ENDOMORFISMO INJETIVO E SOBREJETIVO
DE MÓDULOS FINITAMENTE GERADOS

JOSÉ VERGILIO BETIOLI

ORIENTADOR
PROF. DR. HU SHENG

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação da Universidade Estadual de Campinas como requisito parcial para obtenção do título de Mestre em Matemática.

Este trabalho foi realizado com o auxílio financeiro do Conselho Nacional de Pesquisas (CNPq).

Fevereiro de 1978

À Eliana

Agradeço:

Ao Prof. Dr. Hu Sheng pela proposta do presente trabalho, por sua atenção e disponibilidade, e segura orientação na elaboração do mesmo.

Aos meus amigos e professores por seus estímulos e ensinamentos.

Ao CNPq, que, com seu apoio financeiro, possibilitou a realização deste trabalho.

ENDOMORFISMO INJETIVO E SOBREJETIVO DE MÓDULOS FINITAMENTE GERADOS

N O T A Ç Õ E S

N	- Conjunto dos números naturais
Q	- Corpo dos números racionais
A.C.C.	- Condição de cadeia ascendente
D.C.C.	- Condição de cadeia descendente
f.g.	- Finitamente gerado
s.m.	- Sistema multiplicativo
(x) ou $\langle x \rangle$	- Ideal gerado por x

INTRODUÇÃO

Neste trabalno, que apresentamos, nosso principal objetivo é demonstrar qual a condição necessária e suficiente para que um endomorfismo injetivo ou sobrejetivo de um A-módulo seja um isomorfismo. [6,7]

O enfoque deste trabalho é o teorema 3.6 " Um endomorfismo injetivo de um A-módulo finitamente gerado é um isomorfismo se, e sòmente se o anel A é de dimensão zero".

Sintetizando, no primeiro capítulo colocamos definições e alguns resultados básicos sobre ideais primos, condição de cadeia, módulos finitamente gerados e anéis locais.

A chave para abrir a porta da demonstração do resultado principal é que, se f é um endomorfismo de um A-módulo M, podemos definir em M uma estrutura de A[X]-módulo por x.m = f(m) para todo m em M.

A maioria dos resultados são apresentados sem demonstração mas estas podem ser encontradas na bibliografia aqui citada.

No segundo capítulo desenvolvemos alguns aspectos da teoria de anel de dimensão zero, isto é , um anel onde todo ideal primo é maximal; Um fato interessante é a existência de divisores de zero no anel de dimensão zero (teorema 2.4). E a principal ferramenta a ser utilizada na demonstração do teorema 3.6 é que, se M é um A-módulo finitamente gerado, M é A[X]-módulo e se I é o anulador de M em A[x] então a dimensão de A[x]/I é zero quando a dimensão de A é zero.

O terceiro e último capítulo iniciamos examinando alguns casos clássicos: Se M é um A-módulo que satisfaz D.C.C. (A.C.C.) então o endomorfismo injetivo (sobrejetivo) é um isomorfismo; E obtemos um melhor resultado enfraquecendo a hipótese acima substituindo a condição A.C.C. sobre M por M finitamente gerado.

Através de um exemplo mostramos a necessidade do anel - ser comutativo e, finalmente, concluimos o trabalho, tendo o resultado que nos propusemos a demonstrar.

C A P Í T U L O I

Todos anéis considerados são comutativos com identidade, todo módulo é unitário e qualquer terminologia que não for explícita no texto poderá ser encontrada na bibliografia [1, 2 e 4] .

Neste capítulo serão colocadas definições e algumas demonstrações de propriedades que serão utilizadas nos capítulos seguintes.

§ 1 IDEAIS PRIMOS

1.1.1 - Definições e propriedades

Sejam A um anel, I um ideal de A, A/I o anel quociente e $\emptyset$ o homomorfismo de A em A/I definido por $\emptyset(x) = x + I = \overline{x}$.

<u>Proposição 1.1</u> [1]

Existe uma correspondência biunívoca que preserva ordem entre os ideais b de A que contém I e os ideais $\overline{b} = \{ \overline{x} \mid x \in b \}$ de A/I dados por $b = \emptyset^{-1}(\overline{b}) = \{ x \mid \emptyset(x) \in \overline{b} \}$.

<u>Definição</u>: Seja A um anel, um ideal p de A é <u>Primo</u> se $p \neq A$ e se $x.y \in p$ implicar que $x \in p$ ou $y \in p$.

Observações:

1- Seja f um homomorfismo do anel A no anel B, se q é ideal primo de B então $f^{-1}(q)$ é ideal primo de A.

