Universidade Federal da Paraíba

Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Curso de Bacharelado em Matemática

A igualdade de Auslander-Buchsbaum

Ricardo Burity Croccia Macedo

João Pessoa – PB
dezembro de 2011

Ricardo Burity Croccia Macedo

A igualdade de Auslander-Buchsbaum

Trabalho de Conclusão de Curso apresentado à Coordenação de Curso de Bacharelado em Matemática da Universidade Federal da Paraíba como requisito para obtenção do título de Bacharel em Matemática.
Orientador: Prof. Dr. Cleto Brasileiro Miranda Neto

João Pessoa – PB
dezembro de 2011

Prof. Dr. Cleto Brasileiro Miranda Neto

Catalogação na publicação
Universidade Federal da Paraíba
Biblioteca Setorial do CCEN

B958i Burity, Ricardo.
A igualdade de Auslander-Buchsbaum. / Ricardo Burity. - João Pessoa, 2011.
48f. -

Monografia (Graduação em Matemática) – UFPB/CCEN.
Orientador: Prof. Dr. Cleto Brasileiro Miranda Neto.

1. Álgebra Homológica. 2. Derivações Logarítmicas. 3. Auslander-Buchsbaum. I. Título.

BS/CCEN

CDU: 512.66 (043.2)

A igualdade de Auslander-Buchsbaum

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Bacharelado em Matemática da Universidade Federal da Paraíba como requisito para obtenção do título de Bacharel em Matemática.

Orientador: Prof. Dr. Cleto Brasileiro Miranda Neto

Aprovado em: 20 / 12 / 2011

COMISSÃO EXAMINADORA:

Cleto Brasileiro Miranda Neto

Prof. Dr. Cleto Brasileiro Miranda Neto – UFPB

Prof. Dr. Napoleón Caro Tuesta – UFPB

Prof. Dr. Roberto Callejas Bedregal – UFPB

Agradecimentos

A Deus.

Aos meus pais.

À Renata.

Ao professor Cleto, por ser o meu orientador e pelos valiosos conselhos. Aos professores Napoleón e Bedregal, por participarem da banca, e a todos os outros professores do departamento, pela contribuição na minha formação. Em especial aos professores, Andrade, Eduardo e Everaldo.

Aos meus amigos, pelos momentos compartilhados.

Resumo

A clássica igualdade de Auslander-Buchsbaum fornece uma relação entre dois invariantes algébricos fundamentais: profundidade e dimensão homológica. Nosso objetivo será demonstrar tal resultado e aplicá-lo no contexto de derivações logarítmicas.

Palavras-chave: dimensão homológica, profundidade, derivações logarítmicas.

Abstract

The classical Auslander-Buchsbaum equality furnishes a relationship between two fundamental algebraic invariants: depth and homological dimension. Our goal will be to prove such result and to apply it into the context of logarithmic derivations.

Keywords: homological dimension, depth, logarithmic derivations.

Sumário

Introdução

Neste trabalho, apresentamos alguns conceitos fundamentais da álgebra comutativa com o objetivo de demonstrar a igualdade de Auslander-Buchsbaum.

No primeiro capítulo, exibiremos propriedades básicas de anéis e módulos necessárias ao resultado principal pretendido. No segundo capítulo, definimos profundidade e dimensão homológica de um módulo; além disso, apresentamos o Lema da Serpente, resultado crucial em álgebra homológica, que é utilizado como uma ferramenta para provar o teorema em questão.

Por fim, mostramos uma aplicação da igualdade de Auslander-Buchsbaum no contexto de derivações polinomiais logarítmicas, obtendo uma fórmula para a profundidade do módulo idealizador tangencial, relativo a um ideal principal.

Capítulo 1

Anéis e módulos

1.1 Anéis e ideais

Definição 1.1. Um *anel* é um conjunto A munido de duas operações:

$$\begin{array}{rccc} + : & A \times A & \longrightarrow & A \\ & (x,y) & \longmapsto & x+y \end{array} \qquad \begin{array}{rccc} \cdot : & A \times A & \longrightarrow & A \\ & (x,y) & \longmapsto & x \cdot y \end{array}$$

satisfazendo, para todos $x, y, z \in A$:

i. $(x+y)+z = x+(y+z)$;

ii. $\exists\ 0_A = 0 \in A$ tal que $0+x = x+0 = x$;

iii. Dado $x \in A, \exists\ y \in A$ tal que $x+y = y+x = 0$ (Notação: $y = -x$);

iv. $x+y = y+x$;

v. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;

vi. $x \cdot (y+z) = x \cdot y + x \cdot z, \qquad (y+z) \cdot x = y \cdot x + z \cdot x$.

Definição 1.2. Se existir $1_A = 1 \in A$ tal que $x \cdot 1 = 1 \cdot x = x$, dizemos que A *possui identidade.*

Definição 1.3. Se $x \cdot y = y \cdot x$, $\forall\ x, y \in A$, dizemos que A é *comutativo.*

Observação 1.1. Assumiremos, a partir de agora, que todos os anéis são comutativos com identidade. A operação $x \cdot y$ será denotada por xy, $\forall\ x, y \in A$.

Exemplo 1.1. $\mathbb{Z}$, com as operações usuais de soma e multiplicação, é um anel comutativo com identidade.

Exemplo 1.2. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, com as operações $(a+bi)+(c+di) = a+c+(b+d)i$ e $(a + bi).(c + di) = ac - bd + (ad + bc)i$, para a,b,c,$d \in \mathbb{Z}$, é um anel comutativo com identidade, chamado *anel dos inteiros de Gauss.*

Definição 1.4. Seja A um anel. Um subconjunto $B \subseteq A$ é dito *subanel* (de A) se:

i. $1_A \in B$;

ii. $x, y \in B \Rightarrow x - y \in B,\ xy \in B$.

Definição 1.5. Sejam A, B anéis. Uma função $\varphi : A \longrightarrow B$ é um *homomorfismo* (de anéis) se satisfaz as seguintes condições para todos $x, y \in A$:

i. $\varphi(x + y) = \varphi(x) + \varphi(y)$;

ii. $\varphi(xy) = \varphi(x)\varphi(y)$;

iii. $\varphi(1_A) = 1_B$.

Observação 1.2. Note que $\varphi(0_A) = 0_B$, de fato $0_A + 0_A = 0_A \Rightarrow \varphi(0_A + 0_A) = \varphi(0_A)$ como φ é homomorfismo segue que $\varphi(0_A) + \varphi(0_A) = \varphi(0_A) \Rightarrow \varphi(0_A) = 0_B$.

Exemplo 1.3. A composição de homomorfismos é homomorfismo, isto é, se A, B, C são anéis e $\varphi : A \longrightarrow B$, $\psi : B \longrightarrow C$ são homomorfismos de anéis, então $\psi \circ \varphi : A \longrightarrow C$ é um homomorfismo de anéis.

Proposição 1.1. Sejam A, B anéis e $\varphi : A \longrightarrow B$ homomorfismo de anéis. Então:

i. $S \subseteq A$ é subanel $\Longrightarrow \varphi(S) \subseteq B$ é subanel;

ii. $T \subseteq B$ é subanel $\Longrightarrow \varphi^{-1}(T) \subseteq A$ é subanel.

Demonstração.

i. Por definição de homomorfismo, $\varphi(1_A) = 1_B \Rightarrow 1_B \in \varphi(S)$. Sejam $\varphi(x)$,$\varphi(y) \in \varphi(S)$. Do fato de φ ser homomorfismo, segue que $\varphi(x) - \varphi(y) = \varphi(x - y) \in \varphi(S) \Rightarrow \varphi(x) - \varphi(y) \in \varphi(S)$. Analogamente, $\varphi(x)\varphi(y) = \varphi(xy) \Rightarrow \varphi(x)\varphi(y) \in \varphi(S)$. Portanto, $\varphi(S)$ é subanel de B.

ii. Como $\varphi(1_A) = 1_B \in T$ segue que $1_A \in \varphi^{-1}(T)$. Sejam $a, b \in \varphi^{-1}(T)$. Por definição de imagem inversa, $\varphi(a), \varphi(b) \in T \Rightarrow \varphi(a) - \varphi(b) = \varphi(a - b) \in T \Rightarrow a - b \in \varphi^{-1}(T)$. Mostremos agora que $ab \in \varphi^{-1}(T)$. De fato, $\varphi(a)\varphi(b) = \varphi(ab) \in T \Rightarrow ab \in \varphi^{-1}(T)$. Portanto, $\varphi^{-1}(T)$ é subanel de A.

□

Corolário 1.2. Sejam A, B anéis e $\varphi : A \longrightarrow B$ homomorfismo de anéis. Então, a imagem de φ, $Im(\varphi) = \{y \in B \mid y = \varphi(x),\ x \in A\}$, é subanel de B.

Demonstração. O resultado segue do item i. da proposição anterior. Basta fazer $S = A$. □

Definição 1.6. Seja A um anel. Um subconjunto $I \subseteq A$ é um *ideal* (de A) se:

i. $0_A \in I$;

ii. $x, y \in I \Rightarrow x + y \in I$;

iii. $x \in I, a \in A \Rightarrow xa \in I$. (*lei de absorção*)

Exemplo 1.4. Dados $x_1, \ldots, x_n \in A$ anel. O conjunto $I = (x_1, \ldots, x_n) = \{a_1x_1 + \ldots + a_nx_n \mid a_1, \ldots, a_n \in A\}$ é um ideal. Os elementos $x_1, \ldots, x_n$ são chamados de *geradores* de I. Quando $n = 1$, I é chamado *ideal principal* gerado por x_1. Um ideal $I \subseteq A$ é dito *finitamente gerado* se I é gerado por um número finito de elementos de A.

Exemplo 1.5. Sejam A anel e $I_1, \ldots, I_n \subseteq A$ ideais. O conjunto $I_1 + \ldots + I_n = \{x_1 + \ldots + x_n \mid x_i \in I_i,\ i = 1, \ldots, n\}$ é um ideal, chamado *ideal soma dos I_j's.*

Proposição 1.3. Sejam A, B anéis e $\varphi : A \longrightarrow B$ homomorfismo de anéis. Então:

i. $I \subseteq A$ é ideal e φ é sobrejetor $\Longrightarrow \varphi(I) \subseteq B$ é ideal;

ii. $J \subseteq B$ é ideal $\Longrightarrow \varphi^{-1}(J) \subseteq A$ é ideal.

Demonstração.

i. Pela observação 1.2 temos que $\varphi(0_A) = 0_B \Rightarrow 0_B \in \varphi(I)$. Sejam $\varphi(x)$,$\varphi(y) \in \varphi(I)$. Segue do fato de φ ser homomorfismo que $\varphi(x) + \varphi(y) = \varphi(x + y) \in \varphi(I) \Rightarrow \varphi(x) + \varphi(y) \in \varphi(I)$. Seja agora $b \in B$. Como φ é sobrejetor, existe $a \in I$ tal que $\varphi(a) = b$, logo $\varphi(x)b = \varphi(x)\varphi(a) = \varphi(xa) \Rightarrow \varphi(x)b \in \varphi(I)$. Portanto, $\varphi(I)$ é ideal de B.

ii. $\varphi(0_A) = 0_B \in J \Rightarrow 0_A \in \varphi^{-1}(J)$. Sejam $a, b \in \varphi^{-1}(J)$. Por definição de imagem inversa, $\varphi(a), \varphi(b) \in J \Rightarrow \varphi(a) + \varphi(b) = \varphi(a+b) \in J \Rightarrow a+b \in \varphi^{-1}(J)$. Por fim, seja $c \in A$. Mostremos que $ac \in \varphi^{-1}(J)$. De fato, por J ser ideal, $\varphi(a)\varphi(c) \in \varphi(J) \Rightarrow \varphi(ac) \in \varphi(J) \Rightarrow ac \in \varphi^{-1}(J)$. Portanto, $\varphi^{-1}(J)$ é ideal de A. $\square$

Definição 1.7. Sejam A, B anéis e $\varphi : A \longrightarrow B$ homomorfismo de anéis. Definimos o *núcleo de* φ como o ideal $Ker(\varphi) = \varphi^{-1}(0_B)$. Explicitamente: $Ker(\varphi) = \{x \in A \mid \varphi(x) = 0_B\}$.

Observação 1.3. Sejam A, B anéis e $\varphi : A \longrightarrow B$ homomorfismo de anéis. Note que φ é injetor $\Leftrightarrow Ker(\varphi) = \{0\}$. De fato, sejam $x, y \in A$ tais que $\varphi(x) = \varphi(y) \Rightarrow \varphi(x-y) = 0_B \Rightarrow x - y \in Ker(\varphi) = \{0\} \Rightarrow x = y \Rightarrow \varphi$ é injetor. Reciprocamente, se φ é injetor, então: $x \in Ker(\varphi) \Rightarrow \varphi(x) = 0_B = \varphi(0_A) \Rightarrow x = 0_A \Rightarrow Ker(\varphi) = \{0\}$.

Sejam A um anel e $I \subseteq A$ um ideal. Considere a relação

$$x, y \in A,\ x \sim y \Leftrightarrow x - y \in I.$$

Note que $\sim$ é uma relação de equivalência em A. De fato, para quaisquer $x, y, z \in A$, temos

i. $x \sim x$ pois, $0 = x - x \in I$;

ii. $x \sim y \Rightarrow y \sim x$ pois, se $x - y \in I$ então $y - x = -(x-y) \in I$;

iii. $x \sim y$ e $y \sim z \Rightarrow x \sim z$ pois, se $x - y \in I$ e $y - z \in I$ então $x - z = (x-y) + (y-z) \in I$.

Denotaremos por $\overline{x} = x + I = \{y \in A \mid y \sim x\}$, a *classe residual de* x *com respeito a* I, e por $A/I = \{\overline{x} \mid x \in A\}$ *o conjunto quociente de* A *por* I. Provaremos uma proposição que nos permitirá definir duas operações em A/I que o torne um anel.

Proposição 1.4. Sejam A um anel e $I \subseteq A$ um ideal. Se $\overline{x_1} = \overline{x_2}$ e $\overline{y_1} = \overline{y_2}$ então

i. $\overline{x_1 + y_1} = \overline{x_2 + y_2}$;

ii. $\overline{x_1 y_1} = \overline{x_2 y_2}$.

Demonstração.

i. $\overline{x_1} = \overline{x_2},\ \overline{y_1} = \overline{y_2} \Rightarrow x_1 - x_2,\ y_1 - y_2 \in I \Rightarrow (x_1 - x_2) + (y_1 - y_2) = (x_1 + y_1) - (x_2 + y_2) \in I \Rightarrow \overline{x_1 + y_1} = \overline{x_2 + y_2}$;

ii. $\overline{x_1} = \overline{x_2},\ \overline{y_1} = \overline{y_2} \Rightarrow x_1 - x_2,\ y_1 - y_2 \in I \Rightarrow x_1 = x_2 + a$ e $y_1 = y_2 + b,\ a, b \in I$. Agora note que $x_1y_1 - x_2y_2 = (x_2+a)(y_2+b) - x_2y_2 = x_2y_2 + x_2b + ay_2 + ab - x_2y_2 = x_2b + ay_2 + ab \Rightarrow x_1y_1 - x_2y_2 \in I$, já que $a, b \in I$. Assim, $\overline{x_1y_1} = \overline{x_2y_2}$. □

Os itens i. e ii. nos dizem que as classes da soma e da multiplicação independem de representantes, permitindo munir o conjunto A/I de uma estrutura de anel.

Proposição 1.5. Sejam A um anel e $I \subseteq A$ um ideal. O conjunto $A/I = \{\overline{x} \mid x \in A\}$ é um anel com as operações:

$$\begin{array}{rccc} + : & A/I \times A/I & \longrightarrow & A/I \\ & (\overline{x}, \overline{y}) & \longmapsto & \overline{x+y} \end{array} \qquad \begin{array}{rccc} \cdot : & A/I \times A/I & \longrightarrow & A/I \\ & (\overline{x}, \overline{y}) & \longmapsto & \overline{xy} \end{array}$$

Em particular, A/I é comutativo, e se 1 é a identidade de A então $\overline{1}$ é a identidade de A/I.

Demonstração. Segue da proposição anterior. □

Observação 1.4. Considere o homomorfismo natural $\pi = \pi_I : A \longrightarrow A/I$, definido por $x \longmapsto \overline{x}$, que é claramente sobrejetor. Denote $\overline{A} = A/I$. Sejam $\overline{J} \subseteq \overline{A}$ ideal de $\overline{A}$ e $J \subseteq A$ ideal de A. Então: $\pi(J) = (J + I)/I \Rightarrow \pi^{-1}(\pi(J)) = J + I$. Além disso: $J = \pi^{-1}(\overline{J}) \Rightarrow \pi(J) = \pi(\pi^{-1}(\overline{J})) \Rightarrow \pi(J) = \overline{J} \Rightarrow \overline{J} = (J + I)/I$. Concluímos que há uma bijeção entre o conjunto dos ideais de A/I e o conjunto dos ideais de A que contêm I. Em particular, todo ideal de A/I tem a forma $J/I = \{x + I \mid x \in J\}$, para algum ideal J contendo I.

Definição 1.8. Seja A um anel. Um elemento $x \in A$ é um *divisor de zero* se $xy = 0$, para algum $y \in A \setminus \{0\}$. Um anel $A \neq 0$ é dito *domínio* se 0 é o único divisor de zero de A.

