TÓPICOS DE ÁLGEBRA COMUTATIVA

José Fernandes Andrade
e Aron Simis

INSTITUTO DE MATEMÁTICA PURA E APLICADA
Rua Luiz de Camões, 68
20.060 - Rio de Janeiro - RJ

a

Mariana;

a

Cecília.

Apresentação

Este livro não contém o material de um curso inicial de Álgebra Comutativa. Em particular, não são tratados tópicos sagrados tais como extensões inteiras, lema de normalização de Noether, domínios de Dedekind. Por outro lado, insiste-se na teoria de primos associados, divisores de zero e assemelhados, como pilares da teoria.

A intenção original era cobrir tópicos que, de alguma forma, indicassem a cor predominante da Álgebra Comutativa de nossos dias. Mas, havia o aspecto didático a ser levado em conta (leia-se: uma preocupação com os problemas concretos, em suas raízes, e não uma atitude de edificar um bloco perfeito de proposições, uma consequências das outras, marcialmente enfileiradas). O resultado foi este: um livro que pode ser lido, em princípio, sem a tutela de um primeiro curso; mas, para ser usufruido plenamente, requer um contato prévio com exemplos vários e técnicas familiares de anéis comutativos e módulos.

Se um tal resultado justifica a ida ao prelo é, provavelmente, algo reservado para o futuro responder. Os autores esperam que o livro sirva ao menos como roteiro para estudantes potencialmente interessados em trabalhar na área.

Pode-se dizer que a Álgebra Comutativa visa, grosso modo, entender a relação exata que guardam entre si os invariantes numéricos de anéis e módulos. A dimensão combinatória (cadeias de primos) vis-à-vis a profundidade (R-sequências) vis-à-vis a dimensão homológica (resoluções livres): eis o núcleo. Evidentemente, estamos obscurecendo o papel motor da Gometria Algébrica (multiplicidades, etc.) mas sobre isto já se gastou muita eloquência.

Esperamos que, no pior dos casos, este livro ofereça um panorama - se bem que parcial - dos métodos usuais da Álgebra Comutativa. Há algumas omissões óbvias: polinômio de Hilbert, multiplicidades, séries de Poincaré, estrutura das resoluções livres, cohomologia local. Estas adições, entretanto, conduziriam o livro a proporções não alceáveis (hein, João José?).

Queremos agradecer a Wolmer Verçosa Vasconcelos por inúmeras conversas que influiram, direta ou indiretamente, na execução deste trabalho.

Os agradecimentos restantes são para as equipes "por trás dos bastidores": a do Wilson Góes, pela excelência datilográfica, e a do João José, pelo milagre tipográfico.

ÍNDICE

Capítulo I

Teoria da dimensão e primos associados

§1. Os primos associados de um módulo.

Introduziremos, o quanto antes, as noções fundamentais deste curso.

Suporemos, tacitamente, que todos os anéis são noetherianos (comutativos, com unidade) e todos os módulos, finitamente gerados (adotaremos o ponto de vista de que módulos existem em abundância; um bom antídoto para obstruções psicológicas, neste estágio inicial, é visualizar R-módulos da forma R/I, I um ideal do anel R).

Seja R um anel e M um R-módulo. Poremos:

$Z(M) = \{\text{divisores de zero em } M\} = \{r \in R \mid rx = 0, \text{ algum } x \in M\setminus\{0\}\}$.

Fácil: $R\setminus Z(M)$ <u>é um subconjunto multiplicativo saturado de</u> R (isto é, dados $a,b \in R$, tem-se: $a,b \in R\setminus Z(M) \Leftrightarrow ab \in R\setminus Z(M)$).

Um pouco mais difícil: $Z(M) = \bigcup_\alpha P_\alpha$, P_α <u>ideal primo de</u> R.

(Sugestão: <u>lema de Krull</u>, o qual afirma que ideais máximos relativamente à propriedade de disjunção de um subconjunto multiplicativo são primos. Este lema mostra, em verdade, que o complementar de um subconjunto multiplicativo saturado é união, possivelmente infinita, de ideais primos).

Não aportaríamos muito distante, só com estas informações. Contudo, usando a hipótese de que R é noetheriano e M é um R-módulo finitamente gerado, podemos até "por as mãos" nos constituintes da reunião $Z(M) = \bigcup_{\alpha} P_{\alpha}$. Precisamente, é possível selecionar um conjunto finito de primos cuja reunião é $Z(M)$. Para tal, procedemos da seguinte maneira.

Primeiramente, denotemos por $(0):_R x$ (ou simplesmente $(0):x$ se não houver confusão) o anulador de x. Isto significa, lembremos, que $(0):x = \{r \in R \mid rx = 0\}$. A primeira coisa a fazer é observar que

$$Z(M) = \bigcup_{\substack{x \in M \\ x \neq 0}} (0):x = \bigcup_{\substack{x_i \in M \\ x_i \neq 0}} (0):x_i \ ,$$

onde $(0):x_i$ percorre a família daqueles anuladores (de elementos de M) que são máximos entre todos os anuladores. Novamente, pelo resultado de Krull mencionado acima, vê-se que um tal $(0):x_i$ é um ideal primo. Mas, ainda não é o bastante pois tal família pode ser infinita. Por outro lado, como R é noetheriano, o submódulo $N = \sum_i Rx_i$ de M é finitamente gerado. Digamos, $N = Rx_1 + \ldots + Rx_n$. Então $x_i \in Rx_1 + \ldots + Rx_n \ \forall\, i$, de modo que $(0):x_i \supseteq ((0):x_1) \cap \ldots \cap ((0):x_n)$. Como $(0):x_i$ é primo, resulta finalmente $(0):x_i \supseteq (0):x_1$ (digamos) e, por maximalidade, $(0):x_i = (0):x_1$.

Em conclusão, o conjunto dos distintos $(0):x_i$ na família $\{(0):x_i\}_i$ é finito, cada um deles sendo primo. Este é o resultado que procurávamos.

Observação. Enfatizemos que o resultado acima não significa que sempre que $Z(M) = \bigcup_{\alpha} P_{\alpha}$, então podemos extrair uma subfamília finita $\{P_i\}$ tal que $Z(M) = \bigcup_i P_i$. Por exemplo, se $M = k[X,Y]/(X,Y)$ então $Z(M) = (X,Y)$ é reunião da família dos ideais primos principais contidos em (X,Y).

A situação peculiar ora descrita motiva introduzir a definição seguinte.

<u>Definição I.1</u> - Um ideal primo P de R é um <u>primo associado de</u> M se $P = (0):x$ para algum $x \in M$ (necessariamente, $x \neq 0$).

Notação: $\mathrm{Ass}(M) = \{$primos associados de $M\}$.

<u>Exemplos</u>. (1) <u>Se</u> $P \subset R$ <u>é um ideal primo</u>, $\mathrm{Ass}(R/P) = \{P\}$.

(2) $\mathrm{Ass}(M) = \emptyset \Leftrightarrow M = (0)$ (<u>Exercício</u>).

(3) Sejam $N \subset M$ módulos. Então, $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \cup\, \mathrm{Ass}(M/N)$.

(<u>Demonstração</u>: $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M)$ é imediato a partir da definição. Por outro lado, seja $P \in \mathrm{Ass}(M)$. Então, $P = (0):x$, com $x \in M$. Suponhamos que $P \notin \mathrm{Ass}(N)$. Segue que $x \notin N$ e, denotando $\bar{x} \in M/N$ a classe de x, $(0):x \subset (0):\bar{x}$. Por outro lado, $Rx \cap N = (0)$. Com efeito, se $Rx \cap N \neq (0)$, $Rx \cap N$ admite um primo associado (vide (2)) e tal primo é, como vimos acima, um primo associado de Rx. Mas $Rx \simeq R/P$ como R-módulos, logo este primo é P. Mas $Rx \cap N \subset N$, logo P é primo associado de N, contradizendo a hipótse. Assim, efetivamente $Rx \cap N = (0)$, isto é, $(0):\bar{x} \subset (0):x$. Logo $(0):\bar{x} = (0):x = P$ é um primo associado de M/N).