2- Com as hipóteses da Proposição 1.1, se p é ideal primo de A então $\emptyset(p) = \overline{p}$ é ideal primo de A/I .

3- Das observações acima concluimos que a Proposição 1.1 é válida para ideais primos.

<u>Definição:</u> Sejam f um homomorfismo do anel A no anel B e b um ideal de B; O ideal $f^{-1}(b)$ de A é chamado <u>Contração de b</u> .

<u>Definição:</u> Um subconjunto não vazio S de um anel A é um <u>Sistema Multiplicativo de A</u> (s.m.) se: $1 \in S$ e se $s_1, s_2 \in S$ então $s_1 . s_2 \in S$.

Observação:

4- Se p é um ideal primo de A então A-p é um s.m. de A. Se S= A-I é um s.m. de A e se I é ideal de A então I é ideal primo de A.

1.1.2 - Teorema de Krull

A partir de um sistema multiplicativo de um anel A é sempre possível construir um ideal primo de A; Este importante resultado, que vamos demonstrar, é o Teorema de Krull [4] .

<u>Teorema 1.2</u> Dado um s.m. S do anel A, se I é um ideal de A que é maximal com respeito a exclusão de S então I é primo.

<u>Demonstração:</u> Se $a.b \in I$ vamos provar que $a \in I$ ou $b \in I$.
Suponhamos, por absurdo, que $a \notin I$ e $b \notin I$ então $I \subsetneq (a, I)$: ideal gerado por a e I e $I \subsetneq (b, I)$: ideal gerado por b e I ; Agora co

mo qualquer ideal de A que contém propriamente I intercepta S temos que $\exists$ $s \in S \cap \langle a,I \rangle$ com $s = i + xa$ onde $i \in I$ e $x \in A$ e $\exists$ $t \in S \cap \langle b,I \rangle$ com $t = j + yb$ onde $j \in I$ e $y \in A$ como S é sistema multiplicativo de A implica que $s.t \in S$, mas $s.t = i.j + i.yb + j.xa + xyab \in I$ e isto é absurdo pois $I \cap S = \emptyset$. O que completa a demonstração.

1.1.3 - Ideais em anéis de polinômios

Sejam A um anel, x uma indeterminada, $A[x]$ o anel de polinômios e i o homomorfismo inclusão de A em $A[x]$.

São as seguintes as relações entre ideais primos de A e de $A[x]$:

Lema 1.3

1- Se p é ideal primo de A então $p.A[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in p\}$ é ideal primo de $A[x]$.

2- Se q é ideal primo de $A[x]$ então a contração de q $i^{-1}(q)$ é igual a $q \cap A$ e é um ideal primo de A.

Demonstração(1)Sejam $f = a_0 + a_1x + \dots + a_nx^n \in A[x]$ e $g = b_0 + b_1x + \dots + b_mx^m \in A[x]$ com $f.g \in p.A[x]$, $f \notin p.A[x]$ e $g \notin p.A[x]$ então existem coeficientes a_{i_0} e b_{j_0} (estes com menores índices) respectivamente de f e g tais que $a_{i_0} \notin p$ e $b_{j_0} \notin p$, mas então o coeficiente do termo de grau $i_0 + j_0$ de $f.g$ não pertence a p contradição, Logo $p.A[x]$ é ideal primo de $A[x]$.

Demonstração (2) $i^{-1}(q)$ é ideal primo de A; Vamos provar a igual=

dade, se $x \in i^{-1}(q)$ então $x \in A$ e $i(x) = x \in q$ que implica em $x \in q \cap A$ portanto $i^{-1}(q) \subset q \cap A$. Se $x \in q \cap A$ então $x \in A$ e $i(x) = x \in q$ logo $x \in i^{-1}(q)$ portanto $q \cap A \subset i^{-1}(q)$. O que completa a demonstração.

Observação:

5- Existe uma correspondência biunívoca que preserva ordem entre ideais primos de A e de $A[x]$.

1.1.4 - Ideal maximal e propriedades

Definição: Um ideal m do anel A é Maximal se $m \neq A$ e não existe ideal próprio de A que o contenha.

Vamos garantir a existência de ideais maximais num anel, este resultado pode ser demonstrado utilizando o Lema de Zorn.

Teorema 1.4 [1, pag. 3]

Todo anel não nulo possui ao menos um ideal maximal.

Dado o ideal $I \neq A$, o anel A/I é não nulo e pelo teorema 1.4 existe $\bar{m}$ ideal maximal de A/I e aplicando a proposição 1.1 temos o seguinte resultado:

Corolário 1.5 Se $I \neq A$ é um ideal do anel A então existe um ideal maximal de A que contém I.

