 1 & 0 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 0 & -2 & -6 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & -2 & -6 \end{bmatrix} \begin{bmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & -6 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & -6 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 6 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} = B'$$

Donde segue que

$$B' = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & -2 & -6 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 0 & -2 & -6 \end{bmatrix} \begin{bmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 6 \end{bmatrix} \begin{bmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 0 \\ 4 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 4 & 6 & 6 \end{bmatrix} \begin{bmatrix} 1 & -2 & 3 \\ 0 & 1 & -3 \\ 0 & 0 & 1 \end{bmatrix} = Q^{-1}BP$$

Observe que, para obter a matriz Q^{-1} basta multiplicar na ordem inversa as matrizes elementares que produzem as operações em linhas. Já para obter a matriz P, basta multiplicar as matrizes elementares na ordem em que suas respectivas as operações em colunas são feitas.

No geral, seja $B = (b_{ij})$, $1 \leq i \leq m$ e $1 \leq j \leq n$ uma matriz $m \times n$ com entradas b_{ij} nos inteiros. Fazer uma operação elementar em colunas (em linhas) significa multiplicar a matriz à direita (à esquerda) por uma certa matriz inteira invertível de tamanho $n \times n$ ($m \times m$). Assim, fazer uma sucessão finita de operações elementares entre linhas e colunas da matriz B implica transformar B numa matriz da forma

$$B' = Q^{-1}BP,$$

onde Q é uma matriz $m \times m$ invertível e P é uma matriz $n \times n$ invertível.

Teorema 2.1. *Seja B uma matriz com coeficientes inteiros. Existem produtos Q e P de matrizes elementares, de tamanhos adequados, de modo que $Q^{-1}BP$ é diagonal, digamos*

$$\begin{bmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix} & \\ & 0 \end{bmatrix},$$

onde as entradas da diagonal d_i são positivas, e $d_i \mid d_{i+1}$ para cada $i = 1, \ldots, k-1$.

Demonstração. Se $B = 0$, não temos nada a fazer. Suponhamos que B seja não nula. Assim, através de permutações de linhas e de colunas, podemos considerar uma entrada não nula para a posição b_{11}. Caso esta entrada seja negativa, multiplicaremos a primeira linha por -1, tornando a entrada b_{11} positiva.

Em seguida, vamos zerar a primeira linha e a primeira coluna e sempre que uma operação produzir uma entrada não nula na matriz cujo valor absoluto é menor do que b_{11}, retornamos ao início do processo.

Se a primeira coluna contém uma entrada b_{i1} não nula $i > 1$, aplicando o algoritmo da divisão, existem q_i e r_i inteiros tais que

$$b_{i1} = b_{11}q_i + r_i,$$

com $0 \leq r_i < b_{11}$. Depois, substituímos a i-ésima linha de B por:

$$(i\text{-ésima linha}) - q_i(\text{primeira linha}).$$

Desta maneira, mudamos b_{i1} para r_i. Se $r_i \neq 0$, retornamos ao início do processo. Se $r_i = 0$, produzimos um 0 na primeira coluna.

Após efetuarmos um número finito de operações elementares nas linhas dessa matriz, resulta em uma matriz na qual $b_{i1} = 0$ para todo $i > 1$. Analogamente, usando as operações elementares nas colunas, limpamos a primeira linha. Assim, obtemos uma matriz equivalente a matriz original B que é da forma:

$$\begin{bmatrix} d_1' & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathcal{M}_1 & \\ 0 & & & \end{bmatrix} = B_1$$

Agora, suponhamos que alguma entrada b de $\mathcal{M}_1$, situada na posição b_{ij} da matriz B_1, não é divisível por d_1'. Então, substituímos a primeira coluna de B_1 por:

$$(j\text{-ésima coluna de } B_1) + (\text{primeira coluna de } B_1).$$

produzindo assim uma entrada b na primeira coluna B_1. Com isso, repetimos todo o processo e ao final disso, teremos uma matriz equivalente a matriz B_1 da forma

$$\begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \mathcal{M}_2 & \\ 0 & 0 & & \end{bmatrix},$$

onde $d_1 \mid d_2$ e d_2 divide todas as entradas de $\mathcal{M}_2$. Então, aplicaremos todo o processo na matriz $\mathcal{M}_2$.