(4) <u>Para todo módulo</u> M, $\mathrm{Ass}(M \oplus \ldots \oplus M) = \mathrm{Ass}(M)$.

(<u>Demonstração</u>: segue facilmente de (3)).

Em particular, se $M \simeq R^n$ (= módulo livre), $Ass(M) = Ass(R)$.

(5) Seja $I \subset R$ um ideal. Pelo Exemplo (3), os primos associados do módulo I são primos associados de R. Em particular, se R é um domínio e $I \neq (0)$, (0) é o único primo associado de I!

Insistimos em que estamos considerando I como módulo. Como tal, $Ass\{I\}$ não deve ser confundido com o que é comumente chamado de conjunto dos "primos de I": este último é, na verdade, $Ass(R/I)$; cf. Exemplo (7).

(6) Módulos livres de torção.

Se M é um submódulo de um módulo livre, então pelos Exemplos (3) e (4), temos $Ass(M) \subset Ass(R)$. Em geral, diremos que M é um módulo livre de torção se precisamente tiver lugar a inclusão $Ass(M) \subset Ass(R)$. Se R é um domínio, isto equivale, como é bem conhecido, a dizer que M é submódulo de um módulo livre. Em geral, necessitamos uma hipótese adicional: dizemos que M é genericamente livre se M_S é um R_S-módulo livre, onde $S = R \setminus \bigcup_{P \in Ass(R)} P$. Se este é o caso, vê-se que o homomorfismo canônico $M \to M_S$ é injetor (com efeito, $M \to M_T$ é injetor, com $T = R \setminus \bigcup_{P \in Ass(M)} P$; como por hipótese $M \to M_T$ se fatora através de $M \to M_S$, $M \to M_S$ é também injetor).

(7) $Ass(R/I)$ versus decomposição primária de I.

Esta é a situação básica nas aplicações. Lembremos que um ideal $I \subset R$ admite uma decomposição primária, isto é, é possível escrever $I = Q_1 \cap \ldots \cap Q_m$, com Q_i ideal primário (dizemos que Q_i é <u>componente primária</u> da decomposição). Em verdade, existe sempre uma tal decomposição <u>irredundante</u>, no sentido de serem observadas as seguintes condições: (1) $\bigcap_{i\neq j} Q_i \not\subset Q_j$, para qualquer j; (2) $i\neq j \Rightarrow \sqrt{Q_i} \neq \sqrt{Q_j}$.

Eis o que se pode dizer da unicidade dos $\sqrt{Q_i}$:

$\mathrm{Ass}(R/I) = \{\sqrt{Q_i} \mid Q_i$ ideal primário numa decomposição irredundante de $I\}$

<u>Demonstração</u>: A inclusão $\subset$ decorre das definições. Com efeito, seja $P \in \mathrm{Ass}(R/I)$ e seja $x \in R$ tal que $P = (0):x$ $(= (0):\bar{x}$, com $\bar{x}$ a classe de x em $R/I)$. Como teremos que lidar com vários ideais de R, é conveniente introduzir uma variante de notação: para um R-módulo quociente R/I, poremos $I:x$ para o anulador do elemento x no módulo R/I.

Prosseguindo, temos $I = \bigcap Q_i$. "Tomando anuladores" em ambos os membros, obtemos $I:x = \bigcap_i (Q_i:x)$. Tomando radicais em ambos os membros, tem-se $P = \bigcap_i \sqrt{(Q_i:x)}$. É imediato que $\sqrt{Q_i:x} = \sqrt{Q_i}$, a menos que $x \in Q_i$, quando então $Q_i:x = R$. Resulta, assim, que $P = \sqrt{Q_i}$, para algum i.

Para demonstrar a inclusão inversa, precisamos escolher elementos convenientes. Ponhamos $P_i = \sqrt{Q_i}$. Queremos mostrar que $P_i \in \mathrm{Ass}(R/I)$, isto é, que $P_i = I:x$ na notação estabelecida acima. Nossa primeira tentativa cai sobre um $x \in (\bigcap_{j\neq i} Q_j)\setminus Q_i$ (que existe por irredundância). Podemos ter dificuldade em mostrar que $P_i \cdot x \subset Q_i$, o que nos leva a reajustar as lentes. Ponhamos $J = \bigcap_{j\neq i} Q_j$. Por hipótese, $J \cap Q_i = I$. Escolhamos um $t \gg 0$ tal que $P_i^t \subset Q_i$. Então, temos $JP_i^t \subset J \cap P_i^t \subset J \cap Q_i = I$. Tomamos, em seguida, um $t > 0$ menor possível tal que $JP_i^t \subset I$ e, finalmente, um $x \in JP_i^{t-1} \setminus I$. A inclusão $I: x \supset P_i$ resulta de que $P_i x \subset JP_i^t \subset I$, enquanto que a inclusão $I: x \subset P_i$ resulta de que $x \in JP_i^{t-1} \subset J$, mas $x \notin I$. Com efeito, isto acarreta $x \notin Q_i$ pois $I = J \cap Q_i$. Ora, se $r \in R$ é tal que $rx \in I$, então, por maior razão, $rx \in Q_i$, resultando que $r \in \sqrt{Q_i} = P_i$.

<u>Observação</u>. O resultado acima mostra, efetivamente, que os primos $\sqrt{Q_i}$ que aparecem numa decomposição primária de I são unicamente determinados (isto é, dependem só de I e não da decomposição em questão). A advertência usual, num primeiro curso de Álgebra Comutativa, é no sentido de que, em geral, não existe unicidade das componentes primárias Q_i. De acordo com isto, podemos separar os constituintes de $\mathrm{Ass}(R/I)$ em duas classes:

- a classe dos primos mínimos de $\mathrm{Ass}(R/I)$ (relativamente à inclusão);
- a classe complementar em $\mathrm{Ass}(R/I)$, isto é, os primos que contêm propriamente algum primo de $\mathrm{Ass}(R/I)$.

Não precisamos ter receio: a primeira classe coincide com o conjunto dos primos mínimos de I (relativamente à inclusão). A terminologia resulta, neste caso, não ter qualquer ambiguidade: falamos dos primos mínimos de I. Ora, sucede que a componente primária de um primo mínimo de I também depende só de I (e não de uma decomposição particular). Com efeito, sejam $I = Q \cap \ldots = Q' \cap \ldots$ duas decomposições primárias de I, com $\sqrt{Q} = P = \sqrt{Q'}$ um primo mínimo. Se localizarmos no primo P, teremos $Q_P = Q'_P$. Um cálculo trivial, usando o fato de que Q

(resp. Q') é primário, mostra então que $Q' \subset Q$ (resp. $Q \subset Q'$).

É evidente, em contrapartida, que este argumento não funciona no caso de primos na segunda classe acima. Em verdade, não existe unicidade de componentes primários de tais primos. O primeiro exemplo, já por demais popularizado, é obtido com $R = k[X,Y]$ e $I = (X^2,XY)$. Calcula-se, facilmente, decomposições primárias para I. Assim:

$$I = (X) \cap (X^2,Y) = (X) \cap (X,Y)^2 = \text{etc.}$$

(Note que $\mathrm{Ass}(R/I) = \{(X),(X,Y)\}$).

Primos nesta segunda classe recebem a designação de <u>imersos</u>. À primeira vista, primos desta natureza surgem como um incômodo (necessário) da teoria. Adiante, veremos que contêm, em verdade, informações sutis sobre o comportamento homológico do módulo R/I.