É claro que se r não é unidade de A então $r.A$ é um ideal próprio de A e assim temos o seguinte resultado:

Corolário 1.6 Se r não é unidade de A então $r \in m$, m ideal maximal de A.

§ 2 CONDIÇÃO DE CADEIA E MÓDULOS FINITAMENTE GERADOS

1.2.1 - Definiçoẽs e propriedades

Definição: Um A-módulo M que satisfaz a Condição de Cadeia Descendente (D.C.C.), isto é, para cada cadeia de submódulos de M - $M \supseteq M_1 \supseteq M_2 \supseteq \ldots$ existe $n \in N$ tal que $M_n = M_{n+1} = \ldots$, é chamado ~~A~~-módulo Artiniano.

Definição: Um A-módulo M que satisfaz a Condição de Cadeia Ascendente (A.C.C.), isto é, para cada cadeia de submódulos de M - $M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots$ existe $n \in N$ tal que $M_n = M_{n+1} = \ldots$, é chamado A-módulo Noetheriano.

Definição: Um A-módulo M é Finitamente Gerado (f.g) se existem $m_1, m_2, \ldots, m_n$ elementos de M tal que $M = Am_1 + Am_2 + \ldots + Am_n$.

Observação:

6- Todo submódulo de M é f.g. se e sòmente se M é Noetheriano. [1]

Para que um módulo f.g. seja Noetheriano (ou Artiniano) basta que o anel de escalares o seja; Este é o resultado que vamos enunciar e que será utilizado posteriormente.

Proposição 1.7 [1, pag.76]

Se A é um anel Noetheriano (resp. Artiniano) e M é um A-módulo f.g. então M é um A-módulo Noetheriano (resp. Artiniano).

1.2.2 - A-módulo com estrutura de $A[x]$-módulo

Sejam M um A-módulo e f um endomorfismo de M e definimos $xm = f(m)$ para todo $m \in M$; Se definirmos $\cdot : A[x] \times M \longrightarrow M$ por: $(a_0 + a_1x + \ldots + a_nx^n).m = a_0m + a_1xm + \ldots + a_nx^nm$ para todo $a_i \in A$ e $m \in M$, como $x^km = x^{k-1}(xm) = x^{k-1}f(m) = \ldots = f^k(m)$ e $f^k(m) \in M$ é fácil ver que esta multiplicação por escalar define em M uma estrutura de $A[x]$-módulo.

Lema 1.8 Com as hipóteses acima, se f é sobrejetivo então $xM = M$.
Demonstração: Como f é sobrejetivo $\forall$ $m \in M$, $\exists$ $m' \in M$ tal que $f(m') = m$, mas $f(m') = xm'$ portanto $m = xm' \in xM$ logo $M \subset xM$ e $xM \subset M$ por definição; Assim $xM = M$.

Definição: Seja M um A-módulo
$m \in M$, $Ann_A(m) = \{ a \in A \mid am = 0 \}$ é chamado Anulador de m.
$Ann_A(M) = \{ a \in A \mid aM = 0 \}$ é chamado Anulador de M.

Observação:
7- $Ann_A(m)$ e $Ann_A(M)$ são ideais de A.

Para a demonstração do resultado que vamos enunciar usaremos alguns fatos elementares da teoria dos determinantes; Este resultado é uma das ferramentas a serem utilizadas posteriormente.

Proposição 1.9 Sejam M um A-módulo finitamente gerado, x uma indeterminada e f um endomorfismo de M, M é um $A[x]$-módulo onde $xm = f(m)$ $\forall$ $m \in M$, então $Ann_{A[x]}(M) \neq \{ 0 \}$.

<u>Demonstração</u>: Como M é um A-módulo f.g., claramente M é um $A[x]$-módulo f.g. (gerado pelos mesmos elementos).

Seja (x) o ideal de $A[x]$ gerado por x e suponhamos que M seja gerado por $m_1, m_2, \dots, m_n$ como $f(M) \subset M$ temos que $f(m_i) = xm_i \ \forall i$, $1 \leq i \leq n$

Assim $xm_i = \sum_{j=1}^{n} a_{ij} m_j$, $a_{ij} \in A$ $1 \leq i,j \leq n$

portanto (*) $\sum_{j=1}^{n} (a_{ij} - \delta_{ij} x) m_j = 0$ onde $\delta_{ij} = \begin{cases} 1 \text{ se } i=j \\ 0 \text{ se } i \neq j \end{cases}$,

e $1 \leq i \leq n$. Tomemos a matriz de coeficientes

$$H = \begin{bmatrix} a_{11}-x & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22}-x & a_{23} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn}-x \end{bmatrix}$$

e multipliquemos as linhas do sistema (*) respectivamente por A_{1k}, A_{2k}, $\dots$, A_{nk} onde A_{ik} são os cofatores de H