Procedendo dessa forma repetidamente, chegaremos a uma matriz diagonal da forma

$$\begin{bmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix} & \\ & 0 \end{bmatrix},$$

no qual $d_1 \mid d_2 \mid \cdots \mid d_k$. □

Corolário 2.1. *Seja B uma matriz $m \times n$, e sejam P e Q matrizes de números inteiros invertíveis de tal maneira que $B' = Q^{-1}BP$ tem a forma diagonal descrita no Teorema* (2.1).

(a) *As soluções inteiras das equações homogêneas $B'X' = 0$ são os vetores inteiros X' cujas primeiras k coordenadas são zeros.*

(b) *As soluções inteiras das equações homogêneas $BX = 0$ são aquelas da forma $X = PX'$ onde $B'X' = 0$.*

(c) *A imagem W' da multiplicação por B' consiste nas combinações dos vetores inteiros $d_1e_1, \ldots, d_ke_k$.*

(d) *A imagem de W da multiplicação por B consiste nos vetores $Y = QY'$, onde Y' é em W'.*

O Teorema (2.1) pode ser utilizado para descrever homomorfismos entre grupos abelianos livres.

Corolário 2.2. *Seja $\varphi : M \to M'$ um homomorfismo de grupos abelianos livres. Existem bases de M e M' de tal modo que a matriz do homomorfismo tem a forma diagonal do Teorema* (2.1).

Agora, mostraremos que, dado M um grupo abeliano livre de posto m e N um subgrupo de M, é possível construir, uma base para N a partir de uma base de M.

Teorema 2.2. *Seja M um grupo abeliano livre de posto m, e seja N um subgrupo de M. Então N é um grupo abeliano livre e seu posto é menor do que ou igual a m.*

Demonstração. Sejam $\beta' = \{w_1, \ldots, w_m\}$ uma base de M e $\beta = \{u_1, \ldots, u_n\}$ um conjunto de geradores de N e $i : N \hookrightarrow M$ um homomorfismo inclusão. Escrevemos

$$u_j = b_{1j}w_1 + \cdots + b_{mj}w_m$$

e consideramos a matriz $B = (b_{ij})_{m\times n}$. Pelo Teorema (2.1), obtemos uma matriz $B' = Q^{-1}BP$ diagonal da forma

$$\begin{bmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix} & \\ & 0 \end{bmatrix},$$

onde $d_1 \mid d_2 \mid \cdots \mid d_k$, P é a matriz de mudança de base de $\mathbb{Z}^m$ e Q é a matriz de mudança de base de $\mathbb{Z}^n$. Sejam β_1 e β_1' essas novas bases. Como a base β e o conjunto de geradores

β' foram tomados arbitrariamente, podemos substituir β, β' e B por β_1, β_1' e B'. Assim, $u_j = d_j w_j$, para $1 \leq j \leq k$.

No entanto, a matriz B pode conter algumas colunas nulas, o que correspondem aos geradores u_{ij} cujo vetor coordenada com relação à base β' de M é o vetor nulo. Então, temos que descartar esses geradores. Quando tivermos feito isso, teremos $n = k$ e $n \leq m$. Agora, mostraremos que o conjunto $\beta = \{u_1, \ldots, u_n\}$ é uma base de N. Como β gera N, basta mostrar que β é linearmente independente. Seja $b_1, \ldots, b_n \in \mathbb{Z}$ tais que

$$b_1 u_1 + \cdots + b_n u_n = 0,$$

ou seja,

$$b_1 d_1 w_1 + \cdots + b_n d_n w_n = 0.$$

Visto que $w_1, \ldots, w_n$ são linearmente independentes, então $b_j d_j = 0$, para cada $1 \leq j \leq n$. Como $d_j \neq 0$ para todo $1 \leq j \leq n$, concluímos que $b_j = 0$ para todo$1 \leq j \leq n$. Logo, β é linearmente independente e portanto, uma base de N.

Para finalizarmos a demonstração, precisamos de um conjunto finito de geradores de N. Uma vez que N é subgrupo de M, temos que, pelo Teorema (1.4), N é finitamente gerado. □

3 Estrutura dos Grupos Abelianos

Diante do que foi exposto nos capítulos anteriores, temos subsídios suficiente para demonstramos o intuito principal de nosso trabalho. Sendo assim, neste capítulo mostraremos que todo grupo abeliano finitamente gerado pode ser expresso como soma direta de subgrupos cíclicos. Além disso, faremos uma aplicação deste resultado a operadores lineares.