Exemplo 1.6.

i. $\mathbb{Z}$, o anel dos números inteiros, é um domínio, assim como o anel dos inteiros de Gauss, $\mathbb{Z}[i]$.

ii. $K[x]$, o anel dos polinômios na variável x sobre um corpo K, é um domínio. O mesmo vale para anéis de polinômios em um número qualquer de indeterminadas.

Definição 1.9. Seja A um anel. Um elemento $x \in A$ é *nilpotente* se existe $n \in \mathbb{N} \setminus \{0\}$ tal que $x^n = 0$. Neste caso, o número $min\{n \in \mathbb{N} \setminus \{0\} \mid x^n = 0\}$ é chamado *grau (ou índice) de nilpotência de x.*

Note que se $x \in A$ é nilpotente então x é divisor de zero. A recíproca é falsa: considere no anel dos números inteiros $A = \mathbb{Z}$, o ideal $I = 6\mathbb{Z} = \{6n \mid n \in \mathbb{Z}\}$ e o anel quociente $A/I = \{\overline{m} \mid m \in \mathbb{Z}\}(= \mathbb{Z}_6)$. Nesse contexto, temos que $\overline{2}.\overline{3} = \overline{6} = \overline{0}$ pois $6 \in I$, logo $\overline{2}$ é um divisor de zero em $\mathbb{Z}_6$, mas $\overline{2^n} \neq \overline{0}\ \forall\ n \in \mathbb{N} \setminus \{0\}$, pois caso contrário existiria $n \in \mathbb{N} \setminus \{0\}$ tal que $2^n \in I = 6\mathbb{Z} \Rightarrow 2^n$ é múltiplo de 6, o que é um absurdo.

Definição 1.10. Seja A um anel. Um elemento $x \in A$ é uma *unidade ou elemento invertível* se $xy = 1$ para algum $y \in A$. Notação: $y = x^{-1}$ (o inverso de x, que é único); $A^* = \{unidades\ de\ A\} \subseteq A$.

Definição 1.11. Seja $K \neq 0$ um anel. Dizemos que K é um *corpo* se $K^* = K \setminus \{0\}$.

Exemplo 1.7. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R} \subseteq \mathbb{C}$ são corpos.

Observação 1.5. Note que todo corpo é domínio. De fato, se K é corpo e $x, y \in K$ são tais que $xy = 0$, então, se $x \neq 0$ tem-se $x^{-1}xy = 0 \Rightarrow y = 0 \Rightarrow K$ é domínio. Porém nem todo domínio é corpo, (por exemplo, $\mathbb{Z}$). Além disso, pode-se mostrar que todo domínio finito é corpo. Exemplo: $\mathbb{Z}_p = \mathbb{Z}/(p),\ p \in \mathbb{Z}$ primo.

Proposição 1.6. Seja $K \neq 0$ um anel. São equivalentes:

i. K é corpo ;

ii. Os únicos ideais de K são (0) e (1) ;

iii. Para qualquer anel $A \neq 0$, todo homomorfismo $\varphi : K \longrightarrow A$ é injetor.

Demonstração.

i. $\Rightarrow$ ii. Suponha por absurdo que exista um ideal próprio $I \subsetneq K$ não-trivial ($I \neq \{0\}$). Seja $x \in I \setminus \{0\}$. Como K é corpo, $\exists\ y \in K$ tal que $xy = 1$ e sendo I ideal segue que $xy = 1 \in I \Rightarrow I = K$, absurdo. Portanto, os únicos ideais de K são (0) e (1);

ii. $\Rightarrow$ iii. Sejam $A \neq 0$ um anel e $\varphi : K \to A$ um homomorfismo de anéis. Como $Ker(\varphi)$ é ideal de K temos que $Ker(\varphi) = (0)$ ou $Ker(\varphi) = (1)$. Suponha por absurdo que $Ker(\varphi) = (1) = K$, então $\varphi(1_K) = 0_A$, contradição, já que φ é homomorfismo de anéis. Segue que $Ker(\varphi) = (0)$, o que pela observação 1.3 significa que φ é injetor;

iii. $\Rightarrow$ i. Seja $x \in K$ tal que x não é um elemento invertível. Vamos mostrar que $x = 0$ e, assim, que K é corpo. Note que $(x) \neq (1)$, do contrário $1 \in (x)$ e x seria elemento invertível. Assim, considere o anel quociente $K/(x)$ não-nulo (já que $(x) \neq (1)$) e o homomorfismo sobrejetor $\varphi : K \longrightarrow K/(x)$, definido por $y \longmapsto \overline{y}$. Note que $Ker(\varphi) = (x)$ pois, $\varphi(y) = \overline{y} = \overline{0} \Leftrightarrow y \in (x)$. Como φ é injetivo por hipótese, seque que $x = 0$. $\square$

Definição 1.12. Seja A um anel. Um ideal $P \subsetneq A$ é dito *primo* se, sempre que $xy \in P$, tem-se $x \in P$ ou $y \in P$.

Definição 1.13. Seja A um anel. Um ideal $\mathfrak{M} \subsetneq A$ é dito *maximal* se $\mathfrak{M} \subsetneq J \subseteq A$ (onde $J \subseteq A$ é ideal) implica em $J = A$.

Proposição 1.7. Sejam A anel e $P, \mathfrak{M} \subseteq A$ ideais. Então:

i. $P \subseteq A$ é primo $\Longleftrightarrow A/P$ é domínio;

ii. $\mathfrak{M} \subseteq A$ é maximal $\Longleftrightarrow A/\mathfrak{M}$ é corpo.

Demonstração.

i. Suponha que P é primo e sejam $\overline{x}, \overline{y} \in A/P$ tais que $\overline{xy} = \overline{0}$, isto é, $xy \in P$. Como P é primo, tem-se $x \in P$ ou $y \in P \Rightarrow \overline{x} = \overline{0}$ ou $\overline{y} = \overline{0} \Rightarrow A/P$ é domínio. Reciprocamente, se A/P é domínio e $x, y \in A$ são tais que $xy \in P$, então $\overline{xy} = \overline{0}$, e como A/P é domínio, temos que $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0} \Rightarrow x \in P$ ou $y \in P \Rightarrow P$ é primo.

ii. Suponha que $\mathfrak{M}$ é maximal e seja $\overline{0} \neq \overline{x} \in A/\mathfrak{M}$. Mostremos que $\exists\, \overline{y} \in A/\mathfrak{M}$ tal que $\overline{xy} = \overline{1}$. De fato, considere o ideal $\mathfrak{M} + (x) = \{m + ax \mid m \in \mathfrak{M}, a \in A\}$. Como $\overline{x} \neq \overline{0}$, temos que $x \notin \mathfrak{M} \Rightarrow \mathfrak{M} \subsetneq \mathfrak{M} + (x) \Rightarrow \mathfrak{M} + (x) = A$ pois $\mathfrak{M}$ é maximal, logo $1 \in A = \mathfrak{M} + (x) \Rightarrow \exists\, m_1 \in \mathfrak{M},\ y \in A$ tais que $1 = m_1 + yx \Rightarrow \overline{1} = \overline{m_1} + \overline{yx} = \overline{0} + \overline{yx} = \overline{yx}$. Reciprocamente, suponha que $A/\mathfrak{M}$ é corpo e seja $L \subseteq A$ ideal tal que $\mathfrak{M} \subsetneq L$. Logo $\exists\, a \in L \setminus \mathfrak{M} \Rightarrow \overline{a} \neq \overline{0}$. Como $A/\mathfrak{M}$ é corpo, $\exists\, b \in A$ tal que $\overline{a}\overline{b} = \overline{1} \Rightarrow \overline{ab - 1} = \overline{0} \Rightarrow ab - 1 \in \mathfrak{M} \Rightarrow \exists\ c \in \mathfrak{M}$ tal que $ab - 1 = c \Rightarrow 1 = ab - c \in L$ pois $a \in L$ e $c \in \mathfrak{M} \subsetneq L \Rightarrow L = A \Rightarrow \mathfrak{M}$ é maximal. □

Corolário 1.8. Todo ideal maximal é primo.

Demonstração. Segue da observação 1.5 e da proposição anterior. □

Proposição 1.9. Sejam A anel e $I \subseteq J$ ideais. Considere $\pi : A \longrightarrow A/I$ o homomorfismo sobrejetor. Então:

i. $J \subseteq A$ é primo $\Longleftrightarrow J/I \subseteq A/I$ é primo;

ii. $J \subseteq A$ é maximal $\Longleftrightarrow J/I \subseteq A/I$ é maximal.

Demonstração.

i. Pela proposição 1.7, J é primo $\Leftrightarrow A/J$ é domínio $\Leftrightarrow (A/I)/(J/I)$ é domínio $\Leftrightarrow J/I$ é primo.

ii. Analogamente, pela proposição 1.7, J é maximal $\Leftrightarrow A/J$ é corpo $\Leftrightarrow (A/I)/(J/I)$ é corpo $\Leftrightarrow J/I$ é maximal.

□

A seguir construiremos o ambiente necessário para utilizar o Lema de Zorn a fim de demonstrar que todo anel não-nulo possui ideal maximal.

Seja $S \neq \emptyset$ um conjunto parcialmente ordenado, isto é, S é munido de uma relação $\preceq$ que é reflexiva, transitiva e possui a propriedade de que se $x \preceq y$ e $y \preceq x$ então $x = y$. Um subconjunto $C \subseteq S$ é dito *cadeia* se $x \preceq y$ ou $y \preceq x$ para todo $x, y \in C$. Um elemento $x \in S$ é uma *cota superior* para C em S se $y \preceq x$, $\forall y \in C$. Diz-se que $x \in S$ é um *elemento maximal* se $x \preceq y$ $(y \in S) \Rightarrow x = y$.

Lema de Zorn. *Seja $S \neq \emptyset$ um conjunto parcialmente ordenado tal que todo subconjunto totalmente ordenado possui cota superior em S. Então, S possui elemento maximal.*

Teorema 1.10. *Todo anel $A \neq 0$ possui ideal maximal.*

Demonstração. Seja $\mathfrak{L} = \{$ideais próprios de $A\}$. Note que $(0) \in \mathfrak{L} \Rightarrow \mathfrak{L} \neq \emptyset$, e ordene $\mathfrak{L}$ com a ordem parcial de inclusão $(\subseteq)$. Seja $\{I_\alpha\}_\alpha$ um subconjunto totalmente ordenado de $\mathfrak{L}$. Defina

$I = \bigcup_{\alpha} I_\alpha$, que claramente é um ideal próprio de A (pois $1 \notin I_\alpha$, já que I_α é próprio para todo α). Assim, $I \in \mathfrak{L}$ é uma cota superior para $\{I_\alpha\}_\alpha$, e assim, pelo Lema de Zorn, $\mathfrak{L}$ possui elemento maximal, ou seja, A possui ideal maximal. □

Corolário 1.11. Sejam A anel e $I \subsetneq A$ ideal. Então, $\exists\ \mathfrak{M} \subseteq A$ ideal maximal contendo I.

Demonstração. I próprio $\Rightarrow A/I \neq \overline{0}$. Pelo teorema anterior, $\exists\ N \subseteq A/I$ ideal maximal. Mas, pela observação 1.4, temos que N é da forma $N = \mathfrak{M}/I$, para algum ideal $\mathfrak{M} \supseteq I$. Sendo $N = \mathfrak{M}/I$ maximal, segue da proposição 1.9 (ii) que $\mathfrak{M}$ é maximal. □

Corolário 1.12. Sejam A anel e $x \in A \setminus A^*$. Então, $x \in \mathfrak{M}$, para algum $\mathfrak{M} \subseteq A$ ideal maximal.

Demonstração. Seja $I = (x)$. Então, $I \neq A$ pois $x \notin A^*$. Pelo corolário anterior, $\exists\ \mathfrak{M} \subseteq A$ ideal maximal tal que $I \subseteq \mathfrak{M}$, logo $x \in \mathfrak{M}$. □

Definição 1.14. Um anel A é dito *semi-local* se possuir uma quantidade finita de ideais maximais. Se A possuir apenas um ideal maximal, será dito *anel local.* Se A é um anel local com ideal maximal $\mathfrak{M}$, usa-se a notação $(A, \mathfrak{M})$.

Proposição 1.13. Seja A anel e $\mathfrak{M} \subsetneq A$ ideal. Então,

i. $A \setminus \mathfrak{M} \subseteq A^* \Longrightarrow (A, \mathfrak{M})$ é local;

ii. $\mathfrak{M}$ maximal e $1 + \mathfrak{M} = \{1 + x \mid x \in \mathfrak{M}\} \subseteq A^* \Longrightarrow A$ é local.

Demonstração.

i. Seja $N \subseteq A$ ideal maximal. Em particular, $N \neq A$, isto é, $N \cap A^* = \emptyset$. Então, $N \subseteq \mathfrak{M}$ já que $A \setminus \mathfrak{M} \subseteq A^*$. Como $\mathfrak{M}$ é próprio e N é maximal tem-se $N = \mathfrak{M}$.

ii. Seja $u \in A \setminus \mathfrak{M}$. Defina o ideal $I = \mathfrak{M} + (u)$, como $u \notin \mathfrak{M}$ temos que $\mathfrak{M} + (u) \supsetneq \mathfrak{M}$, e sendo $\mathfrak{M}$ maximal, tem-se $I = A$. Logo $1 \in I \Rightarrow 1 = x + yu$, com $x \in \mathfrak{M}$, $y \in A$. Assim, $yu = 1 - x \in 1 + \mathfrak{M} \subseteq A^* \Rightarrow yu \in A^* \Rightarrow \exists\ z \in A$ tal que $z(yu) = 1 \Rightarrow (zy)u = 1 \Rightarrow u \in A^*$. Pelo item (i) acima, A é local. □

Definição 1.15. O *radical de Jacobson* de um anel $A \neq 0$ é definido por $\mathfrak{R}_A = \bigcap \mathfrak{M}$, com $\mathfrak{M} \subseteq A$ ideal maximal.

Proposição 1.14. $\mathfrak{R}_A = \{x \in A \mid 1 - xy \in A^*,\ \forall\, y \in A\}$.

Demonstração. Seja $x \in \mathfrak{R}_A$, e suponha por absurdo que exista $y \in A$ tal que $1 - xy \notin A^*$. Pelo corolário 1.12, segue que existe $\mathfrak{M} \subseteq A$ ideal maximal tal que $1 - xy \in \mathfrak{M}$. Mas, $x \in \mathfrak{R}_A \Rightarrow x \in \mathfrak{M} \Rightarrow xy \in \mathfrak{M}$ e como $1 - xy \in \mathfrak{M}$, teríamos $1 \in \mathfrak{M}$, absurdo, já que $\mathfrak{M}$ é maximal. Portanto, $1 - xy \in A^*,\ \forall\, y \in A$. Devemos mostrar agora que se $x \in A$ é tal que $1 - xy \in A^*,\ \forall\, y \in A$ então $x \in \mathfrak{R}_A$. Mostremos a equivalência: se $x \notin \mathfrak{R}_A$ então $\exists\, y \in A$ tal que $1 - xy \notin A^*$. De fato, seja $x \notin \mathfrak{R}_A$, então $\exists\, \mathfrak{M} \subseteq A$ ideal maximal tal que $x \notin \mathfrak{M} \Rightarrow \mathfrak{M} + (x) \supsetneq \mathfrak{M} \Rightarrow \mathfrak{M} + (x) = A$, pois $\mathfrak{M}$ é maximal. Logo, $1 = a + bx,\ a \in \mathfrak{M},\ b \in A \Rightarrow a = 1 - bx \in \mathfrak{M} \Rightarrow 1 - bx \notin A^*$. □

Lema da esquiva. *Sejam A anel e $P_1, \ldots, P_n \subseteq A$ ideais primos. Se $I \subseteq A$ é ideal tal que $I \subseteq \bigcup_{i=1}^{n} P_i$, então $I \subseteq P_i$ para algum $i = 1, \ldots, n$.*

Demonstração. Mostremos que $I \nsubseteq P_j\ (j = 1, \ldots, n) \Rightarrow I \nsubseteq \bigcup_{j=1}^{n} P_j$, por indução sobre n. O caso $n = 1$ é trivial. Assim, suponha $n > 1$. É claro que $I \nsubseteq P_j,\ \forall\, j = 1, \ldots, n \Rightarrow I \nsubseteq P_j,\ \forall\, j \neq i$ para cada i. Por indução, $I \nsubseteq \bigcup_{j \neq i} P_j$. Logo, $\exists\, x_i \in I,\ x_i \notin P_j,\ \forall\, j \neq i$. Se $x_i \notin P_i$, para algum i, então $x_i \notin \bigcup_{j=1}^{n} P_j$ e o resultado segue. Do contrário, se $x_i \in P_i,\ \forall\, i = 1, \ldots, n$, defina o elemento $x = x_2x_3 \ldots x_n + x_1x_3 \ldots x_n + \ldots + x_1x_2 \ldots x_{n-1}$. Note que $x \in I$, pois $x_i \in I,\ \forall\, i = 1, \ldots, n$. Afirmamos que $x \notin P_j,\ \forall\, j$. Se por absurdo, $x_j \in P_j$ para algum j, e observando que podemos escrever $x = x_1x_2 \ldots x_{j-1}x_{j+1} \ldots x_n + x^*$, com $x^* \in P_j$, então, $x_1x_2 \ldots x_{j-1}x_{j+1} \ldots x_n \in P_j \Rightarrow \exists\, i \neq j$ tal que $x_i \in P_j$, o que é absurdo. Assim, $x \notin P_j,\ \forall\, j = 1, \ldots, n$, ou seja, $x \notin \bigcup_{j=1}^{n} P_j \Rightarrow I \nsubseteq \bigcup_{j=1}^{n} P_j$. □

Definição 1.16. Sejam A anel e $I, J \subseteq A$ ideais. Define-se *o condutor de I em J* por $J : I = \{a \in A \mid aI \subseteq J\}$, onde por $aI \subseteq J$ entende-se $ax \in J,\ \forall\, x \in I$.