Assim obtemos:

$$\sum_{j=1}^{n} (a_{1j} - \delta_{1j} x) A_{1k} m_j = 0$$

$$\sum_{j=1}^{n} (a_{2j} - \delta_{2j} x) A_{2k} m_j = 0$$

$$\vdots$$

$$\sum_{j=1}^{n} (a_{nj} - \delta_{nj} x) A_{nk} m_j = 0$$

Adicionando vem : $\sum_{i=1}^{n} \sum_{j=1}^{n} (a_{ij} - \delta_{ij} x) A_{ik} m_j = 0$ $\quad k \in \{1,2,\dots,n\}$

Mas $\sum_{i=1}^{n} (a_{ik} - \delta_{ik} x) A_{ik} = \operatorname{Det} H$ [3]

e as outras parcelas são " somas dos produtos dos elementos de uma coluna, ordenadamente, pelos cofatores dos elementos de outra coluna " portanto todas iguais a zero; Assim Det $H.m_k = 0$ $k \in \{1,2,\ldots,n\}$ mas Det $H = (-1)^n x^n + a_1 x^{n-1} + \ldots + a_n$, onde $a_i \in A$,isto é, um polinômio não nulo.

Portanto $Ann_{A[x]}(M) \neq \{0\}$

Posteriormente vamos recorrer a este polinômio não nulo , e portanto vamos denotá-lo por $p(x)$; isto é, $p(x) =$ Det H.

Lema 1.10 - Sejam M um A-módulo f.g., f um endomorfismo sobrejetivo de M, M é um A[x]-módulo, e $I = (x)$ então existe $g \in I$ tal que $(1+g)M = 0$.

Demonstração:

Pelo Lema 1.8 $IM = M$ e suponhamos M gerado por $m_1, m_2, \ldots, m_n$ assim $m_i = \sum_{j=1}^{n} g_{ij} m_j$ onde $g_{ij} \in I$ $\forall i$

portanto $\sum_{j=1}^{n} (g_{ij}-1) m_j = 0$

E como na demonstração da Proposição 1.9 Det $H.M = 0$, mas Det $H = 1 + g$, $g \in I$.

§3 ANEL DE FRAÇOÊS E LOCAL

1.3.1 - Definiçoês e propriedades

Sejam A um anel comutativo com identidade e S um s.m. de A.

<u>Definição</u>: O <u>Anel de Fraçoês de A por S</u> é o conjunto $S^{-1}A = \left\{ \frac{a}{s} \mid a \in A,\ s \in S \right\}$ com as operaçoês: $\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$ e $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$ onde $\frac{a}{s} = \frac{b}{t}$ se e sòmente se $\exists\, s' \in S \mid s'(at - bs) = 0$.

$(S^{-1}A, +, .)$ é um anel comutativo com identidade [2] .

Os detalhes sobre o anel de fraçoês podem ser encontrados em [1] ou [2].

Observaçoês:

8- Se p é ideal primo de A então S = A-p é s.m. de A e ao inves de escrever $S^{-1}A$ escrevemos A_p.

9- Seja A um domínio e $S = A - \{0\}$ então $S^{-1}A = K = q.f(A)$: <u>corpo de fraçoês de A</u> e $S^{-1}A[x] \cong K[x]$.

<u>Definição</u>: <u>Anel Local</u> é um anel com um único ideal maximal.

<u>Lema 1.11</u> Se p é um ideal primo de A então o anel A_p é local.

<u>Demonstração</u>: $pA_p = \left\{ \frac{a}{s} \mid a \in p \text{ e } s \notin p \right\}$ é o único ideal maximal de A_p. De fato: Que pA_p é ideal de A_p é claro; Agora qualquer elemento de A_p que não pertence a pA_p é uma unidade de A_p o que completa a demonstração.

Observação:

10- (A, m) Anel Local então $a \in m$ se e sòmente se a não é uma uni -

dade de A.

Lema 1.12 [1]

Sejam A um anel e S um s.m. de A; Os ideais primos de $S^{-1}A$ estão em correspondência biunívoca com os ideais primos de A que não interceptam S.