§2. <u>Um módulo versus seu anulador</u>.

Precisamos de mais notação. Na seção anterior, consideramos o anulador (em R) de um elemento $x \in M$. Mais geralmente, dados submódulos N e N' de M, definimos $N:N' = \{r \in R \mid rN' \subset N\}$.

Tem-se, evidentemente, $N:N' = (0):(N+N')/N$.

Em particular, temos $(0):M = \{r \in R \mid rM = (0)\}$, o <u>anulador de</u> M. Todos estes subconjuntos de R são, em verdade, ideais de R.

Por exemplo, se $M \simeq R/I$, para um ideal $I \subset R$, então $(0):M = I$. Em geral, a situação não é tão simples. Digamos - a título de vago desafio - que uma boa parte da teoria depende da relação exata entre M e $(0):M$.

Para dar um pouco de substância ao "desafio" acima, construiremos, em linhas gerais, uma teoria de decomposição primária para módulos. Esta teoria foi desenvolvida nos anos de 50 por Cartan, Eilenberg e Serre. Observando através das lentes ímpias do formalismo moderno, esta teoria se nos afigura uma generalização óbvia da teoria de E. Noether, muito menos do que um tributo à diligência de matemáticos excelentes. Em verdade, veremos oportunamente que muitas questões decorrentes desta teoria estão longe daquilo que, por qualquer padrão razoável, possa ser chamado "trivial".

Procedemos da seguinte maneira. É dado um R-módulo M (lembremos nossa convenção: R noetheriano e M finitamente gerado), que permanecerá razoavelmente fixo durante a discussão. Seja N um submódulo de M (pensamos em $N = I$ e $M = R$, para concretizar idéias).

É preciso refazer a teoria praticamente ab initio, de modo que começamos com o <u>radical de</u> N (em M). Pomos, por definição:

$$\text{radical de } N = \sqrt{N:M}.$$

Não é necessário nova notação para o radical de N, mas é importante ter em mente que o radical de N é um ideal em R e não um submódulo de M.

A primeira observação é que $\sqrt{N:M} \subset Z(M/N)$. Com efeito, dado $a \in \sqrt{N:M}$, tomamos o menor n tal que $a^n \cdot M/N = (0)$. Então $a^{n-1} \cdot M/N \neq (0)$ é um submódulo de M/N anulado por a (o caso $n=1$ é facilmente discutido à parte).

Desta observação segue, mediante os resultados do §1 e o Exercício 1, que $\sqrt{N:M}$ está contido em algum $P \in \mathrm{Ass}(M/N)$. Esta é, contudo, uma conclusão frouxa. De fato, provaremos bastante mais, a saber, que $\sqrt{N:M} = \bigcap\limits_{P \in \mathrm{Ass}(M/N)} P$.

Ora, em qualquer caso, sabemos que $\sqrt{N:M} = \bigcap\limits_{P \in \mathrm{Ass}(R/N:M)} P$ (podemos, evidentemente, restringir esta interseção aos primos mínimos do módulo $R/N:M$). O que queremos segue, então, do seguinte lema.

<u>Lema I.2</u> - <u>Seja</u> M <u>um</u> R-<u>módulo. Então</u>:

(i) $\mathrm{Sup}(M) = \mathrm{Sup}(R/0:M)$, onde $\mathrm{Sup}(*) = \{P \subset R,\ P \text{ primo} \mid *_P \neq 0\}$ ("Sup" = suporte)

(ii) $\mathrm{Ass}(M) \subset \mathrm{Sup}(M)$; <u>mais geralmente, todo primo contendo um primo associado de</u> M <u>pertence a</u> $\mathrm{Sup}(M)$.

(iii) <u>Se</u> $P \in \mathrm{Sup}(M)$, <u>então</u> P <u>contém algum</u> $P' \in \mathrm{Ass}(M)$.

<u>Demonstração</u>: (i) Para tal, consideremos um conjunto de geradores $x_1, \dots, x_m$ de M. Tem-se, evidentemente, $(0):M = \bigcap\limits_{i=1}^{m} ((0):x_i)$, logo $\mathrm{Sup}(R/0:M) = \bigcup\limits_{i=1}^{m} \mathrm{Sup}(R/0:x_i)$. Mas, é fácil ver que $\mathrm{Sup}(M) = \bigcup\limits_{i=1}^{m} \mathrm{Sup}(Rx_i)$. Como $R/0:x_i \simeq Rx_i$, temos o resultado procurado.

(ii) Sejam $P \subset P'$ primos tais que $P \in \mathrm{Ass}(M)$. Então, M_P é uma "localização" de $M_{P'}$. Disto resulta que $M_{P'} = (0) \Rightarrow M_P = (0)$.

Mas, $M_P = (0) \Rightarrow Ass(M_P) = \emptyset$, o que é absurdo pois $P \in Ass(M)$ $\Rightarrow P_P \in Ass(M_P)$ (verificação direta).

(iii) Se $M_P \neq (0)$, existe um primo associado a M_P e um tal primo é, necessariamente da forma P'_P, com $P' \subset P$ e $P' \in Ass(M)$ (a verificação deste fato será deixada como exercício). //

<u>Corolário I.3</u> - <u>Para todo</u> R-<u>módulo</u> M, <u>os seguintes conjuntos coincidem</u>:

<u>o conjunto dos elementos mínimos de</u> $Ass(M)$;

<u>o conjunto dos elementos mínimos de</u> $Sup(M)$;

<u>o conjunto dos elementos mínimos de</u> $Sup(R/0{:}M)$.

Denotaremos $Min(M)$ o conjunto acima.

Obtemos, assim, a igualdade $\sqrt{N{:}M} = \bigcap_{P \in Min(M/N)} P$ (aplicando ao módulo M/N o corolário). Esta igualdade permite, por sua vez, deduzir a seguinte proposição.

<u>Proposição I.4</u> - <u>As seguintes condições são equivalentes para um módulo</u> M <u>e um submódulo</u> N <u>de</u> M:

(i) $Ass(M/N)$ <u>tem um único elemento</u>;

(ii) $Z(M/N) \subset \sqrt{N{:}M}$.

<u>Demonstração</u>: Podemos, sem perda de generalidade, supor que $N = (0)$.

(i) $\Rightarrow$ (ii) Seja P o único primo associado de M. Então, na notação acima, $Min(M) = \{P\}$ e, pelo que acabamos de ver, $\sqrt{0{:}M} = P$. Como $Z(M) = P$, temos o resultado.

(ii) $\Rightarrow$ (i). Como $\sqrt{0:M} \subset Z(M)$ sempre vale, temos $Z(M) = \sqrt{0:M}$ por hipótese. Mas, $Z(M) = \bigcup_{P \in Ass^+(M)} P$, onde $Ass^+(M) = \{P \in Ass(M) \mid P$ máximo possível$\}$ é, como vimos no §1, um conjunto finito. Segue-se que $\sqrt{0:M} \subset P$, para algum $P \in Ass^+(M)$ (vide Exercício 1). Consequentemente, $\sqrt{0:M} = P$ e $Ass(M) = \{P\}$. //

<u>Definição I.5</u> - Um submódulo $N \subset M$ é dito <u>primário</u> (em M) se satisfaz as condições equivalentes da Proposição I.4.

Se N é primário, então, como vimos, $\sqrt{N:M}$ é um ideal primo e é o único primo associado de M/N. Em verdade, $N:M$ é um ideal primário. De fato, sejam $a,b \in R$ tais que $ab \in N:M$ e $b \notin \sqrt{N:M}$. Como N é primário, $b \notin Z(M/N)$. Mas $b\cdot(a\cdot M/N) = (0)$, por hipótese; necessariamente, então, $a\cdot M/N = (0)$, isto é, $a \in N:M$.

