Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

Programa de Pós-Graduação em Matemática

Santiago Miler Quispe Mamani

Decomposição de Módulos Livres de Torção como Soma Direta de Módulos de Posto 1

Juiz de Fora

2016

Santiago Miler Quispe Mamani

Decomposição de Módulos Livres de Torção como Soma Direta de Módulos de Posto 1

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Juiz de Fora, na área de concentração em Álgebra, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Flaviana Andrea Ribeiro

Juiz de Fora

2016

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Quispe Mamani, Santiago Miler.
Decomposição de Módulos Livres de Torção como Soma Direta de Módulos de Posto 1 / Santiago Miler Quispe Mamani. – 2016.
73 f.

Orientadora: Flaviana Andrea Ribeiro
Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Programa de Pós-Graduação em Matemática, 2016.

1. Módulos livres de torção. 2. Módulos de posto 1. 3. Nós e Cúspides. I. Andrea Ribeiro, Flaviana, orient. II. Título.

SANTIAGO MILER QUISPE MAMANI

DECOMPOSIÇÃO DE MÓDULOS LIVRES DE TORÇÃO COMO SOMA DIRETA DE MÓDULOS DE POSTO I

Dissertação aprovada pela Comissão Examinadora abaixo elencada como requisito para a obtenção do título de Mestre em Matemática pelo Mestrado Acadêmico em Matemática do Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora.

Flaviana Andréa Ribeiro

Prof^{a}. Dr^{a}. Flaviana Andréa Ribeiro
(Orientadora)
Mestrado Acadêmico em Matemática
Instituto de Ciências Exatas - UFJF

Willian Versolati França

Prof. Dr. Willian Versolati França
Mestrado Acadêmico em Matemática
UFJF

Prof. Dr. Renato Vidal da Silva Martins
UFMG

Juiz de Fora, 25 de abril de 2016.

Dedico este trabalho

A Clemilda Cunha, por ser a pessoa mais especial pra mim

AGRADECIMENTOS

A Deus, que não sessou de interceder por mim em todo momento.

A minha mãe Marcelina e a meus irmãos, Edwin, David Yonatan, Junior Brisko e a minha irmã Kony Maxubel pelo apoio e compreensão.

A minha orientadora e amiga Professora Drª. Flaviana Andrea Ribeiro, pela ajuda na escolha do tema e pela forma como conduziu este trabalho, pelo apoio e incentivo e pela maneira como ensina e convive com seus alunos, se tornando um exemplo a ser seguido.

Ao Professor Dr. Willian Versolati França, pelo seu apoio incondicional, por ter me ensinado a maior parte do que hoje sei sobre Álgebra, motivando, a cada aula, o meu interesse por essa área e auxiliando, nesta fase, com a avaliação e a correção deste trabalho.

Ao professor Dr. Renato Vidal da Silva Martins, por ter aceitado o convite para fazer parte da banca que avaliou este trabalho, colaborando para o resultado final aqui apresentado.

A todos os professores que tornaram possível minha formação, pelos ensinamentos, críticas, conselhos e incentivo, em especial, aos professores Dr. Olimpio Hiroshi Miyagaki, Dr. Lonardo Rabelo, Dr. Sergio Guilherme de Assis Vasconcelos, sempre dispostos a aconselhar-me e a ajudar-me.

À Universidade Federal de Juiz de Fora e ao Departamento de Matemática.

À CAPES e FAPEMIG pelo apoio financeiro.

RESUMO

O objetivo deste trabalho é apresentar o resultado dado por Bass em [4], que determina uma condição no domínio de integridade R para que todo módulo finitamente gerado e livre de torção seja escrito como soma direta de módulos de posto 1. Mostramos que uma condição necessária é que todo ideal em R seja gerado por dois elementos, ou seja, que esses domínios sejam quase domínios de Dedekind. Em seguida, aplicamos o resultado na descrição de módulos livres de torção e de posto finito sobre os anéis de coordenadas de curvas singulares, cujas singularidades são nós ou cúspides.

Palavras-chave: Módulos livres de torção. Módulos de posto 1. Nós e Cúspides.

ABSTRACT

The aim of this paper is to present the result given by Bass in [4], which determines a condition on the integral domain R so that every finitely generated torsion free module is written as a direct sum of modules of rank 1. We show that a necessary condition is that all ideal in R is generated by two elements, in other words, that these domains are almost Dedekind domains. Then, we apply the result in the description of torsion free modules of finite rank over the coordinate rings of singular curves, whose singularities are nodal or cuspidal.

Key-words: Torsion free modules. Modules of rank 1. Nodal and Cuspidal.

LISTA DE ABREVIATURAS E SIGLAS

RM-anel	Anel com a condição mínima restrita
a.c.c.	condição da cadeia ascendente
d.c.c.	condição da cadeia descendente
f.g.	finitamente gerado
respect.	respetivamente
l.i.	linearmente independentes
s.p.g.	sem perda de generalidade
UFJF	Universidade Federal de Juiz de Fora

LISTA DE SÍMBOLOS

$\vdash$	Afirmação
$:=$	Define-se
$\cong$	Isomorfismo
$\varinjlim M_i$	Limite direto
$\exists!$	Existe e é único
$\rightarrow / \leftarrow$	Contradição
$\mathbb{N}$	$\{0, 1, 2, \cdots, n, \cdots\}$
$\mathbb{N}^*$	$\{1, 2, \cdots, n, \cdots\}$
$\langle x_1, x_2, \ldots, x_n \rangle$	Conjunto gerado por $\{x_1, x_2, \ldots, x_n\}$
$\mathfrak{A} \triangleleft R$	$\mathfrak{A}$ é um ideal do anel R

SUMÁRIO

1 INTRODUÇÃO

Em [1] Serre perguntou quando um módulo projetivo sobre o anel de polinômios em n variáveis, $\mathbb{K}[x_1, ..., x_n]$, sobre um corpo $\mathbb{K}$, é livre. Seshadri mostrou que o resultado é verdadeiro para $n = 2$. Mais precisamente, ele mostrou que todo $R[x]$-módulo M é estendido, isto é, é da forma $R[x] \otimes_R M_0$, para algum R-módulo M_0, sempre que R for um domínio de ideais principais [2] ou o anel de coordenadas de uma curva não singular afim sobre um corpo algebricamente fechado [3]. Modificando o argumento de Seshadri em [2], Bass [4] mostrou que R pode ser qualquer anel de Dedekind. Mais ainda, Bass exibiu um exemplo, mostrando que uma condição no fecho inteiro de R é, em geral, necessária para a conclusão.

Problemas como os listados anteriormente são frequentemente resolvidos mostrando-se que um módulo projetivo é a soma direta de módulos de posto 1.

O objetivo desse trabalho é o de apresentar o resultado dado por Bass em [4] que determina a condição no domínio de integridade R para que todo módulo finitamente gerado e livre de torção seja escrito como soma direta de módulos de posto 1. Veremos que uma condição necessária é que todo ideal em R seja gerado por dois elementos, ou seja, que esses domínios sejam quase domínios de Dedekind.

As motivações para o estudo desse tema foram os trabalhos de Seshadri, [6], e mais recentemente, [7] e [8], que caracterizam feixes livres de torção sobre curvas nodais e cuspidais (o caso cuspidal é tratado em [8]) usando ternos na normalização da curva. O ingrediente chave para para a determinação dos ternos é a descrição local do feixe $\mathcal{F}$ nos pontos singulares, isto é, $\mathcal{F}_p \simeq \mathcal{O}_p^{\oplus a} \oplus m_p^{\oplus b}$, onde $a + b$ é o posto do módulo $\mathcal{F}_p$ e p é um ponto singular (nó ou cúspide).

No Capítulo 2 listamos os principais resultados de Álgebra Comutativa que serão usados no texto. Esses resultado não foram demonstrados porque se tratam de resultados clássicos e porque a demonstração deles tornaria o trabalho muito extenso. No entanto, citamos referências onde esses resultados podem ser encontrados.

No Capítulo 3 fazemos um breve estudo das propriedades de módulos livres de torção, limites diretos, posto de um módulo, ideais fracionários e a definição de anéis com a condição de cadeia restrita. Resultados esses que são fundamentais para o desenvolvimento do trabalho.

No capítulo 4, apresentamos as condições necessárias e suficentes no domínio de integridade R para que todo módulo livre de torção e finitamente gerado possa ser escrito como soma direta de módulos livres de torção e posto 1. Mais precisamente, mostramos, seguindo [4], que R deve ser um domínio de integridade Noetheriano cujo fecho inteiro $\overline{R}$ é finito sobre R e tal que $\mu^*(R) \leq 2$, onde $\mu^*(R)$ é o máximo de $\mu_R(\mathfrak{A})$, $\mathfrak{A}$ ideal de R, e

$\mu(\mathfrak{A})$ é o número mínimo de geradores de $\mathfrak{A}$. Mostramos que esse é o caso de domínios de Dedekind. Finalmente, aplicamos o Teorema para decompor módulos sobre os anéis das funções regulares de duas curvas afins, cujas singulares são nó e cúspide.

2 RESULTADOS BÁSICOS

Neste capítulo apresentamos os principais conceitos e resultados de Álgebra Comutativa que serão citados no trabalho. Muitas demonstrações serão omitidas por se tratarem de resultados conhecidos, mas citaremos referências onde tais resultados, junto com suas demonstrações, podem ser encontrados.

De agora em diante, a palavra anel significará um anel comutativo com unidade, que representaremos pela letra R.

2.1 ANÉIS E IDEAIS

Teorema 2.1. *Todo anel* $R \neq \{0\}$ *possui pelo menos um ideal maximal.*

Demonstração. Ver [9], Teorema 1.3, pág.3. ■

Existem anéis com exatamente um ideal maximal, como os corpos. Esta ideia levou à seguinte definição.

Definição 2.1. Um anel R que possui exatamente um ideal maximal $\mathfrak{M}$ é chamado de *anel local*. O corpo $\mathbb{K} = R/\mathfrak{M}$ é chamado de *corpo de resíduos* de R.

Definição 2.2. Um anel R que possui um número finito de ideais maximais é chamado de *anel semi-local*.

Definição 2.3. O *radical de Jacobson* $\mathfrak{R}$ de R é definido como sendo a interseção de todos os ideais maximais de R.

$$\mathfrak{R} := \bigcap_{\mathfrak{M} \subseteq R} \mathfrak{M}, \quad \mathfrak{M} \text{ ideal maximal de } R \tag{2.1}$$

A seguinte Proposição caracteriza o radical de Jacobson.

Proposição 2.1. $x \in \mathfrak{R}$ *se, e somente se,* $1 - xy$ *é uma unidade em* R*, para todo* $y \in R$.

Demonstração. Ver [9], Proposição 1.9, pág.6. ■

Definição 2.4. Definimos o *ideal quociente* dos ideais $\mathfrak{a}, \mathfrak{b}$ do anel R, como sendo o ideal $(\mathfrak{a} : \mathfrak{b}) := \{x \in R : \ x\mathfrak{b} \subseteq \mathfrak{a}\}$.

Em particular, $(\langle 0 \rangle : \mathfrak{b})$ é chamado o *anulador* de $\mathfrak{b}$ e é também denotado por $\mathrm{Ann}(\mathfrak{b})$, ou seja, $\mathrm{Ann}(\mathfrak{b}) = \{x \in R \ : \ x\mathfrak{b} = \langle 0 \rangle\}$.

Se $\mathfrak{b}$ for um ideal principal $\langle x \rangle$, escreveremos $(\mathfrak{a} : x)$ no lugar de $(\mathfrak{a} : \langle x \rangle)$.

Definição 2.5. Definimos o *radical* do ideal $\mathfrak{a}$ de R como sendo

$$r(\mathfrak{a}) := \{x \in R \ : \ x^n \in \mathfrak{a}, \text{ para algum } n \in \mathbb{N}^*\}.$$

2.2 MÓDULOS

Definição 2.6. Se N, P são submódulos de M, definimos

$$(N : P) := \{x \in R : \ xP \subseteq N\},$$

que é um ideal de R.

Em particular, o ideal $(0 : M) = \{x \in R : xM = 0\}$ é chamado o *anulador* de M e será denotado por $\operatorname{Ann}(M)$.

Proposição 2.2 (Lema de Nakayama)**.** *Seja M um R-módulo finitamente gerado e $\mathfrak{a}$ um ideal de R contido no radical de Jacobson $\mathfrak{R}$ de R. Então, $\mathfrak{a}M = M$ implica $M = \{0\}$.*

Demonstração. Ver [9], Proposição 2.6, pág. 21. ■

Corolário 2.1. *Sejam M um R-módulo finitamente gerado, N um submódulo de M, $\mathfrak{a} \subseteq \mathfrak{R}$ um ideal. Então, $M = \mathfrak{a}M + N \Rightarrow M = N$.*

Demonstração. Ver [9], Corolário 2.7, pág. 22. ■

Proposição 2.3 (Propriedade Universal do Produto Tensorial)**.** *Sejam M, N R-módulos. Então, existe um par (T, g) consistido de um A-módulo T e uma aplicação R-bilinear*

$$g : M \times N \longrightarrow T,$$

com a seguinte propiedade:

Dado qualquer R-módulo P e qualquer aplicação R-bilinear $f : M \times N \longrightarrow P$, existe uma única aplicação R-linear $f' : T \longrightarrow P$ tal que $f = f' \circ g$.

Além disso, se (T, g) e (T', g') são dois pares com esta propriedade, então existe um único isomorfismo $j : T \longrightarrow T'$ tal que $j \circ g = g'$.

Demonstração. Ver [9], Proposição 2.12, pág. 24. ■

Observação 2.1. O módulo T acima é chamado de *Produto Tensorial* de M e N, e é denotado por $M \otimes_R N$ ou apenas $M \otimes N$, se não há ambiguidade sobre o anel R.

2.3 ANÉIS E MÓDULOS DE FRAÇÕES

Definição 2.7. Seja R um anel qualquer. Um *subconjunto multiplicativamente fechado* de R é um subconjunto S de R tal que $1 \in S$ e S é fechado sob a multiplicação.

Definamos a relação $\equiv$ sobre $R \times S$ como segue:

$$(x, s) \equiv (y, t) \Leftrightarrow (xt - ys)u = 0, \text{ para algum } u \in S. \tag{2.2}$$

Seja $\dfrac{x}{s} := \overline{(x, s)}$ e seja $S^{-1}R = \left\{\dfrac{x}{s} \,:\, \dfrac{x}{s} \in S^{-1}R\right\}$.

É possível colocar em $S^{-1}R$ uma estrutura de anel definindo adição e multiplicação das "frações" $\dfrac{a}{s}$ do mesmo modo como em álgebra elementar, isto é :

$$\begin{aligned} (x/s) + (y/t) &:= (xt + ys)/st \\ (x/s)(y/t) &:= xy/st \end{aligned}$$

Também temos um homomorfismo de anéis $f : R \to S^{-1}R$ definido por $f(x) = x/1$, que não é injetivo em geral.

Observação 2.2. Se R é um domínio de integridade e $S = R - \{0\}$, então $S^{-1}R$ é o corpo de frações de R.

O anel $S^{-1}R$ é chamado o *anel de frações* de R com respeito a S e tem a seguinte propriedade universal:

Proposição 2.4 (Propriedade Universal do Anel de Frações)**.** *Seja $g : R \to R_1$ um homomorfismo de anéis tal que $g(s)$ é uma unidade em R_1, para todo $s \in S$. Então, existe um único homomorfismo de anéis $h : S^{-1}R \to R_1$ tal que $g = h \circ f$.*

Demonstração. Ver [9], Proposição 3.1, pág. 37. ■

Exemplo 2.1. Seja $\mathfrak{p}$ um ideal primo de R. Então, $S = R - \mathfrak{p}$ é multiplicativamente fechado. Nesse caso, escrevemos $R_{\mathfrak{p}}$ para representar $S^{-1}R$.

Proposição 2.5. *O anel $R_{\mathfrak{p}}$ é anel local é um anel local cujo ideal maximal é o conjunto dos elementos da forma x/s, com $x \in \mathfrak{p}$.*

Demonstração. Sabendo que $R_{\mathfrak{p}}$ é um anel, devemos mostrar apenas que

$$\mathfrak{M} := \{\frac{x}{s} : x \in \mathfrak{p} \text{ e } s \in R - \mathfrak{p}\}$$

é um ideal tal que todo $x/s \in R_{\mathfrak{p}} - \mathfrak{M}$ é invertível.

Para ver que $\mathfrak{M}$ é um ideal, sejam x/s e $x'/s' \in \mathfrak{M}$ e $y/t \in R_{\mathfrak{p}}$. Então,

$$\frac{x}{s} + \frac{x'}{s'} = \frac{xs' + x's}{ss'} \in \mathfrak{M}$$

e

$$(\frac{y}{t})(\frac{x}{s}) = \frac{xy}{st} \in \mathfrak{M},$$

pois $x, x' \in \mathfrak{p}$ e $\mathfrak{p}$ é um ideal.

Para mostrar que $\mathfrak{M}$ é o único ideal maximal de $R_{\mathfrak{p}}$, seja $x/s \in R_{\mathfrak{p}} - \mathfrak{M}$. Então, $x \notin \mathfrak{p}$ e $s/x \in R_{\mathfrak{p}}$. Logo, $1 = (x/s)(s/x)$, ou seja x/s é invertível em $R_{\mathfrak{p}}$. ■

Definição 2.8. O processo de passar de R a $R_{\mathfrak{p}}$ é chamado *localização* de R em $\mathfrak{p}$.

A construção de $S^{-1}R$ pode ser estendida para um R-módulo M.

Definimos a relação $\equiv$ sobre $M \times S$ como segue:

$$(m, s) \equiv (m', s') \Leftrightarrow \exists t \in S \;\; tal \; que \quad t(sm' + s'm) = 0 \tag{2.3}$$

Como antes, esta é uma relação de equivalência e o conjunto

$$S^{-1}M = \{\frac{m}{s} : m \in M \text{ e } s \in S\}$$

com as operações definidas por:

$$\begin{aligned} (m/s) + (m'/t) &:= (mt + m's)/st \text{ e} \\ (a/s)(m/t) &:= am/st, \text{ onde } a/s \in S^{-1}R, \end{aligned}$$

é um $S^{-1}R$-módulo.

Seja $u : M \to N$ um R-homomorfismo de módulos. Então, u define um $S^{-1}R$-homomorfismo de módulos $S^{-1}u : S^{-1}M \to S^{-1}N$, onde $S^{-1}u$ aplica m/s a $u(m)/s$. Temos também que $S^{-1}(v \circ u) = (S^{-1}v) \circ (S^{-1}u)$.

Proposição 2.6. *A operação S^{-1} é exata, isto é, se $M' \xrightarrow{f} M \xrightarrow{g} M''$ é exata em M, então $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ é exata em $S^{-1}M$.*

Demonstração. Ver [9], Proposição 3.3, pág. 39. ■

Proposição 2.7. *Seja M um R-módulo. Então, os $S^{-1}R$-módulos $S^{-1}M$ e $S^{-1}R \otimes_R M$ são isomorfos; mais precisamente, existe um único isomorfismo $f : S^{-1}R \otimes_R M \longrightarrow S^{-1}M$ para o qual $f((x/y) \otimes m) = xm/s$, para todo $x \in R$, $m \in M$, $s \in S$.*

Demonstração. Ver [9], Proposição 3.5, pág. 39. ■

Proposição 2.8. *Seja M um R-módulo. Então, as seguintes afirmações são equivalentes:*

i) $M = \{0\}$.

ii) $M_{\mathfrak{p}} = \{\bar{0}\}$ *para todos os ideais primos* $\mathfrak{p}$ *de* R.

iii) $M_{\mathfrak{M}} = \{\bar{0}\}$ *para todos os ideais maximais* $\mathfrak{M}$ *de* R.

Demonstração. Ver [9], Proposição 3.8, pág. 40. ■

2.4 DECOMPOSIÇÃO PRIMÁRIA

Definição 2.9. Sejam R um anel e $\mathfrak{q}$ um ideal de R. Dizemos que $\mathfrak{q}$ é *primário* se:

i) $\mathfrak{q} \neq R$

ii) $xy \in \mathfrak{q}$, então $x \in \mathfrak{q}$ ou $y^n \in \mathfrak{q}$ para algum $n \in \mathbb{N}^*$

Lema 2.1. *Sejam R um anel e $\mathfrak{q}$ um ideal de R. O ideal $\mathfrak{q}$ é primário se, e somente se, $R/\mathfrak{q} \neq \{\bar{0}\}$ e todo divisor de zero em $R/\mathfrak{q}$ é nilpotente.*

Demonstração. ($\rightarrow$) Como $\mathfrak{q}$ é primário, então se segue diretamente da definição que $R/\mathfrak{q} \neq \{\bar{0}\}$. Agora, seja $\bar{x} \in R/\mathfrak{q}$, $\bar{x} \neq \bar{0}$ tal que $\bar{x}$ é um divisor de zero. Então, existe $\bar{y} \in R/\mathfrak{q}$, $\bar{y} \neq \bar{0}$ tal que $\bar{x} \cdot \bar{y} = \bar{0}$. Como $\bar{x} \neq \bar{0}$ e $\bar{y} \neq \bar{0}$, vemos que $x, y \notin \mathfrak{q}$. Por outro lado, $\bar{x} \cdot \bar{y} = \overline{xy} = \bar{0}$, isto é $xy \in \mathfrak{q}$. Agora, como $y \notin \mathfrak{q}$ e $xy \in \mathfrak{q}$, então $x^n \in \mathfrak{q}$, para algum $n \in \mathbb{N}^*$. Assim, $\bar{x}^n = \bar{0}$. Portanto, $\bar{x}$ é nilpotente.

($\leftarrow$) Como, $R/\mathfrak{q} \neq \{\bar{0}\}$, então $\mathfrak{q} \neq R$. Agora, sejam $x, y \in R$ tais que $xy \in \mathfrak{q}$

- Se $x \in \mathfrak{q}$, então $\mathfrak{q}$ é primário.
- Se $y \in \mathfrak{q}$, então $\mathfrak{q}$ é primário.
- Se $x, y \notin \mathfrak{q}$, então $\bar{x} \neq \bar{0}$ e $\bar{y} \neq \bar{0}$. Por outro lado, $\bar{x} \cdot \bar{y} = \bar{0}$, pois $xy \in \mathfrak{q}$. Assim, pela hipótese, existem $m, n \in \mathbb{N}^*$ tais que $\bar{x}^m = \bar{0}$, $\bar{y}^n = \bar{0}$. Portanto, $x^m \in \mathfrak{q}$, $y^n \in \mathfrak{q}$.

■

Proposição 2.9. *Seja $\mathfrak{q}$ um ideal de R, $\mathfrak{q}$ primário. Então, $r(\mathfrak{q})$ é o menor ideal primo contendo $\mathfrak{q}$.*

Demonstração. Ver [9], Proposição 4.1, pág. 50. ■

Definição 2.10. Se $\mathfrak{q}$ é primário e $\mathfrak{p} = r(\mathfrak{q})$, então dizemos que $\mathfrak{q}$ é $\mathfrak{p}$-primário.

Proposição 2.10. *Seja* $\mathfrak{a}$ *um ideal de* R. *Se* $\mathfrak{M} = r(\mathfrak{a})$ *é maximal, então* $\mathfrak{a}$ *é primário. Em particular, as potências de um ideal maximal* $\mathfrak{M}$ *são* $\mathfrak{M}$*-primárias.*

Demonstração. Ver [9], Proposição 4.2, pág. 51. ∎

Lema 2.2. *Se* $\mathfrak{q}_i$ *com* $1 \leq i \leq n$ *são* $\mathfrak{p}$*-primários, então* $\mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *é* $\mathfrak{p}$*-primário.*

Demonstração. Ver [9], Lema 4.4, pág. 51. ∎

Definição 2.11. Uma *decomposição primária* de um ideal $\mathfrak{a}$ em R é uma expressão de $\mathfrak{a}$ como uma interseção finita de ideais primários $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$.
Diremos que $\mathfrak{a}$ é *decomponível* se $\mathfrak{a}$ admite uma decomposição primária. Neste caso, se

i) todos os $r(\mathfrak{q}_i)$ são distintos, e

ii) temos que $\bigcap_{j \neq i}^{n} \mathfrak{q}_j \not\subseteq \mathfrak{q}_j$ para $1 \leq i \leq n$

a decomposição primária é dita *minimal*.

Observação 2.3. Notemos que, em geral, uma tal decomposição primária não precisa existir. Porém, toda decomposição primária pode ser reduzida a uma minimal.

Definição 2.12. Sejam $\mathfrak{a}$ um ideal de R e $\mathfrak{a} = \bigcap_{l=1}^{n} \mathfrak{q}_l$ uma decomposição primária minimal de $\mathfrak{a}$.

$$\operatorname{Assoc}(\mathfrak{a}) = \{r(\mathfrak{q}_l) \ : \ l = 1, \cdots, m\}.$$

Assim, se $\mathfrak{p}_l \in \operatorname{Assoc}(\mathfrak{a})$, então $\mathfrak{p}_l$ é um ideal primo associado a $\mathfrak{a}$.

Teorema 2.2 (1° Teorema de Unicidade). *Sejam* $\mathfrak{a}$ *um ideal de* R *e* $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *uma decomposição primária minimal de* $\mathfrak{a}$. *Seja* $\mathfrak{p}_\mathfrak{i} = r(\mathfrak{q}_\mathfrak{i})$ *para* $i = 1, \ldots, n$. *Então, os ideias* $\mathfrak{p}_\mathfrak{i}$ *são precisamente os ideais primos da forma* $r(\mathfrak{a} : x)$, *tais que* $x \in R$. *Portanto, não dependem de uma decomposição particular de* $\mathfrak{a}$.

Demonstração. Ver [9], Teorema 4.5, pág. 52. ∎

Os ideiais primos $\mathfrak{p}_\mathfrak{i}$ dados no Teorema 2.2 são chamados ideias associados ou *pertencentes* a $\mathfrak{a}$. Os ideais minimais do conjunto $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_\mathfrak{n}\}$ são chamados ideiais *minimais* ou *isolados* pertencentes a $\mathfrak{a}$. Os outros são chamados primos *mergulhados*.

Proposição 2.11. *Sejam* $\mathfrak{a}$ *um ideal de* R, $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *uma decomposição primária minimal de* $\mathfrak{a}$. *Seja* $\mathfrak{p}$ *um ideal primo de* R *tal que* $\mathfrak{p} \supseteq \mathfrak{a}$. *Então, existe* $\mathfrak{p}_{j_0} \in \operatorname{Assoc}(\mathfrak{a})$, $\mathfrak{p}_{j_0}$ *isolado, tal que* $\mathfrak{p}_{\mathfrak{j}_\circ} \subset \mathfrak{p}$.

Em particular, os ideais primos isolados de Assoc($\mathfrak{a}$) *são exatamente os elementos minimais no conjunto de todos os ideais primos que contém* $\mathfrak{a}$.