Proposição 1.15. Sejam A anel e $I, J \subseteq A$ ideais. Então, o condutor $J : I$ é ideal de A.

Demonstração. Primeiro, note que $0 \in J : I$, pois $0x = 0 \in J,\ \forall\, x \in I$. Sejam $a, b \in J : I \Rightarrow ax, bx \in J,\ \forall\, x \in I \Rightarrow ax + bx \in J \Rightarrow (a + b)x \in J \Rightarrow a + b \in J : I$. Por fim, seja $c \in A$. Vamos mostrar que $ac \in J : I$. Como $a \in J : I$ segue que $ax \in J,\ \forall\, x \in I \Rightarrow cax \in J \Rightarrow ac \in J : I$. Portanto, $J : I$ é ideal. □

No caso especial que $J = (0)$, obtemos o ideal $0 : I = \{a \in A \mid ax = 0, \ \forall \ x \in I\}$, chamado *anulador de I*. Mais particularmente, tomando $I = (x)$, ideal principal gerado por $x \in A$, obtemos o ideal $0 : x = \{a \in A \mid ax = 0\}$ chamado *anulador de x*. Note ainda que denotando $Z(A) = \{\text{divisores de zero de } A\}$, tem-se $Z(A) = \bigcup_{x \in A \setminus \{0\}} 0 : x$.

Definição 1.17. Um anel A é *Noetheriano* se todo ideal de A é finitamente gerado.

Exemplo 1.8.

i. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ são anéis Noetherianos. Mais geralmente, se K é corpo então K é Noetheriano, pois os únicos ideais de K são (0) e (1) (proposição 1.6).

ii. Imagem de anel Noetheriano por homomorfismo de anéis é Noetheriano. De fato, sejam A, B anéis, A Noetheriano e $\varphi : A \longrightarrow B$ homomorfismo de anéis. Vamos mostrar que $Im(\varphi)$ é Noetheriano. Seja $J \subseteq Im(\varphi)$ ideal. Pela proposição 1.3, $\varphi(J)^{-1}$ é ideal de $A \Rightarrow \exists \ a_1, \ldots, a_m \in A$ tais que $\varphi(J)^{-1} = (a_1, \ldots, a_m) \Rightarrow \varphi(\varphi(J)^{-1}) = J = (\varphi(a_1), \ldots, \varphi(a_m)) \Rightarrow J$ é finitamente gerado $\Rightarrow Im(\varphi)$ é Noetheriano.

Proposição 1.16. Seja A anel. São equivalentes:

i. A é Noetheriano.

ii. Toda cadeia ascendente de ideais de A

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

é estacionária, isto é, existe $m \geq 1$ tal que $I_m = I_{m+i}, \ \forall \ i \in \mathbb{N}$.

iii. Qualquer família, não-vazia, de ideais de A possui elemento maximal (com respeito a inclusão).

Demonstração.

i.$\Rightarrow$ ii. Considere uma cadeia de ideais como em ii., tome $I = \bigcup_{n=1}^{\infty} I_n$ ideal de A. Como A é Noetheriano, existem $a_1, \ldots, a_m \in A$ tais que $I = (a_1, \ldots, a_m) \Rightarrow$ para n suficientemente grande $a_i \in I_n, \ \forall \ i = 1, \ldots, m \Rightarrow I_n = I_{n+1} = \ldots$.

ii.$\Rightarrow$ iii. Suponha que exista L uma família, não-vazia, de ideais de A que não possua elemento maximal (com respeito à inclusão). Segue que $I_1 \in L \Rightarrow \exists\ I_2 \in L$ com $I_1 \subsetneqq I_2$. Assim, é possível construir uma cadeia ascendente de ideais de A que é não-estacionária.

iii.$\Rightarrow$ ii. Considere a família, não-vazia, de ideais que compõe a cadeia ascendente em ii.. Segue que esta família possui elemento maximal, o qual satisfaz a condição requerida.

ii.$\Rightarrow$ i. Vamos supor que A é não-Noetheriano e construir uma cadeia ascendente de ideais de A que não é estacionária. De fato, suponha que exista um ideal $I \subseteq A$ que não é finitamente gerado. Então, $a_1, \ldots, a_m \in I \Rightarrow (a_1, \ldots, a_m) \neq I$. Além disso, $a_{m+1} \in I \Rightarrow a_{m+1} \notin (a_1, \ldots, a_m)$. Assim, a seguinte cadeia ascendente de ideais de A:

$$(a_1) \subsetneqq (a_1, a_2) \subsetneqq (a_1, a_2, a_3) \subsetneqq \ldots$$

é não-estacionária. $\square$

Teorema da base de Hilbert. *Seja A anel. Se A é Noetheriano então $A[x_1, \ldots, x_n]$ é Noetheriano.*

Demonstração. Note que $A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$. Assim, por indução, podemos supor $n = 1$. Isto é, provemos que A Noetheriano $\Rightarrow A[x]$ Noetheriano. Mostraremos que $A[x]$ não-Noetheriano $\Rightarrow A$ não-Noetheriano.

Tome $I \subseteq A[x]$ ideal que não é finitamente gerado. Escolha $f_1 \in I$ de grau menor possível. Tome $f_2 \in I \setminus (f_1)$ de grau mínimo. Tome $f_3 \in I \setminus (f_1, f_2)$ de grau mínimo, e assim por diante: $f_k \in I \setminus (f_1, \ldots, f_{k-1})$, $k \geqslant 2$ de grau mínimo.

Seja d_k =grau de f_k, e seja a_k o coeficiente líder de f_k, ou seja: $f_k = a_k x^{d_k} +$ (termos de grau menor que d_k). Pela escolha dos $f_{k's}$, temos $d_1 \leqslant d_2 \leqslant \ldots \leqslant d_k \leqslant \ldots$

Afirmamos que a cadeia $(a_1) \subseteq (a_1, a_2) \subseteq \ldots \subseteq (a_1, \ldots, a_k) \subseteq \ldots$ não é estacionária.

Suponha por absurdo que ela estacione, isto é, $\exists\ k$ tal que $(a_1, \ldots, a_k) = (a_1, \ldots, a_k, a_{k+1}) \Rightarrow a_{k+1} \in (a_1, \ldots, a_k) \Rightarrow a_{k+1} = \sum_{i=1}^{k} b_i a_i$ com $b_i \in A$. Defina

$$g = \sum_{i=1}^{k} b_i x^{d_{k+1} - d_i} f_i,$$

e note que $g \in (f_1, \ldots, f_k)$. Explicitamente:

$g = b_1 x_1^{d_{k+1}-d_1}(a_1 x^{d_1} + \ldots) + b_2 x^{d_{k+1}-d_2}(a_2 x^{d_2} + \ldots) + \ldots + b_k^{d_{k+1}-d_k}(a_k x^{d_k} + \ldots) \Rightarrow$

$g = a_1 b_1 x^{d_{k+1}} + a_2 b_2 x^{d_{k+1}} + \ldots + a_k b_k x^{d_{k+1}} +$ (termos de grau menor que d_{k+1}) $\Rightarrow$

$g = (a_1 b_1 + \ldots + a_k b_k) x^{d_{k+1}} +$ (termos de grau menor que d_{k+1}), denotando $a_1 b_1 + \ldots + a_k b_k = a_{k+1}$ temos que $g = a_{k+1} x^{d_{k+1}} +$ (termos de grau menor que d_{k+1}).

Considere $h = f_{k+1} - g = a_{k+1} x^{d_{k+1}} +$ (termos de grau menor que d_{k+1}) $- a_{k+1} x^{d_{k+1}} -$ (termos de grau menor que d_{k+1}) $\Rightarrow gr(h) < d_{k+1} \Rightarrow gr(h) < gr(f_{k+1})$, onde gr(-) denota grau.

Note que $g \in (f_1, \ldots, f_k)$ e $f_{k+1} \notin (f_1, \ldots, f_k) \Rightarrow h = f_{k+1} - g \in I \setminus (f_1, \ldots, f_k)$ contradizendo a minimalidade de d_{k+1}.

Assim, conseguimos uma cadeia de ideais em A que não estaciona. Portanto, A é não-Noetheriano.

$\square$

1.2 Módulos

Definição 1.18. Seja A um anel. Um conjunto M é um A-*módulo (ou módulo sobre A)* se estiver munido de duas operações:

$$\begin{array}{rccc} + : & M \times M & \longrightarrow & M \\ & (m,n) & \longmapsto & m+n \end{array} \qquad \begin{array}{rccc} \cdot : & A \times M & \longrightarrow & M \\ & (a,m) & \longmapsto & a \cdot m \end{array}$$

satisfazendo, para todos $m, n, p \in M$ e $a, b \in A$:

i. $(m+n)+p = m+(n+p)$;

ii. $\exists\ 0_M = 0 \in M$ tal que $0 + m = m$;

iii. Dado $m \in M, \exists\ n \in M$ tal que $m + n = 0$; (Notação: $n = -m$);

iv. $m + n = n + m$;

v. $(a+b) \cdot m = a \cdot m + b \cdot m$;

vi. $a \cdot (m+n) = a \cdot m + a \cdot n$;

vii. $(ab) \cdot m = a \cdot (b \cdot m)$;

viii. $1 \cdot m = m$.

Observação 1.6. A operação $a \cdot m$ também será denotada por am, $\forall\ a \in A,\ m \in M$.

Exemplo 1.9.

i. $I \subseteq A$ ideal $\Rightarrow I$ é A-módulo, através da lei de absorção. Em particular, A é um A-módulo;

ii. $A = K$ corpo. Um K-módulo é um espaço vetorial sobre o corpo K.

Definição 1.19. Sejam M, N A-módulos. Uma aplicação $f : M \longrightarrow N$ é um *homomorfismo (de A-módulos) ou aplicação A-linear* se satisfaz para todos $m, n \in M,\ a \in A$:

i. $f(m+n) = f(m) + f(n)$;

ii. $f(am) = af(m)$.

Exemplo 1.10. $A = K$ corpo. Neste caso, uma aplicação A-linear é uma transformação linear entre espaços vetoriais sobre K.

Definição 1.20. Sejam M, N A-módulos. Um homomorfismo (de A-módulos) $f : M \longrightarrow N$ é um *isomorfismo (de A-módulos)* se f é bijetivo. Equivalentemente, $f : M \longrightarrow N$ é um isomorfismo se existe $g : N \longrightarrow M$ A-linear tal que $f \circ g = Id_N$ e $g \circ f = Id_M$. Note que g é único, o qual será denotado por $g = f^{-1}$.

Sejam M, N A-módulos. O conjunto $Hom_A(M, N) = \{f : M \longrightarrow N \mid f \text{ é } A\text{-linear}\}$ possui estrutura natural de A-módulo

$$\begin{array}{ccc} A \times Hom_A(M,N) & \longrightarrow & Hom_A(M,N) \\ (a,f) & \longmapsto & af \end{array}$$

onde $af : M \to N$ é definido por $(af)(m) = af(m)$.

Note ainda que a composição de aplicações A-lineares é aplicação A-linear, ou seja, se $f \in Hom_A(M, N)$ e $g \in Hom_A(N, P)$ então $g \circ f \in Hom_A(M, P)$. De fato, sejam $m, m' \in M,\ a \in A$. Então, $(g \circ f)(m + m') = g(f(m + m')) = g(f(m) + f(m')) = g(f(m)) + g(f(m')) = (g \circ f)(m) + (g \circ f)(m')$, assim como, $(g \circ f)(am) = g(f(am)) = g(af(m)) = ag(f(m)) = a(g \circ f)(m)$.

Definição 1.21. Seja M um A-módulo. Um subconjunto $N \subseteq M$ é dito *A- submódulo (de M)* se N possui estrutura de A-módulo; equivalentemente, se N é fechado com relação às operações de M, ou seja, $m, n \in N \Rightarrow m + n \in N$ e $a \in A \Rightarrow am \in N$.

Exemplo 1.11. Sejam M um A-módulo, $M_1, \ldots, M_n \subseteq M$ A-submódulos e $I \subseteq A$ ideal.

i. O conjunto definido por $M_1 + \ldots + M_n = \{m_1 + \ldots + m_n \mid m_i \in M_i,\ i = 1, \ldots, n\}$ é A-módulo.

ii. O conjunto definido por $IM = \{\sum_{i=1}^{n} x_i m_i \mid x_i \in I,\ m_i \in M,\ n \in \mathbb{N}\}$ é A-submódulo de M.

Sejam M um A-módulo e $N \subseteq M$ A-submódulo. Podemos considerar o conjunto quociente $M/N = \{\overline{m} = m + N \mid m \in M\}$, definido pela relação de equivalência $\overline{m_1} = \overline{m_2} \Leftrightarrow m_1 - m_2 \in N$. As operações $+$ e $\cdot$ definidas a seguir fornecem a M/N estrutura de A-módulo:

$$\begin{array}{rccc} + : & M/N \times M/N & \longrightarrow & M/N \\ & (\overline{m}, \overline{n}) & \longmapsto & \overline{m} + \overline{n} = \overline{m+n} \end{array} \qquad \begin{array}{rccc} \cdot : & A \times M/N & \longrightarrow & M/N \\ & (a, \overline{m}) & \longmapsto & a \cdot \overline{m} = \overline{am} \end{array}$$

Chamamos M/N de módulo quociente de M por N.

Definição 1.22. Sejam M, N A-módulos e $f \in Hom_A(M, N)$. O *núcleo de* f é definido como $Ker(f) = \{m \in M \mid f(m) = 0\}$. A *imagem de* f é definida por $Im(f) = \{f(m) \in N \mid m \in M\}$.

Observação 1.7. Note que $Ker(f) \subseteq M$ e $Im(f) \subseteq N$ são A-submódulos. De fato, sejam $m, n \in Ker(f) \Rightarrow 0 = f(m) + f(n) = f(m+n) \Rightarrow m + n \in Ker(f)$. Seja agora $a \in A$. Segue que $0 = af(m) = f(am) \Rightarrow am \in Ker(f)$, logo $Ker(f)$ é A-submódulo de M. Analogamente, sejam $f(m), f(n) \in Im(f) \Rightarrow f(m) + f(n) = f(m+n) \in Im(f)$. Por fim, seja $a \in A$. Segue que $af(m) = f(am) \in Im(f)$, logo $Im(f)$ é A-submódulo de N.
Em particular, podemos considerar o módulo quociente $Coker(f) = N/Im(f)$, chamado *conúcleo de f*.

Proposição 1.17. Sejam M, N A-módulos e $f \in Hom_A(M, N)$. Então:

i. f é injetiva $\Longleftrightarrow Ker(f) = \{0\}$;

ii. f é sobrejetor $\Longleftrightarrow Coker(f) = \{\overline{0}\}$.

Demonstração.

i. Note que $0+0=0 \Rightarrow f(0+0)=f(0) \Rightarrow f(0)+f(0)=f(0) \Rightarrow f(0)=0$. Assim, se f é injetiva segue imediatamente que $Ker(f)=\{0\}$. Reciprocamente, suponha $Ker(f)=\{0\}$ e sejam $m,n \in M$ tais que $f(m)=f(n)$. Então $f(m-n)=0 \Rightarrow m-n \in Ker(f)=\{0\} \Rightarrow m=n \Rightarrow f$ é injetiva.

ii. Imediato. □

Proposição 1.18. Sejam M,P A-módulos. Cada $f: M \longrightarrow P$ A-linear induz uma aplicação A-linear $\overline{f_N}: M/N \longrightarrow Im(f) \subseteq P$, para cada A-submódulo $N \subseteq Ker(f)$.

Demonstração. Defina

$$\begin{array}{rcl} \overline{f_N}: M/N & \longrightarrow & Im(f) \\ \overline{m} & \longmapsto & \overline{f_N}(\overline{m}) = f(m), \end{array}$$

$\overline{f_N}$ está bem definida pois $\overline{m_1}=\overline{m_2} \Rightarrow m_1-m_2 \in N \Rightarrow m_1-m_2 \in Ker(f) \Rightarrow f(m_1-m_2)=0 \Rightarrow f(m_1)=f(m_2) \Rightarrow \overline{f_N}(\overline{m_1})=\overline{f_N}(\overline{m_2})$. Além disso, $\overline{f_N}$ é sobrejetor por construção e é A-linear, pois f é A-linear.

□

Teorema do Isomorfismo. *Sejam M,P A-módulos e $f \in Hom_A(M,P)$. Então,*

$$M/Ker(f) \simeq Im(f).$$

Demonstração. Aplicando a proposição anterior com $N=Ker(f)$ obtemos

$$\begin{array}{rcl} \overline{f_K}: M/Ker(f) & \longrightarrow & Im(f) \\ \overline{m} & \longmapsto & \overline{f_K}(\overline{m}) = f(m), \end{array}$$

A-linear e sobrejetor. Resta mostrarmos que $\overline{f_K}$ é injetiva. De fato, $\overline{m} \in Ker(\overline{f_K}) \Rightarrow \overline{f_K}(\overline{m}) = f(m)=0 \Rightarrow m \in Ker(f) \Rightarrow \overline{m}=\overline{0} \in M/Ker(f) \Rightarrow \overline{f_K}$ é injetiva. Portanto, $\overline{f_K}$ é isomorfismo.