Queremos destacar este fato:

<u>Se</u> $N \subset M$ <u>é primário, então o anulador de</u> M/N <u>é primário</u> (<u>e ambos possuem o mesmo radical</u>).

Em seguida, o resulado central que vimos perseguindo.

<u>Teorema I.6</u> ("<u>Decomposição primária de um submódulo</u>").

<u>Todo submódulo</u> $N \subset M$ <u>escreve-se na forma</u> $N = \bigcap_i Q_i$ (<u>interseção finita</u>), <u>onde</u> Q_i <u>é um submódulo primário de</u> M.

<u>Demonstração</u>: Podemos, sem perda de generalidade, supor que $N = (0)$. Usaremos dois fatos básicos.

<u>Fato 1</u>. $Ass(M)$ é um conjunto finito.

<u>Fato 2</u>. Para todo subconjunto $\mathcal{P} \subset Ass(M)$, existe um submódulo

N de M tal que $\mathrm{Ass}(M/N) = \wp$ e $\mathrm{Ass}(N) = \mathrm{Ass}(M)\setminus\wp$.

Acreditemos no Fato 1, por um momento. Quanto ao Fato 2, observemos que o conjunto dos submódulos L de M tais que $\mathrm{Ass}(L) \subset \mathrm{Ass}(M)\setminus\wp$ é não vazio ((0) pertence!), logo admite um N máximo possível. Pelo Exemplo (3), §1, basta mostrar que $\mathrm{Ass}(M/N) \subset \wp$. Ora, se $P \in \mathrm{Ass}(M/N)$, temos $R/P \simeq L/N$ para algum submódulo $L \subset M$. Novamente, pelo Exemplo (3), $\mathrm{Ass}(L) \subset \subset \mathrm{Ass}(N) \cup \mathrm{Ass}(L/N) = \mathrm{Ass}(N) \cup \{P\}$. Pela escolha de N, tem-se necessariamente $\mathrm{Ass}(L) \not\subset \mathrm{Ass}(M)\setminus\wp$ e, a fortiori, $P \in \wp$.

Dos dois fatos acima deduzimos facilmente o teorema. Com efeito, para cada $P \in \mathrm{Ass}(M)$ existe um submódulo $Q(P) \subset M$ tal que $\mathrm{Ass}(M/Q(P)) = \{P\}$ e $\mathrm{Ass}(Q(P)) = \mathrm{Ass}(M)\setminus\{P\}$ (Fato 2, com $\wp = \{P\}$). Pela Proposição I.4, $Q(P)$ é primário. Mostremos que $(0) = \bigcap_{P\in \mathrm{Ass}(M)} Q(P)$ mostrando, para isto, que $\mathrm{Ass}(\bigcap_{P\in \mathrm{Ass}(M)} Q(P)) = \phi$. Ora, $P' \in \mathrm{Ass}(\bigcap_{P\in \mathrm{Ass}(M)} Q(P)) \Rightarrow P' \in \mathrm{Ass}(Q(P))$, para todo $P \in \mathrm{Ass}(M)$ (Exemplo (3), §1). Por construção, $\bigcap_{P\in \mathrm{Ass}(M)} \mathrm{Ass}(Q(P)) = \phi$; absurdo. //

Como consequência imediata, temos o seguinte resultado básico.

<u>Corolário I.7</u> - <u>Para todo módulo</u> M, $\mathrm{Ass}(M) = \mathrm{Ass}(R/0{:}M)$.

<u>Demonstração</u>: Seja $(0) = \bigcap_{P\in \mathrm{Ass}(M)} Q(P)$ uma decomposição primária de (0), tal como foi construida na demonstração do Teorema I.6. Uma tal decomposição é, como pode-se verificar, irredundante (no mesmo sentido que emprestamos a este termo no caso de ideais). Tomando anuladores, resulta facilmente

$$(0):M = \bigcap_{P\in \mathrm{Ass}(M)} (Q(P):M).$$

Conforme destacamos anteriormente, $Q(P):M$ é um ideal primário tal que $\sqrt{Q(P):M}$ = radical de $Q(P) = P$. Segue que a igualdade acima é uma decomposição primária do ideal $(0):M$. Pelo Exemplo (7), §1, resulta $\mathrm{Ass}(M) = \mathrm{Ass}(R/0:M)$. //

Assim resta-nos apenas lidar com o Fato 1. A beleza da demonstração do Teorema I.6 reside no fato de que os submódulos primários numa decomposição de (0) puderam ser escolhidos diretamente entre aqueles cujos radicais são primos associados de M. Desta forma, obtemos gratuitamente a igualdade de $\mathrm{Ass}(M)$ e {radicais de submódulos primários numa decomposição primária de (0)}. Entretanto, é preciso pagar o preço em algum lugar: no caso, o preço é o Fato 1. Desta forma, faz-se necessária uma demonstração fresquinha do Fato 1.

<u>Demonstração do Fato 1</u>: Podemos supor $M \neq (0)$. Neste caso, seja $P_1 \in \mathrm{Ass}(M)$. Então $R/P_1 \simeq M_1$ para certo $M_1 \subset M$. Segue que $\mathrm{Ass}(M) \subset \{P_1\} \cup \mathrm{Ass}(M/M_1)$. Escolhemos $P_2 \in \mathrm{Ass}(M)\setminus\{P_1\}$, de modo que, necessariamente, $P_2 \in \mathrm{Ass}(M/M_1)$. Portanto, $R/P_2 \simeq M_2/M_1$, para algum $M_2 \subset M$. Continuando desta maneira, obtemos uma cadeia $M_1 \subset M_2 \subset \ldots$. Seja t tal que $M_t = M_{t+1} = \ldots$. Temos, até agora, $\mathrm{Ass}(M) \subset \{P_1, P_2, \ldots, P_t\} \cup \mathrm{Ass}(M/M_t)$. Se ainda existe algum $P \in \mathrm{Ass}(M)\setminus\{P_1,\ldots,P_t\}$, então $P \in \mathrm{Ass}(M/M_t)$. Resulta, então, que $M'/M_t \simeq R/P$, para algum submódulo M' de M. Desta forma, inaugurarímos uma nova cadeia de submódulos e, assim por diante, até obter uma "árvore" de cadeias e o resultado segue-se de um argumento padronizado sobre tais cadeias.

§3. Teoria da dimensão.

Recordemos que a dimensão (de Krull) de um anel R é o supremo dos comprimentos de cadeias

$$P_o \subsetneq P_1 \subsetneq \dots \subsetneq P_n,$$

onde P_i é um ideal primo de R (por definição, o comprimento de uma tal cadeia é n). Notação: $\dim(R)$.

Subentendida nesta noção está a de altura de um ideal primo P: simplesmente, aprovamos apenas as cadeias truncados à direita em P. Notação: $\mathrm{alt}(P)$.

Seja, agora, $I \subset R$ um ideal qualquer. Para calcular $\dim(R/I)$, por definição, temos de considerar as cadeias de primos

$$I \subset P_o \subsetneq P_1 \subsetneq \dots .$$

Em outras palavras, temos $\dim(R/I) = \sup\limits_{P \supset I} \{\dim(R/P)\} =$

$= \sup\limits_{P \in \mathrm{Sup}(R/I)} \{\dim(R/P)\}$ $(= \sup\limits_{P \in \mathrm{Min}(R/I)} \{\dim(R/P)\})$.

Seguindo este modelo, parece natural definir a dimensão de um módulo M (notação análoga: $\dim(M)$) como sendo $\sup\limits_{P \in \mathrm{Sup}(M)} \{\dim(R/P)\}$. Neste caso, $\dim(M) = \dim(R/(0:M))$ (vide §2, Lema I.2). Ora, para qualquer ideal $J \subset R$, tem-se facilmente $\dim(R/J) \leq \dim(R)$. Assim, a dimensão de um módulo não pode exceder a do seu anel de operadores.