3.1 Classificação de grupos abelianos finitamente gerados

O teorema de estrutura para grupos abelianos afirma que um grupo abeliano finitamente gerado M é a soma direta de subgrupos cíclicos e módulo livre. Sabemos que existe uma matriz de apresentação diagonal para M, esse teorema nos permite interpretar o significado desta matriz para o grupo abeliano. Vale lembrar que um grupo C é *cíclico* quando é gerado por apenas um elemento.

Teorema 3.1 (Teorema de Estrutura para Grupos Abelianos)**.** *Um grupo abeliano finitamente gerado M é uma soma direta de subgrupos cíclicos $C_{d_1}, \ldots, C_{d_r}$ e um grupo abeliano livre L,ou seja,*

$$M = C_{d_1} \oplus \cdots \oplus C_{d_r} \oplus L,$$

onde a ordem d_i de C_{d_i} é maior que 1 e d_i divide d_{i+1} para $i = 1, \ldots, r-1$.

Demonstração. Seja M um grupo abeliano finitamente gerado por $\beta = \{v_1, \ldots, v_m\}$. Consideramos B uma matriz de apresentação para M determinada pelo conjunto de geradores β e Y um conjunto completo de relações de M. Pelo Teorema (2.1), a matriz B terá a forma diagonal

$$\begin{bmatrix} \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_k \end{bmatrix} & \\ & 0 \end{bmatrix}_{m \times n},$$

no qual $d_1 \mid d_2 \mid \cdots \mid d_k$.

Vamos eliminar qualquer linha i e coluna j cuja entrada da diagonal seja igual a 1 pois, do contrário teríamos como relação $v_i = 0$ e o elemento zero é inútil como um gerador. Além disso, eliminaremos qualquer coluna de zeros. Assim, depois de reordenar

os d_i's, B terá forma

$$B = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_r \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix}_{m \times r},$$

onde $d_1 > 1$ e $d_1 \mid d_2 \mid \cdots \mid d_r$, com $r \leq k \leq m$. Como isso,

$$d_1 v_1 = 0, \ldots d_r v_r = 0,$$

formando um conjunto completo de relações de M.

Agora, seja C_j o subgrupo cíclico gerado por v_j, para $1 \leq j \leq m$. Então, C_j é cíclico de ordem d_j, se $j \leq r$ e C_j é cíclico infinito , se $j > r$. Mostraremos que M é a soma direta destes grupos cíclicos.

Como β gera M, temos que $M = C_1 + \cdots + C_m$. Basta mostrar que $w_1 + \ldots + w_m = 0$ implica $w_j = 0$, para w_j em C_j. De fato, considere a equação $w_1 + \cdots + w_m = 0$, com w_j em C_j. Uma vez que v_j gera C_j segue que $w_j = y_j v_j$, para algum inteiro y_j. Assim, $Y = (y_1, \ldots, y_m)^t$ é uma relação de M.

Visto que as colunas de B formam um conjunto completo de relações de M, $Y = BX$ para algum vetor X. Isto significa que y_j é um múltiplo de d_j, se $j \leq r$ e $y_j = 0$, se $j > r$. Como $d_j v_j = 0$ se $j \leq r$, temos que $w_j = 0$ se $j \leq r$. Portanto, $w_j = 0$ para $1 \leq j \leq m$. Logo,

$$M = C_{d_1} \oplus \cdots \oplus C_{d_r} \oplus L,$$

onde o grupo abeliano livre L é a soma direta dos grupos cíclicos infinitos C_j, com $j > r$. □

Exemplo 3.1. Considere M um $\mathbb{Z}$-módulo finitamente gerado por v_1 e v_2, com as relações

$$\begin{aligned} v_1 + 4v_2 &= 0 \\ 2v_1 + 4v_2 &= 0. \end{aligned}$$

A matriz de apresentação de M é dado por

$$B = \begin{bmatrix} 1 & 2 \\ 4 & 4 \end{bmatrix} \sim \begin{bmatrix} 4 \end{bmatrix}.$$

Assim, $M \simeq \mathbb{Z}_4$.

Exemplo 3.2. Seja M um grupo abeliano finitamente gerado por v_1, v_2 e v_3, com as relações

$$\begin{aligned} 2v_1 + 2v_2 + 2v_3 &= 0 \\ 2v_1 + 2v_2 &= 0 \\ 2v_1 + 2v_3 &= 0. \end{aligned}$$

Encontremos uma soma direta de grupos cíclicos isomorfo a M.