Demonstração. Ver [9], Proposição 4.6, pág. 52. ■

2.5 DEPENDÊNCIA INTEIRA E VALORIZAÇÃO

2.5.1 Dependência Integral

Definição 2.13. Sejam R_1 um anel, R um subanel de R_1 (tal que $1 \in R$). Um elemento x de R_1 é dito ser *inteiro* sobre R se x é uma raiz de um polinômio mônico com coeficientes em R, isto é, se x satisfaz uma equação da forma:

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{2.4}$$

onde os a_i são elementos de R.

Claramente, todo elemento de R é inteiro sobre R.

Proposição 2.12. *As seguintes afirmações são equivalentes:*

i) $y_0 \in R_1$ *é inteiro sobre* R.

ii) $R[y_0]$ *é um* R*-módulo finitamente gerado.*

iii) $R[y_0]$ *está contido em um subanel* C *de* R_1 *tal que* C *é um* R*-módulo finitamente gerado.*

Demonstração. Ver [9], Proposição 5.1, pág. 59. ■

Corolário 2.2. *Seja* y_i *com* $1 \leq i \leq n$ *elementos de* R_1, *cada* y_i *inteiro sobre* R. *Então, o anel* $R[y_1, y_2 \cdots, y_n]$ *é um* R*-módulo finitamente gerado.*

Demonstração. Ver [9], Corolário 5.2, pág. 60. ■

Corolário 2.3. *O conjunto* C *dos elementos de* R_1 *que são inteiros sobre* R *é um subanel de* R_1 *contendo* R.

Demonstração. Ver [9], Corolário 5.3, pág.60. ■

O anel C no Corolário 2.3 é chamado o *fecho inteiro* de R em R_1. Se $C = R$, então R é dito ser *integralmente fechado* em R_1. Se $C = R_1$, então o anel R_1 é dito ser *inteiro* sobre R.

Teorema 2.3. *Sejam $R \subset R_1$ anéis, R_1 inteiro sobre R e $\mathfrak{q}$ um ideal primo de R_1. Seja $\mathfrak{p} = \mathfrak{q} \cap R$, a contração de $\mathfrak{q}$ em R. Então, $\mathfrak{q}$ é maximal, se e somente se, $\mathfrak{p}$ for maximal.*

Demonstração. Ver [9], Corolário 5.8, pág. 61. ■

Teorema 2.4. *Sejam $R \subset R_1$ anéis, R_1 inteiro sobre R e $\mathfrak{p}$ um ideal primo de R_1. Então existe um ideal primo $\mathfrak{q}$ de R_1 tal que $\mathfrak{q} \cap R = \mathfrak{p}$.*

Demonstração. Ver [9], Teorema 5.10, pág. 62. ■

2.5.2 Domínios de integridade integralmente fechados

Um domínio de integridade é dito ser *integralmente fechado* (sem qualificação) se for integralmente fechado em seu corpo de frações.

Proposição 2.13. *Seja R um domínio de integridade. Então, as seguintes afirmações são equivalentes:*

i) *R é integralmente fechado.*

ii) *$R_{\mathfrak{p}}$ é integralmente fechado, para cada ideal primo $\mathfrak{p}$.*

iii) *$R_{\mathfrak{M}}$ é integralmente fechado, para cada ideal maximal $\mathfrak{M}$.*

Demonstração. Ver [9], Proposição 5.13, pág. 63. ■

2.5.3 Anéis de valorização

Sejam R um domínio de integridade, $\mathbb{K}$ seu corpo de frações. R é um *anel de valorização* de $\mathbb{K}$ se para cada $x \neq 0$, $x \in R$ ou $x^{-1} \in R$.

Proposição 2.14. *As seguintes afirmações se cumprem:*

i) *R é um anel local.*

ii) *Se R' é um anel tal que $R \subseteq R' \subseteq \mathbb{K}$, então R' é um anel de valorização de K.*

iii) *R é integralmente fechado em $\mathbb{K}$.*

Demonstração. Ver [9], Proposição 5.18, pág.65. ■

2.6 CONDIÇÃO DE CADEIA

Seja Σ um conjunto parcialmente ordenado pela relação $\leq$.

Proposição 2.15. *As seguintes condições sobre Σ são equivalentes:*

i) Toda sequência crescente $x_1 \leq x_2, \ldots$ em Σ é estacionária, isto é, existe n tal que $x_n = x_{n+1} = \ldots$

ii) Todo subconjunto não-vazio de Σ tem um elemento maximal.

Se Σ é o conjunto de submódulos do módulo M, ordenado pela relação $\subseteq$, então tal condição $i)$ é chamada *condição de cadeia ascendente* (a.c.c., do inglês ascending chain condition) e $ii)$ é chamada *condição maximal.* Um módulo M que satisfaça qualquer uma destas condições equivalentes é dito ser *Noetheriano*[1].

Se Σ é o conjunto de submódulos do módulo M, ordenado pela relação $\supseteq$, então tal condição $i)$ é chamada *condição de cadeia descendente* (d.c.c., do inglês descending chain condition) e $ii)$ é chamada *condição minimal.* Um módulo M que satisfaça qualquer uma destas condições equivalentes é dito ser *Artiniano*[2].

Proposição 2.16. *M é um R-módulo Noetheriano se, e somente se, todo submódulo de M é finitamente gerado.*

Demonstração. Ver [9], Proposição 6.2, pág. 75. ∎

Uma *cadeia* de submódulos de um módulo M é uma sequência $\{M_i\}_{i=0}^n$ de submódulos de M tal que

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = \{0\}. \tag{2.5}$$

O inteiro positivo n é chamado *comprimento* da cadeia. Uma série de composição de M é uma cadeia maximal, isto é, uma cadeia na qual não podemos inserir submódulos extras. Isto equivale a dizer que cada quociente M_{i-1}/M_i, para $1 \leq i \leq n$, é *simples*, ou seja, não tem submódulos exceto 0 e ele mesmo.

Proposição 2.17. *Suponha que M tem uma série de composição de comprimento n. Então toda série de composição de M tem comprimento n, e toda cadeia em M pode ser estendida para uma série de composição.*

Demonstração. Ver [9], Proposição 6.7, pág. 77. ∎

Denotaremos por $l(M)$ o comprimento de uma série de composição do módulo M. Escreveremos $l(M) = \infty$ se M não tiver uma série de composição.

---

[1] Nome devido a Emmy Noether

[2] Nome devido a Emil Artin

Proposição 2.18. *Um módulo M tem uma série de composição se e somente se satisfaz a.c.c. e d.c.c..*

Demonstração. Ver [9], Proposição 6.8, pág. 77. ■

Considerando o caso particular de módulos sobre um corpo $\mathbb{K}$, isto é, $\mathbb{K}$-espaço vetorial temos:

Proposição 2.19. *Para um $\mathbb{K}$-espaço vetorial V as seguintes condições são equivalentes:*

i) dimensão finita.

ii) comprimento finito.

iii) a.c.c.

iv) d.c.c.

Além disso, se estas condições são satisfeitas, comprimento é igual a dimensão.

Demonstração. Ver [9], Proposição 6.10, pág. 78. ■

2.7 ANÉIS NOETHERIANOS

Lembremos que um anel R é dito ser *Noetheriano* se satisfaz as seguintes três condições equivalentes:

i) Todo conjunto não-vazio de ideais em R tem um elemento maximal.

ii) Toda cadeia ascendente de ideais em R é estacionária.

iii) Todo ideal em R é finitamente gerado.

Proposição 2.20. *Se R é Noetheriano e φ é um homomorfismo sobrejetor de R sobre um anel R_1, então R_1 é Noetheriano.*

Demonstração. Ver [9], Proposição 7.1, pág. 80. ■

Proposição 2.21. *Se R é Noetheriano e S é qualquer subconjunto multiplicativamente fechado de R, então $S^{-1}R$ é Noetheriano.*

Demonstração. Ver [9], Proposição 7.3, pág. 80. ■

Exemplo 2.2. Se R é Noetheriano e $\mathfrak{p}$ é um ideal primo de R, então $R_{\mathfrak{p}}$ é Noetheriano.

Teorema 2.5 (Teorema da Base de Hilbert)**.** *Se R é Noetheriano, então o anel de polinômios $R[x]$ é Noetheriano.*

Demonstração. Ver [9], Teorema 7.5, pág. 81. ■

Corolário 2.4. *Se R é Noetheriano, então $R[x_1, x_2, \ldots, x_n]$ é Noetheriano.*

Teorema 2.6. *Em um anel Noetheriano R todo ideal tem uma decomposição primária.*

Demonstração. Ver [9], Teorema 7.13, pág. 83. ■

2.8 ANÉIS ARTINIANOS

Um anel Artiniano é aquele que satisfaz a d.c.c. ou, equivalentemente, a condição mínima sobre ideais.

Proposição 2.22. *Em um anel Artiniano R todo ideal primo é maximal.*

Demonstração. Ver [9], Proposição 8.1, pág. 89. ■

Corolário 2.5. *Em um anel Artiniano o nilradical é igual ao radical de Jacobson.*

Proposição 2.23. *Um anel Artiniano tem só um número finito de ideais maximais.*

Demonstração. Ver [9], Proposição 8.3, pág. 89. ■

Uma *cadeia* de ideais primos de um anel R, é uma sequência estritamente crescente $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ de ideais primos de R; o comprimento da cadeia é n.

Definimos a dimensão de R como sendo o supremo dos comprimentos de todas as cadeias de ideais primos em R. A dimensão de R é um inteiro $n \geq 0$ ou $+\infty$ (assumindo $R \neq \{0\}$).

Exemplo 2.3. Um corpo tem dimensão 0 e o anel $\mathbb{Z}$ tem dimensão 1.

Teorema 2.7. *Um anel R é Artiniano, se e somente se R é Noetheriano e* $\dim R = 0$

Demonstração. Ver [9], Teorema 8.5, pág. 90. ■

2.9 ANÉIS DE VALORIZAÇÃO DISCRETA

Proposição 2.24. *Seja R um domínio Noetheriano de dimensão* 1. *Então, todo ideal $\mathfrak{a}$ não-nulo em R pode ser expressado únicamente como um produto de ideais primários cujos radicais são todos distintos.*

Demonstração. Ver [9], Proposição 9.1, pág. 93. ∎

Seja $\mathbb{K}$ um corpo. Uma *valorização discreta* sobre $\mathbb{K}$ é uma aplicação sobrejetora v de $\mathbb{K}^*$ em $\mathbb{Z}$ (onde $\mathbb{K}^* = \mathbb{K} - \{0\}$ é o grupo multiplicativo de $\mathbb{K}$) tal que

1. $v(xy) = v(x) + v(y)$, isto é, v é um homomorfismo de grupos e
2. $v(x + y) \geq \min\{v(x), v(y)\}$.

O conjunto consistido de 0 e todos os $x \in \mathbb{K}^*$ tal que $v(x) \geq 0$ é um anel, chamado o *anel de valorização* de v. É frequentemente conveniente estender v a todo $\mathbb{K}$ colocando $v(0) = +\infty$.

Um domínio de integridade R é um *anel de valorização discreta* se existe uma valorização discreta v do seu corpo de frações $\mathbb{K}$, tal que R é um anel de valorização de v.

Proposição 2.25. *Sejam R um domínio Noetheriano local de dimensão um, $\mathfrak{M}$ seu ideal maximal, $\mathbb{K} = R/\mathfrak{M}$ seu corpo residual. Então, as seguintes afirmações são equivalentes:*

i) R é um anel de valorização discreta.

ii) R é integralmente fechado.

iii) $\mathfrak{M}$ é um ideal principal.

iv) $\dim_{\mathbb{K}}(\mathfrak{M}/\mathfrak{M}^2) = 1$.

v) Todo ideal não-nulo é potência de $\mathfrak{M}$.

vi) Existe $x \in R$ tal que todo ideal não-nulo é da forma $\left\langle x^k \right\rangle$, com $k \geq 0$.

Demonstração. Ver [9], Proposição 9.2, pág. 94. ∎

2.10 DOMÍNIOS DE DEDEKIND

Teorema 2.8. *Seja R um domínio Noetheriano de dimensão um. Então, as seguintes afirmações são equivalentes:*

i) R é integralmente fechado.

ii) Todo ideal primário em R é uma potência de um primo.

iii) Todo anel local $R_{\mathfrak{p}}$ com $\mathfrak{p} \neq 0$ é um anel de valorização discreta.

Demonstração. Ver [9], Teorema 9.3, pág. 95. ∎

Um anel satisfazendo as condições de 2.8 é chamado um domínio de Dedekind.

Corolário 2.6. *Em um domínio de Dedekind todo ideal não-nulo tem uma fatoração única como um produto de ideais primos.*

Demonstração. Ver [9], Corolário 9.4, pág. 95. ■

3 CONCEITOS FUNDAMENTAIS

Neste capítulo, apresentaremos alguns resultados de álgebra comutativa que serão importantes para o restante do trabalho.

Em todo lugar, a palavra anel significará um anel comutativo com unidade, que normalmente será representado pela letra R.

3.1 MÓDULOS LIVRES DE TORÇÃO

Definição 3.1. Sejam R um domínio de integridade e M um R-módulo. Um elemento $x \in M$ é um *elemento de torção* de M se $\operatorname{Ann}(x) := \{a \in R; ax = 0\} \neq \{0\}$, isto é, se x é anulado por algum elemento não-nulo de R.

Proposição 3.1. *Sejam R um domínio de integridade e M um R-módulo. Os elementos de torção de M formam um submódulo de M, chamado o submódulo de torção de M e denotado por $T(M)$.*

Demonstração. De fato,

$$T(M) = \{x \in M \ : \ \operatorname{Ann}(x) \neq \{0\}\} = \{x \in M \ : \ \exists a \in R, a \neq 0 \ tal \ que \ ax = 0\}$$

$$T(M) = \{x \in M \ : \ ax = 0, \ para \ algum \ não \ nulo \ a \in R\}.$$

Sejam $m_1, m_2 \in T(M)$. Então, existem $a_1, a_2 \in R$, não nulos, tais que $a_1m_1 = 0$ e $a_2m_2 = 0$. Logo, $a_1a_2(m_1 + m_2) = (a_1a_2)m_1 + (a_1a_2)m_2 = a_2(a_1m_1) + a_1(a_2m_2) = 0$. Como R é um domínio de integridade, $a_1a_2 \neq 0$ e $m_1 + m_2 \in T(M)$.

Sejam $a \in R$, $m \in T(M)$ e $b \in R$, não nulo, tal que $bm = 0$. Então, $b(am) = a(bm) = 0$ e $ab \neq 0$. Logo, $am \in T(M)$. ∎

Definição 3.2. Um R-módulo M é dito *livre de torção* se $T(M) = \{0\}$.

Exemplo 3.1. Seja R um domínio de integridade. Todo R-módulo é livre é livre de torção.

Exemplo 3.2. Seja R um domínio de integridade. Todo R-módulo projetivo é livre de torção. De fato, todo módulo projetivo é somando direto de um módulo livre.

Teorema 3.1. *Seja R um domínio de integridade local. Então todo R-módulo projetivo finitamente gerado é livre.*

Demonstração. Seja $S = \{m_1, \ldots, m_r\}$ um conjunto minimal de geradores de M, isto é, nenhum subconjunto próprio de S gera M. Sejam $F = \bigoplus_{i=1}^{r} R$ módulo livre e $\phi : F \to M$ o

R-homomorfismo sobrejetor definido por $\phi(e_i) = m_i$, onde $\{e_1, \ldots, e_r\}$ é a base canônica de F. Então, como M é projetivo, $F = K \oplus M$, onde $K = \ker(\phi)$. Afirmamos que $K \subset \mathfrak{M}F$, onde $\mathfrak{M}$ é o único ideal maximal de R. Suponhamos por absurdo que exista $y \in K$ tal que $y \notin \mathfrak{M}F$. Como $K \subset F$, temos que $y = \sum_{i=1}^{r} c_i e_i$, com $c_i \in R$, para todo i e $c_j \notin \mathfrak{M}$ para algum j. Mas $0 = \phi(y) = \phi(\sum_{i=1}^{r} c_i e_i) = \sum_{i=1}^{r} c_i \phi(e_i) = \sum_{i=1}^{r} c_i m_i$, nos diz que $c_j m_j = \sum_{i \neq j} c_i e_i$ e, portanto, $m_j = (c_j)^{-1} \sum_{i=1}^{r} c_i e_i$, pois c_j é invertível em R. Absurdo, já que S é minimal. Logo, $K \subset \mathfrak{M}F$ e $F = \mathfrak{M}F + M$. Pelo Corolário 2.1 (Lema de Nakayama), segue que $F = M$. ■

Com o objetivo de estudar os elementos de torção de um R-módulos apresentaremos o conceito de limite direto de módulos.

3.2 LIMITES DIRETOS

Definição 3.3. Seja R um conjunto não vazio. Dizemos que R é *parcialmente ordenado* e escrevemos $(R, \leq)$ se:

i) $x \leq x, \quad \forall x \in R$ (Reflexiva)

ii) $x \leq y \quad \text{e} \quad y \leq x \quad \Rightarrow \quad x = y$ (Anti-simétrica)

iii) $x \leq y \quad \text{e} \quad y \leq z \quad \Rightarrow \quad x \leq z$ (Transitiva)

Definição 3.4. Um conjunto parcialmente ordenado I é chamado um *conjunto dirigido* se, para cada par $i, j \in I$, $\exists k \in I$ tal que $i \leq k$ e $j \leq k$.

3.2.1 Construção do Limite Direto

Sejam R um anel, I um conjunto dirigido e $\{M_i\}_{i \in I}$ uma família de R-módulos indexados por I. Para cada par i, j em I tal que $i \leq j$, seja $\mu_{ij} : M_i \longrightarrow M_j$ um R-homomorfismo de módulos, satisfazendo os seguintes axiomas:

(1) μ_{ii} é a aplicação identidade de M_i, para todo $i \in I$, e

(2) $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ sempre que $i \leq j \leq k$.

Dizemos nesse caso que os módulos M_i e os homomorfismos μ_{ij} formam um sistema direto $\mathbb{M} = (M_i, \mu_{ij})$ sobre o conjunto dirigido I.

Construiremos a seguir um R-módulo M chamado o limite direto do sistema direto $\mathbb{M}$.

Seja $C = \bigoplus_{i\in I} M_i$ e identificamos cada módulo M_i com sua imagem canônica em C. Seja D o submódulo de C gerado por todos os elementos da forma $x_i - \mu_{ij}(x_i)$ onde $i \leq j$ e $x_i \in M_i$. Sejam $M = C/D$, $\mu : C \longrightarrow M$ a projeção canônica e $\mu_i = \mu\,|_{M_i}$.

O módulo M, ou mais corretamente, o par consistindo de M e a família de homomorfismos $\mu_i : M_i \longrightarrow M$, é chamado o limite direto do sistema direto $\mathbb{M}$ e será denotado por $\varinjlim M_i$. Segue da construção que $\mu_i = \mu_j \circ \mu_{ij}$, sempre que $i \leq j$.

Observação 3.1. Os elementos de $C = \bigoplus_{i\in I} M_i$ são famílias $(x_i)_{i\in I}$ tais que $x_i \in M_i$, para cada $i \in I$, e tais que $x_i \neq 0$ somente para um número finito de índices $i \in I$. Por isso, é usual representar um elemento de C como uma soma formal,

$$\sum_{i\in I} x_i = x_{i_1} + x_{i_2} + \cdots + x_{i_s}, \text{ para algum } s \in \mathbb{N}.$$

Proposição 3.2. *Seja (M_i, μ_{ij}) um sistema direto com o conjunto dirigido de índices I, e seja a i-ésima aplicação injetiva $\lambda_i : M_i \to \bigoplus_{i\in I} M_i$.*

i) Todo elemento de M pode ser escrito na forma $\mu_i(x_i)$ para algum $i \in M_i$ e algum $x_i \in M_i$.

ii) $\lambda_i(x_i) + D = D$, se e somente se, $\mu_{it}(x_i) = 0$, para algum $t \geq i$.

Demonstração. (i) Sendo $\mu : C = \bigoplus_{i\in I} M_i \longrightarrow M = C/D$ a projeção canônica, dado $x \in M$, existem $i_1, i_2, \ldots, i_r \in I$ tais que $x_{i_1}, x_{i_2}, \ldots, x_{i_r} \neq 0$ e

$$x = \mu(\sum_{n=1}^{r} x_{i_n}) = \mu(x_{i_1} + x_{i_2} + \cdots + x_{i_r}) = (x_{i_1} + x_{i_2} + \cdots + x_{i_r}) + D.$$

Seja $k \in I$ tal que $i_s \leq k$, $\forall s = 1, 2, \cdots, r$. A existência de tal k está garantida, pois I é um conjunto dirigido. Então,

$$\begin{aligned} x = \mu(\sum_{n=1}^{r} x_{i_n}) &= (x_{i_1} + x_{i_2} + \cdots + x_{i_r}) + D \\ &= (x_{i_1} - \mu_{i_1k}(x_{i_1}) + \mu_{i_1k}(x_{i_1}) + \cdots + x_{i_r} - \mu_{i_rk}(x_{i_r}) + \mu_{i_rk}(x_{i_r})) + D \\ &= (\mu_{i_1k}(x_{i_1}) + \cdots + \mu_{i_rk}(x_{i_r})) + D = \mu_k(x_k). \end{aligned}$$

Como $x_k = \mu_{i_1k}(x_{i_1}) + \cdots + \mu_{i_rk}(x_{i_r}) \in M_k$, temos $x = \mu(x_k) = \mu_k(x_k)$.

(ii) Se, $\mu_{it}(x_i) = 0$, para algum $t \geq i$, então, $\lambda_t(\mu_{it}(x_i)) = 0$. Assim, considerando $D = \langle\{\lambda_k(\mu_{jk}(x_j)) - \lambda_j(x_j) \ : \ j \leq k \text{ e } x_j \in M_j\}\rangle$, obtemos $\lambda_i(x_i) - \lambda_t(\mu_{it}(x_i)) \in D$. Portanto, $\lambda_i(x_i) + D = D$.

Para a recíproca, assumimos $\lambda_i(x_i) + D = D$, isto é, $\lambda_i(x_i) \in D$.
Já que qualquer múltiplo escalar de um gerador de $D = \{\lambda_k(\mu_{jk}(x_j)) - \lambda_j(x_j),\ \text{onde } j \leq k\}$ tem a mesma forma, existe uma expressão

$$\lambda_i(x_i) = \sum_j [\lambda_k(\mu_{jk}(x_j)) - \lambda_j(x_j)] \in D$$

Escolhamos um índice $t \in I$ maior do que qualquer um dos índices nesta expressão. Claramente,

$$\begin{aligned}
\lambda_t(\mu_{it}(x_i)) &= [\lambda_t(\mu_{it}(x_i)) - \lambda_i(x_i)] + \lambda_i(x_i) \\
&= [\lambda_t(\mu_{it}(x_i)) - \lambda_i(x_i)] + \sum_j [\lambda_k(\mu_{jk}(x_j)) - \lambda_j(x_j)].
\end{aligned}$$

Podemos reescrever cada um dos termos do lado direito como uma soma de geradores em que o índice do lado direito é t da seguinte forma:

$$\lambda_k(\mu_{jk}(x_j)) - \lambda_j(x_j) = [\lambda_t(\mu_{jt}(x_j)) - \lambda_j(x_j)] + [\lambda_t(\mu_{kt}(-\mu_{jk}(x_j))) - \lambda_k(-\mu_{jk}(x_j))]$$

pois $\mu_{kt} \circ \mu_{jk} = \mu_{jt}$, pela definição de sitema direto. Portanto, podemos escrever

$$\lambda_t(\mu_{it}(x_i)) = \sum [\lambda_t(\mu_{jt}(x_j)) - \lambda_j(x_j)]$$

após uma alteração de notação. Além disso, podemos assumir que há uma combinação entre todos os termos com o mesmo índice de modo que o elemento se expresse de forma única como $\sum_p \lambda_p(x_p)$.

Concluimos que se, $j \neq t$, então $\lambda_j(x_j) = 0$, daqui $x_j = 0$, para o elemento $\lambda_t(\mu_{it}(x_i))$ tem a j-ésima coordenada 0. Se $j = t$, então $\lambda_t(\mu_{tt}(x_t)) - \lambda_t(x_t) = 0$ porque μ_{tt} é a identidade. Assim, cada termo à direita é 0, de modo que $\lambda_t(\mu_{it}(x_i)) = 0$, de onde $\mu_{it}(x_i) = 0$

$\blacksquare$

Proposição 3.3 (Propriedade Universal do Limite Direto)**.** *Seja N um R-módulo e, para $i \in I$, seja $\alpha_i : M_i \longrightarrow N$ um R-homomorfismo tal que $\alpha_i = \alpha_j \circ \mu_{ij}$ sempre que $i \leq j$. Então, existe um único homomorfismo $\alpha : M \longrightarrow N$ tal que $\alpha_i = \alpha \circ \mu_i$ para todo $i \in I$.*

Demonstração. Sejam $\{M_i\}_{i\in I}$ uma família de R-módulos indexados por um conjunto dirigido I, $C = \bigoplus_{i\in I} M_i$, $D = \langle\{x_i - \mu_{ij}(x_i) :\ i,j \in I,\ i \leq j\}\rangle$, $\mu : C \to M = C/D$ e $\varinjlim M_i := (M, \{\mu_i\}_{i\in I})$.

(Existência) Defina o seguinte R-homomorfismo

$$\begin{array}{rccc}
\tilde{\alpha}: & C & \to & N \\
& \sum x_i & \mapsto & \sum \alpha_i(x_i)
\end{array}$$

Então, $\tilde{\alpha}(D) = 0$. De fato, se $\sum [x_k - \mu_{kl}(x_k)] \in D$, segue da definição de $\tilde{\alpha}$ que

$$\tilde{\alpha}(\sum [x_k - \mu_{kl}(x_k)]) = \sum \alpha_k(x_k) - \alpha_l(\mu_{kl}(x_k)) = \sum \alpha_k(x_k) - \alpha_k(x_k) = 0.$$

Logo, α define um homomorfismo $\alpha : M = C/D \to N$.