1.3.2 - Relação entre ideais de A e de A[x]

Vamos analizar agora qual é a relação que existe entre os ideais de um anel A e os ideais do anel de polinômios A[x] .[4]

Lema 1.13 Sejam A um domínio com corpo quociente K e x uma indeterminada; Então existe uma correspondência biunívoca entre ideais primos de A[x] que contraem à zero em A e os ideais primos em K[x].

Demonstração: Seja $S = A-\{0\}$ então $S^{-1}A = K$ e $S^{-1}A[x] \cong K[x]$ e o resultado segue aplicando o Lema 1.11.

Lema 1.14 Sejam A um anel e x uma indeterminada; Não existe em A[x] uma cadeia de três ideais primos distintos com a mesma contração em A.

Demonstração: Suponhamos que exista em A[x] uma cadeia de ideais primos $pA[x] = q \subsetneqq q_1 \subsetneqq q_2$ com a mesma contração p em A. Agora A/p é domínio, então seja $S = A/p - \{\overline{0}\}$ e assim $S^{-1}(A/p) = q.f(A/p) = K$;

Observando o diagrama:

$$\begin{tikzcd}
A/p \arrow[rr] & & A/p[x] \\
 & & \bar{q}_2 \arrow[dll] \\
0 & & \rotatebox{90}{$\subsetneq$} \\
 & & \bar{q}_1 \arrow[ull] \\
 & & \rotatebox{90}{$\subsetneq$} \\
 & & \bar{0} \arrow[uuull]
\end{tikzcd}$$

Temos $\bar{q}_1 \subsetneq \bar{q}_2$ uma cadeia de ideais primos de $A/p[x]$ que contraem a zero em A/p, pelo Lema 1.12 existe uma correspondência biunívoca entre esses ideais e ideais de $K[x]$ e pela observação 5 - existe correspondência biunívoca que preserva ordem entre ideais primos de K e de $K[x]$, mas K é corpo portanto contradição (pois seus únicos ideais são (O) e K). O que demonstra o Lema.

CAPÍTULO II

ANEL DE DIMENSÃO ZERO

2.1 - Definiçoẽs e propriedades

Neste capítulo apresentamos alguns aspectos da teoria dos anéis de dimensão zero [4] e com os resultados que aquí vamos apresentar pretendemos fazer uma demonstração clara do principal resultado do nosso trabalho.

Definição: O comprimento de uma cadeia de ideais primos de úm anel A é n se : $p_0 \subsetneqq p_1 \subsetneqq p_2 \subsetneqq \cdots \subsetneqq p_n$, n finito e p_i: ideais primos de A.

Definição: A Dimensão de Krull do anel A , que vamos denotar por Dim A , é o supremo dos comprimentos das cadeias de ideais primos em A.

A dimensão de um anel não nulo é um inteiro não negativo ou infinita.

Observaçoẽs:

1- Dim A = O se e sòmente se todo ideal primo de A é maximal.

2- Dim A = O e A é um domínio então A é um corpo.

O anel quociente de um anel de dimensão zero é ainda um anel de dimensão zero; É o que contém o seguinte resultado:

Lema 2.1 Sejam A um anel de dimensão zero e I um ideal de A então A/I é anel de dimensão zero.

Demonstração: Suponhamos $\overline{p}_1 \subseteq \overline{p}_2$ ideais primos de A/I e $\varnothing: A \longrightarrow A/I$ o homomorfismo canônico, então $\varnothing^{-1}(\overline{p}_1) = p_1$ e $\varnothing^{-1}(\overline{p}_2) = p_2$ são ideais primos de A; Agora pela Proposição 1.1 $\overline{p}_1 \subsetneq \overline{p}_2$ implica $p_1 \subsetneq p_2$, mas como Dim A = 0 temos necessàriamente que $\overline{p}_1 = \overline{p}_2$ e portanto Dim (A/I) = 0.

Lema 2.2 Sejam A um anel de dimensão zero e q um ideal primo de A então o anel A_q é de dimensão zero.

Demonstração: É feita de maneira análoga a anterior aplicando o Lema 1.12.

Proposição 2.3 Seja A um anel local de dimensão zero então toda não unidade de A é nilpotente.

Demonstração: Se $r \in A$ não é nilpotente então $S = \{1, r, r^2, \ldots \}$ é um s.m. de A. Tomemos $C = \{ I \text{ ideal de } A \text{ tal que } I \cap S = \varnothing \}$ $C \neq \varnothing$ pois $(0) \in C$.