O resultado básico da teoria da dimensão é o teorema do ideal principal ("Hauptidealsatz" de Krull), em suas diversas variantes. Neste capítulo, daremos a formulação clássica deste teorema, em termos da existência de sistemas de parâmetros.

Nesta discussão, suporemos sempre que R é local e $\underline{m}$, seu ideal máximo.

Definição I.8 - Seja M um R-módulo (como sempre, finitamente gerado). Uma sequência $x_1,\dots,x_s$ de elementos de R é um sistema de parâmetros de M se s é o menor inteiro que satisfaz a condição: $\operatorname{Sup}(M/(x_1,\dots,x_s)M) = \{\underline{m}\}$.

O inteiro s é um invariante de M; denota-lo-emos, provisoriamente, por $s(M)$ (esta notação será desnecessária, em um momento).

A existência de um sistema de parâmetros, de acordo com esta definição, é imediata. Com efeito, a família de seqüências $\underline{x} = x_1,\dots,x_t$ tais que $\operatorname{Sup}(M/\underline{x}M) = \{\underline{m}\}$ é não vazia, pois uma sequência de geradores de $\underline{m}$ pertence a esta família.

Em particular, $s(M) \leq \mu(\underline{m})$ (= número mínimo de geradores de $\underline{m}$) para todo módulo M. Contudo, esta é uma estimativa demasiada grosseira. Podemos melhorá-la consideravelmente.

Proposição I.9 - Para todo módulo M, $s(M) \leq \dim(M)$.

Demonstração: Se $\dim(M) = \infty$, não há nada a provar (em verdade, como veremos em seguida, esta possibilidade inexiste).

Seja, então, $\dim(M) = r < \infty$. Procedamos por indução sobre r. Se $r = 0$, como $\dim(M) = \dim(R/P)$ para algum $P \in \operatorname{Min}(M)$, vemos que $P = \underline{m}$. Logo, $\operatorname{Sup}(M) = \{\underline{m}\}$ e, consequentemente, $s(M) = 0$.

Suponhamos $r \geq 1$. Neste caso, $\underline{m} \not\subset \bigcup P$ onde P percorre o conjunto dos primos $P \in \operatorname{Min}(M)$ tais que $\dim(M) = \dim(R/P)$. Tomemos $x \in \underline{m} \setminus \bigcup P$, $\dim(R/P) = \dim(M)$. Neste caso, tem-se, evidentemente, $\dim(M/xM) \leq \dim(M)-1$. Pela hipótese de indução, $s(M/xM) \leq \dim(M/xM)$. Por outro lado, seja $\underline{x} = x_1,\ldots,x_t$ um sistema de parâmetros de M/xM; como $(M/xM) \,/\, \underline{x}(M/xM) \simeq M((x,\underline{x})M$, resulta que $s(M) \leq s(M/xM)+1$. Segue, então, que $s(M) \leq \dim(M)$, como queríamos. //

Se analisarmos o argumento acima, veremos que mostrou-se o seguinte fato: para obter-se uma sequência $x_1,\ldots,x_r$ tal que $\dim(M) = r$ e $\mathrm{Sup}(M/(x_1,\ldots,x_r)M) = \{\underline{m}\}$, é suficiente tomar $x_i \in \underline{m} \setminus \bigcup P^{(i)}$, onde $P^{(i)}$ percorre a família dos primos $P^{(i)}$ tais que $\dim(M/(x_1,\ldots,x_{i-1})M) = \dim(R/P^{(i)})$, $i = 0,\ldots,r-1$.

Em particular, qualquer $x \in \underline{m} \setminus \bigcup P$, $\dim(M) = \dim(R/P)$, é adequado para iniciar uma tal sequência. Parece natural perguntar se um elemento $x \in R$, escolhido nestas condições, pode sempre iniciar um sistema de parâmetros. A resposta é afirmativa e resulta do que hoje habituou-se chamar de Teorema de Krull-Chevalley-Samuel.

Teorema I.10 (Krull) - Para todo módulo M, $\dim(M) \leq s(M)$.

A demonstração, em um minuto. Antes, algumas consequências importantes.

Corolário I.11 - Para todo módulo M, $\dim(M) < \infty$.

Corolário I.12 ("Primidealsatz", Krull) - Seja R um anel noetheriano (momentaneamente infringindo nossa convenção de que R é sempre local) e $I \subset R$ um ideal. Se $P \in \mathrm{Min}(R/I)$, então $\mathrm{alt}(P) \leq \mu(I)$ (= número menor possível de geradores de I).

<u>Demonstração</u> (do Corolário I.12) - Aplicando o Teorema I.10 com $M = R_P$, resulta $\mathrm{alt}(P)$ $(= \dim(R_P)) \leq s(R_P)$. Mas, I_P é P_P-primário, de modo que, certamente, $s(R_P) \leq \mu(I_P) \leq \mu(I)$. //

<u>Observação</u>: É fácil ver que o "Primidealsatz" implica, por sua vez, o Teorema I.10. Com efeito, temos $\dim(M) = \dim(R/0{:}M)$ e $s(M) = s(R/0{:}M)$ (a última igualdade seguindo-se das igualdades seguintes facilmente verificáveis:

$$\mathrm{Sup}(M/\underline{x}M) = \mathrm{Sup}(M) \cap \mathrm{Sup}(R/(\underline{x})) = \mathrm{Sup}(R/(0{:}M)) \cap \mathrm{Sup}(R/(\underline{x}))$$
$$= \mathrm{Sup}((R/0{:}M)/\underline{x}(R/0{:}M)),$$

para toda sequência $\underline{x}$ de elementos de R).

Ora, pelo Primidealsatz, se S é um anel local e $J \subset S$ um ideal primário pertencente ao ideal máximo de S, tem-se $\dim(S) \leq \mu(J)$. Logo, $\dim(S) \leq s(S)$. Pondo $S = R/0{:}M$, temos o resultado procurado.

Ocupemo-nos da demonstração do Teorema I.10. A maneira mais, digamos, fecunda de obter a desigualdade $\dim(M) \leq s(M)$ é através de duas desigualdades intermediárias $\dim(M) \leq d(M)$ e $d(M) \leq s(M)$, onde $d(M)$ é definido como o grau do polinômio de Hilbert do módulo M. Nesta forma do teorema, devemos pagar tributo igualmente aos trabalhos de Chevalley e Samuel. Entretanto, uma discussão satisfatória (quer dizer, >> definição) do polinômio de Hilbert nos afastaria dos temas principais deste curso. Assim, somos forçados a apresentar uma solução conciliatória, a saber, admitiremos a seguinte hipótese:

(H) Se M é um módulo (R local), então para todo $x \in \underline{m} \setminus \bigcup P$, P percorrendo os primos tais que $\dim(M) = \dim(R/P)$, existe um sistema de parâmetros de M iniciando com x.

Com esta hipótese adicional, a demonstração do Teorema I.10 é fácil, passando por cima do método do polinômio de Hilbert. A hipótese (H) é, afinal, uma consequência imediata da igualdade $\dim(M) = s(M)$ desde que se dê uma demonstração desta igualdade independente de (H). De mais a mais, não vemos danos especiais em pressupor (H). Existem vários exemplos deste procedimento na literatura matemática, que são aceitos de maneira natural até mesmo em estágio inicial de uma disciplina (cf. teorema de Cauchy sobre funções analíticas, com a hipótese da função ser C^1).