(Unicidade) Suponhamos que exista outro $\alpha' : M \longrightarrow N$ tal que $\alpha_i = \alpha' \circ \mu_i$. Então,

$$\begin{aligned} \alpha \circ \mu_i &= \alpha' \circ \mu_i \\ \alpha(\mu_i(x_i)) &= \alpha'(\mu_i(x_i)) \\ \alpha(\overline{x_i}) &= \alpha'(\overline{x_i}) \end{aligned}$$

Logo,

$$\alpha(\overline{\sum x_i}) = \sum \alpha(\overline{x_i}) = \sum(\alpha'(\overline{x_i}) = \alpha'(\overline{\sum x_i}). \tag{3.1}$$

■

Veremos a seguir que a Proposição 3.3 garante que o limite direto é único a menos de isomorfismos. Sejam $M = \varinjlim M_i = (M, \{\mu_i\}_{i\in I})$ e $M' = \varinjlim M_i = (M', \{\mu_i'\}_{i\in I})$ dois R-módulos satisfazendo a propriedade universal do limite direto. Então, para todo N R-módulo e $\alpha_i : M_i \to N$, existem únicos $\alpha : M \to N$ e $\alpha' : M' \to N$ tais que $\alpha' \circ \mu_i' = \alpha_i'$ e $\alpha \circ \mu_i = \alpha_i$, isto é, tais que os seguintes diagramas são comutativos.

$$\begin{tikzcd} M \arrow[rr, "\exists!\,\alpha"] & & N \\ & M_i \arrow[ul, "\mu_i"] \arrow[ur, "\alpha_i"'] & \end{tikzcd} \qquad \text{e} \qquad \begin{tikzcd} M' \arrow[rr, "\exists!\,\alpha'"] & & N \\ & M_i \arrow[ul, "\mu_i'"] \arrow[ur, "\alpha_i'"'] & \end{tikzcd}$$

Fazendo $N = M'$ e $\alpha_i := \mu_i'$ no primeiro diagrama temos que $\exists!\alpha : M \to M'$ tal que

$$\alpha \circ \mu_i = \mu_i'. \tag{3.2}$$

Fazendo $N = M$ e $\alpha_i' := \mu_i$ no segundo diagrama temos que $\exists!\alpha' : M' \to M$ tal que

$$\alpha' \circ \mu_i' = \mu_i. \tag{3.3}$$

Segue das equações (3.2) e (3.3) que

$$(\alpha' \circ \alpha) \circ \mu_i = \alpha' \circ (\alpha \circ \mu_i) = \alpha' \circ \mu_i' = \mu_i$$

e que

$$(\alpha \circ \alpha') \circ \mu_i' = \alpha \circ (\alpha' \circ \mu_i') = \alpha \circ \mu_i = \mu_i'.$$

Ou seja, os diagramas

$$\begin{tikzcd} M \arrow[rr, "\alpha'\circ\alpha", "Id"'] & & M \\ & M_i \arrow[ul, "\mu_i"] \arrow[ur, "\mu_i"'] & \end{tikzcd} \quad \text{e} \quad \begin{tikzcd} M' \arrow[rr, "\alpha\circ\alpha'", "Id"'] & & M' \\ & M_i \arrow[ul, "\mu_i'"] \arrow[ur, "\mu_i'"'] & \end{tikzcd}$$

são comutativos. Logo, pela unidade da aplicação dada na Proposição 3.3 temos que $\alpha' \circ \alpha = Id$ e $\alpha \circ \alpha' = Id$.

Proposição 3.4. *Seja $\{M_i\}_{i\in I}$ uma família de submódulos de um R-módulo, tal que para cada par de índices i, j em I, existe $k \in I$ tal que $M_i + M_j \subseteq M_k$. Defina $i \leq j$ se $M_i \subseteq M_j$ e seja $\mu_{ij} : M_i \longrightarrow M_j$ a inclusão de M_i em M_j. Então, $\varinjlim M_i = \sum M_i = \bigcup M_i$. Em particular, qualquer R-módulo é o limite direto de seus submódulos finitamente gerados.*

Demonstração. Para cada $i \in I$ temos $M_i \subseteq \sum M_i$ e, portanto, $\bigcup M_i \subseteq \sum M_i$. Por outro lado, se $y = \sum_{i\in I} x_i \in \sum M_i$ é qualquer soma finita, $S = \{i \in I; x_i \neq 0\}$ e $j \in I$ é tal que $j \geq i$, para todo $i \in S$, então $\displaystyle\sum_{i\in S} M_i \subseteq M_j$. Logo, $\sum_{i\in I} M_i \subseteq \displaystyle\bigcup_{i\in I} M_i$.

Agora, provemos que $\displaystyle\bigcup_{i\in I} M_i$ cumpre com a propriedade universal.

Sejam $\mu_i : M_i \longrightarrow \displaystyle\bigcup_{i\in I} M_i$ o homomorfismo inclusão, N um R-módulo e, $\forall\, i \in I$, $\alpha_i : M_i \longrightarrow N$ R-homomorfismos tais que $\alpha_i = \alpha_j \circ \mu_{ij}$ sempre que $i \leq j$.

Defina

$$\begin{array}{rcl} \alpha : \displaystyle\bigcup_{i\in I} M_i & \longrightarrow & N \\ x & \longmapsto & \alpha_i(x_i), \ \textit{se } x = x_i \in M_i, \ \textit{para algum } i \in I. \end{array}$$

Vamos mostrar que α está bem definida.

Sejam $x \in \displaystyle\bigcup_{i\in I} M_i$ tal que $x = x_i \in M_i$ e $x = x_j \in M_j$. Sem perda de generalidade, podemos supor que $i \leq j$. Portanto, $\alpha_j(x_j) = \alpha_j(\mu_{ij}(x_i)) = \alpha_i(x_i)$, já que $\mu_{ij}(x_i) = x_j$.

Resta provar que $\alpha_i = \alpha \circ \mu_i$. De fato, $\alpha \circ \mu_i(x_i) = \alpha(x_i) = \alpha_i(x_i)$, para todo x_i. Portanto, $\alpha \circ \mu_i = \alpha_i$.

Para mostrar a unicidade de α, suponhamos que exista outro A-homomorfismo $\beta : \displaystyle\bigcup_{i\in I} M_i \longrightarrow N$ tal que $\beta \circ \mu_i = \alpha_i$. Daí,

$$\begin{aligned} \beta(x_i) &= \beta \circ \mu_i(x_i), \quad \textit{pois } \mu_i \textit{ é a aplicação inclusão} \\ &= \alpha_i(x_i), \quad \textit{já que } \beta \circ \mu_i = \alpha_i \\ &= \alpha \circ \mu_i(x_i), \quad \textit{pois } \alpha_i = \alpha \circ \mu_i \\ &= \alpha(x_i), \quad \textit{pois } \mu_i \textit{ é a aplicação inclusão.} \end{aligned}$$

Portanto, $\beta = \alpha$. ∎

Exemplo 3.3. Seja R um domínio de integridade e $\mathbb{K}$ seu corpo de frações. Sejam $I = R - \{0\} \subseteq \mathbb{K}$, $\xi \in I$ e $R_\xi := \{a/\xi; a \in R\} \subset \mathbb{K}$. Defina

$$\xi \leq \eta \iff R_\xi \subseteq R_\eta \quad e \quad \xi = \eta \Leftrightarrow R_\xi = R_\eta.$$

É fácil ver que e $(I, \leq)$ é um conjunto parcialmente ordenado e um conjunto dirigido. De fato, dados $\xi, \eta \in I$, as inclusões naturais

$$\begin{array}{ccc} R_\xi & \longrightarrow & R_{\xi\eta} \\ \frac{a}{\xi} & \longmapsto & \frac{a\eta}{\xi\eta} \end{array} \qquad \text{e} \qquad \begin{array}{ccc} R_\eta & \longrightarrow & R_{\xi\eta} \\ \frac{b}{\eta} & \longmapsto & \frac{b\xi}{\eta\xi} \end{array}$$

garantem que, para $\zeta = \xi\eta$, temos $\xi \leq \zeta$ e $\eta \leq \zeta$.

Logo, segue da Proposição 3.4 que

$$\varinjlim R_\xi = \sum_{\xi \in I} R_\xi = \bigcup_{\xi \in I} R_\xi \tag{3.4}$$

Como $\mathbb{K} = \bigcup_{\xi \in I} R_\xi$, concluímos que $\mathbb{K} = \varinjlim R_\xi$.

Teorema 3.2. *Seja R um anel, N um R-módulo, e seja $\mathscr{F} = \{M_\lambda; f_{\mu\lambda}\}$ um sistema direto de R-módulos. Então, $\varinjlim(M_\lambda \otimes_R N) = (\varinjlim M_\lambda) \otimes_R N$.*
(Em outras palavras, o produto tensorial comuta com limites diretos).

Demonstração. Ver [13], Teorema A1, pág. 270. ∎

Veremos a seguir que o limite direto é uma ferramenta importante para provar a próxima proposição que por sua vez será útil para estudar módulos sem torção.

Proposição 3.5. *Sejam R um domínio de integridade e M um R-módulo. Temos que:*

i) Se M é qualquer, então $\dfrac{M}{T(M)}$ é livre de torção.

ii) Se $f : M \to N$ é um homomorfismo de módulos, então $f(T(M)) \subseteq T(N)$.

iii) Se $0 \to M' \to M \to M''$ é uma sequência exata, então a sequência $0 \to T(M') \to T(M) \to T(M'')$ é exata.

iv) Se M é um R-módulo qualquer, então $T(M)$ é o núcleo da aplicação $x \mapsto 1 \otimes x$ de M em $\mathbb{K} \otimes_R M$, onde $\mathbb{K}$ é o corpo de frações de R.

Demonstração. **(i)** Como $T(M)$ é um submódulo de M, $\dfrac{M}{T(M)}$ é um R-módulo.

$\vdash$: $T(\dfrac{M}{T(M)}) = \left\{\bar{0}\right\}$. Suponhamos que $a\bar{m} = \bar{0}$, para algum $a \in R$ não nulo. Então $am \in T(M)$, isto é, $\exists\, b \in R$, não nulo, tal que $b(am) = 0$. Como $ba \neq 0$, já que R é um domínio de integridade, $m \in T(M)$ e $\bar{m} = \bar{0}$.

(ii) Seja $m \in T(M)$. Então, $m \in M$ é tal que $am = 0$, para algum $a \in R$ não nulo. Seja f um homomorfismo de módulos. Então, $f(m) \in N$ e $af(m) = f(am) = f(0) = 0$. Assim, $\exists\, a \in R$, $a \neq 0$, tal que $af(m) = 0$. Portanto, $f(m) \in T(N)$.

(iii) Seja $0 \xrightarrow{\alpha} M' \xrightarrow{\beta} M \xrightarrow{\gamma} M''$ uma sequência exata de R-módulos, isto é, aplicações tais que $\mathrm{Im}\,\alpha = \ker\beta$ e $\mathrm{Im}\,\beta = \ker\gamma$. Então, β é injetiva e $\mathrm{Im}\,\beta = \ker\gamma$. Seja $0 \xrightarrow{\overline{\alpha}} T(M') \xrightarrow{\overline{\beta}} T(M) \xrightarrow{\overline{\gamma}} T(M'')$, onde $\overline{\alpha} = \alpha\,|_{\{0\}}$, $\overline{\beta} = \beta\,|_{T(M')}$, $\overline{\gamma} = \gamma\,|_{T(M)}$.

$\vdash$: $0 = \ker\overline{\beta}$.

De fato, $\ker\overline{\beta} \subset \ker\beta = 0$ o que implica $\ker\overline{\beta} = 0$.

$\vdash$: $\mathrm{Im}\,\overline{\beta} = \ker\overline{\gamma}$.

De fato, $\mathrm{Im}\,\overline{\beta} = \{\beta(x)\ :\ x \in T(M')\}$ e $\ker\overline{\gamma} = \{x \in T(M)\ :\ \gamma(x) = 0\}$.

$$\begin{array}{ccccccc} 0 & \longrightarrow & T(M') & \xrightarrow{\overline{\beta}} & T(M) & \xrightarrow{\overline{\gamma}} & T(M'') \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & M' & \xrightarrow{\beta} & M & \xrightarrow{\gamma} & M'' \end{array} \tag{3.5}$$

<u>($\supseteq$)</u> Seja $y \in \mathrm{Im}\,\overline{\beta}$, isto é, $y = \overline{\beta}(x) = \beta(x)$, para algum $x \in T(M')$. Então, $\overline{\gamma}(y) = \overline{\gamma}(\beta(x)) = \gamma(\beta(x)) = (\gamma \circ \beta)(x) = 0$. Assim, $y \in \ker\overline{\gamma}$.

<u>($\subseteq$)</u> Seja $y \in \ker\overline{\gamma}$. Então $\overline{\gamma}(y) = \gamma(y) = 0$. Logo, $y \in \ker\gamma = \mathrm{Im}\,\beta$. Assim $y = \beta(x)$, para algum $x \in M'$.

Também sabemos que $y \in T(M)$. Então, $\exists\, a \in R$, $a \neq 0$, tal que $ay = a\beta(x) = \beta(ax) = 0$. Como β é injetiva, $ax = 0$, isto é, $x \in T(M')$. Portanto, $\overline{\beta}(x) = \beta(x) = y \in \mathrm{Im}\,\overline{\beta}$.

(iv) Devemos mostrar que $T(M) = \ker\varphi$, onde

$$\begin{array}{rcl} \varphi : M & \longrightarrow & \mathbb{K} \otimes_R M \\ x & \longmapsto & 1 \otimes x \end{array}$$

<u>($\subseteq$)</u> Seja $x \in T(M)$. Então, existe $a \in R$, $a \neq 0$, tal que $ax = 0$. Assim, em $\mathbb{K} \otimes_R M$, temos

$$\varphi(x) = 1 \otimes x = \frac{a}{a} \otimes x = \frac{1}{a} \otimes ax = \frac{1}{a} \otimes 0 = 0.$$

Portanto, $T(M) \subseteq \ker\varphi$.

<u>($\supseteq$)</u> Seja $x \in \ker\varphi$. Então, $1 \otimes x = 0$ em $\mathbb{K} \otimes_R M$. Como $\mathbb{K} = \varinjlim R_\xi$ (Exemplo 3.3), pelo Teorema 3.2, temos que

$$\mathbb{K} \otimes_R M = (\varinjlim R_\xi) \otimes_R M \cong \varinjlim (R_\xi \otimes_R M),$$

onde $R_\xi := \{a/\xi; a \in R\}$. Sejam $M_\xi := R_\xi \otimes_R M$, $\xi \leq \eta$ e

$$\begin{array}{rccc} \mu_{\xi\eta} : & M_\xi & \longrightarrow & M_\eta \\ & \frac{a}{\xi} \otimes m & \longmapsto & \frac{a}{\xi} \otimes m \end{array}$$

Então, $\mathbb{K} \otimes_R M = \varinjlim(R_\xi \otimes_R M) \cong \varinjlim M_\xi$ é um isomorfismo tal que $a/\xi \otimes m \mapsto 1/\xi \otimes (am)$. Como $0 = 1 \otimes x \in \mathbb{K} \otimes_R M$, segue da Proposição 3.2 que $0 = 1 \otimes x = \mu_{1\xi}(1 \otimes x)$ em M_ξ, para algum $\xi \in I$, isto é, $1 \otimes x = 1/\xi \otimes (\xi x) = 0$ em $R_\xi \otimes_R M$. Mas $R_\xi \cong R$ implica

$$\begin{array}{ccccc} R_\xi \otimes_R M & \cong & R \otimes_R M & \cong & M \\ \frac{a}{\xi} \otimes x & \mapsto & a \otimes x & \mapsto & ax \end{array}$$

donde concluímos que $0 = 1 \otimes x \in \mathbb{K} \otimes_R M$ implica $\xi x = 0 \in R$. Logo, $x \in T(M)$.

■

Definição 3.5. Seja R um domínio de integridade com o corpo de frações L e seja M um R-módulo. Definimos o posto de M, denotado por $\operatorname{rank}_R M$, por:

$$\operatorname{rank}_R M := \dim_L L \otimes_R M.$$

Lema 3.1. *Sejam R um domínio de integridade e M um R-módulo finitamente gerado, livre de torção e de posto* 1. *Então, M é isomorfo a um ideal de R.*

Demonstração. Seja $\mathbb{K}$ o corpo de frações de R. Como M é livre de torção, segue do item (iv) da Proposição 3.5, que o R-homomorfismo $\phi : M \to \mathbb{K} \otimes_R M$, dado por $\phi(m) = 1 \otimes m$ é injetivo. Logo, $M \cong \phi(M)$. Usando que $\operatorname{rank}_R(M) = \dim_{\mathbb{K}}(\mathbb{K} \otimes_R M) = 1$, temos que $\mathbb{K} \otimes_R M \cong \mathbb{K}$ e, portanto, $\phi(M)$ é isomorfo a um R-submódulo de $\mathbb{K}$. Identificando $\phi(M)$ com sua imagem em $\mathbb{K}$, podemos supor $\phi(M) \subset \mathbb{K}$. Sejam $x_1, \ldots, x_n \in M$, tais que $M = Rx_1 + \ldots + Rx_n$ e $\phi(x_i) = a_i/b_i \in \mathbb{K}$, $\forall\, i = 1, \ldots, n$. Então,

$$\phi(M) = R\varphi(x_1) + \ldots + R\phi(x_n) = R\frac{a_1}{b_1} + \ldots + R\frac{a_n}{b_n} \;\Rightarrow\; b\varphi(M) := I \subseteq R,$$

onde $b = b_1 b_2 \ldots b_n$ e $I = Ra_1 + \ldots + Ra_n$. Logo, $M \cong \phi(M) \cong I$ ideal de R. ■

3.3 IDEAIS FRACIONÁRIOS

Um conceito que será muito usado neste trabalho é o conceito de ideal fracionário que descreveremos a seguir.

Definição 3.6. Sejam R um domínio de integridade e $\mathbb{K}$ seu corpo de frações. Um R-submódulo M de $\mathbb{K}$ é um *ideal fracionário* de R se $xM \subseteq R$, para algum $x \neq 0$ em R. Em particular, os ideais de R, que de agora em diante serão chamados ideais *integrais*, são ideais fracionários. Qualquer elemento $u \in \mathbb{K}$ gera um ideal fracionário, denotado por $\langle u \rangle$ ou Ru, e chamado *principal*.

Seja M é um ideal fracionário. O conjunto de todos $x \in \mathbb{K}$ tais que $xM \subseteq R$ é denotado por $(R : M)$, isto é, $(R : M) := \{x \in \mathbb{K} \ : \ xM \subseteq R\}$.

Lema 3.2. *$(R : M)$ é um R-submódulo de $\mathbb{K}$.*

Demonstração. Como $0 \in (R : M)$, então $(R : M) \neq \emptyset$.

$\vdash$: $x + y \in (R : M)$, $\forall x, y \in (R : M)$.

Sejam $x, y \in (R : M)$. Então, $xM \subseteq R$, $yM \subseteq R$ e

$$(x + y)M \subseteq xM + yM \subseteq R \Rightarrow x + y \in (R : M).$$

$\vdash$: $ax \in (R : M)$, $\forall x \in (R : M)$ e $\forall a \in R$.

Sejam $x \in (R : M)$ e $a \in R$. Então, $xM \subseteq R$ e

$$(ax)M = a(xM) \subseteq R \Rightarrow ax \in (R : M).$$

Logo, $(R : M)$ é um submódulo de $\mathbb{K}$. ∎

Observação 3.2. Denotaremos por M^{-1} o R-módulo $(R : M)$.

Lema 3.3. *Todo A-submódulo M de $\mathbb{K}$ finitamente gerado é um ideal fracionário.*

Demonstração. Sejam $x_1, x_2, \cdots, x_n \in \mathbb{K}$ geradores de M. Como $x_1, x_2, \cdots, x_n \in \mathbb{K}$, podemos escrever $x_i = a_i/b_i$, onde $a_i, b_i \in R$ e $b_i \neq 0$, para todo $i = 1, 2, \cdots, n$. Seja $z = b_1 b_2 \cdots b_n \neq 0$, então

$$x_1 = \frac{a_1 b_2 b_3 \cdots b_n}{z}, x_2 = \frac{a_2 b_1 b_3 \cdots b_n}{z}, \cdots, x_n = \frac{a_n b_1 b_2 \cdots b_{n-1}}{z}.$$

Ou seja, $x_i = y_i/z$, com $y_i, z \in R$, para todo $i = 1, 2, \cdots, n$. Daí segue que,

$$M \subset \left\langle \frac{y_1}{z}, \frac{y_2}{z}, \cdots, \frac{y_n}{z} \right\rangle = \frac{1}{z} \langle y_1, y_2 \cdots, y_n \rangle \subset M \Rightarrow M = \frac{1}{z} \langle y_1, \ldots, y_n \rangle.$$

Logo, $zM \subseteq R$ e M é um ideal fracionário. ∎

A recíproca do Lema anterior é verdadeira em anéis Noetherianos.

Lema 3.4. *Seja R um anel Noetheriano. Então todo ideal fracionário é finitamente gerado.*

Demonstração. Seja M um ideal fracionário, isto é, $M \subseteq \mathbb{K}$ é um R-submódulo e $\exists z \in R$, $z \neq 0$, tal que $zM \subseteq R$. Primeiro, provaremos que zM é um ideal de R.

- Sejam $zm_1, zm_2 \in zM$. Então, $zm_1 + zm_2 = z(m_1 + m_2) \in zM$, já que M é um R-submódulo.

- Sejam $zm \in zM$ e $a \in R$. Então, $a(zm) = z(am) \in zM$, já que M é um R-submódulo.

Como zM é um ideal de R e R é Noetheriano, então zM é finitamente gerado, isto é, existem $m_1, \cdots, m_s \in R$, tais que $zM = \langle m_1, \cdots, m_s \rangle$.

Assim,
$$M = \frac{1}{z} \langle m_1, \cdots, m_s \rangle = \left\langle \frac{m_1}{z}, \cdots, \frac{m_s}{z} \right\rangle$$
é finitamente gerado. ■

Definição 3.7. Um R-submódulo M de $\mathbb{K}$ é um *ideal invertível* se existe um submódulo N de $\mathbb{K}$ tal que $MN = R$. Nesse caso, o R-módulo N é único e igual a $(R : M)$.

De fato,

$$\begin{aligned} N \subseteq (R : M) &= (R : M)R, \ já \ que \ (R : M) \ é \ um \ R - submódulo, \\ &= (R : M)MN, \ pois \ R = MN, \\ &\subseteq RN, \ pela \ definição, \ de \ (R : M) \\ &= N, \ já \ que \ N \ é \ um \ R - submódulo, \end{aligned}$$

Portanto, $N = (R : M)$.

Observemos ainda que um R-módulo M invertível é um ideal fracionário, já que $MN = M(R : M) = R$ implica que existem $x_1, \cdots, x_n \in M$ e $y_1, \cdots, y_n \in (R : M)$, tais que $\sum_{i=1}^{s} x_i y_i = 1$. Logo, para qualquer $x \in M$, temos

$$x = x.1 = \sum_{i=1}^{s} (y_i x) x_i, \ com \ y_i x \in R, \ pois \ y_i \in (R : M). \tag{3.6}$$

Então, M é gerado por $x_1, x_2, \cdots, x_n$ e, portanto, é fracionário pelo Lema 3.3.

Exemplo 3.4. Todo ideal fracionário principal não nulo, $M = \langle u \rangle$, é invertível, sendo $N = \langle u^{-1} \rangle$ seu inverso.

Os ideais invertíveis de um anel R formam um grupo com respeito à multiplicação, cujo elemento identidade é $R = \langle 1 \rangle$.

Observação 3.3. Seja $\phi : M \to N$, um R-homomorfismo de ideiais fracionários de R, e sejam $m_1, m_2 \in M$ tais que $m_1 m_2 \in M$. Então,

$$\phi(m_1 m_2) = m_1 \phi(m_2) = m_2 \phi(m_1).$$

De fato, se $m_1 = \dfrac{a_1}{a_2}$, com $a_1, a_2 \in R$ e $a_2 \neq 0$, temos que

$$a_2 \phi(m_1 m_2) = \phi(a_2 m_1 m_2) = \phi(a_1 m_2) = a_1 \phi(m_2)$$

$$\Rightarrow \phi(m_1m_2) = \frac{a_1}{a_2}\phi(m_2) = m_1\phi(m_2).$$

Analogamente, mostra-se que $\phi(m_1m_2) = m_2\phi(m_1)$.

Lema 3.5. *Dois ideais integrais ou fracionários de R, M e N, são isomorfos como A-módulos, se e somente se, existe $\alpha \in \mathbb{K} - \{0\}$, tal que $M = \alpha N$.*

Demonstração. $\Rightarrow$) Sendo M e N, ideais fracionários, existem $a, b \in R - \{0\}$, tais que $M = \frac{1}{a}I$ e $N = \frac{1}{b}J$, onde I, J são ideais de A. Seja $\phi : M \to N$ um R-isomorfismo de módulos. Então, fixado $x_0 \in I \subset M$, $x_0 \neq 0$, temos, $\forall\, n \in N$, $n = \phi(m)$ e

$$ax_0n = ax_0\phi(m) = x_0\phi(am) = x_0\phi(x), \text{ para algum } x \in I \Rightarrow ax_0n = \phi(x_0x) = x\phi(x_0)$$

$$\Rightarrow x_0n = \frac{x}{a}\phi(x_0) \Rightarrow x_0N = M\phi(x_0) \Rightarrow N = \alpha M, \text{ com } \alpha = \frac{\phi(x_0)}{x_0} \in \mathbb{K}.$$

$\Leftarrow$) Trivial. ■

Lema 3.6. *Sejam R um domínio de integridade, e $M_1, \ldots, M_r, N_1, \ldots, N_r$ ideais (integrais ou fracionários) de R tais que*

$$M_1 \oplus \ldots \oplus M_r \cong N_1 \oplus \ldots \oplus N_r,$$

como R-módulos. Então, existe $\alpha \in \mathbb{K}$, não nulo, tal que $M_1 \ldots M_r = \alpha N_1 \ldots N_r$.

Demonstração. Podemos supor, sem perda de generalidade, que M_i e N_j contém R, para todo i e j. De fato, um ideal fracionário $M = (1/a)I$ é sempre isomorfo a aM e $1 \in aM$. Para cada $i \in \{1, \ldots, n\}$, seja $e_i = (0, \ldots, 1, \ldots, 0)$, onde $1 \in M_i$. Então, para todo $i = 1, \ldots, n$, $\phi(e_i) = \sum_{j=1}^{r} \alpha_{ij}v_j$, onde $\alpha_{ij} \in N_j$ e $v_j = (0, \ldots, 1, \ldots, 0)$, com $1 \in N_j$. Seja $x = \sum_{i=1}^{r} x_ie_i$, tal que $x_i \in M_i$, um elemento genérico de $M_1 \oplus \ldots \oplus M_r$. Temos que

$$\phi(x) = \phi(\sum_{i=1}^{r} x_ie_i) = \sum_{i=1}^{r} x_i\phi(e_i) = \sum_{i=1}^{r} x_i(\sum_{j=1}^{r} \alpha_{ij}v_j) = \sum_{j=1}^{r}(\sum_{i=1}^{r} x_i\alpha_{ij})v_j.$$

Logo,

$$\begin{array}{ccccccccc}
N_1 & = & \alpha_{11}M_1 & + & \alpha_{12}M_2 & + & \ldots & + & \alpha_{1r}M_r \\
N_2 & = & \alpha_{21}M_1 & + & \alpha_{22}M_2 & + & \ldots & + & \alpha_{2r}M_r \\
\vdots & & & & & \vdots & & & \\
N_r & = & \alpha_{r1}M_1 & + & \alpha_{r2}M_2 & + & \ldots & + & \alpha_{rr}M_r
\end{array}$$

Seja $\delta = \det(\alpha_{ij}) = \sum_{\sigma \in S_n}(sgn\sigma)R_\sigma$. Então, $\det(\alpha_{ij})M_1 \ldots M_r \subset N_1 \ldots N_r$. Tomando a inversa de ϕ, teremos $\det(\beta_{ij})N_1 \ldots N_r \subset M_1 \ldots M_r$. Mas, $\phi \circ \phi^{-1} = Id$, implica que $\det(\alpha_{ij})\det(\beta_{ij}) = 1$, ou seja,

$$N_1 \ldots N_r \subset \det(\beta_{ij})^{-1}M_1 \ldots M_r = \det(\alpha_{ij})M_1 \ldots M_r.$$

■

Lema 3.7. *Sejam R um domínio de integridade e M um ideal fracionário de R. Então M é invertível, se e somente se, M for finitamente gerado e $M_{\mathfrak{p}}$, a localização de M em $\mathfrak{p}$, for um ideal invertível de $R_{\mathfrak{p}}$, para todo $\mathfrak{p}$ ideal primo de R.*

Demonstração. $\Rightarrow$) Já vimos que M invertível implica M finitamente gerado e $MM^{-1} = R$. Seja $\mathfrak{p}$ um ideal primo de R. Então, $M_{\mathfrak{p}}M_{\mathfrak{p}}^{-1} = R_{\mathfrak{p}}$ e $M_{\mathfrak{p}}$ é invertível em $R_{\mathfrak{p}}$.