□

Observação 1.8. Sejam M um A-módulo e $N \subseteq M$ A-submódulo. Em total analogia com o caso de ideais, mostra-se que todo A-submódulo de M/N é da forma P/N, onde $P \subseteq M$ é um A-submódulo que contém N.

Fato 1. *Sejam M um A-módulo e $N, P \subseteq M$ A-submódulos. Então,*

$$N/(N \cap P) \ \simeq (N+P)/P$$

Demonstração. Defina $\varphi : N \longrightarrow (N+P)/P$ por $\varphi(n) = n + P = \overline{n}$. Note que φ é A-linear pois $\varphi = \pi \circ i$, onde i é a inclusão de N em $N+P$ e π é a sobrejeção natural de $N+P$ em $(N+P)/P$. Além disso, $Ker(\varphi) = N \cap P$. Assim, o resultado segue do Teorema do Isomorfismo. $\square$

Sejam $P, N \subseteq M$ A-submódulos de M A-módulo. Defina: $P :_A N = \{a \in A \mid aN \subseteq P\}$ o *ideal condutor de N em P*. O caso especial $P = 0$ nos fornece $0 :_A N = \{a \in A \mid an = 0, \ \forall\ n \in N \setminus \{0\}\}$ o *anulador de N*. Note ainda que para cada $m \in M$ é possível definir o *anulador de m*, $0 :_A m = \{a \in A \mid am = 0\}$.

Dados A-módulos $M_1, \ldots, M_n$, o conjunto $M_1 \oplus \ldots \oplus M_n = \{(m_1, \ldots, m_n) \mid m_i \in M_i, \forall\ i = 1, \ldots, n\}$ é um A-módulo (chamado *soma direta de $M_1, \ldots, M_n$*) com as operações naturais: $(m_1, \ldots, m_n) + (m'_1, \ldots, m'_n) = (m_1 + m'_1, \ldots, m_n + m'_n)$ e $a(m_1, \ldots, m_n) = (am_1, \ldots, am_n)$, $a \in A$. Caso importante: $M_i \simeq A, \forall\ i = 1, \ldots, n$. Notação: $\underbrace{A \oplus \ldots \oplus A}_{n} = A^n$.

Definição 1.23. Um A-módulo M é dito *finitamente gerado (sobre A)* se existir um subconjunto finito $\{m_1, \ldots, m_n\} \subseteq M$ tal que $M = \sum_{i=1}^{n} Am_i$, isto é, qualquer $m \in M$ se escreve como $m = a_1m_1 + \ldots a_nm_n$ para certos $a_i \in A$, $i = 1, \ldots, n$. Neste caso, $\{m_1, \ldots, m_n\}$ é um *conjunto de geradores de M (sobre A)*. Tal conjunto é dito *conjunto minimal de geradores* se $m_i \notin \sum_{j \neq i} Am_j$.

Definição 1.24. Seja M um A-módulo finitamente gerado. Um conjunto de geradores $\{m_1, \ldots, m_n\} \subseteq M$ é dito uma *base (de M)* se for linearmente independente sobre A, ou seja, $\sum_{i=1}^{n} a_im_i = 0$ (com $a'_is \in A$) $\Rightarrow a_i = 0, \ \forall\ i = 1, \ldots, n$. Um A-módulo M é dito *livre (sobre A)* quando admite uma base.

Exemplo 1.12.

i. Sejam $A = K$ corpo e V K-espaço vetorial. Se $dim_K V$ é finita, então V é livre como K-módulo.

ii. A^n é livre. De fato, $\{e_1, \ldots, e_n\}$, onde $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, (1 na i-ésima posição, para cada $i = 1, \ldots, n$), é uma base, chamada *base canônica (sobre A)*. Note ainda que, se M é finitamente gerado sobre A então vale: M é livre $\Leftrightarrow M \simeq A^n$ para algum $n > 0$.

Lema de Nakayama. *Sejam M um A-módulo finitamente gerado e $I \subseteq A$ ideal tal que $I \subseteq \mathfrak{R}_A$. Se $IM = M$, então $M = 0$.*

Demonstração. Suponha por absurdo que $M \neq 0$. Então, existe conjunto de geradores $\{m_1, \ldots, m_n\} \subseteq M$ que podemos tomar minimal. Como $m_1 \in \{m_1, \ldots, m_n\} \subseteq M = IM \Rightarrow$

$$m_1 = \sum_{j=1}^{n} x_j m_j,\ x_j \in I \Rightarrow (1 - x_1)m_1 = \sum_{j=2}^{n} x_j m_j \quad (\bigstar_1).$$

Pela proposição 1.14, $\mathfrak{R}_A = \{x \in A \mid 1 - xy \in A^*,\ \forall\ y \in A\}$. Em particular, $x_1 \in I \subseteq \mathfrak{R}_A \Rightarrow 1 - x_1 \in A^*$. Seja $u = (1 - x_1)^{-1}$, multiplicando $(\bigstar_1)$ por u, obtemos $m_1 = \sum_{j=2}^{n}(ux_j)m_j \Rightarrow$ $m_1 \in \sum_{j=2}^{n} Am_j$, contradizendo a minimalidade de $\{m_1, \ldots, m_n\}$. □

Corolário 1.19. Sejam M um A-módulo e $N \subseteq MA$-submódulo tal que M/N é finitamente gerado sobre A. Se $M = IM + N$, onde $I \subseteq \mathfrak{R}_A$ é ideal de A, então $M = N$.

Demonstração. Pela própria estrutura de M/N como A-módulo, temos: $I(M/N) = (IM+N)/N$. Por outro lado, $M = IM + N \Rightarrow I(M/N) = M/N$, pelo Lema de Nakayama temos $M/N = 0 \Rightarrow M = N$. □

Definição 1.25. Uma sequência de A-módulos e aplicações A-lineares

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

é um *complexo* se $Im(f_{i+1}) \subseteq Ker(f_i)\ \forall\ i$. Se $Im(f_{i+1}) = Ker(f_i)$ para algum i, dizemos que a sequência é *exata* em i. Se isto valer para todo i, temos uma *sequência exata (ou complexo exato)*.

Observação 1.9. Sejam M, N, P A-módulos e f, g aplicações A-lineares. Então,

i. $0 \to M \xrightarrow{f} N$ é exata $\Longleftrightarrow f$ for injetiva.

De fato, a sequência em questão é exata $\Leftrightarrow Ker(f) = \{0\} \Leftrightarrow f$ é injetiva (pela proposição 1.17).

ii. $N \xrightarrow{g} P \to 0$ é exata $\Longleftrightarrow g$ for sobrejetiva.

De fato, a sequência acima é exata $\Leftrightarrow Im(g) = P \Leftrightarrow g$ é sobrejetiva.

iii. $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ é exata $\Longleftrightarrow$ f é injetivo, g é sobrejetivo e $Im(f) = Ker(g)$.

Este resultado segue dos itens i. e ii. e da definição de sequência exata. Neste caso, temos uma *sequência exata curta*, e vale $Coker(f) \simeq P$. De fato, $Coker(f) = N/Im(f) = N/Ker(g) \simeq Im(g) = P$, pelo teorema do isomorfismo para módulos.

Note que qualquer sequência exata $\cdots \to M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$ induz sequências exatas curtas: $0 \to Ker(f_i) = Im(f_{i+1}) \to M_i \to Im(f_i) = Ker(f_{i-1}) \to 0$. Em particular, cada $f \in Hom_A(M, N)$ induz a sequência exata curta $0 \to Ker(f) \to M \to Im(f) \longrightarrow 0$.

Exemplo 1.13. Sejam M um A-módulo, $N \subseteq M$ A-submódulo e $\pi : M \longrightarrow M/N$ a projeção A-linear. Então, π induz $0 \to N \to M \to M/N \to 0$ (sequência exata estrutural).

Sejam $(A, \mathfrak{M})$ anel local e $K = A/\mathfrak{M}$ o *corpo residual de A*. Considere $M \neq 0$ A-módulo finitamente gerado e $\mathfrak{M}M \subseteq M$ A-submódulo. Note que o A-módulo $M/\mathfrak{M}M$ é não-nulo, já que $\mathfrak{M}$ é ideal maximal. Além disso, $\mathfrak{M} = \mathfrak{M}M :_A M = \overline{0} :_A M/\mathfrak{M}M$, pois $a \in \mathfrak{M} \Rightarrow a\overline{x} = \overline{ax} = \overline{0}$, $x \in M \Rightarrow a \in \overline{0} :_A M/\mathfrak{M}M$, e se $a \in \overline{0} :_A M/\mathfrak{M}M \Rightarrow a\overline{m} = \overline{0}$, $m \in M \Rightarrow \overline{am} = \overline{0} \Rightarrow am \in \mathfrak{M}M \Rightarrow aM \subseteq \mathfrak{M}M \Rightarrow a \in \mathfrak{M}M :_A M$. Logo, $M/\mathfrak{M}M$ é $A/\mathfrak{M}$-módulo, isto é, $M/\mathfrak{M}M$ é K-espaço vetorial, e satisfaz $dim_K(M/\mathfrak{M}M) < \infty$, já que M é finitamente gerado.

Proposição 1.20. Sejam $(A, \mathfrak{M})$ anel local e M um A-módulo finitamente gerado. Se $m_1, \ldots, m_n \in M$ são tais que $\{\overline{m_1}, \ldots, \overline{m_n}\}$ é base para o K-espaço vetorial $M/\mathfrak{M}M$, então $\{m_1, \ldots, m_n\}$ é conjunto minimal de geradores de M.

Demonstração. Afirmamos que $M = \sum_{i=1}^{n} Am_i + \mathfrak{M}M$. De fato, seja $m \in M$ temos que existem $\lambda_i \in A$ tais que $m + \mathfrak{M}M = \sum_{i=1}^{n}(\lambda_i + \mathfrak{M})(m_i + \mathfrak{M}M) = \sum_{i=1}^{n}(\lambda_i m_i) + \mathfrak{M}M \Rightarrow m - \sum_{i=1}^{n}(\lambda_i m_i) \in \mathfrak{M}M \Rightarrow M = \sum_{i=1}^{n} Am_i + \mathfrak{M}M$. Pelo corolário 1.19, $M = \sum_{i=1}^{n} Am_i \Rightarrow \{m_1, \ldots, m_n\}$ gera M. Para a minimalidade, suponha que por exemplo $m_1 \in \sum_{j=2}^{n} Am_j$. Então $m_1 = \sum_{j=2}^{n} a_j m_j \in M \Rightarrow m_1 + \mathfrak{M}M = \sum_{j=2}^{n}(a_j + \mathfrak{M})(m_j + \mathfrak{M}M)$ em $M/\mathfrak{M}M$, que é absurdo, pois $(m_i + \mathfrak{M}M)$'s são linearmente independentes sobre K.

□

Definição 1.26. A proposição acima nos permite falar em *número mínimo de geradores* de um módulo M finitamente gerado sobre $(A, \mathfrak{M})$, denotado por $\mu(M)$ e dado por $\mu(M) = dim_{A/\mathfrak{M}}(M/\mathfrak{M}M)$.

Exemplo 1.14. Seja $(A, \mathfrak{M})$ anel local e denote $K = A/\mathfrak{M}$

i. Se $M \simeq A^n$ é A-módulo livre então, $M/\mathfrak{M}M = A^n/\mathfrak{M}A^n = (A/\mathfrak{M})^n = K^n \Rightarrow dim_K(M/\mathfrak{M}M) = dim_K(K)^n = n \Rightarrow \mu(A^n) = n$.

ii. Seja $I = (x_1, \ldots, x_n) \subseteq \mathfrak{M} \subseteq A$ ideal tal que $x_i \notin (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$, $\forall\ i = 1, \ldots, n$, sendo $x_0 = x_{n+1} = 0$ pelo abuso de notação. Assim, $n = \mu(I) = dim_K(I/\mathfrak{M}I)$. Se $I = \mathfrak{M}$, o número $\mu(\mathfrak{M}) = dim_K(\mathfrak{M}/\mathfrak{M}^2)$ é chamado de *dimensão de imersão de* A, denotado por $edim(A)$ ou $embdim(A)$.

Definição 1.27. Seja A anel. Um A-módulo M é dito *Noetheriano* se todo A-submódulo $U \subseteq M$ é finitamente gerado.

Proposição 1.21. Se A é Noetheriano e M é um A-módulo finitamente gerado então M é Noetheriano.

Demonstração. Seja $\{m_1, \ldots, m_n\}$ um conjunto de geradores de M. Considere a aplicação A-linear $\varphi : A^n \longrightarrow M$ que associa a cada e_i o elemento m_i $(i = 1, \ldots, n)$ (claramente sobrejetiva). Com isso, basta mostramos que qualquer A-submódulo $U \subseteq A^n$ é finitamente gerado, já que qualquer A-submódulo de M é imagem por φ de algum A-submódulo de A^n. Vamos usar indução em n, seja $u = (u_1, \ldots, u_n) \in U$, note que o conjunto formado pelas primeiras coordenadas de u é um ideal de A, denote-o por I. Como por hipótese A é Noetheriano, temos que $I = (u_1^{(1)}, \ldots, u_1^{(k)})$, e assim para $n = 1$, temos que o resultado é válido. No caso mais geral, seja $u^{(i)} \in U$ com a primeira coordenada $u_1^{(i)}$ $(i = 1, \ldots, k)$. Para algum $u \in U$ arbitrário, seja $u_1 = \sum_{i=1}^{k} a_i u_1^{(i)}$ com $a_i \in A$. Então $u - \sum_{i=1}^{k} a_i u^{(i)}$ é da forma $(0, u_2^*, \ldots, u_n^*)$ sendo assim pertence a $U \cap A^{n-1}$, identificando A^{n-1} como o A-submódulo de A^n que tem 0 na primeira coordenada. Pela hipótese de indução, $U \cap A^{n-1}$ possui um número finito de geradores, $\{v_1, \ldots, v_l\}$. Assim, $\{u^{(1)}, \ldots, u^{(k)}, v_1, \ldots, v_l\}$ é um conjunto de geradores de U. $\square$

Observação 1.10. Analogamente ao caso de anéis, um A-módulo M é Noetheriano se, e somente se, toda cadeia ascendente de A-submódulos é estacionária.

Definição 1.28. Sejam A anel Noetheriano e M um A-módulo. Um ideal primo $P \subseteq A$ é dito *primo associado (de M)* se puder ser escrito como um ideal anulador $P = 0 :_A m = \{a \in A \mid am = 0\}$ para algum $m \in M \setminus \{0\}$. O conjunto dos ideais primos associados de M é denotado $Ass_A(M)$.

Proposição 1.22. Sejam A anel Noetheriano e M um A-módulo. Então, $Ass_A(M) = \{P \subseteq A$ ideal primo $\mid A/P \simeq N$, para algum A-submódulo N de M $\}$.

Demonstração. Seja $P \in Ass_A(M)$. Então $P = 0 :_A m$ para algum $m \in M \setminus \{0\}$. Considere o homomorfismo

$$\begin{array}{rccc} f_m : & A & \longrightarrow & M \\ & A & \longmapsto & am \end{array}$$

Note que $Ker(f_m) = \{a \in A \mid am = 0\} = 0 :_A m = P$. Logo, pondo $N = Im(f_m)$, pelo teorema do isomorfismo, obtemos $A/P \simeq N$. Inversamente, seja $P \subseteq A$ ideal primo tal que $A/P \simeq N$ com $N \subseteq M$ A-submódulo. Assim, existe isomorfismo $g : A/P \longrightarrow N$.

Afirmação: $P = 0 :_A g(\overline{1})$.

Mostremos a primeira inclusão, $P \subseteq 0 :_A g(\overline{1})$. De fato, $x \in P \Rightarrow \overline{x} = \overline{0} \Rightarrow g(\overline{x}) = g(\overline{0}) = 0$. Por outro lado, $0 = g(\overline{x}) = g(\overline{x}\ \overline{1}) = xg(\overline{1}) \Rightarrow x \in 0 :_A g(\overline{1})$. Agora a segunda inclusão, $0 :_A g(\overline{1}) \subseteq P$. Tome $y \in 0 :_A g(\overline{1}) \Rightarrow yg(\overline{1}) = 0 \Rightarrow g(y\overline{1}) = g(\overline{y}) = 0 \Rightarrow \overline{y} \in Ker(g) = \{\overline{0}\} \Rightarrow \overline{y} = \overline{0} \Rightarrow y \in P$. Assim, $P = 0 :_A g(\overline{1}) \Rightarrow P \in Ass_A(M)$.

□

Proposição 1.23. Sejam A anel Noetheriano e M um A-módulo. Então,

i. $P \subseteq A$ é ideal primo $\Longrightarrow Ass_A(A/P) = \{P\}$;

ii. $Ass_A(M) = \emptyset \Longleftrightarrow M = 0$.