Demonstração do Teorema I.10 (pressupondo (H)): Seja $P_o \in \mathrm{Min}(M)$ tal que $\dim(M) = \dim(R/P_o)$. Como $P_o \in \mathrm{Ass}(M)$, $R/P_o \simeq N$ para algum submódulo N de M. Se $I \subset R$ é um ideal, tem-se $\mathrm{Sup}(N/IN) = \mathrm{Sup}(N) \cap \mathrm{Sup}(R/I) \subset \mathrm{Sup}(M) \cap \mathrm{Sup}(R/I) = \mathrm{Sup}(M/IM)$, o que mostra que $s(N) \leq s(M)$. Assim, é suficiente mostrar que $\dim(R/P_o) \leq s(R/P_o)$. Ora, seja $P_o \subsetneq P_1 \subsetneq \ldots \subsetneq P_n$ uma cadeia de primos em R, queremos então mostrar que $n \leq s(R/P_o)$. Por indução sobre n.

Se $n = 0$, não há nada a mostrar. Se $n \geq 1$, tomamos $x \in P_1 \setminus P_o$. Como $P_1 \subsetneq \ldots \subsetneq P_n$ é uma cadeia contendo P_o e x, pelo menos $\dim(R/(P_o,x)) \geq n-1$. Por outro lado, pela hipótese (H), x pode iniciar um sistema de parâmetros de R/P_o, digamos, $x, y_1, \ldots, y_t$. Então, $\mathrm{Sup}(R/\underline{y})+(P_o,x)) = \mathrm{Sup}(R/(x,\underline{y})+P_o) = \{\underline{m}\}$, de modo que $s(R/(P_o,x)) \leq s(R/P_o) - 1$. Aplicando a hipótese de indução, concluimos o resultado procurado. //

Voltando ao comentário feito após a Proposição I.9, sabemos agora que um sistema de parâmetros $x_1,\dots,x_r$ de M pode ser escolhido tomando-se $x_i \notin p^{(i-1)}$, para todo primo $p^{(i-1)}$ tal que $\dim(M/(x_1,\dots,x_{i-1})M) = \dim(R/p^{(i-1)})$, $i=1,\dots,r$. Em verdade, esta é a única maneira possível de escolher um sistema de parâmetros de M, conforme veremos agora. Isto fornece um critério eficientíssimo na prática para verificar se uma dada sequência é um sistema de parâmetros.

Proposição I.13 - *Seja* M *um módulo e seja* $x_1,\dots,x_k$ *uma sequência de elementos em* $\underline{m}$. *Então, tem-se a desigualdade:*

$$\dim(M) \leq \dim(M/(x_1,\dots,x_k)M) + k.$$

Além disso, as seguintes condições são equivalentes:

(i) *Dá-se a igualdade acima.*

(ii) *Para cada* $i = 1,\dots,k$, *tem-se* $x_i \notin p^{(i-1)}$ *para todo primo* $p^{(i-1)}$ *tal que* $\dim(R/p^{(i-1)}) = \dim(M/(x_1,\dots,x_{i-1})M)$.

(iii) $x_1,\dots,x_k$ *é parte de um sistema de parâmetros de* M.

Demonstração: A desigualdade resulta da igualdade $\dim(N) = s(N)$ para um módulo N (Prop.I.9 e Teor.I.10) e da desigualdade $s(N) \leq s(N/xN) + 1$ para qualquer $x \in \underline{m}$, que é imediata.

(i) $\Rightarrow$ (ii) Como acabamos de mencionar, sempre vale $\dim(M) \leq$ $\leq (M/(x_1,\dots,x_{k-1})M) + k-1$ (pois $\dim(-) = s(-)$). Resulta, então:

$$\begin{aligned}\dim(M/(x_1,\dots,x_{k-1})M) - 1 &\leq \dim(M/(x_1,\dots,x_k)M) = \dim(M) - k \\ &\leq \dim(M/(x_1,\dots,x_{k-1})M) + k-1-k \\ &= \dim(M/(x_1,\dots,x_{k-1})M) - 1.\end{aligned}$$

Assim, $\dim(M/(x_1,\ldots,x_k)M) = \dim(M/(x_1,\ldots,x_{k-1})M)-1$.

Resulta $\dim(M) = \dim(M/(x_1,\ldots,x_{k-1})M) + k-1$, etc.

Assim, para todo $i = 1,\ldots,k$, temos $\dim(M/(x_1,\ldots,x_i)M) =$ $= \dim(M/(x_1,\ldots,x_{i-1})M)-1$. É fácil ver que isto só é possível com x_i não pertencente aos primos "na dimensão" de $M/(x_1,\ldots,x_{i-1})M$.

(ii) $\Rightarrow$ (iii) Esta implicação já foi observada antes.

(iii) $\Rightarrow$ (i) Tomemos elementos $x_{k+1},\ldots,x_n \in \underline{m}$ tais que $x_1,\ldots,x_k,x_{k+1},\ldots,x_n$ seja um sistema de parâmetros de M, $n = \dim(M)$. Então,

$$\mathrm{Sup}(M/(x_1,\ldots,x_k)M)/(x_{k+1},\ldots,x_n)(M/(x_1,\ldots,x_k)M)) =$$

$$= \mathrm{Sup}(M/(x_1,\ldots,x_n)M) = \{\underline{m}\},$$

de modo que $\dim(M/(x_1,\ldots,x_k)M) = s(M/(x_1,\ldots,x_k)M) \leq n-k$. //

<u>Corolário I.14 - Seja</u> M <u>um módulo e</u> x, y <u>elementos em</u> $\underline{m}$ <u>tais que</u> $x,y \notin P$, <u>para todo</u> P <u>tal que</u> $\dim(M) = \dim(R/P)$. <u>Então, são equivalentes:</u>

(i) x <u>não pertence aos primos</u> P <u>tais que</u> $\dim(M/yM) =$ $= \dim(R/P)$.

(ii) y <u>não pertence aos primos</u> P <u>tais que</u> $\dim(M/xM) =$ $= \dim(R/P)$.

<u>Demonstração:</u> Resulta da proposição anterior, observando que a noção de sistema de parâmetros independe da ordem dos elementos. //

§4. Interpretação Geométrica.

O que se entende por interpretação geométrica, grosso modo, é o seguinte: 1) Um anel da forma R/I é visto como o anel das funções (definidas em toda parte) de uma variedade algébrica; 2) Os primos em $\mathrm{Ass}(R/I)$ são vistos como as componentes desta mesma variedade.

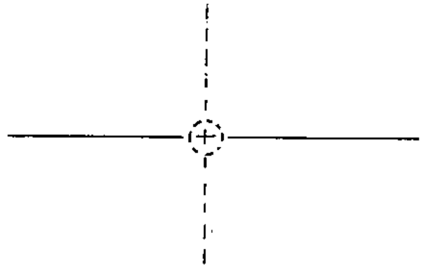
1. Localização da forma S_f.

S é um anel e $f \in S$. Lembremos que S_f denota o anel de frações de S relativamente ao conjunto multiplicativo $\{1,f,f^2,\ldots\}$. A geometria envolvida é a seguinte: S é, digamos, um anel de polinômios $k[X_1,\ldots,X_n]$ e f um polinômio; S_f é o anel das funções (de tipo racional) definidas no complementar dos zeros de f no espaço afim $k^n = \underbrace{k \times \ldots \times k}_{n}$.

É também possível considerar tais localizações em S/I. Há duas possibilidades: (i) $f \in I$. Neste caso, obtém-se apenas as funções definidas no conjunto vazio! (ii) $f \notin I$. Aqui, obtém-se as funções definidas nos zeros simultâneos dos polinômios pertencentes a I excluindo aqueles zeros que já são de f.

Exemplo. $S = k[X,Y]$, $I = (XY)$, $f = X$.

Primeiro, consideramos o anel $k[X,Y]/(XY)$ das funções definidas nos zeros de XY (= os pontos sobre os eixos de coordenadas). Em seguida, excluimos os zeros de X. O resultado são as funções definidas no eixo $Y = 0$ excluida a origem.