Definimos $I \geqslant J$ se e sòmente se $J \subseteq I$. Assim $(C, \geqslant)$ e um conjunto parcialmente ordenado e se $I_1 \subset I_2 \subset I_3 \subset \ldots$ é uma cadeia de ideais de C então $\bigcup I_i$ é seu majorante; Assim pelo Lema de Zorn existe p elemento maximal de C e pelo Teorema 1.2 p é ideal primo de A, mas como Dim A = 0 e A é Local implica que p é único ideal maximal e como r não é unidade de A $r \in p$ (corolário 1.6) que é absurdo. Logo r é nilpotente.

<u>Teorema 2.4</u> Seja A um anel de dimensão zero e se r não é unidade de A então $Ann_A(r) \neq \{0\}$.

<u>Demonstração</u>: Será feita considerando dois casos:

1º caso - A é anel local

Pela Proposição 2.3 r é nilpotente, isto é, existe n menor inteiro positivo tal que $r^n = 0$, então $r^{n-1}.r = 0$ e $r^{n-1} \neq 0$ assim $r^{n-1} \in Ann_A(r)$ e portanto $Ann_A(r) \neq \{0\}$.

2º caso - A não é anel local

Como r não é unidade de A pelo Corolário 1.6 existe q ideal maximal de A tal que $r \in q$; Agora A_q é local (lema 1.11) e Dim $A_q = 0$ (lema 2.2), $qA_q = \left\{ \frac{a}{s} \mid a \in q \text{ e } s \notin q \right\}$ é o ideal maximal de A_q e $r/1 \in qA_q$ pois $r \in q$ logo $r/1$ não é unidade de A_q e pela Proposição 2.3 $r/1$ é nilpotente, isto é, existe n menor inteiro positivo tal que $(r/1)^n = 0$ mas $0 = (r/1)^n = r^n/1$ então, por definição, existe $s \in A-q$ tal que $s.r^n = 0$ que implica $(s.r^{n-1}).r = 0$ onde $s.r^{n-1} \neq 0$, pois $(r/1)^{n-1} \neq 0$, e assim $s.r^{n-1} \in Ann_A(r)$ e portanto $Ann_A(r) \neq \{0\}$.

Sejam A um anel, M um A-módulo f.g., $f: M \longrightarrow M$ um endomorfismo, M é um $A[x]$-módulo onde $x.m = f(m)$ para todo m em M e $I = \mathrm{Ann}_{A[x]}(M)$ é um ideal não nulo de $A[x]$ (Proposição 1.9) .

O resultado que agora vamos demonstrar é a principal ferramenta a ser utilizada na demonstração do Teorema 3.6 .

<u>Teorema 2.5</u> Com as mesmas notações acima se $\mathrm{Dim}\, A = 0$ então $\mathrm{Dim}\,(A[x]/I) = 0$

<u>Demonstração</u>: Na demonstração da Proposição 1.9 existe um polinômio não nulo $p(x) \in I$; Afirmamos que $A[x]/J$ é zero-dimensional onde $J = (p(x))$:

Pois se $\overline{p}_2 \subsetneqq \overline{p}_1$ são ideais primos de $A[x]/J$ e $\emptyset: A[x] \longrightarrow A[x]/J$ é o homomorfismo canônico então $p_i = \emptyset^{-1}(\overline{p}_i)$ $i = 1,2$ são ideais primos de $A[x]$ e $p_2 \subsetneqq p_1$.

Pelo Lema 1.3 $p_1^* = p_1 \cap A$ e $p_2^* = p_2 \cap A$ são ideais primos de A e como $\mathrm{Dim}\, A = 0$ temos que $p_1^* = p_2^*$.

Agora $p_1^* A[x] = p_2^* A[x] \subset p_2$ e $p_2^* A[x] \neq p_2$ pois $p(x) \in p_2$ e $p(x) \notin p_2^* A[x]$ $(1 \notin p_2^*)$.

$$\begin{array}{ccccc}
A & \longrightarrow & A[x] & \xrightarrow{\emptyset} & A[x]/J \\
p_1^* & \longleftarrow & p_1 & \longleftarrow & \overline{p}_1 \\
 & & \cup & & \cup \\
p_2^* & \longleftarrow & p_2 & \longleftarrow & \overline{p}_2 \\
 & \nwarrow & \cup & & \\
 & & p_2^* A[x] & & \\
 & & \cup & & \\
 & & (p(x)) & &
\end{array}$$

Como pelo Lema 1.14 não existe cadeia de três ou mais -

ideais primos distintos em $A[x]$ ($p_1 \supset p_2 \supsetneq p_2^* A[x]$) com a mesma contração em A, temos portanto um absurdo se $p_1 \neq p_2$ e assim necessàriamente $\overline{p}_2 = \overline{p}_1$, o que prova que $\mathrm{Dim}\ (A[x]/ J) = 0$. Como I/J é um ideal de $A[x]/J$ então $\mathrm{Dim}\ (A[x]/J)/(I/J) = 0$ (Lema 2.1) mas pelo 1º Teorema do isomorfismo -

$\mathrm{Dim}\ (A[x]/J)/(I/J) = \mathrm{Dim}\ (A[x]/I)$ e portanto $\mathrm{Dim}\ (A[x]/I)=0$.