A matriz de apresentação de M é dado por

$$B = \begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{bmatrix}.$$

Diagonalizando B, obtemos

$$B \sim \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Portanto, $M \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Exemplo 3.3. Considere M um grupo abeliano finitamente gerado por v_1, v_2 e v_3, com as relações

$$\begin{aligned} 7v_1 + 5v_2 + 2v_3 &= 0 \\ 3v_1 + 3v_2 &= 0 \\ 13v_1 + 11v_2 + 2v_3 &= 0. \end{aligned}$$

Vamos escrever M como soma direta de grupos cíclicos.

Temos que

$$B = \begin{bmatrix} 7 & 3 & 13 \\ 5 & 3 & 11 \\ 2 & 0 & 2 \end{bmatrix}$$

é uma matriz de apresentação de M. Ao diagonalizar B, obtemos

$$B \sim \begin{bmatrix} 6 \\ 0 \end{bmatrix}.$$

Assim, $M \simeq \mathbb{Z}_6 \oplus \mathbb{Z}$.

Proposição 3.1. *Se a e b são inteiros relativamente primos, então o grupo cíclico C_{ab} é isomorfo a soma direta $C_a \oplus C_b$.*

Demonstração. Seja $B = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ uma matriz de apresentação do grupo abeliano finito $C_a \oplus C_b$. Suponha, sem perda de generalidade, $a < b$. Como a não divide b, a matriz diagonal B ainda não está na forma do teorema (2.1). Para isso, faremos algumas manipulações na matriz B.

Primeiramente, substituímos a 1ª coluna pela soma da 1ª coluna com a 2ª coluna e obtemos

$$B \sim \begin{bmatrix} a & 0 \\ b & b \end{bmatrix}.$$

Aplicando o algoritmo da divisão em a e b temos que existem inteiros q_1 e r_1 tais que $b = aq_1 + r_1$, com $0 <\mid r_1 \mid< a$. Assim, multiplicamos a 1ª linha da matriz por $-q_1$ e somamos a 2ª linha. Depois, trocamos a 1ª com a 2ª linha e teremos

$$B \sim \begin{bmatrix} r_1 & b \\ a & 0 \end{bmatrix}$$

. Se $r_1 = 1$, faremos as seguintes operações:

$$B \sim \begin{bmatrix} 1 & b \\ a & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & b \\ 0 & -ab \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & ab \end{bmatrix}.$$

Se $r_1 \neq 1$, aplicaremos novamente o algoritmo da divisão em a e r_1, ou seja, existem inteiros q_2 e r_2 tais que $a = r_1q_2 + r_2$, com $0 <\mid r_2 \mid< r_1$. Deste modo, multiplicamos a 1ª linha da matriz $\begin{bmatrix} r_1 & b \\ a & 0 \end{bmatrix}$ por $-q_2$ e somamos a 2ª linha. Depois, trocamos a 1ª com a 2ª linha e obteremos

$$B \sim \begin{bmatrix} r_2 & -q_2b \\ r_1 & b \end{bmatrix}.$$

Assim, repetindo os procedimentos anteriores um número finito de vezes, encontramos que

$$B \sim \begin{bmatrix} 1 & 0 \\ 0 & ab \end{bmatrix}.$$

Eliminando a linha e a coluna cuja entrada da diagonal é 1 teremos $B \sim \begin{bmatrix} ab \end{bmatrix}$. Logo, $C_a \oplus C_b \simeq C_{ab}$. □

Combinando o teorema (3.1) com a proposição (3.1) resulta no seguinte corolário.

Corolário 3.1 (Forma Alternativa do Teorema de Estrutura)**.** *Todo grupo abeliano finito é uma soma direta de grupos cíclicos de ordem potência de um primo, ou seja,*

$$M \simeq C_{p_1^{u_{11}}} \oplus \cdots \oplus C_{p_s^{u_{1s}}} \oplus \cdots \oplus C_{p_1^{u_{r1}}} \oplus \cdots \oplus C_{p_s^{u_{rs}}},$$

onde $u_{1j} \leq u_{2j} \leq \cdots \leq u_{rj}$ *e* $1 \leq j \leq s$.