$\Leftarrow$) Reciprocamente, seja M um ideal fracionário finitamente gerado tal $M_{\mathfrak{p}}$ invertível, para todo primo $\mathfrak{p}$. Em particular, $M_{\mathfrak{M}}$ invertível, para todo maximal $\mathfrak{M}$. Como $M(R : M) = I$ é um ideal integral de R, temos que $R_{\mathfrak{M}} = M_{\mathfrak{M}}(R : M)_{\mathfrak{M}} = I_{\mathfrak{M}}$, ou seja, $I \not\subseteq \mathfrak{M}$. Como vale para todo maximal, temos que $I = R$. ■

Lema 3.8. *Seja R um domínio de integridade local. Então todo ideal fracionário de R invertível é principal.*

Demonstração. Seja M um ideal fracionário de R invertível e $\mathfrak{M}$ o único ideal maximal de R. Sejam $x_1, \ldots, x_n \in M$ e $y_1, \ldots, y_n \in M^{-1}$ tais que $\sum_{i=1} x_i y_i = 1$. Como $x_i y_i \in R$, para todo $i = 1, \ldots, n$, existe ao menos um j tal que $x_j y_j \notin \mathfrak{M}$. Então, existe $a \in R$ tal que $a(x_j y_j) = 1$ e $m = (may_j)x_j \Rightarrow M = Rx_j$. ■

Lema 3.9. *Seja R um domínio de Dedekind. Então, todo ideal fracionário de R é invertível.*

Demonstração. Seja M um ideal fracionário de R. Então, existe $a \in R - \{0\}$, tal que $aM = I$ é um ideal integral de R. Seja $\mathfrak{p}$ um ideal primo de R. Como R é domínio de Dedekind $R_{\mathfrak{p}}$ é domínio de valorização discreta e, portanto, um domínio de ideais principais. Como todo ideal principal é invertível, segue do Lema 3.7, que I é invertível, e por conseguinte, M é invertível. ■

Proposição 3.6. *Seja R um domínio de integridade e $M \neq \{0\}$ um ideal fracionário de R. Então,*

i) M é um R-módulo livre, se e somente se, é um ideal principal.

ii) M é um ideal invertível, se e somente se, é um R-módulo projetivo finitamente gerado de posto 1.

Demonstração. Ver [13], Teorema 11.3, pág. 80. ■

3.4 ANÉIS COMUTATIVOS COM CONDIÇÃO MÍNIMA RESTRITA

Os conceitos e resultados apresentados nessa seção são encontrados em [10]. As condições de cadeia ascendente e descendente no anel R serão frequentemente chamadas de condição *máxima* e *mínima*, respectivamente.

Definição 3.8. Um anel R será chamado um anel com a *condição mínima restrita*, ou simplesmente *RM-anel*, se para todo ideal $I \neq \{0\}$ em R, R/I satisfaz a condição mínima (isto é, R/I é Artiniano).

Observação 3.4. Ideal próprio de R significa não nulo e diferente de R.

Lema 3.10. *R é um RM-anel, se e somente se, R é Noetheriano e todo ideal primo próprio é maximal.*

Demonstração. $\Rightarrow$) Suponhamos R um RM-anel. Então, para todo ideal $\{0\} \neq I$, R/I satisfaz a condição mínima. Pelo Teorema 2.7, R/I é Noetheriano e todo ideal em R/I, diferente de R/I, é maximal. Afirmamos que R é Noetheriano. De fato, sejam $I \subset R$ um ideal e $x \in I$. Se $I \neq \langle x \rangle$, $\langle x \rangle \subseteq I$ e $\overline{I} \subseteq R/\langle x \rangle$ é finitamente gerado. Logo, se $\overline{I} = \langle \overline{x_1}, \ldots, \overline{x_n} \rangle$, então $I = \langle x_1, \ldots, x_n, x \rangle$. Agora, seja $\mathfrak{p}$ um ideal primo próprio de R e suponhamos $\mathfrak{p} \subset \mathfrak{m} \subseteq R$. Dado $x \in \mathfrak{p}$, temos $\overline{\mathfrak{p}} \subseteq \overline{\mathfrak{m}} \subseteq R/\langle x \rangle$ e $\overline{P} \subset R/\langle x \rangle$ ideal primo. Logo, como todo ideal primo R/I é maximal, temos $\overline{\mathfrak{p}} = \overline{\mathfrak{m}}$ ou $\overline{\mathfrak{p}} = R/\langle x \rangle$. Equivalentemente, $\mathfrak{p} = \mathfrak{m}$ ou $\mathfrak{m} = R$, isto é, $\mathfrak{p}$ é maximal.

$\Leftarrow$) Reciprocamente, seja R um anel Noetheriano tal que todo ideal primo próprio é maximal. Então, R/I é Noetheriano, para todo ideal $I \neq \{0\}$ de R, e a dimensão (de Krull) de R/I é igual a zero. De fato, para todo $\overline{P} \subsetneq R/I$ primo, temos que P é primo próprio ($\{0\} \neq I \subset P$) e, por hipótese, maximal. Logo, $\overline{P}$ é maximal e R/I é Artiniano, ou seja, R é um RM-anel. ■

Corolário 3.1. *Uma condição necessária e suficiente para que um anel satisfaça a condição mínima, isto é, seja Artiniano, é que R seja um RM-anel com divisores de zero ou seja um corpo.*

Demonstração. $\Rightarrow$)Se R satisfaz a condição mínima, então ele é um RM-anel. Além disso, se ele não tiver divisores de zero, então $\langle 0 \rangle$ é primo e, pelo Lema 3.10, maximal. Logo, R é um corpo.

$\Leftarrow$)Reciprocamente, seja R um RM-anel tal que R tem divisores ou é um corpo. Então, pelo Lema 3.10, R é notheriano e todo ideal primo próprio é maximal. Se R não for um corpo, então R tem divisores de zero e, portanto, $\langle 0 \rangle$ não é primo, ou seja, todo ideal primo de R é maximal. ■

Definição 3.9. Dizemos que um anel R tem *posto finito* k se todo ideal em R for gerado por k elementos.

Observação 3.5. De acordo com a definição acima, se um anel tem posto k, então tem posto r, para todo $r \geq k$.

Exemplo 3.5. Domínios de ideais principais tem posto 1.

Lema 3.11. *Seja R um domínio de Dedekind. Então R tem posto finito igual a 2.*

Demonstração. Primeiro vamos mostrar que para todo $I \subset R$ um ideal não nulo, R/I é um domínio de ideais principais. De fato, usando que R é Noetheriano, temos que $I = \bigcap_{i=1}^{n} q_i$, onde q_i é ideal primário, $\sqrt{q_i} = p_i$, e $p_i \neq p_j$, para todo $i, j = 1, 2, \ldots, n$ e $i \neq j$. Além disso, $\dim(R) = 1$ implica que os ideais p_i são maximais e, portanto, dois a dois comaximais. Logo, $\bigcap_{i=1}^{n} q_i = \prod_{i=1}^{n} q_i$. Pelo Teorema 2.8, R domínio de Dedekind implica que os ideais primários de R são potências de ideiais primos, ou seja, $I = \prod_{i=1}^{n} p_i^{k_i}$, com p_i primo e $k_i > 0$, $\forall\, i = 1, \ldots, n$. Novamente, usando que os ideais p_i, são dois a dois comaximais, temos que quaisquer potência dos p_i são dois a dois comaximais e

$$\frac{R}{I} \cong \frac{R}{p_1^{k_1}} \oplus \ldots \oplus \frac{R}{p_n^{k_n}}.$$

Afirmamos que $R/p_i^{k_i}$ é um domínio de ideiais principais. De fato, $R/p_i^{k_i}$ é um anel local, já que os ideiais maximais de $R/p_i^{k_i}$ tem que conter $p_i^{k_i}$ e, portanto, só podem ser p_i. Logo,

$$\frac{R}{p_i^{k_i}} \cong \left(\frac{R}{p_i^{k_i}}\right)_p \cong \frac{R_p}{p_i^{k_i} R_p}.$$

Mas, R Dedekind implica R_p domínio de valorização discreta (Teorema 2.8), logo R_p é domínio de ideais principais e $R_p/p_i^{k_i}R_p$, também o é. Finalmente, dado $a \in I$, temos que $\overline{I} \subset R/\langle a \rangle$ ideal é da forma $\overline{I} = \langle \overline{b} \rangle$ e, por conseguintes, $I = \langle a, b \rangle$. ■

Observação 3.6. Um anel de posto finito é necessariamente Noetheriano, mas a recíproca é falsa. Por exemplo, o anel de polinômios $k[x, y]$, com k um corpo, é Notheriano mas não tem posto finito, já que os ideais da forma

$$\langle x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n \rangle$$

não podem ser gerados por menos de n elementos.

Exemplo 3.6. Um anel R que satisfaz a condição mínima, isto é, Artiniano, tem posto finito. De fato, R é Noetheriano e tem uma série de composição finita. Além disso, se $l(R)$ for o comprimento de uma série de composição de R, então, para todo ideal $I \subset R$, temos $l(I) \leq n$. Mas, $I = \langle x_1, \ldots, x_k \rangle$, com $\{x_1, \ldots, x_n\}$ conjunto minimal de geradores, implica que

$$\langle 0 \rangle \subsetneq \langle x_1 \rangle \subsetneq \langle x_1, x_2 \rangle \subsetneq \ldots \subsetneq \langle x_1, x_2, \ldots, x_{k-1} \rangle \subsetneq I \Rightarrow k \leq n.$$

O teorema a seguir mostra que para domínios de integridade locais a condição mínima restrita é necessária e suficiente para que o anel tenha posto finito.

Teorema 3.3. *Seja R um domínio de integridade local. Então, R tem posto finito, se e somente se, satisfaz acondição mínima restrita.*

Demonstração. Ver [10], Teorema 9, p. 35. ■

4 DECOMPOSIÇÃO DE MÓDULOS LIVRES DE TORÇÃO

O objetivo desse capítulo é determinar, como em [4], as condições necessárias no domínio de integridade R para que todo R-módulo livre de torção seja escrito como soma direta de módulos de posto 1. Mais precisamente, vamos demonstrar o seguinte teorema.

Teorema 4.1. *Seja R um domínio de integridade Noetheriano cujo fecho inteiro $\overline{R}$, é um R-módulo finitamente gerado. Então, todo R-módulo livre de torção é uma soma direta de módulos de posto 1, se e somente se, $\mu^*(R) \leq 2$. Além disso, neste caso, todo R-módulo livre de torção de posto 1 é um S-módulo projetivo para um único anel S tal que $R \subseteq S \subseteq \overline{R}$.*

Para isso, precisaremos algumas definições e alguns resultados sobre módulos de livres de torção. Durante todo este capítulo, *módulo* significará módulo finitamente gerado.

4.1 NOÇÕES BÁSICAS

Definição 4.1. Seja M é um R-módulo. Definimos o inteiro positivo $\mu_R(M)$, como sendo o menor número de elementos necessários para gerar M, isto é,

$$\mu_R(M) := \min\{n \in \mathbb{N} : \ M = \langle x_1, \ldots, x_n\rangle, x_1 \ldots, x_n \in M\}$$

e

$$\mu^*(R) := \sup\{\mu_R(\mathfrak{A}) : \ \mathfrak{A} \text{ é um ideal finitamente gerado de } R\}.$$

Lema 4.1. *Seja M um R-módulo finitamente gerado e $\psi : M \to N$, um R-homomorfismo sobrejetor. Então $\mu_R(N) \leq \mu_R(M)$.*

Demonstração. Suponhamos $M = \langle m_1, \ldots, m_k\rangle$. Como ψ é um R-homomorfismo sobrejetor, dado $n \in N$, existe $m \in M$ tal que $n = \psi(m)$. Escreva $m = \sum_{i=1}^{k} r_i m_i$. Então,

$$\begin{aligned} n &= \psi(\sum_{i=1}^{k} r_i m_i) \\ n &= \sum_{i=1}^{k} r_i \psi(m_i), \ \ onde \ \ \psi(m_i) \in N \end{aligned}$$

e $\{\psi(m_1), \ldots, \psi(m_k)\}$ gera N. Assim, N é R-módulo finitamente gerado e

$$\mu_R(N) \leq \mu_R(M).$$

■

Lema 4.2. *Seja $\mathfrak{M}$ um ideal de R. Então, $\mu_R(R/\mathfrak{M}) = 1$.*

Demonstração. Observemos que o R-homomorfismo $\psi : R \to R/\mathfrak{M}$ é sobrejetor e que $\mu_R(R) = 1$, pois $R = \langle 1 \rangle$, como R-módulo. Logo, pelo Lema 4.1,

$$1 \leq \mu_R(R/\mathfrak{M}) \leq \mu_R(R) = 1.$$

■

Observação 4.1. Se um anel R tem posto finito k, (ver Definição 3.9), então $\mu^*(R) \leq k$. Reciprocamente, se R for Noetheriano e $\mu^*(R) \leq k$, então R tem posto finito k.

Lema 4.3. *Sejam $\mathfrak{M}$ e $\mathfrak{N}$ ideais maximais distintos de R. Então,*

$$\frac{R}{\mathfrak{M} \cap \mathfrak{N}} \cong \frac{R}{\mathfrak{M}} \oplus \frac{R}{\mathfrak{N}}.$$

Demonstração. A aplicação

$$\begin{array}{rccc} \psi : & R & \longrightarrow & \dfrac{R}{\mathfrak{M}} \oplus \dfrac{R}{\mathfrak{N}} \\ & r & \longmapsto & (r + \mathfrak{M}, r + \mathfrak{N}) \end{array}$$

é claramente um homomorfismo, cujo núcleo é o ideal $\mathfrak{M} \cap \mathfrak{N}$. Para ver que ψ é sobrejetora, sejam $y \in R/\mathfrak{M} \oplus R/\mathfrak{N}$ e $a, b \in R$ tais que $y = (a + \mathfrak{M}, b + \mathfrak{N})$. Como $\mathfrak{M}$, $\mathfrak{N}$, são comaximais, temos que $\mathfrak{M} + \mathfrak{N} = R$. Logo, $a - b \in R = \mathfrak{M} + \mathfrak{N}$ e, portanto, $a - b = m + n$. Seja $r := a - m = b + n$, isto é, $a = r + m$ e $b = r - n$. Então, temos que

$$y = (a + \mathfrak{M}, b + \mathfrak{N}) = (r + m + \mathfrak{M}, r - n + \mathfrak{N}) = (r + \mathfrak{M}, r + \mathfrak{N}) = \psi(r).$$

■

Lema 4.4. *Sejam R um anel, $\mathfrak{M}$ um ideal de R e M, N R-módulos. Então,*

$$\frac{M \oplus N}{\mathfrak{M}(M \oplus N)} \cong \frac{M}{\mathfrak{M}M} \oplus \frac{N}{\mathfrak{M}N}.$$

Demonstração. É fácil ver que $\mathfrak{M}(M \oplus N) = \mathfrak{M}M \oplus \mathfrak{M}N$, que a aplicação

$$\begin{array}{rccc} \psi : & \dfrac{M \oplus N}{\mathfrak{M}M \oplus \mathfrak{M}N} & \longrightarrow & \dfrac{M}{\mathfrak{M}M} \oplus \dfrac{N}{\mathfrak{M}N} \\ & (m, n) + \mathfrak{M}M \oplus \mathfrak{M}N & \longmapsto & (m + \mathfrak{M}M, n + \mathfrak{M}N) \end{array}$$

está bem definida e um é $R/\mathfrak{M}$-isomorfismo de módulos. ■

Lema 4.5. *Seja R um anel local com ideal maximal $\mathfrak{M}$. Então,*

$$\mu_R(M) = \mu_R(\frac{M}{\mathfrak{M}M}).$$

Demonstração. Seja $\pi : M \to M/\mathfrak{M}M$ a projeção canônica. Se $\{x_1, \ldots, x_n\}$ é um conjunto de geradores de M, então $\{\pi(x_1), \pi(x_2), \ldots, \pi(x_n)\}$ é um conjunto de geradores de $M/\mathfrak{M}M$. Logo, $\mu_R(M/\mathfrak{M}M) \leq \mu_R(M)$. Agora, seja $\{\overline{y_1}, \ldots, \overline{y_k}\}$ um conjunto mínimo de geradores de $M/\mathfrak{M}M$. Como π é sobrejetor, existem $x_1, \ldots, x_k \in M$ tais que $\overline{y_1} = \pi(x_1), \ldots, \overline{y_k} = \pi(x_k)$. Seja $N = \langle x_1, \ldots, x_k\rangle \subseteq M$.

Afirmamos que $M = \mathfrak{M}M + N$.

$\underline{(\supseteq)}$ Óbvia.

$\underline{(\subseteq)}$ Seja $m \in M$. Então,

$$\begin{aligned}
\pi(m) &= a_1\overline{y_1} + \ldots + a_k\overline{y_k} \\
&= a_1\pi(x_1) + \ldots + a_k\pi(x_k) \\
&= \pi(a_1x_1 + \ldots + a_kx_k) \Rightarrow m - \sum_{i=1}^{k} a_ix_i \in \mathfrak{M}M \Rightarrow m \in \mathfrak{M}M + N
\end{aligned} \tag{4.1}$$

Pelo Lema 2.2 (Nakayama), segue que $M = N$. Logo,

$$\mu_R(M) \leq k = \mu_R(\frac{M}{\mathfrak{M}M}).$$

■

Lema 4.6. *Seja R um anel local com ideal maximal $\mathfrak{M}$. Então,*

$$\mu_R(\frac{M}{\mathfrak{M}M}) = \mu_{\frac{R}{\mathfrak{M}}}(\frac{M}{\mathfrak{M}M}).$$

Demonstração. Temos que $M/\mathfrak{M}M$ é um R-módulo tal que $a\overline{m} := \overline{a}\,\overline{m} := \overline{am}$, para todo $a \in R$ e para todo $\overline{m} \in M/\mathfrak{M}M$. Logo, $\{\overline{x_1}, \ldots, \overline{x_n}\}$ gera $M/\mathfrak{M}M$ como R-módulo, se e somente se, $\{\overline{x_1}, \ldots, \overline{x_n}\}$ gera $M/\mathfrak{M}M$ como $R/\mathfrak{M}M$-módulo. Assim,

$$\mu_R(\frac{M}{\mathfrak{M}M}) = \mu_{\frac{R}{\mathfrak{M}}}(\frac{M}{\mathfrak{M}M}).$$

■

Proposição 4.1. *O anel R é local, se e somente se, μ_R é aditiva; isto é, se e somente se,*

$$\mu_R(M \oplus N) = \mu_R(M) + \mu_R(N),$$

para todo M e N R-módulos.

Demonstração. ($\Leftarrow$) Suponhamos que μ_R é aditiva e que R não é local. Sejam $\mathfrak{M}$ e $\mathfrak{N}$ ideais maximais de R, distintos. Pelo Lema 4.2 temos que

$$1 = \mu_R(\frac{R}{\mathfrak{M} \cap \mathfrak{N}}) = \mu_R(\frac{R}{\mathfrak{M}}) = \mu_R(\frac{R}{\mathfrak{N}})$$

e, pelo Lema 4.3, temos que

$$\mu_R(\frac{R}{\mathfrak{M}\cap\mathfrak{N}}) = \mu_R(\frac{R}{\mathfrak{M}} \oplus \frac{R}{\mathfrak{N}}).$$

Como μ_R é aditiva por hipótese,

$$1 = \mu_R(\frac{R}{\mathfrak{M}\cap\mathfrak{N}}) = \mu_R(\frac{R}{\mathfrak{M}}) + \mu_R(\frac{R}{\mathfrak{N}}) = 1 + 1.$$

Absurdo. Logo, R é local.

($\Rightarrow$) Seja R um anel local com ideal maximal $\mathfrak{M}$. Devemos mostrar que μ_R é aditiva. Segue dos Lemas 4.5 e 4.6, respectivamente, que

$$\mu_R(M \oplus N) = \mu_R\left(\frac{M \oplus N}{\mathfrak{M}(M \oplus N)}\right) = \mu_{\frac{R}{\mathfrak{M}}}(\frac{M}{\mathfrak{M}M} \oplus \frac{N}{\mathfrak{M}N}).$$

Como $R/\mathfrak{M}$ é um corpo, temos que

$$\mu_{\frac{R}{\mathfrak{M}}}(\frac{M}{\mathfrak{M}M} \oplus \frac{N}{\mathfrak{M}N}) = \mu_{\frac{R}{\mathfrak{M}}}(\frac{M}{\mathfrak{M}M}) + \mu_{\frac{R}{\mathfrak{M}}}(\frac{N}{\mathfrak{M}N}).$$

Novamente, pelos Lemas 4.6 e 4.5, respectivamente, temos

$$\mu_{\frac{R}{\mathfrak{M}}}(\frac{M}{\mathfrak{M}M}) + \mu_{\frac{R}{\mathfrak{M}}}(\frac{N}{\mathfrak{M}N}) = \mu_R(\frac{M}{\mathfrak{M}M}) + \mu_R(\frac{N}{\mathfrak{M}N}) = \mu_R(M) + \mu_R(N).$$

Concluímos assim que $\mu_R(M \oplus N) = \mu_R(M) + \mu_R(N)$. ∎

Proposição 4.2. *Seja R um domínio de integridade com corpo de frações L. Então*

$$\dim_L(L \otimes_R M) \leq \mu_R(M),$$

com a igualdade acontecendo, se e somente se, M for um R-módulo livre.

Demonstração. Lembremos inicialmente que $L \otimes_R M$ é um L espaço vetorial com a operação:

$$\begin{array}{rcl} \cdot : L \times (L \otimes_R M) & \longrightarrow & L \otimes_R M \\ (\lambda, \sum_{i=1}^{n} l_i \otimes m_i) & \longmapsto & \sum_{i=1}^{n} (\lambda \cdot l_i) \otimes m_i \end{array}$$

Seja $p = \mu_R(M)$ e seja $\{m_1, \ldots, m_p\}$ um conjunto de geradores de M. Provaremos que $L \otimes_R M = \langle 1 \otimes m_1, \ldots, 1 \otimes m_p \rangle$.

$\underline{(\supseteq)}$ Óbvia.

$\underline{(\subseteq)}$ Seja $l \otimes m$ um elemento básico de $L \otimes_R M$. Então,

$$l \otimes m = l \otimes (\sum_{i=1}^{p} r_i m_i) = \sum_{i=1}^{p} (lr_i)(1 \otimes m_i).$$

Logo, $L \otimes_R M = \langle 1 \otimes m_1, \ldots, 1 \otimes m_p \rangle$, como L-espaço vetorial, e

$$\dim_L(L \otimes_R M) \leq p = \mu_R(M).$$

Suponhamos agora que M é livre, isto é, possui uma base, e seja $\{m_1, \ldots, m_p\}$ base de M. Então,

$$(L \otimes_R M) = \langle 1 \otimes m_1, \ldots, 1 \otimes m_p \rangle\,, \text{ como } L\text{-espaço vetorial.} \tag{4.2}$$

Devemos mostrar que $1 \otimes m_1, \ldots, 1 \otimes m_p$ são linearmente independentes sobre L.

Sejam $a_i/b_i \in L$, para $i = 1, \ldots, p$, não todos nulos, tais que

$$\begin{aligned} \textstyle\sum_{i=1}^{p}(a_i/b_i)(1 \otimes m_i) = 0 \quad &\Rightarrow b \textstyle\sum_{i=1}^{p}(a_i/b_i)(1 \otimes m_i) = 0, \quad \text{onde } b = b_1 \ldots b_p \\ &\Rightarrow \textstyle\sum_{i=1}^{p}(a_i b_i') \otimes m_i = 0, \quad \text{onde } b_i' = b_1 \ldots b_{i-1} b_{i+1} \ldots b_p \\ &\Rightarrow 1 \otimes \textstyle\sum_{i=1}^{p}(a_i b_i') m_i = 0 \in L \otimes_R M. \end{aligned}$$

Como R é um domínio de integridade, temos, pela Proposição 3.5, que existe $a \in R$ não nulo, tal que

$$\sum_{i=1}^{p} a(a_i b_i') m_i = 0 \Rightarrow a(a_i b_i') = 0, \ \forall\, i = 1, \ldots, p$$

pois $\{m_1, \ldots, m_p\}$ é base de M. Sendo $a \neq 0$ e $b_i' \neq 0$, $\forall\, i = 1, \ldots, p$, temos $a_i = 0$, $\forall\, i = 1, \ldots, p$. Portanto, $\dim_L(L \otimes_R M) = p = \mu_R(M)$.

Reciprocamente, suponhamos que $\dim_L L \otimes_R M = \mu_R(M)$. Devemos mostrar que M é um R-módulo livre.

Sejam $p = \mu_R(M)$ e $\{m_1, \ldots, m_p\}$ um conjunto mínimo de geradores de M. Vamos mostrar que $\{m_1, \ldots, m_p\}$ é linearmente independente sobre R. De fato, se $\alpha_i \in R$, para $i = 1, \ldots, p$, são tais que $\alpha_1 m_1 + \ldots + \alpha_p m_p = 0$, então:

$$1 \otimes (\alpha_1 m_1 + \ldots + \alpha_p m_p) = 1 \otimes 0 \Rightarrow$$

$$\alpha_1(1 \otimes m_1) + \ldots + \alpha_p(1 \otimes m_p) = 0$$

Como $L \otimes_R M$ é gerado, como espaço vetorial sobre L, por $\{1 \otimes m_1, \ldots, 1 \otimes m_p\}$ e $\dim_L(L \otimes_R M) = p$, temos que $\alpha_1 = \ldots = \alpha_p = 0$. Logo, $\{m_1, \ldots, m_p\}$ é linearmente independentes sobre R e $\{m_1, \ldots, m_p\}$ é base do R-módulo M. ■

Observação 4.2. Dados R um domínio de integridade e $\mathfrak{M}$ um ideal maximal de R, o anel $R_{\mathfrak{M}}$ é por definição o anel de frações $S^{-1}R$, onde $S = R \backslash \mathfrak{M}$.