Demonstração.

i. A inclusão $\{P\} \subseteq Ass_A(A/P)$ é clara, pois para qualquer $x \in A \setminus P$ vale: $P = P :_A x = \overline{0} :_A \overline{x} \Rightarrow P \in Ass_A(A/P)$. Seja agora $Q \in Ass_A(A/P)$, então $\exists\ x \in A \setminus P$ tal que $Q = \overline{0} :_A \overline{x}$, logo $Q = P :_A x = P$.

ii. A implicação $M = 0 \Rightarrow Ass_A(M) = \emptyset$ segue imediatamente da definição. Suponha agora que $Ass_A(M) = \emptyset$, e por absurdo que $M \neq 0$. Logo, a família de ideais anuladores $\mathfrak{A} = \{0 :_A m \mid m \in$

$M \setminus \{0\}\}$ é não-vazia. Como A é Noetheriano, $\mathfrak{A}$ possui um elemento maximal (com respeito a inclusão). Seja $Q = 0 :_A n$ o tal elemento, para algum $n \in M \setminus \{0\}$. Sejam $x, y \in A$ tais que $xy \in Q$ e suponha que $y \notin Q$. Afirmamos que $x \in Q$. Note que $xy \in Q = 0 :_A n \Rightarrow xyn = 0 \Rightarrow x \in 0 :_A (yn)$. Como $yn \neq 0$ (pois $y \notin Q$) tem-se $0 :_A (yn) \in \mathfrak{A}$. Pela maximalidade de Q, vale $0 :_A (yn) \subseteq Q = 0 :_A n \Rightarrow x \in Q$. Isso mostra que Q é primo, e sendo $Q = 0 :_A n$, tem-se $Q \in Ass_A(M)$, absurdo já que supomos $Ass_A(M) = \emptyset$. □

Proposição 1.24. Seja $0 \to N \to M \to M/N \to 0$ uma sequência exata curta de módulos sobre A anel Noetheriano. Então:

$$Ass_A(N) \subseteq Ass_A(M) \subseteq Ass_A(N) \cup Ass_A(M/N).$$

Demonstração. A inclusão $Ass_A(N) \subseteq Ass_A(M)$ é clara. Seja $P \in Ass_A(M) \setminus Ass_A(N)$. Queremos mostrar que $P \in Ass_A(M/N)$. De fato, $\exists\ m \in M \setminus N$ tal que $P = 0 :_A m$. Em particular, $P \subseteq N :_A m \Rightarrow P \subseteq N :_A m = \overline{0} :_A \overline{m}$.

Afirmação: $Am \cap N = 0$.

Suponha por absurdo que $Am \cap N \neq 0$. Então, pela proposição 1.23, $\exists\ Q \in Ass_A(Am \cap N)$, logo: $Q \in Ass_A(Am \cap N) \subseteq Ass_A(Am) = Ass_A(A/P)$, através da aplicação A-linear $f : A \longrightarrow M$ definida por $a \longmapsto am$, que possui $Ker(f) = P$ e $Im(f) = Am$, pelo teorema do isomorfismo $A/P \simeq Am$. Assim, $Q = P$, já que $Ass_A(A/P) = \{P\}$. Mas $P \in Ass_A(Am \cap N) \subseteq Ass_A(N) \Rightarrow P \in Ass_A(N)$, que é absurdo. Portanto, $Am \cap N = 0$. Tínhamos $P \subseteq \overline{0} :_A \overline{m} = N :_A m$. Mostremos que $N :_A m \subseteq P$. De fato, seja $a \in N :_A m \Rightarrow am \in N \cap Am = 0 \Rightarrow am = 0 \Rightarrow a \in 0 : Am = P$. Assim, $P = \overline{0} :_A \overline{m} \Rightarrow P \in Ass_A(M/N)$. □

Proposição 1.25. Seja A anel Noetheriano. Então, $\displaystyle\bigcup_{P \in Ass_A(M)} P = Z(M)$, onde $Z(M) = \{a \in A \mid am = 0$, para algum $m \in M \setminus \{0\}\}$, ou seja, $Z(M)$ é o conjunto dos divisores de zero de M.

Demonstração. Os elementos de $P \in Ass_A(M)$ claramente são divisores de zero de M, já que $P = 0 :_A m$ para algum $m \in M$ não-nulo. Inversamente, seja $a \in A$ tal que $am = 0$ para algum $m \in M \setminus \{0\}$, pela proposição anterior, temos que $Ass_A(Am) \neq \emptyset \Rightarrow \exists\ P \subseteq A$ ideal primo e $a' \in A \setminus \{0\}$ tal que $P = 0 :_A (a'm) \Rightarrow a \in P$ já que $a(a'm) = a'(am) = 0$. □

Proposição 1.26. Sejam A anel Noetheriano e M um A-módulo finitamente gerado, $M \neq 0$. Então, existe uma cadeia de A-submódulos de M,

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_n = M,$$

tal que $M_i/M_{i-1} \simeq A/P_i$, $\forall\ i = 1, \ldots, n$, onde P_i é ideal primo para todo $i = 1, \ldots, n$.

Demonstração. $M \neq 0 \Rightarrow Ass_A(M) \neq \emptyset \Rightarrow \exists\ P_1 \in Ass_A(M)$. Pela proposição 1.22, $\exists\ M_1 \subseteq M$ tal que $A/P_1 \simeq M_1$. Se $M_1 = M$ então, considere a cadeia $0 \subsetneq M$, com $M = M_1 \simeq A/P_1$. Se $M_1 \subsetneq M$ então $M/M_1 \neq 0 \Rightarrow \exists\ P_2 \in Ass_A(M/M_1) \Rightarrow A/P_2 \simeq M_2/M_1$ para algum A-submódulo $M_2 \subseteq M$ tal que $0 \subsetneq M_1 \subsetneq M_2 \subseteq M$. Procedendo dessa forma, obtemos uma cadeia

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \quad (\bigstar_2)$$

sendo A Noetheriano e M A-módulo finitamente gerado temos que M é Noetheriano, assim a cadeia $(\bigstar_2)$ é estacionária. Portanto, para algum natural $n < \infty$, $M_n = M$. $\square$

Teorema 1.27. *Sejam A anel Noetheriano e M um A-módulo finitamente gerado, $M \neq 0$. Então, $Ass_A(M)$ é finito. Em particular, $Ass_A(A)$ é finito.*

Demonstração. A proposição anterior fornece uma cadeia

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_n = M,$$

com $M_i/M_{i-1} \simeq A/P_i$, e P_i ideal primo para $i = 1, \ldots, n$. Tome a sequência exata curta

$$0 \to M_1 \to M_2 \to M_2/M_1 \to 0$$

Logo, $Ass_A(M_1) \subseteq Ass_A(M_2) \subseteq Ass_A(M_1) \bigcup Ass_A(M_2/M_1)$. Note que $M_1 \simeq A/P_1 \Rightarrow Ass_A(M_1) = \{P_1\}$, e $M_2/M_1 \simeq A/P_2 \Rightarrow Ass_A(M_2/M_1) = P_2$. Assim, $Ass_A(M_2) \subseteq \{P_1, P_2\}$. Agora, tome

$$0 \to M_2 \to M_3 \to M_3/M_2 \to 0$$

Logo, $Ass_A(M_3) \subseteq Ass_A(M_2) \bigcup Ass_A(M_3/M_2)$, e como $Ass_A(M_3/M_2) = \{P_3\}$, pois $M_3/M_2 \simeq$

A/P_3, temos que $Ass_A(M_3) \subseteq \{P_1, P_2, P_3\}$. Procedendo analogamente, e denotando por n o índice de estabilização da cadeia (isto é, $M_n = M$), obtemos $Ass_A(M) = Ass_A(M_n) \subseteq \{P_1, \ldots, P_n\} \Rightarrow |Ass_A(M)| < \infty$. □

Corolário 1.28. Sejam A anel Noetheriano e M um A-módulo finitamente gerado. Se $I \subseteq A$ é um ideal que contém apenas divisores de zero de M então existe $m \in M \setminus \{0\}$, tal que $Im = 0$.

Demonstração. Por hipótese temos que $I \subseteq \bigcup_{P \in Ass_A(M)} P \Rightarrow I \subseteq \bigcup_{i=1}^{n} P_i$, já que pelo teorema anterior, $Ass_A(M) = \{P_1, \ldots, P_n\}$, assim, pelo Lema da esquiva, $I \subseteq P_j \in Ass_A(M)$ para algum $j = 1, \ldots, n \Rightarrow \exists\ m \in M \setminus \{0\}$ tal que $Im = 0$. □

Capítulo 2

Um pouco de teoria homológica

2.1 Profundidade de um módulo

Definição 2.1. Seja M A-módulo. Um elemento $a \in A$ é dito *M-elemento regular (ou não-divisor de zero de M)* se $ax = 0$ com $x \in M$ implicar $x = 0$. Uma sequência $\{a_1, \ldots, a_m\}$ de elementos de A é chamada *M-sequência regular* se:

i. $M \neq (a_1, \ldots, a_m)M$;

ii. a_{i+1} é não-divisor de zero de $M/(a_1, \ldots, a_i)M$, para $i = 0, \ldots, m-1$.

Denotando $M_i = M/(a_1, \ldots, a_i)M$, a condição ii. é equivalente à aplicação A-linear

$$\begin{array}{rccc} \mu_{a_{i+1}}: & M_i & \longrightarrow & M_i \\ & \overline{x} & \longmapsto & a_{i+1}\overline{x} \end{array}$$

ser injetiva para cada $i = 0, \ldots, m-1$. De fato, a_{i+1} é não-divisor de $M/(a_1, \ldots, a_i)M \iff a_{i+1}\overline{x} = \overline{0},\ x \in M \Rightarrow \overline{x} = \overline{0} \iff Ker(\mu_{a_{i+1}}) = \{\overline{0}\} \iff \mu_{a_{i+1}}$ é injetiva. Em particular, a_1 é não-divisor de zero de $M_0 = M$.

Sejam A anel Noetheriano, M A-módulo finitamente gerado e $I \subseteq A$ ideal tal que $IM \neq M$. Se $\{a_1, \ldots, a_n\}$ é M-sequência regular, $a_1, \ldots, a_n \in I$, então $(a_1, \ldots, a_i)M \neq (a_1, \ldots, a_{i+1})M$, $\forall\ i = 1, \ldots, m-1$. De fato, suponha por absurdo que $(a_1, \ldots, a_i)M = (a_1, \ldots, a_{i+1})M \Rightarrow M_i = \frac{M}{(a_1, \ldots, a_i)M} = \frac{M}{(a_1, \ldots, a_i, a_{i+1})M} = M_{i+1}$, assim $\mu_{a_{i+1}}$ não seria injetiva, que é absurdo. Logo, $(a_1, \ldots, a_i)M \neq$

$(a_1, \ldots, a_{i+1})M, \ \forall\ i = 1, \ldots, m-1$.

Sendo M A-módulo sobre A anel Noetheriano, temos que qualquer M-sequência regular $\{a_1, \ldots, a_m\}$ com $a_i \in I, \ \forall\ i = 1, \ldots, m$, pode ser alongada a uma *sequência regular maximal*, isto é, a uma M-sequência regular $\{a_1, \ldots, a_n\} \subseteq I$ $(n \geq m)$ tal que qualquer $a \in I$ é divisor de zero de $M/(a_1, \ldots, a_n)M$, o resultado segue do fato de que A é Noetheriano, logo todo ideal de A possui um número finito de geradores.

Lema 2.1. Sejam A anel Noetheriano, M A-módulo finitamente gerado. Sejam $a, b \in A$ tais que $\{a, b\}$ é uma M-sequência regular e b não é um divisor de zero de M, então $\{b, a\}$ também é uma M-sequência regular.

Demonstração. De fato, a condição i. para $\{b, a\}$ ser M-sequência regular é trivialmente satisfeita. Resta-nos mostrar que a não é divisor de zero de M/bM. Para isto, suponha por absurdo que a seja divisor de zero de M/bM, então existiria $m \in M$ tal que $m \notin bM$ com $am = bm'$ $(m' \in M)$. Sendo $\{a, b\}$ M-sequência regular devemos ter $m' \in aM$ assim, $m' = am''$ para algum $m'' \in M$. Assim, $am = bm' = bam'' \Rightarrow a(m - bm'') = 0$, como a é não-divisor de zero de M temos que $m - bm'' = 0 \Rightarrow m = bm''$, que é absurdo, já que $m \notin bM$. □

Proposição 2.2. Sejam A anel Noetheriano, M A-módulo finitamente gerado e $I \subseteq A$ ideal tal que $IM \neq M$. Então, quaisquer duas M-sequências regulares maximais em I possuem o mesmo número de elementos.

Demonstração. Entre todas as M-sequências regulares maximais em I existe uma com o número mínimo de elementos n. Vamos mostrar o resultado usando indução em n. Se $n = 0$, então I consiste apenas de elementos divisores de zero de M, e não a nada a ser mostrado. Por isso, sejam $n > 0$, $\{a_1, \ldots, a_n\}$ uma M-sequência regular maximal em I e $\{b_1, \ldots, b_n\}$ outra M-sequência regular em I. Mostremos que I consiste apenas de divisores de zero de $M/(b_1, \ldots, b_n)M$.

Se $n = 1$ então I consiste apenas de divisores de zero de M/a_1M. Pelo corolário 1.28, existe $m \in M$ com $m \notin a_1M$ tal que $Im \subseteq a_1M$. Em particular, $b_1m = a_1m'$ para algum $m' \in M$. Se tivéssemos $m' \in b_1M$ então teríamos $m' = b_1m'' \Rightarrow b_1m = a_1b_1m'' \Rightarrow b_1(m - a_1m'') = 0 \Rightarrow m = a_1m''$ já que para o caso $n = 1$ b_1 é não-divisor de zero de M, o que implica $m \in a_1M$, absurdo, assim $m' \notin b_1M$. Como $a_1Im' = Ib_1m \subseteq a_1b_1M$ temos que $Im' \subseteq b_1M$, já que a_1 também é não-divisor de zero de M, e portanto I consiste apenas de divisores de zero de M/b_1M.

Se $n > 1$, denote $M_i = M/(a_1, \ldots, a_i)M$ e $M_i' = M/(b_1, \ldots, b_i)M$, $i = 0, \ldots, n-1$, e tome $c \in I$ tal que c é não-divisor de zero de M_i e M_i' para todo $i = 0, \ldots, n-1$, note que tal c existe, pois pela proposição 1.25 o conjunto dos divisores de zero de M_i e M_i' é a união dos ideais primos associados de M_i e de M_i', que pelo teorema 1.27 é uma união finita, e além disso, que I não está contido em nenhum desses ideais primos associados, já que se estivésse, teríamos que I consiste apenas de divisores de zero de M.

Assim, aplicando o lema anterior repetidamente, obtemos que $\{c, a_1, \ldots, a_{n-1}\}$ e $\{c, b_1, \ldots, b_{n-1}\}$ são M-sequências regulares em I, onde $\{c, a_1, \ldots, a_{n-1}\}$ é maximal, desde que $\{a_1, \ldots, a_{n-1}, c\}$ é maximal com base no caso $n = 1$ (aplicado a M_{n-1}) tratado anteriormente. Então, $\{a_1, \ldots, a_{n-1}\}$ e $\{b_1, \ldots, b_{n-1}\}$ são M/cM-sequências regulares em I; a primeira é maximal, então por hipótese de indução a segunda também é. Mas, se $\{b_1, \ldots, b_{n-1}, c\}$ é M-sequência regular maximal, então $\{b_1, \ldots, b_n\}$ também o é, novamente pelo caso $n = 1$. O que prova a proposição. □

Esta proposição nos permite está bem posta a seguinte definição:

Definição 2.2. Sejam A anel Noetheriano, M A-módulo finitamente gerado e $I \subseteq A$ ideal tal que $IM \neq M$. O número de elementos de uma M-sequência regular maximal em I é chamado de *profundidade de I em M*, denotado por $prof(I, M)$. Se $(A, \mathfrak{M})$ é anel Noetheriano local, então chamamos $prof(\mathfrak{M}, M)$ de *profundidade de M* e escrevemos $prof(M)$. Em particular, definimos $prof(A)$, a profundidade de um anel A.

Note que $prof(I, M) = 0 \Longleftrightarrow I$ consiste de apenas divisores de zero de M. Além disso, se $(A, \mathfrak{M})$ é anel Noetheriano local, então $prof(M) = 0$ é equivalente a $\mathfrak{M} \in Ass_A(M)$.

Proposição 2.3. Sejam A anel Noetheriano, M A-módulo finitamente gerado e $I \subseteq A$ ideal tal que $IM \neq M$. Se $\{a_1, \ldots, a_m\}$ é uma M-sequência regular em I, então

$$prof(I, M/(a_1, \ldots, a_m)M) = prof(I, M) - m.$$

Demonstração. Seja $\{a_1, \ldots, a_n\}$ $(n \geq m)$ uma M-sequência regular maximal. Assim, temos que $prof(I, M) = n$ e como $\overline{b} = \overline{0} \Leftrightarrow b \in (a_1, \ldots, a_m)M$ segue que $prof(I, M/(a_1, \ldots, a_m)M) = n - m$. □

A proposição a seguir vai relacionar a profundidade com o número de geradores de um ideal.

Proposição 2.4. Sejam A anel Noetheriano, M A-módulo finitamente gerado e $I \subseteq A$ ideal tal que $IM \neq M$. Considere n o número de geradores de I e $prof(I, M) = m$. Então, $m \leq n$ e existe um conjunto de geradores $\{a_1 \ldots, a_n\}$ de I para o qual $\{a_1, \ldots, a_m\}$ é uma M-sequência regular.

Demonstração. Seja $\{a_1, \ldots, a_n\}$ um conjunto de geradores de I e seja $(a_1, \ldots, a_k) \subseteq \bigcup_{P \in Ass_A} P$, $(a_1, \ldots, a_{k+1}) \nsubseteq \bigcup_{P \in Ass_A} P$ para $k = 0, \ldots, n$. Se $k = n$, então $I \subseteq \bigcup_{P \in Ass_A} P \Rightarrow I$ consiste apenas de divisores de M, o que implica $prof(I, M) = 0$, e o resultado é válido. Se $k < n$, mostremos que existe $b \in I$ não-divisor de zero de M tal que $(a_1, \ldots, a_{k+1}) = (b, a_1, \ldots, a_k)$. Passando para M/bM e $I/(b)$, o resultado segue por indução.