Teorema 3.2 (Unicidade do Teorema de Estrutura)**.** *Se um grupo abeliano finito M é uma soma direta de subgrupos cíclicos de ordens potência de um primo $p_j^{r_{ij}}$, com $1 \leq i \leq r$ e $1 \leq j \leq s$, então os inteiros d_j do teorema* (3.1) *são unicamente determinados pelo grupo M.*

Demonstração. Sejam $p_1, \ldots, p_s$ os primos distintos na decomposição de M. Vamos listar todas as potências de um primo que aparecem na decomposição de M da seguinte maneira:

$$\begin{matrix} p_1^{u_{11}} & p_2^{u_{12}} & \ldots & p_s^{u_{1s}} \\ p_1^{u_{21}} & p_2^{u_{22}} & \ldots & p_s^{u_{2s}} \\ \vdots & \vdots & & \vdots \\ p_1^{u_{r1}} & p_2^{u_{r2}} & \ldots & p_s^{u_{rs}} \end{matrix},$$

onde r é o número de ocorrência dos primos que aparecem mais vezes e $u_{1j} \leq u_{2j} \leq \cdots \leq u_{rj}$, $1 \leq j \leq s$. Eventualmente, alguns dos u_{ij} terão que ser nulos. Seja d_{ij} o produto das potências de um primo na linha i, ou seja,

$$d_i = p_1^{u_{i1}} \cdot p_2^{u_{i2}} \ldots p_s^{u_{is}},$$

onde $1 \leq i \leq r$. É claro que $d_1 \mid d_2 \mid \cdots \mid d_r$. Como as potências de um primo que aparecem em cada d_i são primas entre si, pela proposição (3.1) podemos concluir que

$$C_{d_i} = C_{p_1^{u_{i1}}} \oplus C_{p_2^{u_{i2}}} \oplus \cdots \oplus C_{p_s^{u_{is}}}.$$

Daí, segue que

$$M \simeq C_{p_1^{u_{11}}} \oplus \cdots \oplus C_{p_s^{u_{1s}}} \oplus \cdots \oplus C_{p_1^{u_{r1}}} \oplus \cdots \oplus C_{p_s^{u_{rs}}} \simeq C_{d_1} \oplus \cdots \oplus C_{d_r}.$$

Em suma, dado uma lista dos $p_j^{u_{ij}}$, os d_i's ficam determinados , a menos de associados. Reciprocamente, dado uma lista dos d_i's, os $p_j^{u_{ij}}$ são as potências de um primo na decomposição dos d_i's. Logo, os d_i's são unicamente determinados por M. □

Exemplo 3.4. Seja o grupo abeliano finito $G = \mathbb{Z}_{20} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_{108}$. Pelo corolário (3.1), G é uma soma direta de subgrupos cíclicos de ordens potência de um primo, ou seja,

$$G = \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{2^3} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^3}.$$

Assim, as potências de um primo que aparecem na decomposição de G são 2^2, 5, 2^3, 5, 2^2 e 3^3 e dispõem-se de acordo com a seguinte tabela:

$$\begin{matrix} 2^2 & 3^0 & 5^0 \\ 2^2 & 3^0 & 5 \\ 2^3 & 3^3 & 5 \end{matrix}.$$

Portanto,

$$\begin{aligned} d_1 &= 2^2 = 4 \\ d_2 &= 2^2 \cdot 5 = 20 \\ d_3 &= 2^3 \cdot 3^3 \cdot 5 = 1080. \end{aligned}$$

Logo, $G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{1080}$.

Exemplo 3.5. Vamos encontrar explicitamente todos os grupos abelianos de ordem $400 = 2^4 \cdot 5^2$, a menos de isomorfismo.

Temos que, a menos de isomorfismo, existem exatamente 5 grupos abelianos de ordem 2^4, a saber:

$$\mathbb{Z}_{2^4},\ \mathbb{Z}_2 \oplus \mathbb{Z}_{2^3},\ \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2},\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \text{ e } \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