Lema 4.7. *Sejam R um domínio de integridade e $\mathfrak{M}$ um ideal maximal de R. Sejam A um $R_{\mathfrak{M}}$-módulo gerado por $\langle a_1, \ldots, a_n \rangle$ e $B = \langle a_1, \ldots, a_n \rangle$ como R-submódulo de A. Então,*

$$A \cong R_{\mathfrak{M}} \otimes_R B.$$

Demonstração. A aplicação

$$\begin{array}{rccc} g: & R_{\mathfrak{M}} \times B & \longrightarrow & A \\ & (\frac{r}{s}, b) & \mapsto & \frac{r}{s} b \end{array}$$

é claramente um homomorfismo R-bilinear. Devemos então mostrar que o par (A, g) possui a propriedade universal para o produto tensorial $R_{\mathfrak{M}} \otimes_R B$.

Sejam P um R-módulo e $f : R_{\mathfrak{M}} \times B \longrightarrow P$ uma aplicação R-bilinear. Mostraremos que existe um R-homomorfismo $h : A \to$ tal que $h \circ g = f$, ou seja, que o diagrama

$$\begin{tikzcd} R_{\mathfrak{M}} \times B \arrow[r, "f"] \arrow[d, "g"'] & P \\ A \arrow[ur, "\exists!\, h"'] & \end{tikzcd}$$

é comutativo.

Existência do R-homomorfismo

Defina

$$\begin{array}{rccc} h: & A & \longrightarrow & P \\ & \sum \frac{r_i}{s_i} a_i & \mapsto & \sum f(\frac{r_i}{s_i}, a_i) \end{array}$$

Afirmamos que h é um R-homomorfismo.

De fato, dados $a = \sum \frac{r_i}{s_i} a_i$, $a' = \sum \frac{r'_i}{s'_i} a_i \in A$ e $r \in R$, temos que

$$\begin{aligned} h(a + ra') &= h(\sum \frac{r_i}{s_i} a_i + r(\sum \frac{r'_i}{s'_i} a_i)) \\ &= h(\sum (\frac{r_i}{s_i} + r(\frac{r'_i}{s'_i}))a_i) \\ &= \sum f(\frac{r_i}{s_i} + r\frac{r'_i}{s'_i}, a_i) \\ &= \sum (f(\frac{r_i}{s_i}, a_i) + rf(\frac{r'_i}{s'_i}, a_i)) \\ &= \sum f(\frac{r_i}{s_i}, a_i) + r \sum f(\frac{r'_i}{s'_i}, a_i) \\ &= h(a) + rh(a') \end{aligned}$$

Além disso, para $(r/s, b) \in R_{\mathfrak{M}} \times B$, onde $b = \sum \alpha_i a_i$, com $\alpha_i \in R$, para todo i, temos

$$\begin{aligned}
(h\circ g)(\frac{r}{s},b) &= h(g(\frac{r}{s},b))\\
&= h(\frac{r}{s}b)\\
&= h(\frac{r}{s}\sum \alpha_i a_i)\\
&= h(\sum(\frac{r}{s}\alpha_i)a_i)\\
&= \sum f(\frac{r}{s}\alpha_i,a_i)=\sum f(\frac{r}{s},\alpha_i a_i)=f(\frac{r}{s},\sum\alpha_i a_i)=f(\frac{r}{s},b).
\end{aligned}$$

Logo, $h\circ g=f$.

Unicidade

Seja $h':A\longrightarrow P$ outro R-homomorfismo tal que $h'\circ g=f$. Então, $h\circ g=h'\circ g$.

Logo, para todo $(r/s,b)\in R_{\mathfrak{M}}\times B$,

$$h(g(\frac{r}{s},b))=h'(g(\frac{r}{s},b))\Rightarrow h(\frac{r}{s}b)=h'(\frac{r}{s}b).$$

Finalmente, para todo $a=\sum\frac{r_i}{s_i}a_i\in A$,

$$h(a)=h(\sum\frac{r_i}{s_i}a_i)=\sum h(\frac{r_i}{s_i}a_i)=\sum h'(\frac{r_i}{s_i}a_i)=h'(\sum\frac{r_i}{s_i}a_i)=h'(a).$$

Portanto, $h=h'$. ■

Definição 4.2. Um submódulo N de um módulo M é dito ser fechado em M se M/N for livre de torção. Para um suconjunto S de M, definimos o fecho de S em M como sendo o menor submódulo fechado de M contendo S.

Exemplo 4.1. Sejam R um domínio de integridade e S um suconjunto de um R-módulo M. O conjunto

$$\overline{S}=\{m\in M;\exists\, r\in R\backslash\{0\},\ \text{tal que}\ r\,m\in\langle S\rangle\},$$

é o fecho de S em M.

Para ver que $\overline{S}$ é um submódulo de M, sejam $m_1,m_2\in\overline{S}$ e $r\in R$. Sejam r_1 e r_2, elementos não nulos de R, tais que $r_1m_1,r_2m_2\in\langle S\rangle$. Então,

$$r_1r_2(m_1+rm_2)=r_2(r_1m_1)+r_1r(r_2m_2)\in\langle S\rangle,$$

e $r_1r_2\neq 0$, pois R é domínio de integridade.

Para ver que $S\subset\overline{S}$, observe que $1.s\in\langle S\rangle$, para todo $s\in S$.

Devemos agora mostrar que $M/\overline{S}$ é livre de torção. De fato, $r\overline{m}=\overline{0}$ em $M/\overline{S}$, implica que $rm\in\overline{S}$, isto é, existe $t\in R\backslash\{0\}$, tal que $t(rm)=(tr)m\in\langle S\rangle$. Se r for não nulo, teremos $m\in\overline{S}$, ou seja, $\overline{m}=\overline{0}$.

Para concluir, seja N um submódulo fechado de M contendo S. Então, para todo $m \in \overline{S}$, temos $r\overline{m} = \overline{0} \in M/N$, para algum $0 \neq r \in R$, já que $rm \in \langle S \rangle \subset N$. Logo, $\overline{m} = \overline{0} \in M/N$, o que implica que $m \in N$ e, portanto, $\overline{S} \subset N$.

4.2 CONDIÇÃO NECESSÁRIA PARA DECOMPOSIÇÃO

A proposição a seguir é o primeiro passo na direção de determinar condições necessárias e suficentes no domínio de integridade R, para que todo R-módulo livre de torção se decomponha como soma direta de módulos de posto 1.

Proposição 4.3. *Seja R um domínio de integridade para o qual todo R-módulo livre de torção é soma direta de módulos de posto no máximo $k\,(k \geq 1)$. Então, para cada ideal maximal $\mathfrak{M}$ de R, $\mu^*(R_{\mathfrak{M}}) \leq k+1$.*

Demonstração. Primeiro mostraremos que a hipótese sobre R é herdada por todo $R_{\mathfrak{M}}$, onde $\mathfrak{M}$ é um ideal maximal de R; isto é, se todo R-módulo livre de torção é soma direta de módulos de posto no máximo k, então todo $R_{\mathfrak{M}}$-módulo livre de torção é soma direta de módulos de posto no máximo k, para todo $\mathfrak{M}$ ideal maximal de R.

De fato, sejam $\mathfrak{M}$ ideal maximal de R e $A = \langle a_1, \ldots, a_n \rangle$ um $R_{\mathfrak{M}}$ livre de torção. Pelo Lema 4.7, temos que $A \cong R_{\mathfrak{M}} \otimes_R B$, onde $B = \langle a_1, \ldots, a_n \rangle$ como R-módulo. Além disso, sendo A um $R_{\mathfrak{M}}$-módulo livre de torção, temos que B é um R-módulo livre de torção. Usando a hipótese sobre R, temos que $B = B_1 \oplus \ldots \oplus B_l$ onde os $B_i's$ são R-módulos de posto $\leq k$, $\forall i = 1, \ldots, l$. Então,

$$A \cong R_{\mathfrak{M}} \otimes_R B = R_{\mathfrak{M}} \otimes_R (B_1 \oplus \ldots \oplus B_l) = (R_{\mathfrak{M}} \otimes_R B_1) \oplus \ldots \oplus (R_{\mathfrak{M}} \otimes_R B_l).$$

Para concluir, devemos mostrar que $\operatorname{rank}_{R_{\mathfrak{M}}}(R_{\mathfrak{M}} \otimes_R B_i) \leq k, \ \ i = 1, \ldots, l$. Mas, $\operatorname{rank}_R B_i = \dim_L(L \otimes_R B_i) \leq k, \ \forall\, i$, onde L é o corpo de frações de R e

$$\begin{aligned} \operatorname{rank}_{R_{\mathfrak{M}}} B_i &= \dim_{L'}\left(L' \otimes_{R_{\mathfrak{M}}} (R_{\mathfrak{M}} \otimes_R B_i)\right) \\ &= \dim_{L'}\left((L' \otimes_{R_{\mathfrak{M}}} R_{\mathfrak{M}}) \otimes_R B_i\right) \\ &= \dim_{L'}(L' \otimes_R B_i) \end{aligned}$$

onde L' é o corpo de frações de $R_{\mathfrak{M}}$. Como $L' = L$, temos que

$$\operatorname{rank}_{R_{\mathfrak{M}}} B_i = \dim_{L'}(L' \otimes_R B_i) = \dim_L(L \otimes_R B_i) \leq k.$$

Devemos agora mostrar que $\mu^*(R_{\mathfrak{M}}) \leq k+1$. Para simplificar notação, vamos denotar $R_{\mathfrak{M}}$ por R e assumir que R é um anel local. A demonstração desse fato será feita por contradição.

Suponhamos por absurdo que exista um ideal $\mathfrak{A} = \sum_{i=1}^{k+2} Ra_i \subset R$, com $\mu_R(\mathfrak{A}) = k+2$. Sejam $F = R^{k+2}$ e $\alpha = (a_1, \ldots, a_{k+2}) \in F$. Afirmamos que

$$\mathfrak{A} = \{f(\alpha); f \in Hom_R(F, R)\}. \tag{4.3}$$

$\underline{(\supseteq)}$ Seja $f \in Hom_R(F,R)$ e $\mathfrak{B} = \{e_1, \ldots, e_{k+2}\}$ a base canônica de F. Então,

$$f(\alpha) = f(\sum_{i=1}^{k+2} a_i e_i) = \sum_{i=1}^{k+2} f(a_i e_i) = \sum_{i=1}^{k+2} a_i f(e_i) \in \sum_{i=1}^{k+2} Ra_i = \mathfrak{A}.$$

Portanto, $\{f(\alpha); f \in Hom_R(F,R)\} \subseteq \mathfrak{A}$.

$\underline{(\subseteq)}$ Seja $x \in \mathfrak{A}$. Então, $x = \sum_{i=1}^{k+2} a_i x_i$, com $x_i \in R$, para todo $i = 1, \ldots, k+2$. Defina, estendendo por linearidade, o R-homomorfismo $f : F \longrightarrow R$ dado por $f(e_i) = x_i$. Então, $f(\alpha) = f(\sum_{i=1}^{k+2} a_i e_i) = \sum_{i=1}^{k+2} a_i x_i = x$. Assim, $x \in \{f(\alpha); f \in Hom_R(F,R)\}$ e $\mathfrak{A} \subseteq \{f(\alpha); f \in Hom_R(F,R)\}$.

Observe que 4.3 é uma descrição invariante de $\mathfrak{A}$. A escolha de outra base de F nos dará um outro conjunto de geradores de $\mathfrak{A}$. De fato, se $\{v_1, \ldots, v_{k+2}\}$ for outra base de F e $\alpha = \sum_{i=1}^{k+2} b_i v_i$, com $b_i \in R$. Então

$$\mathfrak{A} = \{f(\alpha); f \in Hom_R(F,R)\} = \left\{\sum_{i=1}^{k+2} b_i f(v_i); f \in Hom_R(F,R)\right\} = \langle b_1, b_2, \ldots, b_{k+2}\rangle .$$

Afirmamos que α não pertence a nenhum somando direto de F.

Suponhamos por absurdo que $F = A \oplus B$ e que $\alpha \in A$. Como R é um anel local, A e B são livres (Teorema 3.1), isto é, $A \cong R^l$ e $B \cong R^t$. Então $\alpha \in A = R^l$, com $l < k+2$.

Seja $\{v_1, \ldots, v_l, v_{l+1}, \ldots, v_{k+2}\}$ base de F, tal que $\{v_1, \ldots, v_l\}$ é base de A e $\{v_{l+1}, \ldots, v_{k+2}\}$ é base de B. Então, $\alpha = b_1 v_1 + \ldots + b_l v_l + 0 v_{l+1} + \ldots + 0 v_{k+2}$ e $\mathfrak{A} = \langle b_1, b_2, \ldots, b_l\rangle$. Absurdo, pois $\mu_R(\mathfrak{A}) = k+2$.

Agora, sejam K o fecho de $\{\alpha\}$ em F e $A = F/K$. Então, A é livre de torção e $\mu_R(A) \leq k+2$, pois $F \to F/K$ é sobrejetora e $\mu_R(F) = k+2$. Como a sequência

$$0 \to K \to F \to A = F/K \to 0,$$

é exata e L é um corpo, temos que a sequência

$$0 \to K \otimes_R L \to F \otimes_R L \to A \otimes_R L \to 0,$$

é exata, donde concluímos que $\mathrm{rank}_R(F) = \mathrm{rank}_R(K) + \mathrm{rank}_R(A)$. Mas

$$\begin{aligned} K &= \{x \in F; \exists\, r \in R \backslash \{0\}, \text{ tal que } rx \in \langle \alpha \rangle\} \\ &= \{x \in F; \exists\, r \in R \backslash \{0\}, \text{ tal que } rx = s\alpha, s \in R\}. \end{aligned}$$

Logo, $\mathrm{rank}_R(K) = \dim_L(L \otimes_R K) = 1$. De fato, dado um elemento básico $l \otimes x \in L \otimes_R K$, $x \in K$ e, portanto, existe $r \in$ não nulo, tal que $rx = s\alpha$, para algum $s \in R$. Então,

$$l \otimes x = l(1 \otimes x) = \frac{l}{r}(1 \otimes rx) = \frac{l}{r}(1 \otimes s\alpha) = \frac{ls}{r}(1 \otimes \alpha) \Rightarrow L \otimes_R K = \langle 1 \otimes \alpha \rangle.$$

Assim, $\text{rank}(A) = \text{rank}(F) - \text{rank}(K)$, implica $\text{rank}(A) = (k+2) - 1 = k+1$.

Se mostrarmos que A é indecomponível, isto é, não se escreve como soma direta de módulos, teremos uma contradição, pois por hipótese, todo R-módulo livre de torção é soma direta de submódulos de posto $\leq k$.

Suponhamos então que $A = B \oplus C$. Mostraremos que A, B ou C é um módulo livre. Usando a Proposição 4.2, basta mostrarmos que $\text{rank}(A) = \mu(A)$, $\text{rank}(B) = \mu(B)$ ou $\text{rank}(C) = \mu(C)$. Temos que

$$\text{rank}(B) + \text{rank}(C) = \text{rank}(A) = k + 1$$

e, pela Proposição 4.1,

$$\mu(B) + \mu(C) = \mu(A) \leq k + 2.$$

Mas, $\text{rank}(B) \leq \mu(B)$ e $\text{rank}(C) \leq \mu(C)$. Então, ou $\text{rank}(A) = k+1 = \mu(A)$ ou $\text{rank}(A) = k+1 < \mu(A) = k+2$. No último caso,

$$\text{rank}(A) = \mu(A) - 1 \Rightarrow \text{rank}(B) + \text{rank}(C) = \mu(B) + \mu(C) - 1.$$

Se $\text{rank}(C) < \mu(C)$, então

$$\begin{aligned} \text{rank}(C) \leq \mu(C) - 1 \ &\Rightarrow \mu(B) - \text{rank}(B) = \text{rank}(C) - \mu(C) - 1 \leq 0 \\ &\Rightarrow \mu(B) \leq \text{rank}(B) \\ &\Rightarrow \mu(B) = \text{rank}(B) \\ &\Rightarrow B \text{ é livre.} \end{aligned}$$

Se $\text{rank}(C) = \mu(C)$, C é livre. Logo, se A não for livre, B ou C será.

Se A for livre, segue da sequência exata

$$0 \longrightarrow K \longrightarrow F \longrightarrow \frac{F}{K} = A \longrightarrow 0$$

que K é livre e, somando direto de A. Como $\alpha \in K$, isso é um absurdo, pois já mostramos que α não pertence a nenhum somando direto de A. Logo, B é livre ou C é livre.

Se B é livre (projetivo), seja $f = \pi_1 \circ \pi : F \to B$, onde $\pi : F \to A = F/K$ e $\pi_1 : A = B \oplus C \to B$ são as projeções canônicas. Como $\alpha \in K \subset F$ e B é projetivo, temos que $f(\alpha) = 0$ e que sequência exata

$$0 \ \to \ker f \ \to \ F \ \to \ B \ \to \ 0 \tag{4.4}$$

se *decompõe*, isto é, $F = \ker f \oplus B$. Mas α não está em nenhum somando direto de F, então $B = 0$. Analogamente mostramos que C livre implica $C = 0$. ■

Lema 4.8. *Sejam $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_r$ ideais de um anel R, dois a dois comaximais, e sejam $\alpha_1, \ldots, \alpha_r$ elementos de um R-módulo A. Então, existe $\alpha \in A$, tal que $\alpha \equiv \alpha_i (mod\, \mathfrak{A}_i A)$, para todo $i = 1, \ldots, r$.*

Demonstração. Mostraremos por indução em r.

Se $r = 2$, $\mathfrak{A}_1$ e $\mathfrak{A}_2$ comaximais implica que $R = \mathfrak{A}_1 + \mathfrak{A}_2$. Então, $1 = u_1 + u_2$ com $u_1 \in \mathfrak{A}_1$ e $u_2 \in \mathfrak{A}_2$. Para $e_1 = 1 - u_1$ e $e_2 = 1 - u_2$, temos que $e_1 \equiv 0 \,(\text{mod}\ \mathfrak{A}_2)$, $e_1 \equiv 1 \,(\text{mod}\ \mathfrak{A}_1)$, $e_2 \equiv 0 \,(\text{mod}\ \mathfrak{A}_1)$ e $e_2 \equiv 1 \,(\text{mod}\ \mathfrak{A}_2)$. Seja $\alpha = e_1\alpha_1 + e_2\alpha_2$, então

$$\alpha \equiv \alpha_i \,(\text{mod}\ \mathfrak{A}_i A),\ \text{para}\ i = 1, 2.$$

Suponhamos a afirmação verdadeira para todo inteiro menor que r. Então, existe $\alpha' \in A$, tal que

$$\alpha' \equiv \alpha_i \,(\text{mod}\ \mathfrak{A}_i A), \forall\, i = 1, \ldots, r-1. \tag{4.5}$$

Como $\mathfrak{A}_r$ e $\mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_{r-1}$ são comaximais, pelo caso $r = 2$, existe $\alpha \in A$ tal que

$$\alpha \equiv \alpha' \,(\text{mod}\ (\mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_{r-1})A) \quad e \quad \alpha \equiv \alpha_r \,(\text{mod}\ \mathfrak{A}_r A). \tag{4.6}$$

Então, $\alpha - \alpha' \in (\mathfrak{A}_1 \cap \ldots \cap \mathfrak{A}_{r-1})A \subset \mathfrak{A}_i A$, para todo $i = 1, \ldots, r-1$. Isto é,

$$\alpha \equiv \alpha' \,(\text{mod}\ \mathfrak{A}_i A), \forall\, i = 1, \ldots, r-1.$$

Segue das equações (4.5) e (4.6), que $\alpha \equiv \alpha_i(\text{mod}\ \mathfrak{A}_i A)$, para todo $i = 1, \ldots, r$. ■

Proposição 4.4 (COHEN)**.** *Seja R um domínio de integridade Noetheriano para o qual $\mu^*(R_{\mathfrak{M}}) \leq k$, para todo ideal maximal $\mathfrak{M}$. Então,* $\mathbb{K} - \dim R \leq 1$ *(dimensão de Krull) e $\mu^*(R) \leq \max\{2, k\}$.*

Demonstração. Primeiro mostraremos que todo ideal primo próprio de R é maximal. De fato, seja $\mathfrak{p}$ um ideal primo próprio de R. Então, $\mathfrak{p} \subset \mathfrak{M}$, para algum $\mathfrak{M} \subset R$ ideal maximal. Como $\mu^*(R_{\mathfrak{M}}) \leq k$, temos que $R_{\mathfrak{M}}$ tem posto finito. Logo, pelo Teorema 4.1, $R_{\mathfrak{M}}$ satisfaz a condição da cadeia mínima restrita, ou equivalentemente, todo ideal primo próprio de $R_{\mathfrak{M}}$ é maximal. Mas, $\mathfrak{p}R_{\mathfrak{M}} \subseteq R_{\mathfrak{M}}$ é um ideal primo próprio. Logo, $\mathfrak{p}R_{\mathfrak{M}} = \mathfrak{M}R_{\mathfrak{M}}$.

Afirmamos que $\mathfrak{p}R_{\mathfrak{M}} = \mathfrak{M}R_{\mathfrak{M}}$ implica $\mathfrak{p} = \mathfrak{M}$. De fato, se $\mathfrak{p}R_{\mathfrak{M}} = \mathfrak{M}R_{\mathfrak{M}}$, teremos que, para todo $m \in \mathfrak{M}$, existem $p \in \mathfrak{p}$ e $b \notin \mathfrak{M}$ tais que $m/1 = p/b$ em $R_{\mathfrak{M}}$. Logo, existe $a \notin \mathfrak{M}$, tal que $a(p - bm) = 0$ em R. Mas, R é domínio de integridade, então $bm = p \in \mathfrak{p}$ e $m \in \mathfrak{p}$, pois $b \notin \mathfrak{M}$ e $\mathfrak{M} \subset \mathfrak{p}$. Portanto, $\mathfrak{M} = \mathfrak{p}$.

Da afirmação anterior segue que $(0) \subseteq \mathfrak{p}$ é a maior cadeia possível de ideais primos em R. Portanto, $\dim R \leq 1$. Vale observar que R pode não ter ideais primos próprios, isto é, R pode ser um corpo e, nesse caso, $\dim(R) = 0$.

Suponhamos agora que $\mu^*(R_{\mathfrak{M}}) \leq k = 1$, isto é, $\mu^*(R_{\mathfrak{M}}) = 1$. Então, $\mathfrak{M}R_{\mathfrak{M}}$ é principal, para todo $\mathfrak{M} \subset R$ maximal. Temos ainda que $\dim(R) = 1$ implica $\dim(R_{\mathfrak{M}}) = 1$ (todo ideal primo de $R_{\mathfrak{M}}$ é da forma $\mathfrak{p}R_{\mathfrak{M}}$, onde $\mathfrak{p}$ é um ideal primos de R contido em $\mathfrak{M}$). Logo, pela Proposição 2.25, temos que $R_{\mathfrak{M}}$ é um anel de valorização discreta. Mas, todo primo de R é maximal, logo $R_{\mathfrak{p}}$ é anel de valorização discreta, para todo $\mathfrak{p}$ ideal primo. Segue do Teorema 2.8 que R é um domínio de Dedekind. Portanto, pelo Lema 3.11, $\mu^*(R) = 2$. Concluímos então, que para $k = 1$, $\mu^*(R) = 2 = \max\{2, k = 1\}$.

No que segue trataremos do caso, $\mu^*(R_{\mathfrak{M}}) \leq k$ e $k > 1$.

Seja $\mathfrak{A}$ um ideal não nulo em R. Então, exite somente um número finito de ideais maximais contendo $\mathfrak{A}$. Para ver isso, usamos que R é um anel Noetheriano e, portanto, pelo Teorema 2.6, $\mathfrak{A} = \bigcap\limits_{i=1}^{n} \mathfrak{q}_i$, onde $\mathfrak{q}_i$ são ideais primários tais que seus radicais são ideais primos distintos. Sejam $\mathfrak{p}_i = r(\mathfrak{q}_i)$, $\forall\, i = 1, \ldots, n$. Então, pelo Teorema 2.9, os ideais $\mathfrak{p}_i$ são os primos minimais contendo $\mathfrak{q}_i$ e, pela Proposição 2.11:

$$\{\mathfrak{p}_j \in Assoc(\mathfrak{A}) \ : \ \mathfrak{p}_j \text{ é } isolado\} = \left\{\begin{matrix} Os\ elmentos\ minimais\ no\ conjunto\ de\ todos \\ os\ ideais\ primos\ contendo\ \mathfrak{A} \end{matrix}\right\}$$

Como todos os ideais maximais contendo $\mathfrak{A}$ pertencem ao 2º membro da igualdade, concluimos que a cardinalidade de ideais maximais contendo $\mathfrak{A}$ é finita.

Sejam $\mathfrak{M}_1, \ldots, \mathfrak{M}_n$ os ideais maximais contendo $\mathfrak{A}$ e

$$\mathfrak{A}R_{\mathfrak{M}_i} = \langle \frac{\alpha_{i1}}{1}, \frac{\alpha_{i2}}{1}, \ldots, \frac{\alpha_{ik}}{1} \rangle, \ \forall\, i = 1, \ldots, n,$$

já que $\mu^*(R_{\mathfrak{M}}) \leq k$. Sendo $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_n$ ideais comaximais de R e $\alpha_{11}, \alpha_{21}, \ldots, \alpha_{n1} \in \mathfrak{A}$, temos, pelo Lema 4.8, que existe $\alpha_1 \in \mathfrak{A}$ tal que $\alpha_1 \equiv \alpha_{i1} \,(\mathrm{mod}\ \mathfrak{M}_i\mathfrak{A})$. Do mesmo modo, para $\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni} \in \mathfrak{A}$, existe $\alpha_i \in \mathfrak{A}$, tal que $\alpha_2 \equiv \alpha_{i2} \,(\mathrm{mod}\ \mathfrak{M}_i\mathfrak{A})$, $\forall\, i = 1, \ldots, n$.

Afirmamos que $\mathfrak{A}R_{\mathfrak{M}_1} = \left\langle \frac{\alpha_1}{1}, \frac{\alpha_{12}}{1}, \ldots, \frac{\alpha_{1k}}{1} \right\rangle$.

($\subseteq$) É óbvia.