Seja $\{P_1, \ldots, P_s\}$ o conjunto dos elementos maximais de $Ass_A(M)$ (com respeito a inclusão). Por hipótese existe um elemento da forma $a + ra_{k+1}$ com $a \in (a_1, \ldots, a_k)$, $r \in A$, que não pertence a $\bigcup_{l=1}^{s} P_l$. Se $a_{k+1} \in P_i$ para $i = 1, \ldots, \sigma$ e $a_{k+1} \notin P_j$ $j = \sigma + 1, \ldots, s$, então tome $t \in \bigcap_{j=\sigma+1}^{s} P_j$, $t \notin \bigcup_{i=1}^{\sigma} P_i$ e defina $b = ta + a_{k+1}$. Então, $b \notin P_i$ $(i = 1, \ldots, s)$, ou seja, b é não-divisor de zero de M. Além disso, $(a_1, \ldots, a_{k+1}) = (b, a_1, \ldots, a_k)$.

$\square$

2.2 Dimensão homológica de um módulo

Sejam A anel Noetheriano e M A-módulo finitamente gerado. Considere $\{x_1, \ldots, x_m\}$ um conjunto de geradores de M, e defina a aplicação A-linear $\alpha_0 : A^m \longrightarrow M$ por $\alpha_0(a_1, \ldots, a_m) = a_1x_1 + \ldots + a_mx_m$ (que é claramente sobrejetiva). Esta construção é equivalente a sequência exata curta

$$0 \to Ker(\alpha_0) \to A^m \xrightarrow{\alpha_0} M \to 0.$$

Neste caso, $Ker(\alpha_0)$ é denominado *módulo de relações dos geradores* $x_1, \ldots, x_m$ e denotado por $\mathrm{Syz}(M)$, mais precisamente, $\mathrm{Syz}(M) = \{(b_1, \ldots, b_m) \in A^m \mid b_1x_1 + \ldots + b_mx_m = 0\}$, cada $(b_1, \ldots, b_m) \in \mathrm{Syz}(M)$ é chamado *sizigia de M (a rigor, de $\{x_1, \ldots, x_m\}$)*. Sendo A Noetheriano, temos que $\mathrm{Syz}(M)$ é finitamente gerado, assim podemos proceder da seguinte forma: suponha que

$\mathrm{Syz}(M)$ seja gerado por m_1 elementos, assim podemos considerar a sequência exata curta,

$$0 \to \mathrm{Syz}(\mathrm{Syz}(M)) = \mathrm{Syz}^2(M) \to A^{m_1} \to \mathrm{Syz}(M) \to 0,$$

que por composição obtemos

$$A^{m_1} \to A^m \to M \to 0,$$

chamada de *apresentação livre de M*. Assim, podemos iterar este processo, o que será indicado por

$$\cdots \to A^{m_{i+1}} \xrightarrow{\alpha_{i+1}} A^{m_i} \to \cdots \to A^{m_1} \xrightarrow{\alpha_1} A^m \xrightarrow{\alpha_0} M \to 0, \quad (\bigstar_3)$$

onde entende-se que $Ker(\alpha_i) = Im(\alpha_{i+1}),\ i = -1, 0, 1, 2, \ldots$, identificando α_{-1} pela aplicação A-linear nula. Uma sequência como em $(\bigstar_3)$, isto é, uma sequência exata de A-módulos livres é chamada de *resolução livre de M*

Uma tal sequência é infinita, em princípio. Mas podemos truncá-la em qualquer etapa, tornando-a finita:

$$0 \to \mathrm{Syz}^{m_n}(M) \to A^{m_{n-1}} \to \cdots \to A^{m_1} \to A^m \to M \to 0.$$

Neste caso, não estamos tratando mais de uma resolução livre, já que $\mathrm{Syz}^{m_n}(M)$ pode não ser livre. Se suceder que $\mathrm{Syz}^{m_n}(M)$ é livre, então temos uma resolução livre finita, de comprimento $n =$ número de módulos livres menos um. Isto motiva a seguinte definição:

Definição 2.3. Sejam A anel Noetheriano e M A-módulo finitamente gerado. A *dimensão homológica de M* é o comprimento de uma resolução livre finita de M de menor comprimento possível, denotada por $dh_A(M)$. Quando estiver implícito o anel A em questão, escrevemos $dh_A(M) = dh(M)$. Se M não admitir resolução livre finita, então $dh(M) = \infty$.

Lema de Schanuel. *Sejam A Noetheriano e M A-módulo finitamente gerado. Dadas duas sequências exatas de A-módulos*

$$0 \to K_n \xrightarrow{\alpha_{n-1}} F_{n-1} \xrightarrow{\alpha_{n-2}} \cdots \xrightarrow{\alpha_0} F_0 \xrightarrow{\alpha} M \to 0$$

$$0 \to K_n' \xrightarrow{\alpha_{n-1}'} F_{n-1}' \xrightarrow{\alpha_{n-2}'} \cdots \xrightarrow{\alpha_0'} F_0' \xrightarrow{\alpha'} M \to 0$$

onde $n \geq 1$ e F_i, F_i' são A-módulos livres para $i = 0, \ldots, n-1$. Então,

$$K_n \oplus F'_{n-1} \oplus F_{n-2} \oplus \cdots \simeq K'_n \oplus F_{n-1} \oplus F'_{n-2} \oplus \cdots$$

Demonstração. Mostremos por indução em n. Considere o caso $n = 1$:

$$0 \to K_1 \xrightarrow{\alpha_0} F_0 \xrightarrow{\alpha} M \to 0$$

$$0 \to K_1' \xrightarrow{\alpha_0'} F_0' \xrightarrow{\alpha'} M \to 0 \ .$$

Vamos mostrar que

$$K_1 \oplus F_0' \simeq K_1' \oplus F_0 \ .$$

De fato, sendo F_0, F_0' A-módulos livres e α, α' aplicações A-lineares sobrejetivas, existem aplicações A-lineares $\gamma : F_0 \longrightarrow F_0'$ e $\gamma' : F_0' \longrightarrow F_0$ tais que $\alpha = \alpha' \circ \gamma$ e $\alpha' = \alpha \circ \gamma'$. Para cada $(x, y) \in F_0 \oplus F_0'$ seja $\beta(x, y) = (x, y - \gamma(x))$ e $\beta'(x, y) = (x - \gamma'(y), y)$, note que β, β' são isomorfismos de $F_0 \oplus F_0'$ em $F_0 \oplus F_0'$, com efeito, β é A-linear, pois se (x, y), $(z, w) \in F_0 \oplus F_0'$ então $\beta((x, y) + (z, w)) = (x + z, y + w - \gamma(x + z)) = (x + z, y + w - \gamma(x) - \gamma(z)) = (x, y - \gamma(x)) + (z, w - \gamma(z)) = \beta(x, y) + \beta(z, w)$; assim como, se $a \in A$ então $\beta(a(x, y)) = (ax, ay - \gamma(ax)) = (ax, ay - a\gamma(x)) = a(x, y - \gamma(x)) = a\beta(x, y)$. Mostremos agora que β é injetiva, se $(x, y) \in Ker(\beta)$ então $\beta(x, y) = (x, y - \gamma(x)) = (0, 0)$ o que implica que $x = y = 0$, assim β é injetiva. Por fim, se $(c, d) \in F_0 \oplus F_0'$ então, tome $x = c$ e $y = \gamma(c) + d$ (que faz sentido pois $\gamma(c) \in F_0'$) e obtenha $\beta(x, y) = \beta(c, \gamma(c) + d) = (c, \gamma(c) + d - \gamma(c)) = (c, d)$, mostrando a sobrejetividade de β, analogamente mostra-se que β' é isomorfismo. Além disso, observe que $\beta^{-1}(x, y) = (x, y + \gamma(x))$, assim defina $\psi = \beta^{-1} \circ \beta'$. Identificando K_1 como $Im(\alpha_0) \subseteq F_0$ e K_1' como $Im(\alpha_0') \subseteq F_0'$. Mostremos agora que $\psi : K_1 \oplus F_0' \longrightarrow F_0 \oplus K_1'$ é isomorfismo, com isso o resultado é obtido, já que $F_0 \oplus K_1' \simeq K_1' \oplus F_0$.

i. ψ está bem definida. De fato, seja $(x, y) \in K_1 \oplus F_0' \Rightarrow \psi(x, y) = \beta^{-1}(\beta'(x, y)) = \beta^{-1}(x - \gamma'(y), y) = (x - \gamma'(y), y + \gamma(x - \gamma'(y))) = (x - \gamma'(y), y + \gamma(x) - \gamma(\gamma'(y)))$. Basta mostrarmos que $y + \gamma(x) - \gamma(\gamma'(y)) \in K_1'$ para ψ está bem definida, mas como $K_1' = Im(\alpha_0') = Ker(\alpha')$ basta verificarmos que $\alpha'(y + \gamma(x) - \gamma(\gamma'(y))) = 0 \in M$. De fato, $\alpha'(y + \gamma(x) - \gamma(\gamma'(y))) =$

$\alpha'(y) + \alpha'(\gamma(x)) - \alpha'(\gamma(\gamma'(y))) = \alpha'(y) + \alpha(x) - \alpha'(y) = \alpha(x) = 0$ pois $x \in K_1$.

ii. ψ é aplicação A-linear. Se deve ao fato de β^{-1} e β' serem aplicações A-lineares.

iii. ψ é injetiva. De fato, seja $(x, y) \in Ker(\psi) \Rightarrow \psi(x, y) = (x - \gamma'(y), y + \gamma(x) - \gamma(\gamma'(y))) = (0, 0) \Rightarrow x = \gamma'(y)$ e $y + \gamma(x) - \gamma(\gamma'(y)) = 0 \Rightarrow y + \gamma(x) - \gamma(x) = 0 \Rightarrow y = 0 \Rightarrow x = 0$. Assim, ψ é injetiva.

iv. ψ é sobrejetiva. De fato, seja $(c, d) \in F_0 \oplus K_1'$, vamos mostrar que existe $(x, y) \in K_1 \oplus F_0'$ tal que $\psi(x, y) = (c, d)$. Tome $y = d - \gamma(c)$ e $x = \gamma'(d) - \gamma'(\gamma(c)) + c$, perceba que isto é possível pois $K_1' \simeq Im(\alpha_0') \subseteq F_0'$, logo podemos tomar $y = d - \gamma(c)$ e para mostrarmos que $x = \gamma'(d) - \gamma'(\gamma(c)) + c$ está bem posto, basta percebermos que $\alpha(x) = 0 \in M$, já que $K_1 \simeq Im(\alpha_0) = Ker(\alpha)$. Com efeito, $\alpha(x) = \alpha(\gamma'(d) - \gamma'(\gamma(c)) + c) = \alpha(\gamma'(d)) - \alpha(\gamma'(\gamma(c))) + \alpha(c) = \alpha'(d) - \alpha(c) + \alpha(c) = \alpha'(d) = 0$ pois $d \in K_1'$. Por fim, façamos a verificação da sobrejetividade:
$\psi(x, y) = \psi(\gamma'(d) - \gamma'(\gamma(c)) + c, d - \gamma(c)) = (\gamma'(d) - \gamma'(\gamma(c)) + c - \gamma'(d - \gamma(c)), d - \gamma(c) + \gamma(\gamma'(d) - \gamma'(\gamma(c)) + c) - \gamma(\gamma'(d - \gamma(c)))) = (c, d - \gamma(c) + \gamma(\gamma'(d)) - \gamma(\gamma'(\gamma(c))) + \gamma(c) - \gamma(\gamma'(d)) + \gamma(\gamma'(\gamma(c)))) = (c, d)$.

Assim, finalizamos o caso $n = 1$. Suponha agora $n > 1$ e que o resultado seja válido para $n - 1$. Sejam $K_{n-1} = Im(\alpha_{n-2})$, $K_{n-1}' = Im(\alpha_{n-2}')$. Então

$$K_{n-1}' \oplus F_{n-2} \oplus F_{n-3}' \oplus \cdots \simeq K_{n-1} \oplus F_{n-2}' \oplus F_{n-3} \oplus \cdots ,$$

com isso obtemos as seguintes sequências exatas (provenientes das sequências exatas $0 \to K_n \to F_{n-1} \to K_{n-1} \to 0$ e $0 \to K_n' \to F_{n-1}' \to K_{n-1}' \to 0$)

$$0 \to K_n \to F_{n-1} \oplus F_{n-2}' \oplus F_{n-3} \oplus \cdots \to K_{n-1} \oplus F_{n-2}' \oplus F_{n-3} \oplus \cdots \to 0$$

$$0 \to K_n' \to F_{n-1}' \oplus F_{n-2} \oplus F_{n-3}' \oplus \cdots \to K_{n-1}' \oplus F_{n-2} \oplus F_{n-3}' \oplus \cdots \to 0$$

Aplicando o caso $n = 1$ nas sequências acima, obtemos o resultado. □

Lema da Serpente. *Dado*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & K_1 & & K_2 & & K_3 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \rightarrow & M_1 & \xrightarrow{\alpha_1} & M_2 & \xrightarrow{\alpha_2} & M_3 & \rightarrow & 0 \\
 & & \downarrow{\scriptstyle\gamma_1} & & \downarrow{\scriptstyle\gamma_2} & & \downarrow{\scriptstyle\gamma_3} & & \\
0 & \rightarrow & N_1 & \xrightarrow{\beta_1} & N_2 & \xrightarrow{\beta_2} & N_3 & \rightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & C_1 & & C_2 & & C_3 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

um diagrama comutativo de A-módulos e aplicações A-lineres exato, isto é, as linhas e as colunas do diagrama são sequências exatas e o diagrama comuta no sentido que $\gamma_2 \circ \alpha_1 = \beta_1 \circ \gamma_1$ e $\gamma_3 \circ \alpha_2 = \beta_2 \circ \gamma_2$. Sejam $\alpha'_i : K_i \longrightarrow K_{i+1}$ e $\beta'_i : C_i \longrightarrow C_{i+1}$ $(i = 1, 2)$ aplicações A-lineares induzidas por α_i e β_i. Então, existe aplicação A-linear $\delta : K_3 \longrightarrow C_1$ tal que a sequência

$$0 \to K_1 \xrightarrow{\alpha'_1} K_2 \xrightarrow{\alpha'_2} K_3 \xrightarrow{\delta} C_1 \xrightarrow{\beta'_1} C_2 \xrightarrow{\beta'_2} C_3 \to 0 \quad (\bigstar_4)$$

é exata.

Demonstração. Consideremos as aplicações injetivas do diagrama como sendo inclusões.

i. Construção de δ. Para cada $x \in K_3$ tome $x' \in M_2$ tal que $\alpha_2(x') = x$, isto é possível pois α_2 é sobrejetiva, assim defina $y' = \gamma_2(x')$. Assim, $\beta_2(y') = \gamma_3(\alpha_2(x')) = \gamma_3(x) = 0$, já que $x \in K_3$, então $y' \in Ker(\beta_2) = N_1$. Defina $\delta(x)$ como sendo a imagem de y' em C_1. Mostremos que δ está bem definida, ou seja, que não depende da escolha do x', de fato, sejam $x'' \in M_2$ tal que $\alpha_2(x'') = x$ e $y'' = \gamma_2(x'')$, então $x' - x'' \in Ker(\alpha_2) = Im(\alpha_1)$ o que implica, $\exists\ m_1 \in M_1$ tal que $\alpha_1(m_1) = x' - x''$, e como o diagrama é comutativo $\gamma_2(\alpha_1(m_1)) = \gamma_2(x' - x'') = \beta_1(\gamma_1(m_1))$, e como β_1 é injetiva, temos que $\gamma_2(x' - x'') = \gamma_2(x') - \gamma_2(x'') = y' - y'' \in Im(\gamma_1)$. Assim, y' e y''

tem a mesma imagem em C_1 pois denotando a aplicação A-linear de N_1 em C_1 por f, temos que $Im(\gamma_1) = Ker(f) \Rightarrow f(y' - y'') = 0 \Rightarrow f(y') = f(y'')$. Portanto, δ está bem definida. Além disso, segue de imediato que δ é uma aplicação A-linear, pois δ é a composição de aplicações A-lineares.

ii. Exatidão de $(\bigstar_4)$ em K_3. Mostremos que $Ker(\delta) \subseteq Im(\alpha_2')$, de fato se $\delta(x) = 0$ então $y' \in Ker(f) = Im(\gamma_1)$. Assim, seja $y'' \in M_1$ tal que $\gamma_1(y'') = y'$ e defina $x'' = \alpha_1(y'')$, então $\alpha_2(x' - x'') = \alpha_2(x') - \alpha_2(x'') = \alpha_2(x') - \alpha_2(\alpha_1(y'')) = x$, já que $y'' \in M_1$. Além disso, $\gamma_2(x' - x'') = \gamma_2(x') - \gamma_2(x'') = y' - \gamma_2(\alpha_1(y'')) = y' - \beta_1(\gamma_1(y''))$, já que o diagrama é comutativo, e por β_1 ser injetiva, temos que $\gamma_2(x' - x'') = y' - \gamma_1(y'') = y' - y' = 0 \Rightarrow x' - x'' \in K_2$. Portanto, $x \in Im(\alpha_2')$. Mostremos agora a inclusão $Im(\alpha_2') \subseteq Ker(\delta)$, de fato se $x \in Im(\alpha_2')$ então existe $a \in K_2$ tal que $x = \alpha_2'(a) \Rightarrow \gamma_2(a) = 0$ pois $a \in K_2$, portanto $\delta(x) = 0 \Rightarrow x \in Ker(\delta)$.

iii. Exatidão de $(\bigstar_4)$ em C_1. Mostremos que $Ker(\beta_1') \subseteq Im(\delta)$, de fato se $z \in Ker(\beta_1')$ então $z \in C_1$, denote por $y \in N_1$ o elemento que representa z em N_1 e por g a aplicação A-linear de N_2 em C_2, sendo assim, $g(\beta_1(y)) = 0 \Rightarrow \beta_1(y) \in Ker(g) = Im(\gamma_2)$. Logo, existe $x' \in M_2$ tal que $\gamma_2(x') = \beta_1(y)$. Tome $x = \alpha_2(x')$, pela definição de δ temos que $\delta(x) = z$, o que mostra a primeira inclusão. Mostremos agora a inclusão $Im(\delta) \subseteq Ker(\beta_1')$, seja $b \in Im(\delta)$ vamos verificar que $\beta_1'(b) = 0$, de fato $\beta_1'(b) = \beta_1'(\delta(x))$ para algum $x \in K_3 \Rightarrow \beta_1'(b) = g(y')$, com $y' = \gamma_2(x')$, onde y' representa b em N_1, para algum $x' \in M_2$ tal que $\alpha_2(x') = x \Rightarrow \beta_1'(b) = 0$, pois $y' \in Im(\gamma_2) = Ker(g)$.

iv. Exatidão de $(\bigstar_4)$ em K_1, ou seja, a injetividade de α_1'. Segue do fato de α ser injetiva.

v. Exatidão de $(\bigstar_4)$ em K_2. Equivalentemente, $Im(\alpha_1') = Ker(\alpha_2')$, segue de imediato de $Im(\alpha_1) = Ker(\alpha_2)$.

vi. Exatidão de $(\bigstar_4)$ em C_2. Equivalentemente, $Im(\beta_1') = Ker(\beta_2')$, segue de imediato de $Im(\beta_1) = Ker(\beta_2)$.

vii. Exatidão de $(\bigstar_4)$ em C_3, ou seja, a sobrejetividade de β_2'. Segue do fato de β_2 ser sobrejetiva.