A menos de isomorfismo, existem exatamente 2 grupos abelianos de ordem 5^2, a saber:

$$\mathbb{Z}_{5^2} \text{ e } \mathbb{Z}_5 \oplus \mathbb{Z}_5.$$

Então, os grupos possíveis são:

$$\begin{aligned} G_1 &= \mathbb{Z}_{2^4} \oplus \mathbb{Z}_{5^2} \simeq \mathbb{Z}_{400}, \\ G_2 &= \mathbb{Z}_{2^4} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_5 \oplus \mathbb{Z}_{80}, \\ G_3 &= \mathbb{Z}_2 \oplus \mathbb{Z}_{2^3} \oplus \mathbb{Z}_{5^2} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{200}, \\ G_4 &= \mathbb{Z}_2 \oplus \mathbb{Z}_{2^3} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_{10} \oplus \mathbb{Z}_{40}, \\ G_5 &= \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{5^2} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_{100}, \\ G_6 &= \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_{20} \oplus \mathbb{Z}_{20}, \\ G_7 &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{5^2} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{100}, \\ G_8 &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{20}, \\ G_9 &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{5^2} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{50}, \\ G_{10} &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{10}. \end{aligned}$$

3.2 Aplicação a operadores lineares

Podemos fazer uma classificação análoga a de grupos abelianos para o anel de polinômios em uma variável $A = K[t]$, sobre um corpo K. Lembremos que o principal argumento usado na demonstração do teorema (2.1) para a diagonalização de matrizes com coeficientes inteiros foi o algoritmo da divisão que tem sua versão no anel A. Pelo

teorema da base de Hilbert [A] tem-se que A é um anel Noetheriano, assim todo A-módulo V é finitamente gerado e tem uma matriz de apresentação. Temos a seguinte versão do teorema (2.1) para uma matriz com entradas em A:

Teorema 3.3. *Sejam $A = K[t]$ o anel de polinômios na variável t sobre um corpo K e B uma A-matriz de tamanho $m \times n$. Existem matrizes P e Q, produto de A-matrizes elementares, tal que $B' = Q^{-1}BP$ é diagonal, sendo que cada entrada não nula da diagonal d_i de B' é um polinômio mônico, e ainda $d_1|d_2 \ldots |d_k$.*

Exemplo 3.6.

$$B = \begin{bmatrix} t^2-3t+1 & t-2 \\ (t-1)^3 & t^2-3t+2 \end{bmatrix} \overset{linha}{\to} \begin{bmatrix} t^2-3t+1 & t-2 \\ t^2-t & 0 \end{bmatrix} \overset{col}{\to}$$

$$\overset{col}{\to} \begin{bmatrix} -1 & t-2 \\ t^2-t & 0 \end{bmatrix} \overset{col}{\to} \begin{bmatrix} -1 & 0 \\ t^2-t & t^3-3t^2+2t \end{bmatrix} \overset{linha}{\to} \begin{bmatrix} 1 & 0 \\ 0 & t^3-3t^2+2t \end{bmatrix}.$$

Na sequência vamos estender o teorema de estrutura para anéis de polinômio. Vamos considerar um A-modulo *cíclico* C sendo um A-módulo gerado por um único elemento. Dessa forma, existe um homomorfismo sobrejetor $\varphi : A \longrightarrow C$ tal que $r \mapsto rv$, onde o núcleo $I = \ker(\varphi)$ é um ideal principal de A e pelo teorema do isomorfismo $C \simeq A/(d)$, para algum polinômio d. Isso significa que o módulo de relações é gerado por um único elemento.

Teorema 3.4 (Teorema de Estrutura para Módulos sobre Anéis de Polinômio)**.** *Seja $A = K[t]$ o anel de polinômios em uma variável sobre o corpo K. Seja V é um A-módulo finitamente gerado. Então V é uma soma direta de módulos cíclicos $C_1, \ldots, C_k$ com um A-módulo livre L, onde C_i é isomorfo a $A/(d_i)$, os elementos d_i são polinômios mônicos de grau positivo, e $d_1|d_2 \ldots |d_k$.*

Observação 3.1. A condição $d_1|d_2 \ldots |d_k$ pode ser trocada por: cada d_i é uma potência de um polinômios mônico irredutível. Além disso, mostra-se a unicidade dessas potências de primos que não vamos provar.