($\subseteq$) Temos que $\alpha_1 \equiv \alpha_{11} \,(\mathrm{mod}\ \mathfrak{M}_1\mathfrak{A})$, ou seja, $\alpha_1 - \alpha_{11} \in \mathfrak{M}_1\mathfrak{A}$. Então,

$$\begin{aligned}
&\alpha_1 = \alpha_{11} + \textstyle\sum_{i=1}^{l} m_i u_i, \ \text{ com } m_1, \ldots, m_l \in \mathfrak{M}_1 \\
&\Rightarrow \frac{\alpha_1}{1} = \frac{\alpha_{11}}{1} + \sum_{i=1}^{l} \frac{m_i}{1}\frac{u_i}{1}, \ \text{ onde } \frac{u_i}{1} = \sum_{j=1}^{k} \frac{a_{ij}}{b_{ij}}\frac{\alpha_{1j}}{1} \\
&\Rightarrow \frac{\alpha_1}{1} = \frac{\alpha_{11}}{1} + \sum_{i=1}^{l} \frac{m_i}{1}(\sum_{j=1}^{k} \frac{a_{ij}}{b_{ij}}\frac{\alpha_{1j}}{1}) \\
&\Rightarrow \frac{\alpha_1}{1} = \frac{\alpha_{11}}{1} + \sum_{i=1}^{l}(\sum_{j=1}^{k}(\frac{m_i}{1}\frac{a_{ij}}{b_{ij}})\frac{\alpha_{1j}}{1}) \\
&\Rightarrow \frac{\alpha_1}{1} = \frac{\alpha_{11}}{1} + (\sum_{i=1}^{l}\frac{m_i}{1}\frac{a_{i1}}{b_{i1}})\frac{\alpha_{11}}{1} + \ldots + (\sum_{i=1}^{l}\frac{m_i}{1}\frac{a_{ik}}{b_{ik}})\frac{\alpha_{1k}}{1} \\
&\Rightarrow \frac{\alpha_1}{1} = \frac{\alpha_{11}}{1} + z_1\frac{\alpha_{11}}{1} + z_2\frac{\alpha_{12}}{1} + \ldots + z_k\frac{\alpha_{1k}}{1}, \ \text{ onde } z_i = \sum_{i=1}^{l}\frac{m_i}{1}\frac{a_{i1}}{b_{i1}} \in \mathfrak{M}_1R_{\mathfrak{M}_1}, \\
&\Rightarrow \frac{\alpha_1}{1} = (\frac{1}{1} + z_1)\frac{\alpha_{11}}{1} + z_2\frac{\alpha_{12}}{1} + \ldots + z_k\frac{\alpha_{1k}}{1}.
\end{aligned}$$

Como, $(1 + z_1) \notin \mathfrak{M}_1R_{\mathfrak{M}_1}$, temos que $(1 + z_1)$ é invertível em $R_{\mathfrak{M}_1}$ e

$$\mathfrak{A}R_{\mathfrak{M}_1} = \langle \frac{\alpha_{11}}{1}, \frac{\alpha_{12}}{1}, \ldots, \frac{\alpha_{1k}}{1} \rangle \subset \langle \frac{\alpha_1}{1}, \frac{\alpha_{12}}{1}, \ldots, \frac{\alpha_{1k}}{1} \rangle.$$

De maneira análoga, obtemos $\mathfrak{A}R_{\mathfrak{M}_i} = \left\langle \frac{\alpha_1}{1}, \frac{\alpha_{i2}}{1}, \ldots, \frac{\alpha_{ik}}{1} \right\rangle$, $\forall i = 1, \ldots, n$.

Sejam, $\mathfrak{N}_1, \ldots, \mathfrak{N}_r$ os ideais maximais de R contendo α_1. Como $\alpha_1 \in \mathfrak{A}$, os ideais maximais $\mathfrak{M}_i$ estão entre os $\mathfrak{N}_j$. Sem perda de generalidade, supomos $\mathfrak{N}_1 = \mathfrak{M}_1, \mathfrak{N}_2 = \mathfrak{M}_2, \ldots, \mathfrak{N}_n = \mathfrak{M}_n, \mathfrak{N}_{n+1}, \ldots, \mathfrak{N}_r$. Então,

$$\mathfrak{A}R_{\mathfrak{M}_i} = \left\langle \frac{\alpha_1}{1}, \frac{\alpha_{i2}}{1}, \ldots, \frac{\alpha_{ik}}{1} \right\rangle,$$

$\forall i = 1, \ldots, n$ e

$$\mathfrak{A}R_{\mathfrak{M}_{n+j}} = \left\langle \frac{\alpha_1}{1}, \frac{\alpha_{n+j,2}}{1}, \ldots, \frac{\alpha_{n+j,k}}{1} \right\rangle = R_{\mathfrak{N}_{n+1}},$$

$\forall\, j = 1, \ldots, r-n$, pois $\mathfrak{A} \nsubseteq R_{\mathfrak{M}_{n+j}}$.

Aplicando novamente o Lema 4.8, temos que existem $\alpha_i \in \mathfrak{A}$, $\forall\, i = 1, \ldots, k$, tais que $\alpha_i \equiv \alpha_{ji} \,(\mathrm{mod}\, \mathfrak{N}_j\mathfrak{A})$, $\forall\, j = 1, \ldots r$, e $\mathfrak{A}R_{\mathfrak{N}_j} = \left\langle \frac{\alpha_1}{1}, \frac{\alpha_2}{1}, \ldots, \frac{\alpha_k}{1} \right\rangle$.

Seja $\mathfrak{A}_0 = \langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle \subseteq R$. Então, $\mathfrak{A}_0 R_{\mathfrak{N}_j} = \mathfrak{A}R_{\mathfrak{N}_j}$, $\forall j = 1, \ldots, r$ e, se $\mathfrak{M} \neq \mathfrak{N}_j$, $\mathfrak{A}_0 R_{\mathfrak{M}} = \mathfrak{A}R_{\mathfrak{M}} = R_{\mathfrak{M}}$.

Concluindo, mos que $\mathfrak{A}_0 \subseteq \mathfrak{A} \subseteq R$ e se $\mathfrak{M} \subseteq R$ for um ideal maximal, como a sequência

$$0 \longrightarrow \mathfrak{A}_0 \longrightarrow \mathfrak{A} \longrightarrow \frac{\mathfrak{A}}{\mathfrak{A}_0} \longrightarrow 0,$$

é exata, segue da Proposição 2.6, que a sequência

$$0 \longrightarrow \mathfrak{A}_0 R_{\mathfrak{M}} \longrightarrow \mathfrak{A}R_{\mathfrak{M}} \longrightarrow (\frac{\mathfrak{A}}{\mathfrak{A}_0})R_{\mathfrak{M}} \longrightarrow 0$$

é exata. Mas, $\mathfrak{A}_0 R_{\mathfrak{M}} = \mathfrak{A}R_{\mathfrak{M}}$, implica $(\frac{\mathfrak{A}}{\mathfrak{A}_0})R_{\mathfrak{M}} = 0$, $\forall \mathfrak{M} \subseteq R$ ideal maximal, portanto, $\mathfrak{A} = \mathfrak{A}_0$. ■

Nesse ponto, podemos concluir a metade fácil do teorema principal. Mais precisamente, é possível afirmar que se R for um domínio de integridade Noetheriano, tal que todo R-módulo livre de torção é soma direta de módulos de posto 1, então, pelas Proposições 4.3 e 4.4, $\mu^*(R) \leq 2$.

Agora, começaremos a parte mais difícil que é a decomposição de certos módulos livres de torção.

Lema 4.9. *Seja R um domínio de integridade Noetheriano com $\mathbb{K} - \dim R \leq 1$ e sejam $\mathfrak{B} \subset \mathfrak{A}$ ideais não nulos de R tais que $\mathfrak{A}^{-1} = \mathfrak{B}^{-1}$. Então, se $\mu_R(\mathfrak{A}) \leq 2$, $\mathfrak{A} = \mathfrak{B}$.*

Demonstração. Sem perda de generalidade podemos supor que R é local. Se R não for local, seja $\mathfrak{M}$ um ideal maximal de R tal que $\mathfrak{B} \subset \mathfrak{A} \subset \mathfrak{M}$. Então, $\mathfrak{B}R_{\mathfrak{M}} \subset \mathfrak{A}R_{\mathfrak{M}} \subset \mathfrak{M}R_{\mathfrak{M}}$ e $(\mathfrak{B}R_{\mathfrak{M}})^{-1} = (\mathfrak{A}R_{\mathfrak{M}})^{-1}$, pois $\mathfrak{A}^{-1} = \mathfrak{B}^{-1}$. Além disso, $\dim R \leq 1$ e $\mu_R(\mathfrak{A}) \leq 2$ implicam que $\dim(R_{\mathfrak{M}}) \leq 1$ e $\mu_{R_{\mathfrak{M}}}(\mathfrak{A}R_{\mathfrak{M}}) \leq 2$. Assim, mostrando a afirmação no caso R regular, teremos $\mathfrak{B}R_{\mathfrak{M}} = \mathfrak{A}R_{\mathfrak{M}}$, para todo ideal $\mathfrak{M}$ maximal. Mais uma vez, usando que $\dim(R) \leq 1$, podemos afirmar que todo ideal prórpio de R é maximal e, portanto, $\mathfrak{B}R_\mathfrak{p} = \mathfrak{A}R_\mathfrak{p}$, para todo ideal $\mathfrak{p}$ primo. Logo, $\mathfrak{A} = \mathfrak{B}$.

Supondo R local, mostraremos que se $\mathfrak{B} \neq \mathfrak{A}$, então $\mathfrak{A}^{-1} \neq \mathfrak{B}^{-1}$. Divideremos a demonstração em afirmações para facilitar o entendimento.

Afirmação 1: Como $\mu_R(\mathfrak{A}) \leq 2$, podemos escrever $\mathfrak{A} = \langle a, b\rangle$, com $a \notin \mathfrak{B}$ e $b \in \mathfrak{B}$.

Seja $\mathfrak{M} \subseteq R$ o único ideal maximal de R. Porque $\mu_R(\mathfrak{A}) \leq 2$, temos que

$$\dim_{\mathbb{K}}(\frac{\mathfrak{A}}{\mathfrak{M}\mathfrak{A}}) \leq 2, \text{ onde } \mathbb{K} = \frac{R}{\mathfrak{M}}.$$

Logo, $\dfrac{\mathfrak{A}}{\mathfrak{M}\mathfrak{A}} = \langle \overline{b}, \overline{a}\rangle$, podendo a e b serem escolhidos de modo que $a \notin \mathfrak{B}$ e $b \in \mathfrak{B}$. Cosequentemente, temos $\mathfrak{A} = \langle b, a\rangle$.

Afirmação 2: Aumentando $\mathfrak{B}$ se necessário, podemos supor que $\dfrac{\mathfrak{A}}{\mathfrak{B}} \cong \dfrac{\mathfrak{R}}{\mathfrak{M}}$.

De fato, temos que $\dfrac{\mathfrak{A}}{\mathfrak{M}\mathfrak{A} + \langle b\rangle} \cong \dfrac{R}{\mathfrak{M}}$ e $\mathfrak{B} \subseteq \mathfrak{M}\mathfrak{A} + \langle b\rangle := \mathfrak{B}'$.

Além disso, como $\mathfrak{B} \subseteq \mathfrak{B}' \subseteq \mathfrak{A}$, então

$$\mathfrak{A}^{-1} \subseteq (\mathfrak{B}')^{-1} \subseteq \mathfrak{B}^{-1} = \mathfrak{A}^{-1} \Rightarrow (\mathfrak{B}')^{-1} = \mathfrak{A}^{-1}.$$

Aqui é importante observar que $\mathfrak{B}' \subsetneq \mathfrak{A}$, pois $\mathfrak{B}' = \mathfrak{A}$, implicaria $\mathfrak{M}\mathfrak{A} + \langle b\rangle = \mathfrak{A}$, e pelo Lema de Nakayama, $\mathfrak{A} = \langle b\rangle \subseteq \mathfrak{B}$.

Estamos então na seguinte situação: $\mathfrak{A} = \langle b, a\rangle$, $a \notin \mathfrak{B}$, $b \in \mathfrak{B}$ e $\mathfrak{B} = \mathfrak{M}\mathfrak{A} + \langle b\rangle$.

Afirmação 3: Nas condições acima, existe $y \in \mathfrak{B}^{-1}$, tal que $y \notin \mathfrak{A}^{-1}$.

Como $\dim R \leq 1$ e R é um domínio de integridade, temos que $\dim(R/\langle b\rangle) = 0$. Pelo Teorema 2.7, $R/\langle b\rangle$ é Artiniano. Consideremos então a seguinte cadeia em $R/\langle b\rangle$:

$$\ldots \subseteq \overline{\mathfrak{M}^k\mathfrak{B}} \subseteq \ldots \subseteq \overline{\mathfrak{M}^2\mathfrak{B}} \subseteq \overline{\mathfrak{M}\mathfrak{B}} \subseteq \overline{\mathfrak{B}} \subseteq \frac{R}{\langle b\rangle}.$$

Então, existe k tal que $\overline{\mathfrak{M}^k\mathfrak{B}} = \overline{\mathfrak{M}^{k+1}\mathfrak{B}} = \ldots$ e, pelo Corolário 2.1 do Lema de Nakayama, $\overline{\mathfrak{M}^k B} = \overline{0}$. Ou seja,

$$\begin{aligned} \mathfrak{M}^k\mathfrak{B} \subseteq \langle b\rangle \;\; &\Rightarrow \;\; \mathfrak{M}^k(\mathfrak{M} + \langle b\rangle) \subseteq \langle b\rangle \\ &\Rightarrow \;\; \mathfrak{M}^{k+1}\langle a, b\rangle + \mathfrak{M}^k\langle b\rangle \subseteq \langle b\rangle \\ &\Rightarrow \;\; \mathfrak{M}^{k+1}a \subseteq \langle b\rangle = Rb \end{aligned}$$

Seja $l = \min\{k : \mathfrak{M}^k a \subseteq Rb\}$. Então, $\mathfrak{M}^l a \subseteq Rb$ e $\mathfrak{M}^{l-1}a \nsubseteq Rb$. Seja $x \in \mathfrak{M}^{l-1}$, tal que $xa \notin Rb$. Então, $xb^{-1}a \notin R$ e, portanto, $xb^{-1} \notin \mathfrak{A}^{-1}$. Mas,

$$\mathfrak{M}xa \subseteq \mathfrak{M}^l a \subseteq Rb \Rightarrow \mathfrak{M}xa \subseteq Rb \Rightarrow \mathfrak{M}xab^{-1} \subseteq R \Rightarrow xb^{-1}\mathfrak{M}a \subseteq R.$$

Das igualdades $\mathfrak{B} = \mathfrak{M}\mathfrak{A} + \langle b \rangle = \mathfrak{M}a + \langle b \rangle$, segue que

$$xb^{-1}\mathfrak{B} = \underbrace{xb^{-1}\mathfrak{M}a}_{\subseteq R} + \underbrace{xb^{-1}R}_{\subseteq R}b \subseteq R.$$

Assim, $y = xb^{-1} \in \mathfrak{B}^{-1}$, mas $y = xb^{-1} \in \mathfrak{A}^{-1}$. Absurdo, pois por hipótese, $\mathfrak{A}^{-1} = \mathfrak{B}^{-1}$. Logo, $\mathfrak{B} = \mathfrak{A}$. ■

Proposição 4.5. *Seja R um domínio de integridade Noetheriano, tal que $\mu^*(R) \leq 2$. Então, um submódulo projetivo fechado de um R-módulo livre de torção é um somando direto.*

Demonstração. Pelos Teorema 3.3 e Corolário 3.4 em [5], é suficiente provar que $\mathfrak{A} = (\mathfrak{A}^{-1})^{-1}$, para todo ideal não nulo $\mathfrak{A}$ em R. Como $\mu^*(R) \leq 2$ e, todo ideal em $R_\mathfrak{p}$, para ideal primo $\mathfrak{p}$ de R é estendido, temos que $\operatorname{rank}(R_\mathfrak{p}) \leq 2$, $\forall$ ideal primo $\mathfrak{p}$ em R. Então, pela Proposição 4.4, $\dim R \leq 1$. Por outro lado, sabemos que $\mathfrak{A} \subset (\mathfrak{A}^{-1})^{-1}$ e, como $\mu_R((\mathfrak{A}^{-1})^{-1}) \leq 2$, segue do Lema 4.9, que $\mathfrak{A}^{-1} = ((\mathfrak{A}^{-1})^{-1})^{-1}$. Para concluir, observamos que $((\mathfrak{A}^{-1})^{-1})^{-1} = \mathfrak{A}$. ■

Observação 4.3. Na demonstração da Proposição 4.5, aplicamos o Lema 4.9 a $\mathfrak{A} \subset (\mathfrak{A}^{-1})^{-1}$, embora $(\mathfrak{A}^{-1})^{-1}$ não seja necessariamente um ideal de R. Porém, para a demonstração do lema precisamos apenas que $(\mathfrak{A}^{-1})^{-1}$ seja gerado por no máximo dois elementos, o que de fato acontece pois $(\mathfrak{A}^{-1})^{-1}$, por ser um ideal fracionário, é da forma

$$(\mathfrak{A}^{-1})^{-1} = \frac{1}{z}I,$$

para algum $z \in R$ e algum ideal $I \subset R$. De $\mu^*(R) \leq 2$, segue que I é gerado por no máximo dois elementos.

Lema 4.10. *Seja R um domínio de integridade local Noetheriano com ideal maximal $\mathfrak{M}$ e fecho inteiro $\overline{R}$. Suponhamos $\mu^*(R) = 2$. Então,*

i) *$R_1 = \mathfrak{M}^{-1}$ é um anel próprio finitamente gerado e inteiro sobre R.*

ii) *Todo ideal não principal $\mathfrak{A}$ de R é um R-módulo; isto é, $R_1\mathfrak{A} = \mathfrak{A}$.*

iii) *Se S é um anel próprio finitamente gerado e inteiro sobre R, então $R_1 \subseteq S$ e $\mu^*(S) \leq 2$.*

Demonstração. (i) Pela definição de $\mathfrak{M}^{-1}$, temos que $\mathfrak{M} \subseteq \mathfrak{M}\mathfrak{M}^{-1} \subseteq R$. Como $\mathfrak{M}$ é ideal maximal de R, temos que $\mathfrak{M}\mathfrak{M}^{-1} = \mathfrak{M}$ ou $\mathfrak{M}\mathfrak{M}^{-1} = R$. Se $\mathfrak{M}\mathfrak{M}^{-1} = R$, teremos

$$1 = x_1y_1 + \ldots + x_ny_n, \text{ onde } x_i \in \mathfrak{M} \text{ e } y_i \in \mathfrak{M}^{-1}.$$

Mas $1 \notin \mathfrak{M}$, logo $x_jy_j \notin \mathfrak{M}$, para algum $j = 1, \ldots, n$ e, portanto, existe $u \in R$ tal que $u(x_iy_i) = 1$. Nesse caso, $\mathfrak{M} = \langle x_j \rangle$. Conclusão: R é domínio de integridade Noetheriano, local, $\mu^*(R_{\mathfrak{M}}) \leq 2$ (já que $\mu^*(R) \leq 2$), $\dim R \leq 1$ (Proposição 4.4) e $\mathfrak{M}$ é um ideal principal. Então, R é um anel de valorização discreta (e também um DIP), o que implica $\mu^*(R) = 1$. Absurdo.

Logo, $\mathfrak{M}\mathfrak{M}^{-1} = \mathfrak{M}$.

Para ver que $R_1 = \mathfrak{M}^{-1}$ é um anel, basta provarmos que é fechado sob o produto. Usando que $\mathfrak{M}\mathfrak{M}^{-1} = \mathfrak{M}$, temos que $ma, mb \in R$, $\forall\, m \in \mathfrak{M}$ e $\forall\, a, b \in \mathfrak{M}^{-1}$. Logo, $m(ab) = (ma)b \in R$, pois $ma \in \mathfrak{M}$.

Afirmamos que $R_1 = \mathfrak{M}^{-1}$ é inteiro sobre R. Para provar isso, usaremos o truque do determinante. Suponhamos $\mathfrak{M} = \langle x_1, \ldots, x_n \rangle$, como R-módulo. Dado $a \in R_1$, temos $ax_i \in \mathfrak{M} = \langle x_1, \ldots, x_n \rangle$, para todo $i = 1, \ldots, n$. Logo,

$$\begin{array}{ccccccccc} ax_1 & = & a_{11}x_1 & + & a_{12}x_2 & + & \ldots & + & a_{1n}x_n \\ ax_2 & = & a_{21}x_1 & + & a_{22}x_2 & + & \ldots & + & a_{2n}x_n \\ \vdots & & & & \vdots & & & & \\ ax_n & = & a_{n1}x_1 & + & a_{n2}x_2 & + & \ldots & + & a_{nn}x_n \end{array}$$

ou equivalentemente,

$$\underbrace{\begin{bmatrix} (a_{11} - a) & a_{12} & \ldots & a_{1n} \\ a_{21} & (a_{22} - a) & \ldots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \ldots & (a_{nn} - a) \end{bmatrix}}_{A \in M_{n\times n}(R)} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{4.7}$$

Multiplicando o sistema (4.7) pela matriz adjunta de A, temos que $\operatorname{adj}(A)AX = \operatorname{adj}(A)0 = 0$. Logo, $\det(A)I_nX = 0$, isto é, $\det(A)x_i = 0$, para todo $i = 1, \ldots, n$. Como $\mathfrak{M} \neq 0$, $0 = \det(A)$. Mas, $\det(A)$ é um polinômio mônico em a, coeficentes em R, de grau no máximo n. Ou seja, a é inteiro sobre R.

Para concluirmos o item (i) devemos mostrar que R_1 é prórpio, isto é, $R \subsetneq R_1$.

Primeiramente, observamos que, pela Proposição 4.4, $\dim R \leq 1$. Porém, $\dim R = 0$, implicaria que R é um corpo e $\mu^*(R) = 1$. Absurdo, pois por hipótese $\mu^*(R) = 2$. Portanto, $\dim R = 1$.

Afirmamos que $\mathfrak{M}$ é primo de um ideal principal, isto é, exite $a \in R$, tal que $\sqrt{\langle a \rangle} = \mathfrak{M}$. Dado, $a \in R$, como R é Noetheriano, temos que $\langle a \rangle = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$, onde $\mathfrak{q}_i$ são primários e $r(\mathfrak{q}_i) = \mathfrak{p}_i$ são ideiais primos distintos. Mas, $\dim R = 1$, implica que todo ideal primo não nulo é maximal e, como R é local, $r = 1$ e $\mathfrak{M} = \mathfrak{p}_1$. Nesse caso, temos que $(Ra : \mathfrak{M}) \neq Ra$. Para ver isso, usamos que $\sqrt{\langle a \rangle} = \mathfrak{M}$ implica $\mathfrak{M}^s \subset Ra$, para algum $s \geq 0$ e, portanto, $(Ra : \mathfrak{M}^s) = R$. Se $(Ra : \mathfrak{M}) = Ra$, teríamos $Ra = (Ra : \mathfrak{M}^s) = R$ e $\mathfrak{M} = R$.

Finalmente, se $\mathfrak{M}$ é primo de um ideal principal, vamos mostrar que $R \neq R_1$. Sabemos que $(Ra : \mathfrak{M}) \neq Ra$, podemos afirmar que existe $x \in (Ra : \mathfrak{M})$ tal que $x \notin Ra$. Então, $x\mathfrak{M} \subseteq Ra$ e $x \notin Ra$. Logo, $\dfrac{x}{a}\mathfrak{M} \subseteq R$ e $\dfrac{x}{a} \notin R$. Ou seja, $\dfrac{x}{a} \in R_1 = \mathfrak{M}^{-1}$ e $\dfrac{x}{a} \notin R$. Portanto, $R \neq R_1$.

(ii) Seja $R \subseteq \mathfrak{A}$ um ideal fracionário não principal e seja $\mathfrak{B} = \mathfrak{M}^{-1}\mathfrak{A}$. Então, $\mathfrak{M}\mathfrak{B} = \mathfrak{M}\mathfrak{M}^{-1}\mathfrak{A} = \mathfrak{M}\mathfrak{A}$, pois $\mathfrak{M}\mathfrak{M}^{-1} = \mathfrak{M}$. Como $\mathfrak{A}$ é um R-módulo não principal e $\mu^*(R) = 2$, $\dim_{R/\mathfrak{M}}(\dfrac{\mathfrak{A}}{\mathfrak{M}\mathfrak{A}}) = 2$ e $\mathfrak{A} = \langle a, b\rangle$, com a, b linearmente independente sobre $\mathfrak{M}\mathfrak{A}$. Mas, $\mathfrak{M}\mathfrak{B} = \mathfrak{M}\mathfrak{M}^{-1}\mathfrak{A} = \mathfrak{M}\mathfrak{A}$, nos diz que a, b são linearmente independentes sobre $\mathfrak{M}\mathfrak{B}$ e que $\dfrac{\mathfrak{B}}{\mathfrak{M}\mathfrak{B}} = \bar{a}\mathbb{K} \oplus \bar{b}\mathbb{K}$, onde $\mathbb{K} = R/\mathfrak{M}$, já que $\mu_R(\mathfrak{B}) \leq 2$. Portanto, $\mathfrak{B} = \langle a, b\rangle$, como R-módulo e $\mathfrak{M}^{-1}\mathfrak{A} = \mathfrak{A}$.

(iii) Seja S um anel próprio finito e inteiro sobre R. Então, S é ideal fracionário e, se S não for principal, por (ii), tem-se que $R_1S = S$. Então, $R_1 \subseteq R_1S = S$.

Para ver que $\mu^*(S) \leq 2$, basta ver um S-ideal como um R-ideal. ■

Lema 4.11. *Seja R é um anel comutativo Noetheriano e $0 \to A \to B \to C \to 0$ uma sequência exata de R-módulos finitamente gerados. Então, a sequência se decompõe, se e somente se, a sequência se decompõe localmente.*

Demonstração. Ver [14], Teorema 1 (3E), pág.21. ■

Lema 4.12. *Seja R um domínio de integridade Noetheriano local com ideal maximal $\mathfrak{M}$ e $\mathbb{K} - \dim R = 1$. Seja A um R-módulo livre de torção e $\alpha \in A\backslash\{0\}$, tal que $\overline{\{\alpha\}}$ é um somando direto de A. Então, existe um inteiro $n > 0$ tal que se $\alpha' \equiv \alpha$ $(mod\, \mathfrak{M}^n A)$, $\overline{\{\alpha'\}}$ é um somando direto de A.*

Demonstração. Escrevamos $A = A_0 \oplus B$, onde

$$A_0 = \overline{\{\alpha\}} = \{\gamma \in A : \exists\, r \in R\backslash\{0\},\ \text{tal que } r\gamma \in R\alpha\}.$$

$\vdash$: Existe $a \in R$, $a \neq 0$, tal que $aA_0 \subseteq R\alpha$. A_0 sendo um somando direto de um módulo finitamente gerado é finitamente gerado. Suponhamos $A_0 = Rx_1 + Rx_2 + \ldots + Rx_m$. Como $x_i \in A_0$, $\forall\, i = 1, \ldots, m$, existem $r_i \in R\backslash\{0\}$, tais que $r_ix_i \in R\alpha$. Então, $a = r_1r_2\ldots r_m \in R$ é não nulo e $aA_0 \subseteq R\alpha$.