$(k[X,Y]/(XY))_X$ = funções definidas no eixo $y = 0$ menos $(0,0)$

Podemos até calcular com os anéis e obter tal resultado. Assim,

$$(k[X,Y]/(XY))_X \simeq (k[X,Y]_X)/(XY)k[X,Y]_X \simeq k[X,Y]_X/(Y)k[X,Y]_X$$
$$\simeq (k[X,Y]/(Y))_X \simeq k[X]_X.$$

2. Localização da forma S_P, P um primo.

Esta é a forma de localização mais popular em Álgebra Comutativa e Geometria Algébrica. Como antes, pensamos primeiro no caso em que $S = k[X_1,\ldots,X_n]$. Se $P = \underline{m}$ é um ideal máximo, a interpretação é esta: um elemento de $S_{\underline{m}}$ é uma função racional cujo denominador f não pertence a $\underline{m}$, logo f é $\neq 0$ em $k[X_1,\ldots,X_n]/\underline{m}$. Ora, (se k é algebricamente fechado) os zeros de $\underline{m}$ consistem de um único ponto em k^n. Assim, obtemos: os elementos de $S_{\underline{m}}$ são as funções, de tipo racional, definidas no único zero de $\underline{m}$ (k algebricamente fechado ou $\underline{m}$ da forma $(X_1-\alpha_1,\ldots,X_n-\alpha_n)$).

Se P não é máximo, interpretação análoga vale, com uma pequena sutileza. Os zeros de P constituem agora toda uma subvariedade em k^n (de dimensão >0), cujos pontos são os zeros dos ideais máximos $\underline{m}$ contendo P. Ora, vale aqui a igualdade $P = \bigcap_{\underline{m}\supset P} \underline{m}$ (vide Exercício 5). Um elemento de S_P é da forma g/f, com $f \notin P$. Então, existe ao menos um $\underline{m} \supset P$ tal que $f \notin \underline{m}$. Pela interpretação feita neste caso, concluimos: os elementos de S_P são funções, de tipo racional, definidas em pelo menos um ponto da variedade dos zeros de P (pode-se dizer mesmo: em todos os pontos da variedade de P exceto nos pontos de uma subvariedade de codimensão >0 a saber, os zeros do ideal (P,f)).

Aqui também, podemos complicar o cenário, localizando quocientes S/I num primo $P \subset S$. Tem-se $(S/I)_P \simeq S_P/IS_P$, de modo que se $I \not\subset P$, novamente obtemos apenas a função identicamente nula. Se $I \subset P$, obtemos funções de tipo racional, restringidas à variedade dos zeros de I, que estão definidas em pelo menos um ponto da variedade dos zeros de P. A situação limite é quando $I = P$; neste caso, obtemos um corpo, o corpo das funções racionais da variedade de P.

3. Primos associados versus componentes da variedade.

A rigor, somente os primos em $\mathrm{Min}(R/I)$ correspondem a entes geométricos - as componentes irredutíveis da variedade de I. Assim, do ponto de vista estrito da "topologia subjacente" à variedade de I, os primos imersos de R/I não desempenham qualquer papel, uma vez que eles correspondem a subvariedades contidas nas componentes irredutíveis. Se quisermos atribuir-lhes algum resquício de significado topológico, o modelo é uma variedade acompanhada de suas componentes irredutíveis e de um punhado de subvariedades de codimensão >0 "distinguidas".

Exemplo. $R = k[X,Y]$, $I = (X^2, XY)$.

Os primos associados de R/I são (X) e (X,Y). O primeiro corresponde à (única) componente irredutível da variedade de I, enquanto que (X,Y) corresponde a uma subvariedade de codimensão 1. Assim, o quadro topológico consiste do eixo $X = 0$ e da origem $(0,0)$ como ponto "distinguido" (se quisermos "distinguir" outro ponto no eixo $X = 0$, digamos, $(0,\alpha)$, consideraremos o ideal $I = (X^2, X(Y-\alpha))$, etc.)

Observação: Se $P \in \mathrm{Ass}(R/I)$ é um primo imerso, é claro que $\dim(R/P) \lneq \dim(R/I)$. Contudo, esta condição não é suficiente para que um $P \in \mathrm{Ass}(R/I)$ seja imerso. Quer dizer, não devemos confundir primos imersos com primos mínimos P tais que $\dim(R/P) \lneq \dim(R/I)$, já que estes últimos correspondem ainda a componentes irredutíveis da variedade de I, se bem que de dimensão menor do que a dimensão da variedade (vide Exercício 6).

Os primos imersos desempenham papel importante em questões "aritméticas" (vide a definição de profundidade no Cap.II) e homológicas (vide Cap.III e IV).

4. Sistemas de parâmetros.

Novamente visualizamos o caso de um módulo da forma R/I, com R local. A principal situação geométrica surge com $R = S_P = k[X_1,\ldots,X_n]_P$ e $I \subset P$. Para simplificar, suporemos P

máximo, até mesmo da forma $(X_1-\alpha_1,\ldots,X_n-\alpha_n)$. Dizer que $x_1,\ldots,x_d \in R$ é um sistema de parâmetros de R/I significa, neste caso, que o ponto $(\alpha_1,\ldots,\alpha_n) \in k^n$ é o único zero simultâneo de I e $x_1,\ldots,x_d$; em outras palavras, obtemos o fato geométrico de que por todo ponto de uma variedade $V \subset k^n$ de dimensão d, passam sempre d hipersuperfícies de k^n de tal forma que este ponto é componente isolada da interseção das hipersuperfícies com V.

É importante observar que num sistema de parâmetros não exige-se que os parâmetros estejam em "posição transversal" (no sentido usual do espaço tangente de V no ponto em questão ser soma direta dos espaços tangentes das hipersuperfícies neste mesmo ponto). A situação transversal corresponde a um anel local regular (vide Cap.III, §1).

Exercícios

1. Seja R um anel comutativo e $P_1,\ldots,P_n$ ideais de R dos quais ao menos $n-2$ são primos. Se $I \subset R$ é um ideal tal que $I \subset \bigcup_{i=1}^{n} P_i$, então $I \subset P_j$ para algum j, $1 \le j \le n$. (Sugestão: pode-se supor que $P_i \not\subset P_j$ se $i \neq j$. Por indução sobre n: se $n = 2$, sejam $x_1 \in I\setminus P_1$ e $x_2 \in I\setminus P_2$. Neste caso, obtemos $x_1 \in P_2$ e $x_2 \in P_1$, logo $x_1+x_2 \notin P_1,P_2$; absurdo pois $x_1+x_2 \in I$. Se $n \ge 3$, suponhamos P_n primo e $I \not\subset P_i$, $i = 1,\ldots,n$. Então, existe $x \in IP_1\cdots P_{n-1}\setminus P_n$. Pela hipótese de indução, existe $y \in I\setminus(P_1 \cup\cdots\cup P_{n-1})$. Deduz-se que $y,y+x \in P_n$; contradição).

<u>Observação</u>. A hipótese de I estar contido numa reunião <u>finita</u> é essencial - vide a observação que precede a Definição I.1.

2. ("Esquiva") - Sejam $P_1,\ldots,P_n$ primos de um anel R e $x_1,\ldots,x_m \in R$ tais que $\{x_1,\ldots,x_m\} \not\subset P_i$, $i = 1,\ldots,n$. Mostre que existem $a_2,\ldots,a_m \in R$ tais que $x_1 + \sum_{j=2}^{m} a_j \cdot x_j \notin P_i$, $i=1,\ldots,n$. (Sugestão: se $x_1 \in (P_1 \cap\ldots\cap P_s)\setminus(P_{s+1} \cup\ldots\cup P_n)$, $x \in (x_2,\ldots,x_n) \setminus \bigcup_{i=1}^{s} P_i$ e $y \in (P_{s+1} \cap\ldots\cap P_n)\setminus(\bigcup_{i=1}^{s} P_i)$, então $x_1 + yx$ é um tal elemento).