$\square$

Definição 2.4. Sejam $(A, \mathfrak{M})$ anel local Noetheriano e M A-módulo finitamente gerado. Uma resolução livre de M

$$\cdots \xrightarrow{\alpha_n} F_n \xrightarrow{\alpha_{n-1}} F_{n-1} \to \cdots \to F_1 \xrightarrow{\alpha_0} F_0 \xrightarrow{\alpha} M \to 0$$

é chamada *minimal* se $Im(\alpha_n) \subseteq \mathfrak{M}F_n, \ \forall \ n \in \mathbb{N}$.

Denotando $K_n = Im(\alpha_{n-1})$ para $n \geq 1$, segue que $\mu(F_0) = \mu(M)$ e $\mu(F_n) = \mu(K_n)$ para $n > 0$. De fato, $Im(\alpha_0) \subseteq \mathfrak{M}F_0 \subseteq F_0$ induz a sequência exata $F_0/Im(\alpha_0) \to F_0/\mathfrak{M}F_0 \to 0$, o que implica $\mu(F_0/Im(\alpha_0)) \geq \mu(F_0)$, mas como $Im(\alpha_0) = Ker(\alpha)$, pelo teorema do isomorfismo, $F_0/Im(\alpha_0) \simeq M$, logo $\mu(M) \geq \mu(F_0)$. A desigualdade $\mu(M) \leq \mu(F_0)$ é clara pois α é sobrejetiva. Portanto, $\mu(M) = \mu(F_0)$. Analogamente para $\mu(F_n) = \mu(K_n), \ n > 0$.
Além disso, note que qualquer A-módulo M (nas condições da definição acima) possui resolução livre minimal, basta escolher F_0 tal que $\mu(F_0) = \mu(M)$, assim $K_1 = Ker(\alpha) \subseteq \mathfrak{M}F_0$. Em seguida escolha F_1 tal que $\mu(F_1) = \mu(K_1)$, e assim por diante.

Proposição 2.5. Sejam $(A, \mathfrak{M})$ anel local Noetheriano e M A-módulo finitamente gerado. Dadas duas resoluções livres minimais de M

$$\cdots \to F_n \xrightarrow{\alpha_{n-1}} F_{n-1} \to \cdots \xrightarrow{\alpha_0} F_0 \xrightarrow{\alpha} M \to 0$$

$$\cdots \to F'_n \xrightarrow{\alpha'_{n-1}} F'_{n-1} \to \cdots \xrightarrow{\alpha'_0} F'_0 \xrightarrow{\alpha'} M \to 0$$

tem-se $\mu(F_n) = \mu(F'_n), \ \forall \ n \in \mathbb{N}$.

Demonstração. Procederemos por indução. Temos que $\mu(F_0) = \mu(F'_0) = \mu(M)$. Assim, defina $K_n = Im(\alpha_{n-1})$, $K'_n = Im(\alpha'_{n-1})$ para $n \geq 1$. Pelo Lema de Schanuel,

$$K_n \oplus F'_{n-1} \oplus F_{n-2} \oplus \cdots \simeq K'_n \oplus F_{n-1} \oplus F'_{n-2} \oplus \cdots \ .$$

Supondo que $\mu(F_i) = \mu(F'_i)$ para $i < n$, segue do caso 1 que $\mu(F_n) = \mu(K_n)$ e $\mu(K'_n) = \mu(F'_n)$, e pelo Lema de Schanuel que $\mu(F_n) = \mu(K_n) = \mu(K'_n) = \mu(F'_n)$. $\square$

Os invariantes $\beta_i = \mu(F_i)$ são chamados *números de Betti* do A-módulo M. Por definição, os números de Betti de um anel A são os números de Betti do A-módulo $A/\mathfrak{M}$.

Finalmente, o resultado principal deste trabalho:

A igualdade de Auslander-Buchsbaum. *Sejam* $(A, \mathfrak{M})$ *anel local Noetheriano e* M *A-módulo finitamente gerado. Se* $dh(M) < \infty$, *então*

$$dh(M) + prof(M) = prof(A).$$

A demonstração requer uma certa preparação.
Sejam $0 \to K \to F \to M \to 0$ uma sequência exata com F A-módulo livre e $x \in \mathfrak{M}$. Considere o seguinte diagrama comutativo com linhas e colunas exatas

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & K' & & F' & & M' & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & K & \to & F & \to & M & \to & 0 \\
 & & \downarrow{\scriptstyle \mu_x} & & \downarrow{\scriptstyle \mu_x} & & \downarrow{\scriptstyle \mu_x} & & \\
0 & \to & K & \to & F & \to & M & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & K/xK & & F/xF & & M/xM & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

onde $\mu_x : M \longrightarrow M$ é aplicação A-linear que associa a cada $m \in M$ o elemento $xm \in M$ e $M' = \{m \in M \mid xm = 0\} = Ker(\mu_x)$, a mesma definição é válida para F' e K', ou seja, $F' = Ker(\mu_x)$ em F e $K' = Ker(\mu_x)$ em K. Assim, pelo Lema da Serpente,

$$0 \to K' \to F' \to M' \to K/xK \to F/xF \to M/xM \to 0 \quad (\bigstar_5)$$

é exata.

Nesse contexto, considere os seguintes lemas:

Lema 2.6. Se x é não-divisor de zero de M, então M é livre se, e somente se, M/xM é livre como $A/(x)$-módulo.

Demonstração. Suponha que M seja livre, seja $\{m_1, \ldots, m_r\} \subseteq M$ uma base para M. Afirmamos que $\{m_1 + xM, \ldots, m_r + xM\}$ é base de M/xM como $A/(x)$-módulo. De fato, claramente $\{m_1 + xM, \ldots, m_r + xM\}$ gera M/xM, assim se $(a_1 + (x))(m_1 + xM) + \ldots + (a_r + (x))(m_r + xM) = (0 + xM)$ em M/xM, para $a_i + (x) \in A/(x),\ i = 1, \ldots, r$, então $a_1m_1 + \ldots + a_rm_r = xm$, para algum $m \in M \Rightarrow a_1m_1 + \ldots + a_rm_r = x(b_1m_1 + \ldots b_rm_r)$, para certos $b_i's \in A$, o que implica $(a_1 - b_1x)m_1 + \ldots + (a_rb_rx)m_r = 0 \Rightarrow a_i = b_ix$, pois $m_1, \ldots, m_r$ são linearmente independentes sobre A. Sendo assim, $a_i \in (x) \Rightarrow (a_i + (x)) = (0 + (x)), \forall\ i = 1, \ldots, r$.

Reciprocamente, suponha que M/xM é $A/(x)$-módulo livre. Podemos supor que $\mu(F) = \mu(M)$, basta considermos um conjunto de geradores minimal de M, e associar F ao A-módulo livre A^r, onde r é o número de elementos do tal conjunto minimal. Assim, $F/xF \to M/xM$ é um isomorfismo, pois $\mu(F) = \mu(M)$ e $M/xM,\ F/xF$ são A-módulos livres. Como x é não-divisor de zero de M, temos que $M' = (0)$ o que implica $K/xK = (0)$, pela exatidão de $(\bigstar_5)$, assim $K = xK$, aplicando Lema de Nakayama a K e $(x) \subseteq \mathfrak{M}$ obtemos que $K = 0$ e portanto $M \simeq F$ que é livre. $\square$

Lema 2.7. Se x é não-divisor de zero de A e M, então

$$dh_A(M) = dh_{A/(x)}(M/xM)$$

.

Demonstração. Como x é não-divisor de zero de M, $M' = 0$ e obtemos a seguinte sequência exata $0 \to K/xK \to F/xF \to M/xM \to 0$. Note ainda que $F' = 0$, de fato sendo F livre, existe $m \in \mathbb{N}$ tal que $F \simeq A^m$, mostremos que $F' = 0$: seja $f \in F' \Rightarrow \exists\ (a_1, \ldots, a_m) \in A^m$ elemento correspondente a f, como $xf = 0$ temos que $x(a_1, \ldots, a_m) = 0 \Rightarrow (a_1, \ldots, a_m) = 0$ já que x é não-divisor de zero de A por hipótese, assim $f = 0 \Rightarrow F' = 0$. E sendo $F' = 0$ temos que $K' = (0)$, ou seja, x é não-divisor de zero de K.

Se ambas as dimensões homológicas da igualdade em questão são infinitas, nada a ser mostrado. Se

$dh_A(M) = 0$ então M é livre, logo pelo lema anterior M/xM é livre, sendo assim $dh_{A/(x)}(M/xM) = 0$, analogamente se $dh_{A/(x)}(M/xM) = 0$. Agora suponha $dh_A(M) = m$, com $0 < m < \infty$. Logo, $dh_A(K) = m - 1$, procedendo por indução, podemos supor que $dh_{A/(x)}(K/xK) = dh_A(K)$. E como $dh_{A/(x)}(M/xM) \neq 0$, segue que

$$dh_{A/(x)}(M/xM) \stackrel{*}{=} dh_{A/(x)}(K/xK) + 1 = dh_A(K) + 1 = dh_A(M).$$

A igualdade ($\stackrel{*}{=}$) é justificada pelo fato de x não ser divisor de zero de K, provado anteriormente. Um argumento similar se $dh_{A/(x)}(M/xM) = m$ com $0 < m < \infty$. $\square$

Lema 2.8. Se $prof(A) > 0$. E $prof(M) = 0$, então $prof(K) = 1$

Demonstração. Como $prof(A) > 0$, existe $x \in \mathfrak{M}$ tal que x é não-divisor de zero de A. Neste caso, ($\bigstar_5$) produz a seguinte sequência exata

$$0 \to M' \to K/xK \to F/xF \to M/xM \to 0.$$

pois, sendo F livre, existe $m \in \mathbb{N}$ tal que $F \simeq A^m$, mostremos que $F' = 0$, de fato, seja $f \in F' \Rightarrow \exists\ (a_1, \ldots, a_m) \in A^m$ elemento correspondente a f, como $xf = 0$ temos que $x(a_1, \ldots, a_m) = 0 \Rightarrow (a_1, \ldots, a_m) = 0$ já que x é não-divisor de zero de A, assim $f = 0 \Rightarrow F' = K' = 0$. Sendo $prof(M) = 0$, temos que $\mathfrak{M}$ consiste apenas de divisores livres de M, com isso, pelo corolário 1.28, existe $m \in M \setminus \{0\}$ com $\mathfrak{M}m = 0$. Em particular $xm = 0$, assim, $m \in M'$, o que implica $\mathfrak{M} \in Ass(M')$ pois $\mathfrak{M} = 0 :_A m$, já que $\mathfrak{M}m = 0$ garante $\mathfrak{M} \subseteq 0 :_A m$ e a outra inclusão é garantida pelo fato de A ser anel local, porque se $am = 0,\ a \in A$ então a pertence a algum ideal maximal de A, sendo $\mathfrak{M}$ o único ideal maximal de A, temos $a \in \mathfrak{M}$. Portanto, $\mathfrak{M} \in Ass(K/xK)$ o que implica que $\mathfrak{M}$ consiste apenas de divisores de zero de K/xK, ou seja, $prof(K/xK) = 0$. Como x é não-divisor de zero de K pois $K' = (0)$, temos que $prof(K) = 1$. $\square$

Demonst. (Igualdade de Auslander-Buchsbaum).

Seja $n = dh(M)$ e

$$0 \to F_n \xrightarrow{\alpha_{n-1}} F_{n-1} \to \cdots \xrightarrow{\alpha_0} F_0 \xrightarrow{\alpha} M \to 0 \quad (\bigstar_6)$$

uma resolução livre minimal para M, $K_i = Im(\alpha_{i-1})$ $(i = 1, \ldots, n)$.

Mostremos o resultado por indução em $d = prof(A)$. *Se* $d = 0$ *então existe* $x \in A \setminus \{0\}$ *tal que* $x\mathfrak{M} = 0$. *Se* $n > 0$, *então* $F_n \subseteq \mathfrak{M}F_{n-1}$ *o que implica* $xF_n \subseteq x\mathfrak{M}F_{n-1} = (0)$, *assim* $F_n = 0$, *que é um absurdo. Portanto,* $n = 0$, M *é livre, logo* $M \simeq A^m$ *para algum* $m \in \mathbb{N}$, *o que implica* $prof(M) = prof(A) = 0$.

Agora seja $d > 0$ *e suponha que o resultado é válido para anéis com profundidade menor que* d. *Se* $prof(M) > 0$, *então existe* $x \in \mathfrak{M}$ *tal que* x *é não-divisor de zero de* A *ou* M, *já que* $\mathfrak{M} \nsubseteq \bigcup P$ *sendo* $P \in Ass(A) \cup Ass(M)$. *Assim,* $prof(A/(x)) = d - 1$, $prof(M/xM) = prof(M) - 1$, *pelo lema 2.7,* $dh_{A/(x)}(M/xM) = dh(M)$. *Pela hipótese de indução,* $dh_{A/(x)}(M/xM) + prof(M/xM) = prof(A/(x)) \Rightarrow dh(M) + prof(M) - 1 = d - 1 \Rightarrow dh(M) + prof(M) = d = prof(A)$.

Se $d > 0$ *e* $prof(M) = 0$, *a partir de* ($\bigstar_6$) *considere a sequência exata curta*

$$0 \to K_1 = Im(\alpha_0) = Ker(\alpha) \to F_0 \xrightarrow{\alpha} M \to 0 \ ,$$

então, aplicando o lema 2.8, obtemos que $prof(K_1) = 1$. *Assim, utilizando o resultado do parágrafo anterior para o* A*-módulo* K_1 *(possível pois* $prof(K_1) = 1 > 0$*) obtemos que*

$$dh(K_1) + prof(K_1) = prof(A) \ ,$$

como $dh(K_1) = dh(M) - 1$, *segue que* $dh(M) - 1 + 1 = prof(A) \Rightarrow dh(M) = prof(A)$. □

Vamos agora exibir o resultado no contexto de *anéis regulares.*

Definição 2.5. Seja $A \neq 0$ anel qualquer. Dizemos que A é *graduado* (*a rigor,* $\mathbb{N}$*-graduado)* se existir uma família $\{A_n\}_{n \in \mathbb{N}}$ de subgrupos aditivos $A_n \subseteq A$ satisfazendo:

i. $A = \bigoplus\limits_{n \geqslant 0} A_n$

ii. $A_i A_j \subseteq A_{i+j}, \ \forall i, j \in \mathbb{N}$.

Dizemos que A_n é *a componente homogênea de grau* n *de* A. Cada elemento de A_n é chamado *elemento homogêneo de grau* n.

Definição 2.6. Seja A um anel graduado. Um ideal $I \subseteq A$ é dito *homogêneo* (*ou graduado*) se for gerado por elementos homogêneos. Note que $A_+ = \bigoplus\limits_{n \geqslant 1} A_n$ é ideal homogêneo, chamado de *ideal irrelevante*.

Definição 2.7. Seja A anel. *A dimensão de Krull de A*, ou simplesmente *dimensão de A* é o número

$dim(A) = sup\{n \in \mathbb{N} \mid$ existe cadeia $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n$, com P_i ideais primos, $i = 1, \ldots, n\}$.