$\vdash$: Existe um inteiro $n > 0$ tal que $\mathfrak{M}^n \subseteq a\mathfrak{M}$. Como R é Noetheriano, pelo Teorema 2.6, $\langle a\rangle$ possui decomposição primária, isto é, $\langle a\rangle = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_l$, onde $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Mas, R é local e $\mathbb{K} - \dim R = 1$. Então, $l = 1$ e $\mathfrak{p}_1 = \mathfrak{M} = r(\langle a\rangle)$. Logo, existe um inteiro $s > 0$, tal que $\mathfrak{M}^s \subseteq \langle a\rangle$. Assim, $\mathfrak{M}^{s+1} = \mathfrak{M}^s\mathfrak{M} \subseteq \langle a\rangle\, \mathfrak{M} = a\mathfrak{M}$.

$\vdash$: Seja $n > 0$ tal que $\mathfrak{M}^n \subseteq a\mathfrak{M}$ e seja $\alpha' \equiv \alpha\, (\text{mod } \mathfrak{M}^n A)$. Então, podemos escrever $\alpha' = \alpha + \beta$, com $\beta \in B$. De fato, $\alpha' - \alpha \in \mathfrak{M}^n A$, implica

$$\alpha' = \alpha + \beta,\ \text{com } \beta \in \mathfrak{M}^n A = \mathfrak{M}^n(A_0 \oplus B) = \mathfrak{M}^n A_0 \oplus \mathfrak{M}^n B \Rightarrow$$

$$\beta = \beta_0 + \beta_1, \text{ onde } \beta_0 \in A_0\mathfrak{M}^n \text{ e } \beta_1 \in \mathfrak{M}^n B \subset B \Rightarrow$$
$$\beta_0 \in \mathfrak{M}^n A_0 \subseteq \mathfrak{M} a A_0 \subseteq \mathfrak{M} R\alpha = \mathfrak{M}\alpha.$$

Assim, $\beta_0 = m\alpha$, para algum $m \in \mathfrak{M}$ e $\alpha + \beta_0 = (1+m)\alpha$. Desde que $1+m$ é uma unidade em R, $A_0 = \overline{\{\alpha(1+m)\}}$ e, trocando α por $(1+m)\alpha$, podemos assumir que $\beta = \beta_1 \in B$.

$\vdash$: Seja $A_0' = \overline{\{\alpha'\}}$ em A. Afirmamos que $A_0' \cap B = \{0\}$. Seja $\gamma \in A_0' \cap B$. Então,

$$\gamma \in A_0' \Rightarrow t\gamma = s\alpha', \text{ para algum } t \in R\backslash\{0\} \text{ e algum } s \in R,$$
$$\text{e } \gamma \in B \Rightarrow t\gamma \in B \Rightarrow t\gamma = s\alpha' = s(\alpha+\beta) = \underbrace{s\alpha}_{\in A_0} + \underbrace{s\beta}_{\in B}$$

Logo,

$$s\alpha = 0 \Rightarrow s = 0 \ (A \text{ é livre de torção }) \Rightarrow t\gamma = 0 \Rightarrow \gamma = 0.$$

$\vdash$: Seja $A' = A_0' \oplus B$. Então, $A = A'$. Para isso, é suficiente mostrar que $A_0 \subseteq A'$. Seja $\gamma \in A_0 = \overline{\{\alpha\}}$. Então, $a\gamma \in aA_0 \subset R\alpha$, ou seja, $a\gamma = r\alpha \in A$, para algum $r \in R$ e, portanto, $a\gamma = r\alpha = r(\alpha' - \beta)$. Lembrando que, $\beta \in \mathfrak{M}^n A \subseteq a\mathfrak{M}A \subseteq aA$, podemos escrever $\beta = a\beta'$, para algum $\beta' \in A$. Então,

$$a\gamma = r\alpha' - ra\beta' \Rightarrow a(\gamma + r\beta') = r\alpha' \in A_0' \subseteq A_0' \oplus B = A'.$$

Porém, já que B é fechado em A ($B \cong A/A_0$), e $a\beta' = \beta \in B$, temos que $\beta' \in B$. Logo, $r\beta' \in B \subseteq A'$ e, finalmente, $\gamma \in A'$. ■

4.3 CONDIÇÃO SUFICIENTE PARA A DECOMPOSIÇÃO

Na demonstração do Teorema 4.4, faremos indução no comprimento $l(\overline{R}/R)$, onde $\overline{R}$ é o fecho inteiro de R. O caso $l(\overline{R}/R) = 0$ é o caso clássico para domínios de Dedekind que será demonstrado na seção a seguir.

4.3.1 Decomposição de módulos livres de torção sobre domínios de Dedekind

O objetivo dessa seção é mostrar que se R for um domínio de Dedekind, então todo R-módulo livres de torção é soma direta de módulos de posto 1. Mais precisso, mostraremos que se for um domínio de integridade no qual todo ideal finitamente gerado é invertível, então todo R-módulo livre de torção é soma direta de módulos de posto 1.

Os resultados apresentados nesta seção podem ser encontrados em [11].

Definição 4.3. Sejam R um domínio de integridade e M um R módulo. Um submódulo S de M é *puro* se

$$\alpha S = S \cap \alpha M, \ \forall\, \alpha \in R.$$

Lema 4.13. *Sejam M um R-módulo. Então,*

i) Qualquer somando direto de M é um submódulo puro;

ii) Um submódulo puro de um submódulo puro é puro;

iii) O submódulo de torção de M é puro;

iv) M/S livre de torção implica S puro;

v) Se M for livre de torção, $\bigcap_{i\in I} S_i$, onde S_i são submódulos puros, é puro.

Demonstração. $i)$ Suponhamos $M = S \oplus N$ e seja $s \in S \cap \alpha M$. Então, $s = \alpha m = \alpha(s_1 + n)$, onde $s_1 \in S$, $m \in M$ e $n \in N$. Logo,

$$s = \alpha(s_1 + n) \Rightarrow s - \alpha s_1 = \alpha n \in S \cap N = \{0\} \Rightarrow \alpha n = 0 \Rightarrow s = \alpha s_1 \in S.$$

$ii)$ Sejam $T \subset S \subset M$ submódulos de M tais que $\beta T = T \cap \beta S$, $\forall\, \beta \in R$, e $\alpha S = S \cap \alpha M$, $\forall\, \alpha \in R$. Então,

$$\beta T = T \cap \beta S = T \cap (S \cap \beta M) = (T \cap S) \cap (\beta M) = T \cap \beta M.$$

$iii)$ Seja $T(M)$ o submódulo de torção de M. Então, $\alpha T(M) \subset T(M) \cap \alpha M$, $\forall\, \alpha \in R$. Reciprocamente, se $m \in T(M) \cap \alpha M$, existe $r \in R$, não nulo, tal que $rm = 0$. Por outro lado, $m = \alpha m_1$, para algum $m_1 \in M$. Logo, $r(\alpha m) = (r\alpha)m_1 = 0$, ou seja, $m_1 \in T(M)$.

$iv)$ Seja S submódulo de M tal que M/S é livre de torção. Se $s \in S \cap \alpha M$, então $s = \alpha m$, para algum $m \in M$. Logo,

$$\overline{0} = \overline{s} = \overline{\alpha m} = \alpha \overline{m} \Rightarrow \overline{m} = \overline{0} \Rightarrow m \in S, \text{ se } \alpha \neq 0.$$

$v)$ Sejam S_i submódulos de M tais que $\alpha S_i = S_i \bigcap \alpha M$, para todo i e para todo $\alpha \in R$. Então,

$$\alpha(\bigcap_i S_i) = \bigcap_i (\alpha S_i) = \bigcap_i (S_i \cap \alpha M) = (\bigcap_i S_i) \cap \alpha M.$$

■

Observação 4.4. Sejam M um R-módulo e S um subconjunto de M. O fecho $\overline{S}$ de S de um R-módulo M é puro, pois $M/\overline{S}$ é livre de torção. Logo, pelo item $v)$ do Lema 4.13, a interseção de todos os submódulos puros S_i, tais que $S \subset S_i$, é o menor submódulo puro de M contendo S. É fácil ver que $\overline{S}$ está contido em qualquer submódulo puro contendo S, portanto, é o menor submódulo puro de M, contendo S.

Definição 4.4. Um R-módulo M é dito ser divisível se $\alpha M = M$, para todo $\alpha \in R\backslash\{0\}$.

Lema 4.14. *Seja M um R-módulo divisível. Um submódulo N de M é divisível, se e somente se, é puro.*

Demonstração. Seja N submódulo divisível de M. Então,

$$\beta N = N, \forall\, \beta \in R\backslash\{0\} \Rightarrow \beta N = \beta N \cap \beta M = N \cap \beta M,$$

ou seja, todo submódulo divisível de um módulo qualquer é puro. Reciprocamente, suponhamos M tal que $\alpha M = M$, para todo $\alpha \in R\backslash\{0\}$, e seja N um submódulo puro de M. Então, $\beta N = N \cap \beta M = N \cap M = M, \forall \beta \in R$. ■

Lema 4.15. *Sejam M um R-módulo, S um submódulo de M, tal que $M/S = \bigoplus_{i \in I} U_i$ e T_i a imagem inversa de U_i em M. Suponhamos que S é somando direto em cada T_i. Então, S é um somando direto de M.*

Demonstração. Se $T_i = S \oplus W_i$, seja $W = \bigcup_{i \in I} W_i$. Então, $M = S + W$ e $S \cap W = \{0\}$, pois

$$\begin{aligned} x \in S \cap W \quad &\Rightarrow x = \textstyle\sum_{i=1}^{k} y_i;\ y_i \in W_i \text{ e } \overline{x} = \sum_{i=1}^{k} \overline{y_i} = \overline{0} \in M/S \\ &\Rightarrow y_i \in S, \forall\, i = 1, \ldots, k \Rightarrow y_i \in S \cap W_i = \{0\}. \end{aligned}$$

■

Proposição 4.6. *Sejam R um domínio de integridade, M um R-módulo e $S \subset M$ um submódulo, tal que $M/S \cong \bigoplus_{j \in J} I_j$ e I_j é isomorfo a um ideal invertível de R, para todo $j \in J$. Então, S é um somando direto de M.*

Demonstração. Pelo Lema 4.15, podemos supor que $M/S \cong I$, onde I é um R-módulo invertível. Suonhamos inicialmente que M é livre de torção. Devemos mostrar que $M = S \oplus T$, para algum submódulo T de M. Por hipótese, $II^{-1} = R$ e, portanto, existem $\alpha_i \in I$, $\beta_i \in I^{-1}$, tais que $\sum \alpha_i \beta_i = 1$. Sejam $\pi : M \to M/S$ a projeção canônica e $f : M/S \to I$ isomorfismo. Então, para todo i, $\alpha_i = f \circ \pi(x_i)$, para algum $x_i \in M$. Dado $\gamma \in I - \{0\}$, sejam $z = \sum(\gamma\beta_i)x_i \in M$ e T o menor submódulo puro de M que contém o submódulo gerado por z (veja Observação 4.4). Mostraremos que que $M = S \oplus T$.

$\vdash$: $S \cap T = \{0\}$. Se $y \in S \cap T$, $y \in S$ e $y \in T \subset \overline{\{z\}}$ (Observação 4.4). Logo, existem $r, t \in R$, $r \neq 0$, tais que

$$\begin{aligned} ry = tz = \textstyle\sum t(\gamma\beta_i)x_i \quad &\Rightarrow f(\pi(ry)) = rf(\pi(y)) = rf(0) = 0 \\ &\Rightarrow t(\gamma\beta_i) \textstyle\sum f(\pi(x_i)) = 0 \Rightarrow (t\gamma) \sum \beta_i \alpha_i = 0 \\ &\Rightarrow t\gamma = 0 \Rightarrow t = 0, (\gamma \neq 0 \text{ e } M \text{ é livre de torção}) \\ &\Rightarrow ry = 0 \Rightarrow y = 0, \text{ pois } M \text{ é livre de torção.} \end{aligned}$$

$\vdash$: $M = T + S$. Basta mostrarmos que $\pi(T) = M/S$. Como $M/S \cong I = \langle \alpha_1, \ldots, \alpha_k \rangle$, sejam $\alpha_1 = f(y_1), \ldots, \alpha_k = f(y_k)$, onde $y_i = \pi(x_i) \in M/S$, para todo i. Se mostrarmos que $y_i = \pi(t_i)$, para algum $t_i \in T$, o resultado segue. Seja,

$$t_i = \alpha_i \gamma^{-1} z = \alpha_i \gamma^{-1}(\sum (\gamma \beta_j) x_j) = \sum (\alpha_i \beta_j) x_j \Rightarrow$$

$$f(\pi(t_i)) = f(\pi(\sum (\alpha_i \beta_j) x_j)) = \sum (\alpha_i \beta_j) f(y_j) \Rightarrow$$

$$f(\pi(t_i)) = \sum (\alpha_i \beta_j) \alpha_j = \alpha_i = f(y_i) \Rightarrow \pi(t_i) = y_i.$$

Finalmente, se M não for livre de torção, seja $\phi : F = \bigoplus_{i \in I} R \to M$, um R-homomorfismo sobrejetor. Então,

$$F = \bigoplus_{i \in I} R \xrightarrow{\phi} M \xrightarrow{\pi} M/S \cong \bigoplus_{j \in J} I_j$$

e, para $G = \ker(\pi \circ \phi)$, temos que

$$F \to F/G \cong M/S \cong \bigoplus_{j \in J} I_j.$$

Logo, pelo que acabamos de mostrar, $F = G \oplus H$. Seja $V = \phi(H) \subset M$. Então,

$$\pi(\phi(F)) = \pi(\phi(G + H)) = \pi(\phi(G)) + \pi(\phi(H)) = \pi(\phi(H)) = \pi(V),$$

ou seja, $M = S + V$. Para ver que M é soma direta de S e V, observe que $V = \phi(H)$ e $\pi(V) = \pi(\phi(H))$. Logo, se $s = \phi(h)$, para $s \in S$ e $h \in H$, teremos

$$\pi(s) = \pi(\phi(h)) = 0 \Rightarrow h \in G \Rightarrow h \in G \cap H = \{0\} \Rightarrow s = 0.$$

∎

Teorema 4.2. *Seja R um domínio de integridade no qual todo ideal finitamente gerado é invertível e seja M um R-módulo com submódulo de torção T. Então, T é somando direto de M e M/T é isomorfo a uma soma direta de módulos de posto* 1 *(isomorfos a ideais invertíveis).*

Demonstração. A demonstração de que T é somando direto de M segue do Lema 4.6 assim que provarmos que M/T é soma direta de módulos invertíveis. Suponhamos M livre de torção e sejam $z \in M - \{0\}$ e I_1 o menor submódulo puro de M contendo o submódulo gerado por z, isto é, $I_1 = \overline{\{z\}}$, o fecho de $\{z\}$ em M. Então, I_1 é puro de posto 1 e, por hipótese, invertível. Como M/I_1 é livre de posto estritamente menor que o posto de M, usamos indução, temos $M/I_1 \cong I_2 \oplus \ldots \oplus I_n$, onde os I_i são invertíveis. Logo, $M = I_1 \oplus M_2$, com $M_2 \cong I_2 \oplus \ldots \oplus I_n$. ∎

Teorema 4.3. *Sejam R um domínio de Dedekind e M um R-módulo finitamente gerado e livre de torção. Então, M é isomorfo a uma soma direta de módulos de posto* 1.

Demonstração. Segue do Lema 3.9 que todo ideal de R é invertível. Pelo Teorema 4.2, o resultado segue. ■

Corolário 4.1. *Sejam R um domínio de ideais principais e M um R-módulo finitamente gerado e livre de torção. Então, M é isomorfo a uma soma direta de módulos de posto* 1.

Demonstração. Todo domínio de ideais principais que não for um corpo é um domínio de Dedekind e pelo Teorema 4.3 o resultado segue. ■

4.3.2 Demonstração do teorema principal

Agora provaremos o teorema principal que será enunciado novamente a seguir.

Teorema 4.4. *Seja R um domínio de integridade Noetheriano cujo fecho inteiro, $\overline{R}$, é um R-módulo finitamente gerado. Então, todo R-módulo livre de torção é uma soma direta de módulos de posto* 1*, se e somente se, $\mu^*(R) \leq 2$. Além disso, neste caso, todo R-módulo livre de torção de posto* 1 *é um S-módulo projetivo para um único anel S tal que $R \subseteq S \subseteq \overline{R}$.*

Demonstração. ($\Rightarrow$) Se R for um domínio de integridade Noetheriano, tal que todo R-módulo livre de torção A é soma direta de módulos de posto 1, então, pela Proposição 4.3, $\mu^*(R_{\mathfrak{M}}) \leq 2$, para todo ideal maximal $\mathfrak{M}$ de R e, pela Proposição 4.4, e $\mu^*(R) \leq 2$.

($\Leftarrow$) Para a demonstração desta implicação faremos indução no comprimento finito $l(\overline{R}/R)$. Suponhamos $l(\overline{R}/R) = 0$. Então, $\overline{R}/R = \{0\}$, ou seja, $R = \overline{R}$ e R é integralmente fechado. Como $\mu^*(R) \leq 2$ por hipótese, temos, pela Proposição 4.4, que $\mathbb{K} - \dim R \leq 1$. Se $\mathbb{K} - \dim R = 0$, como R é um domínio de integridade, R é um corpo e o resultado segue da teoria de Álgebra Linear. Se $\mathbb{K} - \dim R = 1$, então R é um domínio de Dedekind e, pelo Teorema 4.3, o resultado segue.

Dividiremos o restante da demonstração em três casos: R local, semi-local e geral.

Primeiro Caso: R é um domínio de integridade local Noetheriano, cujo fecho inteiro $\overline{R}$ é um R-módulo finitamente gerado e $\mu^*(R) \leq 2$. Seja A um R-módulo livre de torção. Devemos mostrar que A é soma direta de módulos de posto 1.

Sem perda de generalidade, podemos supor que A não tem somando direto livre. Seja $A_0 = \overline{\{\alpha\}}$ um submódulo fechado de posto 1. Pelo Lema 3.1, A_0 é isomorfo, como R-módulo, a um ideal de R. Se A_0 for cíclico, isto é, $A_0 \cong Rx$, A_0 é livre e, portanto, projetivo. Então, pela Proposição 4.5, A_0 é um somando direto de A, o que é absurdo, pois por hipótese A não tem somando direto livre. Logo, A_0 não é principal. Pelo Lema 4.10-(ii), A_0 é um R_1-módulo, isto é, $R_1A_0 = A_0$ onde $R_1 = \mathfrak{M}^{-1}$ e $\mathfrak{M}$ é o único ideal maximal de R. Desde que todo elemento de A está em um submódulo fechado de posto 1, temos que A é um R_1-módulo. Pelo Lema 4.10-(i) e (ii), temos que $l_{R_1}(\overline{R}/R_1) < l_R(\overline{R}/R)$ e $\mu^*(R_1) \leq 2$, respectivamente.

Observação 4.5. Não podemos terminar a demonstração no caso local por indução porque $R_1 = \mathfrak{M}^{-1}$ é semi-local. De fato, sendo R_1 inteiro sobre R, temos que $\dim R_1 = \dim R$ (Teorema 2.4) e $\mathfrak{q}$ é um ideal maximal de R_1, se e somente se, $\mathfrak{q} \cap R = \mathfrak{p}$ for um ideal maximal de R. Como $\dim R_1 = \dim R \leq 1$ todo ideal primo próprio de R_1 é maximal. Então, como $\mathfrak{M}$ é um ideal de R_1 ($\mathfrak{M}R_1 = R_1$), os ideais maximais de R_1 são os primos de R_1 pertencentes a $\mathfrak{M}$.

Tratemos então de mostrar que A tem um somando direto de posto 1 no caso R semi-local.

Segundo Caso: R é um domínio de integridade semi-local Noetheriano, cujo fecho inteiro $\overline{R}$ é um R-módulo finitamente gerado e $\mu^*(R) \leq 2$. Seja A um R-módulo livre de torção. Devemos mostrar que A tem um somando direto de posto 1.

Faremos indução no comprimento $l_R(\overline{R}/R)$.

Se $l_R(\overline{R}/R) = 0$, R é domínio de Dedekind e A é soma direta de módulos de posto 1 (Teorema 4.3). Portanto tem um somando direto de posto 1.

Suponhamos a afirmação verdadeira se R for semi-local tal que $l_R(\overline{R}/R) < r$. Devemos mostrar que a afirmação vale para anéis semi-locais tais que $l_R(\overline{R}/R) = r$.

Seja $\mathfrak{M}$ um ideal maximal de R e seja A um R-módulo livre de torção. Então, $A_{\mathfrak{M}}$ é um $R_{\mathfrak{M}}$-módulo livre de torção. Como no caso local, supondo que $A_{\mathfrak{M}}$ não tem somando direto livre, temos que $A_{\mathfrak{M}}$ é um R_1- módulo livre de torção, para um anel R_1 tal que $R_{\mathfrak{M}} \subset R_1 \subset \overline{R_{\mathfrak{M}}}$ e $l_{R_1}(\overline{R_{\mathfrak{M}}}/R_1) < l_{R_{\mathfrak{M}}}(\overline{R_{\mathfrak{M}}}/R_{\mathfrak{M}})$. Observemos neste momento que $l_{R_{\mathfrak{M}}}(\overline{R_{\mathfrak{M}}}/R_{\mathfrak{M}}) \leq l_R(\overline{R}/R) = r$. Então, como R_1 é também semi-local, podemos usar a hipótese de indução e garantir que $A_{\mathfrak{M}}$ tem um somando direto de posto 1 da forma $\overline{\{\alpha\}}$, para algum α in A.

Sendo R semi-local, sejam $\mathfrak{M}_1, \ldots, \mathfrak{M}_r$ os ideais maximais de R. Para cada $i = 1, \ldots, r$, seja $\alpha_i \in A$ tal que o fecho de $\{\alpha_i\}$ no $R_{\mathfrak{M}_i}$-módulo $A_{\mathfrak{M}_i}$ é um somando direto. Pelo Lema 4.12, existe $n_i > 0$ tal que se $\alpha \equiv \alpha_i \pmod{\mathfrak{M}_i^{n_i} A_{\mathfrak{M}_i}}$, então $\overline{\{\alpha\}}$ em $A_{\mathfrak{M}_i}$ é um somando direto de $A_{\mathfrak{M}_i}$. Como $\mathfrak{M}_1, \ldots, \mathfrak{M}_r$ são comaximais, $\mathfrak{M}_1^{n_1}, \ldots, \mathfrak{M}_r^{n_r}$ são comaximais, quaisquer que sejam os inteiros positivos $n_1, \ldots, n_r$, então podemos escolher $\alpha \in A$, tal que $\alpha \equiv \alpha_i \pmod{\mathfrak{M}_i^{n_i} A_{\mathfrak{M}_i}}$, $\forall\, i = 1, \ldots, r$. (Lema 4.3). Seja $A_0 = \overline{\{\alpha\}}$, o fecho de α em A. Desde que, o fecho comuta com a localização a sequência exata

$$0 \to A_0 \to A \to A/A_0 \to 0$$

se decompõe localmente. Logo, pelo Lema 4.11, A_0 é um somando direto de A.

Terceiro Caso: R é um domínio de integridade Noetheriano, cujo fecho inteiro $\overline{R}$ é um R-módulo finito e $\mu^*(R) \leq 2$. Seja A um R-módulo livre de torção. Devemos mostrar que A é soma direta de módulos de posto 1.

Seja $I \subseteq R$ o condutor de $\overline{R}$ para R, isto é,

$$I = \{a \in R \ : \ a\overline{R} \subseteq R\} = Ann(\overline{R}/R)$$

e sejam $\mathfrak{M}_1, \ldots, \mathfrak{M}_r$ os ideais maximais de R contendo I. Como $\dim R \leq 1$, os ideais maximais de R contendo I são os primos pertencentes a I. Seja $S = R - \bigcup_{i=1}^{r} \mathfrak{M}_i$. Então, A_S é um R_S-módulo e R_S é semi-local. Pelo caso semi-local podemos escolher $\alpha \in A$, não nulo, tal que o fecho de $\{\alpha\}$ em A_S é um somando direto do R_S-módulo A_S. Seja $A_0 = \overline{\{\alpha\}}$ o fecho de α em A. Vamos mostrar que a sequência de R-módulos,

$$0 \to A_0 \to A \to A/A_0 \to 0,$$

se decompõe localmente. Para $\mathfrak{M} = \mathfrak{M}_i$, com $i = 1, \ldots, r$, o reultado segue por construção. Para, $\mathfrak{M} \neq \mathfrak{M}_1, \ldots, \mathfrak{M}_r$, $R_{\mathfrak{M}}$ é um domínio de valorização discreta. De fato, se $\mathfrak{M} \neq \mathfrak{M}_1, \ldots, \mathfrak{M}_r$, então $I \nsubseteq \mathfrak{M}$. Logo, existe $a \in I$, tal que $a \notin \mathfrak{M}$, isto é, $a\overline{R} \subseteq R$, $a \notin \mathfrak{M}$. Assim,

$$\overline{R} \subseteq \frac{1}{a}R \subset R_{\mathfrak{M}} \Rightarrow \overline{R}R_{\mathfrak{M}} \subseteq R_{\mathfrak{M}}.$$

Por outro lado, segue da injetividade da aplicação $R \longrightarrow \overline{R}$, que $R_{\mathfrak{M}} \subseteq \overline{R}R_{\mathfrak{M}}$. Portanto, $\overline{R_{\mathfrak{M}}} = \overline{R}R_{\mathfrak{M}} = R_{\mathfrak{M}}$ e $R_{\mathfrak{M}}$ é integralmente fechado. Concluímos assim que $R_{\mathfrak{M}}$ é Noetheriano, $\dim R_{\mathfrak{M}} = 1$ e é integralmente fechado, isto é, um anel de valorização discreta.

Então, $R_{\mathfrak{M}}$ é um domínio de ideais principais e, por conseguinte, $(A/A_0)_{\mathfrak{M}}$ é $R_{\mathfrak{M}}$-módulo livre. De fato, A_0 fechado, implica A/A_0 livre de torção. Como $R_{\mathfrak{M}}$ é domínio de valorização discreta, A/A_0 livre de torção é livre. Logo,

$$0 \to A_0 \to A \to A/A_0 \to 0$$

se decompõe como $R_{\mathfrak{M}}$-módulo, isto é, A_0 é somando direto. Fianlmente, $A = A_0 \oplus B$, e por indução no posto de A, B é soma direta de R-módulos de posto 1.