Voltando ao exemplo (3.6), com $A = \mathbb{Q}[t]$ o A-módulo V apresentado pela matriz B é o módulo apresentado pela matriz B' e usando a propriedade (1.1), V é representado pela matriz $[f]$ onde $f = t^3 - 3t^2 + 2t = t(t-1)(t-2)$ e portanto $V \simeq A/(f)$. Mas como fatores $t, t-1, t-2$ são polinômios irredutíveis em A temos o isomorfismo

$$V \simeq A/(t) \oplus A/(t-1) \oplus A/(t-2).$$

Agora vamos a nosso principal objetivo que é aplicar esse conceito a operadores lineares. Dado um operador linear $T : V \longrightarrow V$ em um espaço vetorial V sobre um

corpo K podemos definir nesse espaço vetorial V uma estrutura de A-módulo por definir o produto

$$\begin{array}{rccc} . & : & A \times V & \longrightarrow & V \\ & & (f(t), v) & \longmapsto & f(t).v, \end{array}$$

onde a ação $f(t).v = a_n T^n(v) + a_{n-1}T^{n-1}(v) + \ldots + a_1 T(v) + a_0 v$ para qualquer polinômio $f(t) = a_n t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in K[t]$.

Vamos usar a seguinte notação:

$$f(t).v = [f(T)]v \text{ ou simplesmente } f(t)v = [f(T)]v,$$

onde $f(T)$ denota o operador linear associado ao polinômio $f(t)$. Com essa notação tem-se $tv = T(v)$. Definida a operação ., é fácil verificar que V é um A-módulo. Reciprocamente,

Proposição 3.2. *Seja $A = K[t]$ o anel de polinômios em uma variável sobre um corpo K. Se V é um A-módulo, então temos um operador linear $T : V \longrightarrow V$ no K-espaço vetorial V.*

Demonstração. Desde que V é um A-módulo, podemos definir a multiplicação por polinômios constantes que são os elementos de K, e assim V se torna um espaço vetorial sobre K. Novamente pelo fato de V ser um A-módulo, podemos definir a multiplicação de elementos de V pelo elemento $t \in A$. Vamos denotar essa operação de multiplicação por t em V como sendo T, ou seja, T é a aplicação

$$V \xrightarrow{T} V \text{ tal que } T(v) = tv.$$

Sendo V um A módulo, em particular vale a distributividade da soma sobre o produto e então $t(v + v') = tv + tv'$ o que significa $T(v + v') = T(v) + T(v')$, para todo $v, v' \in V$. Além disso, dado $c \in K$ temos $tcv = ctv$ e assim $T(cv) = cT(v)$. Portanto, a aplicação T é um operador linear no espaço vetorial V. □

Resumindo, constatamos que as regras que associa a cada $K[t]$-módulo V um operador linear de V e vice-versa são operações inversas.

Exemplo 3.7. Considere o $K[t]$-módulo $V = K[t]$, ou seja, V é um módulo de posto 1. Por outro lado, V é um espaço vetorial sobre K de dimensão infinita tendo como base $\beta = \{1, t, t^2, \ldots\}$. Isso nos possibilita identificar V com o espaço vetorial $\mathcal{Z}$ de dimensão infinita dos vetores linhas $(a_0, a_1, a_2, \ldots)$ onde apenas um número finto de entradas é não nulo. Mediante essa identificação, temos o operador associado ao $K[t]$-módulo $V = K[t]$

$$(a_0, a_1, a_2, \ldots) \overset{t}{\mapsto} (a_1, a_2, \ldots),$$

chamado de *operador shift*. Tendo a relação entre $K[t]$-módulos e operadores lineares vamos agora considerar V um K-espaço vetorial de dimensão finita n e T um operador linear em V. Podemos ver V como um $K[t]$-módulo, este finitamente gerado como um $K[t]$-módulo e portanto possui uma matriz de apresentação. Dessa forma, estamos trabalhando com duas matrizes: a matriz de apresentação $r \times s$ que apresenta o módulo V com entradas sendo polinômios em $K[t]$ representado por s relações entre r geradores; a outra matriz $n \times n$ é a do operador linear T.

Sendo V um $K[t]$-módulo aplicamos o teorema (3.3) obtendo uma decomposição de V em soma direta de submódulos cíclicos como segue

$$V = C_1 \oplus \ldots \oplus C_k,$$

onde cada C_i é isomorfo a $K[t]/(f_i)$, f_i polinômio mônico em $K[t]$, e a parte livre é zero desde que V é de dimensão finita. Considerando β_i uma base de $C_i, i = 1, \ldots, k$ temos que $\beta = (\beta_1, \ldots, \beta_k)$ é uma base de V sendo que cada espaço C_i é invariante por T o que significa a matriz de T tem uma forma de diagonal em blocos.