CAPÍTULO III

ENDOMORFISMO INJETIVO E SOBREJETIVO DE MÓDULOS FINITAMENTE GERADOS

3.1 - Casos clássicos

Vamos examinar agora quando um endomorfismo injetivo ou sobrejetivo de um A-módulo é um isomorfismo; Começamos com o seguinte caso clássico:

Teorema 3.1 Se M é um A-módulo Artiniano e f é um endomorfismo injetivo em M então f é um isomorfismo.

Demonstração: Basta provarmos que $M = f(M)$

Definimos $f^k(M) = \{ f^k(m) \in M \ / \ f^k(m) = \underbrace{f \circ f \circ f \circ \ldots \circ f}_{k\text{-vezes}}(m) \text{ e } m \in M \}$

$f^k(M) \neq \emptyset$ pois $0 \in f^k(M)$, $f^k(M)$ é claramente um submódulo de M para cada $k \in N$ e $f^k(M) \subseteq f^{k-1}(M)$, Assim $M \supseteq f(M) \supseteq f^2(M) \supseteq f^3(M) \supseteq \ldots$ é uma cadeia decendente de submódulos de M e como M é Artiniano $\exists$ $n \in N$ tal que $f^n(M) = f^{n+1}(M) = \ldots$; Mas $f^n(M) = f^n[f(M)]$ e como f^n é injetivo (pois f é injetivo) temos que $M = f(M)$.

Corolário 3.2 Sejam A um Anel Artiniano e M um A-módulo f.g. se f é um endomorfismo injetivo em M então f é um isomorfismo.

Demonstração: Da Proposião 1.7 segue que M é um A-módulo Artiniano e portanto o resultado segue do Teorema 3.1.

Agora vamos demonstrar um resultado dual do Teorema 3.1.

Teorema 3.3 Se M é um A-módulo Noetheriano e f é um endomorfismo sobrejetivo em M então f é um isomorfismo.

Demonstração: Basta provarmos que f é injetivo

Consideremos $N_k = \{ x \in M \ / \ f^k(x) = 0 \}$ para $k \in \mathbb{N}$; Claramente N_k é submódulo de M e $N_k \subseteq N_{k+1}$ para todo $k \in \mathbb{N}$. Desta forma $N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots$ é uma cadeia ascendente de submódulos de M, como M é Noetheriano $\exists\, n \in \mathbb{N}$ tal que $N_n = N_{n+1}$, Assim se $f(m) = 0$ então $m \in N_1 \subseteq N_n$ e $\exists\, m' \in M$ tal que $f^n(m') = m$, pois f^n é sobrejetivo.

Agora $0 = f(m) = f[f^n(m')] = f^{n+1}(m')$ e então $m' \in N_{n+1} = N_n$

logo $m = f^n(m') = 0$.

Corolário 3.4 Sejam A um anel Noetheriano e M um A-módulo f.g. Se f é um endomorfismo sobrejetivo de M então f é um isomorfismo.

Demonstração: Da Proposição 1.7 segue que M é um A-módulo Noetheriano e o resultado segue do Teorema 3.3.

Vamos procurar enfraquecer a condição " M ser Noetheriano " no Teorema 3.3, de modo que este ainda se verifique, esta condição é a de M ser finitamente gerado.

Teorema 3.5 Se M é um A-módulo f.g. e f é um endomorfismo sobrejetivo em M então f é um isomorfismo.

Demonstração: Basta provarmos que f é injetivo

Do Lema 1.8 segue que M é um $A[x]$-módulo e $xM = M$; Consideremos $I = (x)$: o ideal de $A[x]$ gerado por x, assim $IM = M$ e pelo Lema 1.10 $\exists\, g \in I$ tal que $(1+g)M = 0$, por outro lado, podemos escrever $g = g'x$ com $g' \in A[x]$ e então $(1+g'x)m = 0$ para todo $m \in M$ assim (I) $m + g'xm = 0$, Portanto se $f(m) = 0$ como $xm = f(m)$ - (definição) da equação (1) segue que $m = 0$. O que prova que f é injetivo.