Para concluirmos a demonstração do teorema, devemos ainda mostrar que todo R-módulo livre torção e posto 1 é um S-módulo projetivo, para um único anel S, tal que $R \subseteq S \subseteq \overline{R}$. Seja A um R-módulo livre de torção e posto 1. Então, pelo Lema 3.1, $A \cong \mathfrak{A}$, como R-módulo, e $\mathfrak{A} \subseteq R$ é ideal. Vamos mostrar que $\mathfrak{A}$ é um S-módulo projetivo para um único anel S, $R \subseteq S \subseteq \overline{R}$.

Para garantir a existência do anel S faremos indução em no comprimento $l_R(\overline{R}/R)$. Suponhamos $l_R(\overline{R}/R) = 0$, isto é, R é integralmente fechado. Então, R é um domínio de Dedekind e, pelo Lema 3.9, temos que $\mathfrak{A}$ é invertível, logo é um R-módulo projetivo

(Proposição 3.6). Se $l_R(\overline{R}/R) > 0$, usamos a Proposição 2.24, para escrevermos $\mathfrak{A} = \prod_{i=1}^{n} \mathfrak{q}_i$, onde $\mathfrak{q}_i$ são ideais primários e $\mathfrak{M}_i = r(\mathfrak{q}_i)$ são maximais, $\forall\, i = 1, \ldots, n$. Se $\mathfrak{A}$ for invertível, então $\mathfrak{A}$ é novamente um R-módulo projetivo. Se $\mathfrak{A}$ não for invertível, então $\mathfrak{q}_i$ não é invertível, para algum i. Nesse caso, como na demonstração do item (i) do Lema 4.10, podemos mostrar que $\mathfrak{M}_i^{-1} \subseteq \overline{R}$ é um anel próprio sobre R e $\mathfrak{q}_i$ é um $\mathfrak{M}_i^{-1}$-módulo. Mas

$$\mathfrak{M}_i^{-1}\mathfrak{A} = \mathfrak{M}_i^{-1} \prod_{j=1}^{n} \mathfrak{q}_j = \prod_{j \neq i} \mathfrak{q}_j (\mathfrak{M}_i^{-1}\mathfrak{q}_i) = \prod_{j \neq i} \mathfrak{q}_j \mathfrak{q}_i = \mathfrak{A},$$

implica que $\mathfrak{A}$ é um $\mathfrak{M}_i^{-1}$-módulo. Como, $l_R(\overline{R}/R) > l_{\mathfrak{M}_i^{-1}}(\overline{R}/\mathfrak{M}_i^{-1})$, pela hipótese de indução, existe $\mathfrak{M}_i^{-1} \subseteq S \subseteq \overline{R}$ tal que $\mathfrak{A}$ é um S-módulo projetivo.

Finalmente, vamos mostrar que S é único. Se, $R \subseteq S \subseteq \overline{R}$, então o corpo de frações de R e S são iguais. Além disso, $\mathfrak{A}$ um S-módulo projetivo de posto 1 implica $\mathfrak{A}$ invertível, isto é, $\mathfrak{A}\mathfrak{A}^{-1} = S$. Mas $\mathfrak{A}\mathfrak{A}^{-1} = S$ implica $S = \{\alpha \in \mathbb{K} : \alpha\mathfrak{A} \subseteq \mathfrak{A}\}$. De fato, se $\alpha \in \mathbb{K}$ for tal que $\alpha\mathfrak{A} \subseteq \mathfrak{A}$, então

$$\alpha\mathfrak{A}\mathfrak{A}^{-1} \subseteq \mathfrak{A}\mathfrak{A}^{-1} \Rightarrow \alpha S \subseteq S \Rightarrow \alpha \in S \Rightarrow \{\alpha \in \mathbb{K} : \alpha\mathfrak{A} \subseteq \mathfrak{A}\} \subset S.$$

A outra inclusão é óbvia. ∎

4.4 APLICAÇÃO DO TEOREMA PRINCIPAL

Nesta seção, usaremos o Teorema 4.4 para descrever módulos livres de torção finitamente gerados sobre dois domínios de integridade específicos. A saber, os anéis de funções regulares nos pontos singulares das curvas planas afins $Y^2 = X^2 + X^3$ e $Y^2 = X^3$ sobre um corpo k algebricamente fechado.

4.4.1 **Curva Nodal**

Sejam k um corpo algebricamente fechado e $\mathcal{C} \subset k^2$ a curva plana definida pela equação

$$Y^2 - X^2 - X^3 = 0.$$

É fácil ver que $p = (0, 0)$ é o único ponto singular de $\mathcal{C}$ e que o anel das funções regulares em p, denotado por R, é $R = k[x, y]_{\mathfrak{M}}$, onde $x = \overline{X}$, $y = \overline{Y} \in k[X, Y]/\langle Y^2 - X^2 - X^3 \rangle$ e $\mathfrak{M} = \langle x, y \rangle$. Então, R é um anel local Notheriano de dimensão igual a 1.

$\vdash$: O corpo de frações de R é $k(y/x)$.

De fato, sabemos que $k(x, y)$ que é o corpo de frações de $k[x, y]$ e de R. Como $y^2 = x^2 + x^3$ em $k[x, y]$, temos que $x + 1 = (y/x)^2$ e $y = (y/x)^3 - (y/x)$ pertencem a $k(y/x)$. Logo, $k[x, y] \subset k(y/x)$ e, portanto, $k(x, y) \subset k(y/x)$. Claramente, temos que $k(y/x) \subset k(x, y)$. Logo, $k(x, y)$, o corpo de frações de $k[x, y]$ e de R é igual a $k(y/x)$.

$\vdash$: O fecho inteiro de $k[x,y]$ é $k[y/x]$.

Das inclusões $k[x,y] \subset k[y/x] \subset k(y/x)$ e da igualdade $(y/x)^2 = x+1 \in k[x,y]$, temos que $k[y/x]$ é inteiro sobre $k[x,y]$. Para mostrar que os elementos inteiros de $k(x/y)$ estão em $k[y/x]$, façamos $t = y/x$ para simplificar as notações. Suponhamos $z = a(t)/b(t) \in K(t)$ inteiro sobre $k[x,y] = k[t^2-1, t^3-t]$. Então, existe $p(T) = T^n + \ldots + a_1T + a_0 \in k[x,y] = k[t^2-1,t^3-t][T]$, polinômio não nulo, tal que

$$\begin{gathered}\frac{a(t)^n}{b(t)^n} + \cdots + a_1\frac{a(t)}{b(t)} + a_0 = 0 \Rightarrow \\ a(t)^n + a_{n-1}a(t)^{n-1}b(t) + \ldots + a_1a(t)b(t)^{n-1} + a_0b(t)^n = 0 \Rightarrow \\ a(t)^n = -a_{n-1}a(t)^{n-1}b(t) - \ldots - a_1a(t)b(t)^{n-1} - a_0b(t)^n.\end{gathered}$$

Como t é transcendente sobre k, podemos supor que $a(t)$ e $b(t)$ não tem fator comum e portanto, última equação segue que $b(t) \in k$.

$\vdash$: O fecho inteiro de R é $\overline{R} = k[y/x]_{\mathfrak{M}}$. Além diso, $\overline{R} = R + (y/x)R$.

De fato, como localização comuta com fecho inteiro, temos que

$$\overline{R} = \overline{k[x,y]_{\mathfrak{M}}} = \overline{k[x,y]}_{\mathfrak{M}} = k[y/x]_{\mathfrak{M}}.$$

De $(y/x)^2 = x+1 \in R$, segue que $\overline{R} = R + (y/x)R$.

$\vdash$: $\overline{R}/R$ é um k-espaço vetorial e $\dim_k(\overline{R}/R) = 1$.

Vimos na afirmação anterior que $\overline{R} = R + (y/x)R$. Mas todo elemento em $R = k[x,y]_{\mathfrak{M}}$ é a localização de um polinômio da forma $f(x,y) = \sum a_{ij}x^iy^j + a_{00}$, onde $a_{ij} \in k$, para todo i,j. Logo, $(y/x)R = R + (y/x)k$ e $\overline{R} = R + k(y/x)$. Daí segue que $\overline{R}/R \cong k$.

$\vdash$: O ideal $\mathfrak{M} \subset R \subset \overline{R}$ é um ideal de $\overline{R}$. De fato, $\mathfrak{M} = \langle x,y\rangle = xR + yR$,

$$\begin{gathered}x(\frac{y}{x}) = y \in \langle x,y\rangle \qquad \text{e} \qquad y(\frac{y}{x}) = \frac{y^2}{x} = \frac{x^2+x^3}{x} = x + x^2 \in \langle x,y\rangle \\ \Rightarrow \mathfrak{M}\overline{R} \subset \mathfrak{M}.\end{gathered}$$

Na verdade, temos que $\mathfrak{M} = \langle x\rangle\overline{R}$, pois

$$\langle x,y\rangle\overline{R} = x\overline{R} + y\overline{R} = x\overline{R} + x(\frac{y}{x})\overline{R} \subset x\overline{R}.$$

Observe ainda que $x = (y/x)^2 - 1 = (y/x-1)(y/x+1) \subset \overline{R}$ implica que $(y/x-1)\overline{R}$ e $(y/x+1)\overline{R}$ são os únicos ideais maximais de $\overline{R}$ contendo $\mathfrak{M}$.

$\vdash$: Todo ideal em $\overline{R}$ é principal.

Para simplificar as notações, vamos usar $t = y/x$ e, nesse caso, teremos:

$$k[x,y] = k[t^2-1, t^3-t], \mathfrak{M} = \langle x,y\rangle = \langle t^2-1, t^3-t\rangle \text{ e } \overline{k[x,y]} = k[t],$$

$$R = k[t^2-1, t^3-t]_{\mathfrak{M}}, \overline{R} = k[t]_{\mathfrak{M}} \text{ e } \mathfrak{M} = \langle t^2-1\rangle \overline{R}.$$

Observemos que todo ideal em $k[t]$ é principal e, portanto, todo ideal em $\overline{R} = k[t]_{\mathfrak{M}}$ é principal. Mais do que isso, todo polinômio em $k[t]$ pode ser escrito na forma

$$f(t) = (t-1)^n(t+1)^m g(t), \text{ onde } n, m \in \mathbb{N},\ g(1) \neq 0 \text{ e } g(-1) \neq 0. \tag{4.8}$$

Logo, todo ideal J em $\overline{R} = k[t]_{\mathfrak{M}}$ é da forma

$$J = (t-1)^n(t+1)^m k[t]_{\mathfrak{M}}, \text{ para algum par } (n,m) \in \mathbb{N} \times \mathbb{N},$$

já que $g(1) \neq 0$ e $g(-1) \neq 0$ é equivalente a $g(t) \notin \mathfrak{M}$, ou seja, é invertível em $k[t]_{\mathfrak{M}}$.

Nesse ponto é importante salientar a seguinte propriedade do anel $\overline{R}$. Sejam $J = (t-1)^n(t+1)^m k[t]_{\mathfrak{M}}$ e $P = (t-1)^{1+n}(t+1)^{1+m} k[t]_{\mathfrak{M}}$ ideias de $\overline{R}$ tais que $n, m \in \mathbb{N}$. Então, $P \subset J$ e $\dim_k(J/P) = 2$. De fato, J/P é isomorfo a $k \times k$, ou mais explicitamente,

$$J/P \cong (t-1)^n(t+1)^m[k + (t-1)k].$$

Logo, $\dim_k(J/P) = 2$.

$\vdash$: Todo ideal em R é um ideal é gerado por no máximo dois elementos.

Seja $I \subset R$ um ideal. Como R é local, temos que $I \subset \mathfrak{M} \subset \overline{R}$. Segue da equação 4.8 que todo elemento em $\overline{R}$ é da forma $f(t) = (t-1)^n(t+1)^m g(t)$, onde $n, m \in \mathbb{N}$, $g(t) \in k[t]$ e $g(t) \notin \mathfrak{M}$. Sejam n, m os menores inteiros positivos tais que $(t-1)^n(t+1)^m g(t) \in I$ e $g(t)$ é invertível em R. Então,

$$(t-1)^n(t+1)^m g(t)k + (t-1)^{n+1}(t+1)^{m+1}\overline{R} \subset I \subset (t-1)^n(t+1)^m\overline{R}.$$

Mas $(t-1)^n(t+1)^m g(t)k + (t-1)^{n+1}(t+1)^{m+1}\overline{R} \subsetneq (t-1)^{n+1}(t+1)^{m+1}\overline{R}$ implica

$$\dim_k\left(\frac{(t-1)^n(t+1)^m\overline{R}}{(t-1)^n(t+1)^m g(t)k + (t-1)^{n+1}(t+1)^{m+1}\overline{R}}\right) < \dim_k\left(\frac{(t-1)^n(t+1)^m\overline{R}}{(t-1)^{n+1}(t+1)^{m+1}\overline{R}}\right) = 2.$$

Logo,

$$\dim_k\left(\frac{(t-1)^n(t+1)^m\overline{R}}{(t-1)^n(t+1)^m g(t)k + (t-1)^{n+1}(t+1)^{m+1}\overline{R}}\right) \leq 1.$$

Por outro lado, $(t-1)^n(t+1)^m g(t)k + (t-1)^{n+1}(t+1)^{m+1}\overline{R} \subsetneq (t-1)^n(t+1)^m\overline{R}$, pois $(t-1)^{n+1}(t+1)^m \in (t-1)^n(t+1)^m\overline{R}$, mas $(t-1)^{n+1}(t+1)^m \notin (t-1)^n(t+1)^m g(t)k + (t-1)^{n+1}(t+1)^{m+1}\overline{R}$ (lembre que $g(t)$ é invertível em $\mathfrak{M}$).

Logo,

$$\dim_k\left(\frac{(t-1)^n(t+1)^m\overline{R}}{(t-1)^n(t+1)^m g(t)k + (t-1)^{n+1}(t+1)^{m+1}\overline{R}}\right) = 1.$$

Temos então que

$$I = (t-1)^n(t+1)^m g(t)k + (t-1)^{n+1}(t+1)^{m+1}\overline{R} = (t-1)^n(t+1)^m R$$

ou

$$I = (t-1)^n(t+1)^m\overline{R} = (t-1)^n(t+1)^m R + (t-1)^n(t+1)^{m+1}R,$$

já que $\overline{R} = R + (t+1)R$ como R-módulo.

Usando o Teorema 4.4, temos que todo R-módulo M livre de torção e finitamente gerado se decompõe, isto é,

$$M = M_1 \oplus M_2 \oplus \ldots \oplus M_n,$$

onde M_i são R-módulos livres de torção e posto 1, para todo $i = 1, \ldots, n$.

Além disso, para cada M_i, existe um único anel $R \subset S_i \subset \overline{R}$, tal que é M_i é um S_i-módulo projetivo. Mas, $\overline{R}/R \cong R/\mathfrak{M}$ implica $S_i = R$ ou $S_i = \overline{R}$. Logo,

$$M \cong R^{\oplus a} \bigoplus \overline{R}^{\oplus b}.$$

Temos também que $\overline{R} \cong \mathfrak{M}$, como R-módulo o que nos permite escrever

$$M \cong R^{\oplus a} \bigoplus \mathfrak{M}^{\oplus b}.$$

O caso cuspidal é análogo e vamos apenas explicitar as diferenças.

4.4.2 Curva Cuspidal

Sejam k um corpo algebricamente fechado e $\mathcal{C} \subset \mathbb{K}^2$ a curva plana definida por

$$Y^2 - X^3 = 0.$$

Então, $p = (0,0)$ é o único ponto singular de $\mathcal{C}$ e o anel das funções regulares em p, é o anel

$$R = \mathbb{K}[x,y]_{\mathfrak{M}},$$

onde $x = \overline{X}$, $y = \overline{Y} \in \mathbb{K}[X,Y]/\langle Y^2 - X^3\rangle$ e $\mathfrak{M} = \langle x, y\rangle$. É fácil ver que R é um anel local Notheriano de dimensão igual a 1 .

$\vdash$: O corpo de frações de R é $k(x,y) = k(y/x)$. De fato, como $y^2 = x^3$ em $\mathbb{K}[x,y]$, temos $x = (y/x)^2$, $y = (y/x)^3$ em $k(y/x)$. Logo, $k[x,y] \subset k(y/x)$ e $k(x,y) \subset k(y/x)$. Claramente, temos que $k(y/x) \subset k(x,y)$. Logo, $k(x,y)$, o corpo de frações de $k[x,y]$ e de R, é igual a $k(y/x)$.

$\vdash$: O fecho inteiro de $k[x,y]$ é $k[y/x]$. Então, $k[x,y] \subset k[y/x] \subset k(y/x)$ e, como $(y/x)^2 = x \in k[x,y]$, temos que $k[y/x]$ é inteiro sobre $k[x,y]$. Para mostrar que os elementos inteiros de $k(x/y)$ estão em $k[y/x]$, façamos $t = y/x$ para simplificar as notações. Suponhamos $z = a(t)/b(t) \in K(t)$ inteiro sobre $k[x,y] = k[t^2,t^3]$. Então, existe $p(T) = T^n + \ldots + a_1T + a_0 \in k[x,y] = k[t^2,t^3][T]$, polinômio não nulo, tal que

$$\frac{a(t)^n}{b(t)^n} + \cdots + a_1\frac{a(t)}{b(t)} + a_0 = 0 \Rightarrow$$
$$a(t)^n + a_{n-1}a(t)^{n-1}b(t) + \ldots + a_1a(t)b(t)^{n-1} + a_0b(t)^n = 0 \Rightarrow$$
$$a(t)^n = -a_{n-1}a(t)^{n-1}b(t) - \ldots - a_1a(t)b(t)^{n-1} - a_0b(t)^n.$$

Como t é transcendente sobre k, podemos supor que $a(t)$ e $b(t)$ não tem fator comum e portanto, última equação segue que $b(t) \in k$.

$\vdash$: O fecho inteiro de R é $\overline{R} = k[y/x]_{\mathfrak{M}}$. Além diso, $\overline{R} = R + (y/x)R$.

De fato, como localização comuta com fecho inteiro, temos que

$$\overline{R} = \overline{k[x,y]_{\mathfrak{M}}} = \overline{k[x,y]}_{\mathfrak{M}} = k[y/x]_{\mathfrak{M}}.$$

De $(y/x)^2 = x \in R$, segue que $\overline{R} = R + (y/x)R$.

$\vdash$: $\overline{R}/R$ é um k-espaço vetorial e $\dim_k(\overline{R}/R) = 1$.

Vimos na afirmação anterior que $\overline{R} = R + (y/x)R$. Mas todo elemento em $R = k[x,y]_{\mathfrak{M}}$ é a localização de um polinômio da forma $f(x,y) = \sum a_{ij}x^iy^j + a_{00}$, onde $a_{ij} \in k$, para todo i,j. Logo, $(y/x)R = R + (y/x)k$ e $\overline{R} = R + k(y/x)$. Daí segue que $\overline{R}/R \cong k$.

$\vdash$: O ideal $\mathfrak{M} \subset R \subset \overline{R}$ é um ideal de $\overline{R}$. De fato, $\mathfrak{M} = \langle x,y\rangle = xR + yR$,

$$x(\frac{y}{x}) = y \in \langle x,y\rangle \qquad \text{e} \qquad y(\frac{y}{x}) = \frac{y^2}{x} = \frac{x^3}{x} = x^2 \in \langle x,y\rangle$$
$$\Rightarrow \mathfrak{M}\overline{R} \subset \langle x,y\rangle \subset \overline{R}.$$

Além disso, temos que $\mathfrak{M} = \langle x\rangle\overline{R}$, pois

$$\langle x,y\rangle\overline{R} = x\overline{R} + y\overline{R} = x\overline{R} + x(\frac{y}{x})\overline{R} \subset x\overline{R}.$$

Observe ainda que $x = (y/x)^2 \subset \overline{R}$ implica que $(y/x)\overline{R}$ é o único ideal maximal de $\overline{R}$ contendo $\mathfrak{M}$.

$\vdash$: Todo ideal em $\overline{R}$ é principal.

Como no caso nodal, façamos $t = y/x$. Nesse caso, teremos:

$$k[x,y] = k[t^2,t^3], \mathfrak{M} = \langle x,y\rangle = \langle t^2,t^3\rangle \text{ e } \overline{k[x,y]} = k[t],$$

$$R = k[t^2,t^3]_{\mathfrak{M}}, \overline{R} = k[t]_{\mathfrak{M}} \text{ e } \mathfrak{M} = \langle t^2\rangle\overline{R}.$$

Observemos que todo ideal em $k[t]$ é principal e, portanto, todo ideal em $\overline{R} = k[t]_{\mathfrak{M}}$ é principal. Mais do que isso, todo polinômio em $k[t]$ pode ser escrito na forma

$$f(t) = t^{2n}g(t), \text{ onde } n \in \mathbb{N},\ t^2 \nmid g(t). \tag{4.9}$$

Logo, todo ideal J em $\overline{R} = k[t]_{\mathfrak{M}}$ é da forma

$$J = t^{2n}k[t]_{\mathfrak{M}}, \text{ para algum } n \in \mathbb{N}.$$

Também nesse caso, temos que se $J = t^{2n}k[t]_{\mathfrak{M}}$ e $P = t^{2n+2}k[t]_{\mathfrak{M}}$ são ideias de $\overline{R}$ tais que $n \in \mathbb{N}$. Então, $\dim_k(J/P) = 2$. De fato,

$$J/P \cong t^n[k + tk].$$

Logo, $\dim_k(J/P) = 2$.

$\vdash$: Todo ideal em R é um ideal gerado por no máximo dois elementos.

Seja $I \subset R$ um ideal. Como R é local, temos que $I \subset \mathfrak{M} \subset \overline{R}$. Segue da equação 4.9 que todo elemento em $\overline{R}$ é da forma $f(t) = t^{2n}g(t)$, onde $n\mathbb{N}$, $g(t) \in k[t]$ e $g(t) \notin \mathfrak{M}$. Seja n o menor inteiro positivo tal que $t^{2n}g(t) \in I$ e $g(t)$ é invertível em R. Então,

$$t^{2n}g(t)k + t^{2n+2}\overline{R} \subset I \subset t^{2n+2}\overline{R}.$$

Mas $t^{2n}g(t)k + t^{2n+2}\overline{R} \subsetneq t^{2n}\overline{R}$ implica

$$\dim_k\left(\frac{t^{2n}\overline{R}}{t^{2n}g(t)k + t^{2n+2}\overline{R}}\right) < \dim_k\left(\frac{t^{2n}\overline{R}}{t^{2n+2}\overline{R}}\right) = 2.$$

Logo,

$$\dim_k\left(\frac{t^{2n}\overline{R}}{t^{2n}g(t)k + t^{2n+2}\overline{R}}\right) \leq 1.$$

Por outro lado, $t^{2n}g(t)k + t^{2n+2}\overline{R} \subsetneq t^{2n}\overline{R}$, pois $t^{2n+2} \in t^{2n}\overline{R}$, mas $t^{2n+2} \notin t^{2n}g(t)k + t^{2n+2}\overline{R}$ (lembre que $g(t)$ é invertível em $\mathfrak{M}$).

Logo,

$$\dim_k\left(\frac{t^{2n}\overline{R}}{t^{2n}g(t)k + t^{2n+2}\overline{R}}\right) = 1.$$

Temos então que

$$I = t^{2n}g(t)k + t^{2n+2}\overline{R} = t^{2n}R$$

ou

$$I = t^{2n}\overline{R} = t^{2n}R + t^{2n+1}R,$$

já que $\overline{R} = R + tR$ como R-módulo.

Usando o Teorema 4.4, temos que todo R-módulo M livre de torção e finitamente gerado se decompõe, isto é,

$$M = M_1 \oplus M_2 \oplus \ldots \oplus M_n,$$

onde M_i são R-módulos livres de torção e posto 1, para todo $i = 1, \ldots, n$.

Além disso, para cada M_i, existe um único anel $R \subset S_i \subset \overline{R}$, tal que é M_i é um S_i-módulo projetivo. Mas, $\overline{R}/R \cong k$ implica $S_i = R$ ou $S_i = \overline{R}$. Logo,

$$M \cong R^{\oplus a} \bigoplus \overline{R}^{\oplus b}.$$

Temos também que $\overline{R} \cong \mathfrak{M}$, como R-módulo o que nos permite escrever

$$M \cong R^{\oplus a} \bigoplus \mathfrak{M}^{\oplus b}.$$

REFERÊNCIAS

[1] SERRE, J. P. *Faisceaux algébriques cohérents* Ann. of Math. 61, p. 197-278, 1955.

[2] SESHADRI, C. S. *Triviality of vector bundles over the product of the affine space* K^2 Proc. Natl. Acad. Sci. USA. 44, 456-458, 1958.

[3] SESHADRI, C. S. *Algebraic vector bundles over the product of an affine curve and the affine line*, Proc. Amer. Math. Soc. 10, p. 670-673, 1959.

[4] BASS, H. *Torsion free and projective modules*, Trans. Amer. Math. Soc.102, p. 319-327, 1962.

[5] BASS, H. *Injective dimension in Noetherian ring*, Trans. Amer. Math. Soc.102, p. 18-29, 1962.

[6] SESHADRI, C. S. *Fibrés Vectoriels sur les Courbes Algébriques* Astérisque 96, 1982.

[7] LANGE, H.; AVRITZER, D.; RIBEIRO, F. A. *Torsion Free Sheaves on Nodal Curves and Triples* Bull. Braz. Math. Soc., New Series 41(3), p. 421-447, 2010.

[8] AVRITZER, D.; MARTINS, R. V.; RIBEIRO, F. A. *On Torsion Free Sheaves on Cuspidal Curves* arXiv:1203.5329v1 [math.AG].

[9] ATIYAH, M. F.; MACDONALD, I. G. *Introduction to Commutative Algebra.* University of Oxford: Addison-Wesley Publishing Company, Inc., 1969.

[10] COHEN, I. S. *Commutative rings with restricted minimum condition*, Duke Math. J. 17, p. 27-42, 1950.

[11] KAPLANSKY, I. *Modules over Dedekind rings and valuation rings*,Trans. Amer. Math. Soc. 72 p. 327-340, 1952.

[12] DUMMIT, D. S.; FOOTE, R. M. *Abstract Algebra.* Third Edition, United States of America: John Wiley and Sons, Inc., 2004.

[13] MATSUMURA, H.; REID, M. *Commutative Ring Theory.* Cambridge: Cambridge University Press, 1989.

[14] MATSUMURA, H. *Commutative Algebra.* Second Edition. Massachusetts: The Benjamin/Cumming Publishing Company, Inc., 1980.

[15] PASSMAN, D. S. *A Course In Ring Theory.* Wisconsin,: AMS Chelsea Publishing, 2004.

[16] ZARISKI, O.; SAMUEL, P.; COHEN, I. S. *Commutative Algebra.* Volume I. Princeton: D. Van Nostrand Company, Inc., 1958.

[17] EISENBUD, D. *Commutative Algebra, with a View Toward Algebraic Geometry.* Springer-Verlag, 1995.