Seja V um $K[t]$-módulo cíclico gerador por um elemento v_0, e como $K[t]$ é um domínio de ideais principais já vimos que V é isomorfo a $K[t]/(f)$ para algum $f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$ mônico de grau n em $K[t]$. Mas precisamente, temos o isomorfismo $K[t]/(f) \longrightarrow V$ dado por $1 \mapsto v_0$. Pelo algoritmo da divisão,

$$K[t]/(f) = \{b_{n-1}t^{n-1} + \ldots + b_1 t + b_0 | b_i \in K\},$$

e portanto o conjunto $\{1, t, \ldots, t^{n-1}\}$ é uma base de $K[t]/(f)$ como $K[t]$-módulo, consequentemente o conjunto $\beta = \{v_0, tv_0, \ldots, t^{n-1}v_0\}$ é uma base de V como K-espaço vetorial. Se consideramos o operador shift do exemplo (3.7) $T : V \longrightarrow V$, multiplicação por t, e escrevemos os vetores da base β da forma $(v_0, v_1, \ldots, v_{n-1})$, onde $v_i = T^i(v_0)$ temos

$$T(v_0) = v_1, T(v_1) = T^2(v_0) = v_2, \ldots, T(v_{n-2}) = T^{n-1}(v_0) = v_{n-1}$$

e

$$\begin{aligned} [f(T)](v_0) &= T^n(v_0) + a_{n-1}T^{n-1}(v_0) + \ldots + a_1 T(v_0) + a_0 v_0 = \\ &= T(v_{n-1}) + a_{n-1}v_{n-1} + \ldots + a_1 v_1 + a_0 v_0 = 0 \end{aligned}$$

e portanto,

$$T(v_{n-1}) = -a_{n-1}v_{n-1} - \ldots - a_1v_1 - a_0v_0.$$

Dessa forma, vamos ter a matriz de T na base β

$$[T]_\beta = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix},$$

cujo polinômio característico é $f(t)$.

Teorema 3.5. *Seja T um operador linear em um espaço vetorial de dimensão finita V sobre um corpo K. Existe uma base para V tal que a matriz de T é composta de blocos do tipo descrito acima.*

Essa matriz é chamada de *forma canônica racional* do operador T.

Exemplo 3.8. Seja $K = \mathbb{R}$. Considere a matriz B na forma racional

$$B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

que tem como polinômio característico $f(t) = t^3 - 1 = (t-1)(t^2+t+1)$. Desde que $(t-1)$ e t^2+t+1 são polinômios irredutíveis sobre K, o $K[t]$-módulo cíclico V que B representa é uma soma direta de módulos cíclicos, que mediante a consideração acima sua matriz de apresentação em blocos é dada por

$$B' = \left[\begin{array}{c|cc} 1 & & \\ \hline & 0 & -1 \\ & 1 & -1 \end{array}\right].$$

Sobre o corpo dos números complexos o polinômio t^2+t+1 é redutível com fatores irredutíveis $t-\omega, t-\omega^2$, onde $\omega = e^{\frac{2\pi i}{3}}$ e a matriz de apresentação do módulo V é diagonalizável, mais precisamente,

$$B'' = \begin{bmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{bmatrix}.$$

Referências

[A] M. Artin, *Algebra*, 2ª ed., Prentice Hall, 1991.

[G-F] M.L. Galvão, P.J. Freitas *Dimensão de Módulos Livres sobre Anéis Comutativos*. Disponível: http://revistas.rcaap.pt/boletimspm/article/download/3831/2895. Acesso em 15/11/2016

[G-L] A. Garcia,Y. Lequain, *Elementos de Álgebra*, Projeto Euclides, 4ª ed., Rio de Janeiro, IMPA, 2006.

[J] N. Jacobson, *Basic Algebra*, vol.1, W.H. Freeman and Company, New York, 1910.

[Pe] F.A. Pereira, *Introdução à Teoria de Módulos*. Disponível em: http://www.impa.br/opencms/pt/eventos/downloads/jornadas_2006/trabalhos/jornadas_fernanda_pereira.pdf. Acesso em 24/09/2016.

[Pi] J. Picado, *Álgebra Comutativa*, Universidade de Coimbra, 2013. Disponível em http://www.mat.uc.pt/ picado/algcom/apontamentos/TextosApoio.pdf. Acesso em 11/10/2016.