O seguinte exemplo mostra que se retirarmos a comutatividade do anel A o Teorema 3.5 não mais se verifica.

Exemplo:

Seja V: espaço vetorial sobre Q, $\mathrm{Dim}_Q V = \infty$ e $\{v_i\}_{i \in N}$ base de V então $A = \mathrm{Hom}_Q(V,V)$ é um anel não comutativo e - $V \oplus V \cong V$ [5, pag. 35].

Assim $A \oplus A \cong A$ [5, pag. 32].

Tomemos $M = A \oplus A$ então M é um A-módulo finitamente gerado (gerado por $(1,0)$ e $(0,1)$) e definimos $f: M \longrightarrow M$ por $f(r,0) = 0$ e $f(0,s) = \theta(s)$ onde $r, s \in A$.

É claro que f é um endomorfismo sobrejetivo mas não injetivo.

3.2 - Teorema 3.6

Teorema 3.6 Seja A um anel comutativo com identidade, um endomorfismo injetivo de um A-módulo f.g. é um isomorfismo se e sòmente se A é um anel de dimensão zero.

Demonstração: Seja p um ideal primo de A então pelo corolário 1.4 existe m ideal maximal de A tal que $p \subseteq m$. Afirmamos que $p = m$:

Pois se $p \neq m$ tomemos $M = A/p$, M é um A-módulo f.g.(gerado por $\overline{1}$) e seja $a \in m-p$ definimos então um endomorfismo $f : M \longrightarrow M$ por $f(\overline{r}) = \overline{ra}$, f é bem definida e injetora , de fato:

Para $r, s \in A$

$\overline{r} = \overline{s}$ equivale $r-s \in p$ equivale $(r-s)a \in p$ equivale $\overline{ra} = \overline{sa}$.

Agora,por hipótese, f é um isomorfismo portanto $\exists\ \overline{r} \in M$ tal que $f(\overline{r}) = \overline{ra} = \overline{1}$ que equivale a $1-ra \in p \subseteq m$ que é contradição pois $a \in m$. Assim $p = m$ e portanto $\operatorname{Dim} A = 0$.

Reciprocamente, se M é um A-módulo f.g. e $f: M \longrightarrow M$ um endomorfismo injetivo , pelo Lema 1.9 M é um $A[x]$-módulo, $I = \operatorname{Ann}_{A[x]}(M)$ é um ideal não nulo de $A[x]$ e pelo Teorema 2.4 $\operatorname{Dim} (A[x]/I) = 0$.

Dado $\overline{x} \in A[x]/I$, $\overline{x} = x + I$, afirmamos que $\overline{x}$ é uma unidade, de fato: Pois se $\overline{x}$ não é uma unidade pelo Teorema 2.3 $\operatorname{Ann}_A (\overline{x}) \neq \{0\}$ então $\exists\ \overline{u} \in \operatorname{Ann}_A(\overline{x})$ tal que $u \notin I$ ($\overline{u} \neq \overline{0}$) e $\overline{ux} = \overline{0}$ então $ux \in I$ e então $uxM = 0$; Agora $uxm = uf(m) = f(um) = 0 \ \forall\ m \in M$ então $um = 0 \ \forall\ m \in M$, pois f é injetivo

Logo $u \in I$ que é contradição.

$\overline{x}$ unidade então $\exists\ \overline{v} \in A[x]/I$ tal que $\overline{xv} = \overline{1}$ que equivale a $xv - 1 \in I$ que implica $(xv - 1)m = 0\ \forall\ m \in M$ então $xvm = m$ mas $xvm = vf(m) = f(vm)$, isto é, $m = f(vm)$ logo f é sobrejetivo, o que prova que f é um isomorfismo.

... x ...

B I B L I O G R A F I A

[1] - ATIYAH, M.F. e MACDONALD, H.G. : Introduction to Commutative Algebra - Addison Wesley (1969).

[2] - BOURBAKI, N. : Eléments de Mathématique, Fasc. XXVII Algèbre Commutative - Hermann , Paris (1961).

[3] - HOFFMANN e KUNZE : Linear Algebra , Prentice Hall (1964) .

[4] - KAPLANSKI, I. : Commutative Rings, Allyn and Bacon (1970).

[5] - LANG, S. : Algebra , Addison Wesley (1965).

[6] - VASCONCELOS, W. : Injetive Endomorfismos of Finitely Generated Modules - Proc. Amer. Math. Soc. 25(1970) 900---901.

[7] - VASCONCELOS, W. : Regular Endomorfismo of Finitely Generated Modules - J. London Math. Soc. (2) 4(1971) 27---32.