Exemplo 2.1. Seja $A = k[x_1, \ldots, x_n]$, anel dos polinômios nas variáveis $x_1, \ldots, x_n$ sobre k corpo. Então, $dim(A) = n$. De fato, mostra-se que $0 \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \ldots \subsetneq (x_1, \ldots, x_n)$ é máxima.

Definição 2.8. Se $(A, \mathfrak{M})$ é um anel Noetheriano local (ou $\mathbb{N}$-graduado *standard*) então A é dito *regular* se $\mu(\mathfrak{M}) = dim(A)$ (resp. $\mu(A_+) = dim(A)$).

Exemplo 2.2. $k[x_1, \ldots, x_n]$ é regular.

É um fato clássico que, se A é regular, qualquer A-módulo M finitamente gerado possui dimensão homológica finita. Neste contexto, com demonstração totalmente análoga, vale:

Teorema 2.9. *Se A é regular e M é finitamente gerado sobre A então*

$$dh(M) + prof(M) = prof(A)$$

Capítulo 3

Aplicação: Derivações logarítmicas

Apresentaremos uma aplicação da igualdade de Auslander-Buchsbaum no contexto de derivações polinomiais logarítmicas e caracterizaremos, em termos de dimensão homológica, quando um dado polinômio é um *divisor livre.*

A partir de agora, salvo menção explícita do contrário, $A = k[x_1, \dots, x_n]$ é o anel dos polinômios nas variáveis $x_1, \dots, x_n$ sobre um corpo k, que é Noetheriano, pelo teorema da base de Hilbert, e local no sentido homogêneo (detalharemos esta afirmação a seguir).

Vamos graduar A com a graduação padrão: $gr(x_i) = 1$ para $i = 1, \dots, n$, onde $gr(-)$ denota grau. Note que $A = k \oplus (x_1, \dots, x_n) \Rightarrow (x_1, \dots, x_n)$ é ideal maximal, já que $k \simeq \frac{k \oplus (x_1,\dots,x_n)}{(x_1,\dots,x_n)}$. Nesse sentido, A é local (homogêneo).

Definição 3.1. Uma *derivação de* A é uma aplicação $d : A \to A$ satisfazendo:

i. $d(f + g) = d(f) + d(g),\ \forall\ f, g \in A$ (aditividade)

ii. $d(fg) = fd(g) + gd(f),\ \forall\ f, g \in A$ (regra de Leibniz)

O conjunto das derivações de A é denotado $Der(A)$. Note que $Der(A)$ possui estrutura natural de A-módulo:

$$\begin{array}{ccc} A \times Der(A) & \longrightarrow & Der(A) \\ (f, d) & \longmapsto & fd \end{array}$$

onde fd é definida por:

$$\begin{array}{rccc} fd: & A & \longrightarrow & A \\ & g & \longmapsto & (fd)(g) = fd(g) \end{array}$$

Desta maneira, podemos definir o conjunto das derivações de A que se anulam em k, explicitamente: $Der_k(A) = \{d \in Der(A) \mid d|_k = 0\} \subseteq Der(A)$, que é claramente A-submódulo de $Der(A)$. Cada elemento de $Der_k(A)$ é chamado *k-derivação de A*.

Note que as derivações parciais usuais do cálculo diferencial são k-derivações de A, além disso, o conjunto formado por tais derivações é uma base para o A-módulo $Der_k(A)$, isto é, toda k-derivação de A se escreve $d = \sum_{i=1}^{n} g_i \frac{\partial}{\partial x_i}$ com cada $g_i \in A$ unicamente determinado. Portanto,

$$Der_k(A) \ = \ \bigoplus_{i=1}^{n} A \frac{\partial}{\partial x_i} \simeq A^n.$$

Definição 3.2. Seja $f \in A$. O A-módulo $T_k(f) = \{d \in Der_k(A) \mid d(f) = gf, \ g \in A\}$ (A-submódulo de $Der_k(A)$) é chamado *idealizador tangencial de f (ou Módulo de Saito de f).*

O caso de nosso interesse é quando $f \in A$ é um *polinômio homogêneo*, isto é, quando todo monômio de f possuir mesmo grau.

Observação 3.1. $T_k(f) \neq 0$. De fato, basta notar que $f.Der_k(A) \subseteq T_k(f)$. Além disso, sendo f homogêneo de grau $d \geq 0$, é válida a *identidade de Euler*

$$x_1 \frac{\partial f}{\partial x_1} + \ldots + x_n \frac{\partial f}{\partial x_n} = fd$$

E assim obtemos a *derivação de Euler (ou derivação radial)*

$$\epsilon = \sum_{i=1}^{n} x_i \frac{\partial}{\partial x_i}$$

que pertence a $T_k(f)$ (devido à relação de Euler).

Observação 3.2. Associado a $f \in A$ de grau $d \geq 0$, temos o *ideal jacobiano* de f

$$J_f = (\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}, f)$$

mas sendo f homogêneo tem-se pela identidade de Euler, $\frac{x_1}{d}\frac{\partial f}{\partial x_1} + \ldots + \frac{x_n}{d}\frac{\partial f}{\partial x_n} = f$, logo, $f \in (\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$. Assim, no caso homogêneo,

$$J_f = (\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})$$

Proposição 3.1. Seja $f \in A$ polinômio homogêneo de grau $d \geq 0$. Então, a sequência

$$0 \to \mathrm{Syz}(J_f) \to T_k(f) \to A\epsilon \to 0 \quad (\bigstar_7)$$

é exata. Sendo $\mathrm{Syz}(J_f) = \{(f_1, \ldots, f_n) \in A^n \mid \sum_{j=1}^{n} f_j \frac{\partial f}{\partial x_j} = 0\}$, que claramente pode ser expresso como $\mathrm{Syz}(J_f) = \{d \in Der_k(A) \mid d(f) = 0\}$.

Demonstração. Mostremos primeiro que $T_k(f) \to A\epsilon \to 0$ é exata. Defina

$$\begin{array}{ccc} T_k(f) & \xrightarrow{\varphi} & A\epsilon \\ d & \longmapsto & g_d\epsilon \end{array}$$

sendo $g_d \in A$ tal que $d(f) = g_d f$

i. φ está bem definida.

De fato, se $d(f) = g_d f$ e $d(f) = g'f$, $g_d, g' \in A$ então $g_d f = g'f$ o que implica que $g_d = g'$ e portanto φ está bem definida.

ii. φ é aplicação A-linear.

De fato, se $d(f) = gf$ e $d'(f) = g'f$, $g, g' \in A$ então $(d + d')(f) = d(f) + d'(f) = gf + g'f = (g + g')f$, assim $\varphi(d + d') = (g + g')\epsilon = g\epsilon + g'\epsilon = \varphi(d) + \varphi(d')$. Agora, seja $h \in A$ então $(hd)(f) = hd(f) = hg_d f$ assim $\varphi(hd) = hg_d\epsilon = h\varphi(d)$. Portanto, φ é aplicação A-linear.

iii. φ é sobrejetiva.

De fato, seja $h\epsilon \in A\epsilon$. Pela identidade de Euler,

$$f = \frac{x_1}{d}\frac{\partial f}{\partial x_1} + \ldots + \frac{x_n}{d}\frac{\partial f}{\partial x_n}.$$

Assim,

$$hf = \frac{x_1 h}{d}\frac{\partial f}{\partial x_1} + \ldots + \frac{x_n h}{d}\frac{\partial f}{\partial x_n}.$$

Então, defina:

$$d_h = \frac{x_1 h}{d}\frac{\partial}{\partial x_1} + \ldots + \frac{x_n h}{d}\frac{\partial}{\partial x_n}.$$

Logo, $d_h(f) = hf$. Portanto, $\varphi(d_h) = h\epsilon$, o que mostra a exatidão de $T_k \to A\epsilon \to 0$.

Agora mostremos que $Ker(\varphi) = \mathrm{Syz}(J_f)$. De fato, $Ker(\varphi) = \{d \in T_k(f) \mid \varphi(d) = 0\epsilon\}$, mas dado $d \in T_k(f)$ existem $h_1, \ldots, h_n \in A$ tais que $d = h_1\frac{\partial}{\partial x_1} + \ldots + hn\frac{\partial}{\partial x_n}$. Assim, identificando d como sendo $d = (h_1, \ldots, h_n)$ temos que $Ker(\varphi) = \{d \in T_k(f) \mid d(f) = 0\} = \{d \in T_k(f) \mid \sum_{i=1}^{n} h_i \frac{\partial f}{\partial x_i} = 0\}$. Assim, $(h_1, \ldots, h_n) \in \mathrm{Syz}(J_f)$, logo $Ker(\varphi) \subseteq \mathrm{Syz}(J_f)$. Mostremos agora a inclusão $\mathrm{Syz}(J_f) \subseteq Ker(\varphi)$, de fato, dado $(h'_1, \ldots, h'_n) \in \mathrm{Syz}(J_f)$ temos que $h'_1\frac{\partial f}{\partial x_1} + \ldots + h'_n\frac{\partial f}{\partial x_n} = 0$. Logo, $(h'_1, \ldots, h'_n) \in Ker(\varphi)$. Assim, $Ker(\varphi) = \mathrm{Syz}(J_f)$. Portanto,

$$0 \to \mathrm{Syz}(J_f) \to T_k(f) \to A\epsilon \to 0$$

é exata. □

Definição 3.3. Sejam A anel qualquer e N, M, T A-módulos. Uma sequência exata $0 \to N \xrightarrow{i} M \xrightarrow{\phi} T \to 0$ é dita *cindida* se existir $\psi : T \to M$ aplicação A-linear tal que $\phi \circ \psi = Id_T$. Neste caso, ψ é chamada *cisão.*

Observação 3.3. Sejam A anel qualquer e M, N, T A-módulos. Se T é livre então toda sequência exata $0 \to N \xrightarrow{i} M \xrightarrow{\phi} T \to 0$ é cindida. De fato, basta definir a cisão como sendo a aplicação A-linear que associa cada elemento da base de T a sua imagem inversa.

Além disso, se $\psi : T \to M$ é cisão, então $M = i(N) \oplus \psi(T)$. De fato $(i(N) \oplus \psi(T))/i(N) \simeq \psi(T)$, por outro lado, pelo Fato 1, $(i(N) \oplus \psi(T))/i(N) \simeq \psi(T)/i(N) \cap \psi(T)$, o que implica $i(N) \cap \psi(T) = \{0\}$.

Como $i(N) \simeq N$ e $\psi(T) \simeq T$, pois ψ é injetiva, já que se $\psi(t) = 0 \Rightarrow \phi \circ \psi(t) = t \Rightarrow \phi(0) = t \Rightarrow t = 0$, segue que $M \simeq N \oplus T$.

Teorema 3.2. *Seja $f \in A$ polinômio homogêneo. Então,*

$$T_k(f) = \mathrm{Syz}(J_f) \oplus A\epsilon$$

Demonstração. Como $A\epsilon$ é livre, temos que ($\bigstar_7$) é cindida. Assim, $T_k(f) = \mathrm{Syz(J_f)} \oplus \psi(A\epsilon)$. Exibindo a cisão:

$$\begin{array}{rccc} \psi: & A\epsilon & \longrightarrow & T_k(f) \\ & h\epsilon & \longmapsto & d_h \end{array}$$

sendo $d_h = \displaystyle\sum_{i=1}^{n} \frac{x_i h}{d} \frac{\partial}{\partial x_i}$.
Claramente $d_h \in T_k(f)$, pois $d_h(f) = hf$. Além disso, $\varphi \circ \psi = I_{A\epsilon}$, de fato, $\varphi(\psi(h\epsilon)) = \varphi(d_h) = h\epsilon$. Finalmente, $Im(\psi) = \psi(A\epsilon) = A\epsilon$. Portanto,

$$T_k(f) = \mathrm{Syz(J_f)} \oplus A\epsilon$$

□

Observação 3.4. Seja $A = k[x_1, \ldots, x_n]$ o anel de polinômios sobre k (corpo). Então $prof(A) = n$. De fato, $\{x_1, \ldots, x_n\}$ é uma sequência regular máxima. Além disso, como A é regular segue que $dh(A)$ é finita.

Teorema 3.3.

$$prof(T_k(f)) = prof(A/J_f) + 2$$

Demonstração. A partir da sequência exata $0 \to \mathrm{Syz}(J_f) \to A^n \to J_f \to 0$ obtemos que $dh(J_f) = dh(\mathrm{Syz}(J_f)) + 1$. Analogamente, a sequência exata $0 \to J_f \to A \to A/J_f \to 0$ nos fornece $dh(A/J_f) = dh(J_f) + 1$. Logo, $dh(A/J_f) = dh(\mathrm{Syz}(J_f)) + 2$. Como $A\epsilon$ é livre, pelo teorema 3.2, temos que $dh(T_k(f)) = dh(\mathrm{Syz}(J_f)) \Rightarrow dh(T_k(f)) = dh(A/J_f) - 2$. Pela igualdade de Auslander-Buchsbaum, $dh(T_k(f)) + prof(T_k(f)) = prof(A) \Rightarrow prof(T_k(f)) = n - dh(A/J_f) + 2$. Mais uma vez pela igualdade de Auslander-Buchsbaum, $dh(A/J_f) + prof(A/J_f) = prof(A) \Rightarrow dh(A/J_f) = prof(A) - prof(A/J_f) \Rightarrow prof(T_k(f)) = n - prof(A) + prof(A/J_f) + 2 = prof(A/J_f) + 2$. □

A fim de caracterizar a liberdade do módulo de Saito, enunciaremos o Teorema de Quillen-Suslin (como resposta afirmativa à famosa Conjectura de Serre).

Definição 3.4. Sejam A um anel qualquer e M A-módulo. M é dito *projetivo* se existe M' A-módulo tal que $M \oplus M'$ é livre.

Teorema de Quillen-Suslin. *Seja $A = k[x_1, \ldots, x_n]$ anel de polinômios sobre k (corpo). Se M é um A-módulo projetivo, então M é livre.*

Definição 3.5. Dizemos que $f \in A$ é um *divisor livre (algébrico)* se o A-módulo $T_k(f)$ é livre.

Teorema 3.4. *Seja $f \in A$ um polinômio homogêneo. Então, f é um divisor livre se, e somente se, $dh(J_f) \leq 1$.*

Demonstração. Pelo teorema 3.2, obtemos a sequência exata curta

$$0 \longrightarrow \mathrm{Syz}(J_f) \longrightarrow T_k(f) \longrightarrow A\,\epsilon \longrightarrow 0$$

Suponha que f é um divisor livre. Logo, $T_k(f)$ livre $\Rightarrow$ $\mathrm{Syz}(J_f)$ é um módulo projetivo, assim pelo Teorema de Quillen-Suslin, obtemos que $\mathrm{Syz}(J_f)$ é livre. Assim,

$$0 \to \mathrm{Syz}(J_f) \to T_k(f) \to J_f \to 0$$

é uma resolução livre para J_f e portanto $dh(J_f) \leq 1$.
Reciprocamente, se $dh(J_f) \leq 1$ então, da sequência exata

$$0 \longrightarrow \mathrm{Syz}(J_f) \longrightarrow A^n \longrightarrow J_f \longrightarrow 0$$

segue que $\mathrm{Syz}(J_f)$ é livre $\Rightarrow$ $T_k(f)$ é livre, ou seja, f é divisor livre. □

Exemplo 3.1.

i. O polinômio $f = x^3 + y^3 + z^3 - 3xyz \in \mathbb{C}[x, y, z]$ é um divisor livre. De fato, neste caso tem-se

$$J_f \;=\; (3x^2 - 3yz,\; 3y^2 - 3xz,\; 3z^2 - 3xy),$$

e utilizando o programa de computação algébrica Macaulay para o cálculo da dimensão homológica do ideal jacobiano, obtemos que $dh(J_f) = 1$.

ii. O polinômio $f = 8xy^3 + 9x^2w^2 - 18xyzw - 3y^2z^2 + 6z^3w \in \mathbb{Q}[x, y, z, w]$ é um divisor livre, por cálculos similares aos do exemplo anterior.

Referências Bibliográficas

[AA] SIMIS, A., ANDRADE, J. F., *Tópicos de Álgebra Comutativa.* IMPA, Minas Gerais, 1981.

[A] ATIYAH, M. F., MACDONALD, I. G., *Introduction to Commutative Algebra.* Addison - Wesley Publishing Company, Inc., Reading, Massachusets, 1969.

[B] BAYER, D., STILLMAN M., *Macaulay*: A system for computation in algebraic geometry and commutative algebra. 1992. Available via anonymous ftp from `math.harvard.edu`.

[G] GONCALVES, A., *Introdução à Álgebra.* IMPA, 5ª Ed., Rio de Janeiro, 2007.

[K] KUNZ, E., *Introduction to Commutative Algebra and Algebraic Geometry.* Birkhäuser, 1985.

[L] LANG, S., *Estruturas Algébricas.* Ed. LTC, Rio de Janeiro, 1999.

[MN] MIRANDA NETO, C. B., *Notas de Aula de Álgebra Comutativa.* Paraíba, 2010.

[MN2] MIRANDA NETO, C., B., *Teoria dos módulos idealizadores diferenciais*, Tese de Doutorado (Orientador: Prof. A. Simis), Departamento de Matemática, UFPE, 2006.

[MN3] MIRANDA NETO, C., B., Vector fields and a family of linear type modules related to free divisors, J. Pure Appl. Algebra 215 (2011), 2652–2659.

[S] SAITO, K., Theory of logarithmic differential forms and logarithmic vector fields, J. Fac. Sci. Univ. Tokyo Sect. 1A Math. 27 (1980), 265–291.