3. Em cada um dos casos abaixo, determine os primos associados do módulo M e a decomposição primária de (0) em M.

$M = k[X,Y]/(X^2,XY)$

$M = k[X,Y,Z]/(XY,XZ,YZ)$

$M = k[X,Y]/(X(Y-1),Y)$

$M = k[X,Y,Z]/(X^2,YZ,Y^2)$

$M = k[x,y,z]/(x,z)^2$, com $xy = z^2$.

$M = k[X,Y,Z,W]/(XZ,YW,XW+YZ)$

$M = k[X,Y,Z,W]/(XW-YZ,\ XZ^2-Y^2W)$

4. Seja $R = k[X,Y,Z]$ e $P = (Y^2-XZ,\ Z^2-X^2Y,\ X^3-YZ)$.

a) Mostre que P é um ideal primo de altura 2. (Sugestão: mostre que P é o núcleo do k-homomorfismo $R \to k[T]$ tal que $X \mapsto T^3$, $Y \mapsto T^4$, $Z \mapsto T^5$).

b) Mostre que P^2 não é um ideal primário. (Sugestão: mostre que $(X,Y,Z) \in \mathrm{Ass}(R/P^2)$).

<u>Observação</u>. O ideal P acima é o ideal das funções polinomiais

que se anulam sobre uma curva irredutível em k^3; esta curva é a mais simples dentre as curvas espaciais descritas por Macaulay [Mac].

5. Se $R = k[X_1,\ldots,X_n]$ e $I \subset R$ é um ideal radical, mostre que I é a interseção dos ideais máximos que o contêm.

(Sugestão: se $x \in \bigcap_{\underline{m} \supset I} \underline{m} \setminus I$, seja P um ideal de R máximo com respeito à propriedade de conter I e ser disjunto de $S = \{1, x, x^2, \ldots\}$; mostre que P é um ideal máximo, usando a forma de Zariski do teorema dos zeros: uma k-álgebra finitamente gerada é um corpo somente se for uma extensão algébrica de k).

6. Seja $R = k[X,Y,Z]$ e $I = (XZ, YZ)$. Mostre que $P = (X,Y)$ é um primo mínimo de R/I e que $\dim(R/P) \lneq \dim(R/I)$.

7. Determine a dimensão e um sistema de parâmetros para cada um dos módulos do Exercício 3.

8. Sejam $f, g \in k[X_1,\ldots,X_n]$ sem fator comum. Mostre que $\mathrm{alt}(f,g) = 2$ e (f,g) não admite primos imersos.

9. Seja M um R-módulo (finitamente gerado) e seja $I \subset R$ um ideal. Mostre que $\sqrt{0:M/IM} = \sqrt{I + (0:M)}$. (Sugestão: seja $m_1,\ldots,m_r$ um sistema de geradores de M e $x \in (0:M/IM)$. Então $xM \subset IM$ dá lugar a um sistema de equações nas (incógnitas" $m_1,\ldots,m_r$, com coeficientes $a_{ij} \in I$. Aplique a regra usual de Cramer).

10. Seja M um R-módulo (finitamente gerado) e $I \subset R$ um ideal tal que $M = IM$. Mostre:

(a) Existe um $x \in I$ tal que $(1-x)M = (0)$

(Sugestão: proceda de maneira análoga ao exercício anterior).

(b) (Lema de Nakayama). Se $I \subset$ radical de Jacobson de R, então $M = (0)$.

Deduza de (a):

(c) Se $R,\underline{m}$ é local, $x \in \underline{m}$ e M um R-módulo, então $\bigcap_{n\geq 0} x^n M = (0)$.

Capítulo II

M-sequências e módulos de Cohen-Macaulay

§1. M-sequências e profundidade.

No Capítulo I consideramos sistemas de parâmetros de um módulo M sobre um anel local $R,\underline{m}$. A propriedade característica destes sistemas era a de evitar primos associados "na dimensão" de certos módulos. Neste capítulo, queremos estudar as sequências cujos elementos evitam não só os primos "na dimensão", mas todos os primos associados.

Não há necessidade de supor R local, de maneira que voltamos à convenção inicial: R noetheriano e M finitamente gerado.

Definição II.1 - Uma sequência $x_1,\ldots,x_n \in R$ é uma M-sequência (ou uma sequência regular em M) se:

(i) $(x_1,\ldots,x_n)M \neq M$

(ii) $x_i \notin Z(M/(x_1,\ldots,x_{i-1})M)$, $i = 1,\ldots,n$.

Exemplo. Se $R,\underline{m}$ local, então, o comprimento de uma M-sequência a elementos em $\underline{m}$ é limitada por $\dim(M)$.

Isto segue imediatamente do critério para subsistema de parâmetros (Cap.I, Prop. I.13 (ii)).

<u>Definição II.2</u> - Seja $I \subset R$ um ideal e M um R-módulo. A <u>I-profundidade</u> de M é o supremo dos comprimentos de M-sequências a elementos em I. <u>Notação</u>: $\mathrm{prof}_I(M)$.

É concebível, em geral, que os comprimentos de M-sequências a elementos em I possam crescer indefinidamente. Queremos mostrar, em seguida, que se $IM \neq M$, tal fenômeno não acontece.

Primeiramente, observemos que M-sequências <u>máximas</u> (quer dizer, que não admitem extensões próprias) sempre existem. De fato, basta observar que se $x_i \in Z(M/(x_1,\ldots,x_{i-1})M)$ então a inclusão de ideais $(x_1,\ldots,x_{i-1}) \subset (x_1,\ldots,x_i)$ é própria, o que é imediato.

<u>Proposição II.3 - Se</u> $IM \neq M$, <u>duas M-sequências máximas a elementos em</u> I <u>têm mesmo comprimento</u>. <u>Em particular, se</u> $IM \neq M$, tem-se $\mathrm{prof}_I(M) < \infty$.

<u>Demonstração</u>: Primeiramente, se $x_1,\ldots,x_n$ é uma M-sequência a elementos em I, é fácil ver que

$$
\begin{aligned}
x_1,\ldots,x_n \text{ é máxima } &\Leftrightarrow I \subset Z(M/\underline{x}M), \quad \underline{x} = x_1,\ldots,x_n \\
&\Leftrightarrow I \subset (0) :_{M/\underline{x}M} a \quad \text{para algum } a \in M \setminus \underline{x}M, \\
&\Leftrightarrow (\underline{x}M :_M I)/\underline{x}M \neq (0) \\
&\Leftrightarrow \mathrm{Hom}_R(R/I, M/\underline{x}M) \neq (0).
\end{aligned}
$$

Assim, basta verificar que se $y_1,\ldots,y_m$ $(m \geq n)$ é outra M-sequência máxima, a elementos em I, então $\mathrm{Hom}_R(R/I,M/\underline{x}M) \simeq$ $\simeq \mathrm{Hom}_R(R/I,M/\underline{y}M)$, onde $\underline{y} = y_1,\ldots,y_n$.

A maneira mais rápida de verificar isto é mostrar que qualquer destes dois módulos é isomorfo a um módulo que depende somente de n, I e M, nomeadamente, $\mathrm{Ext}_R^n(R/I,M)$.

Como a intromissão destes módulos pode parecer pouco desejável a esta altura, oferecemos como alternativa aguardar o Capítulo III, §4, quando pode-se fazer uma demonstração diferente, usando o complexo de Koszul. Mas, a demonstração via Ext é tão simples - requer-se apenas o conhecimento de algumas propriedades mecânicas destes módulos - que queremos apresentá-la. Provaremos, em verdade, que para todo módulo M tal que $IM \neq M$ e toda M-sequência $x_1,\ldots,x_n$ em I, tem-se $\mathrm{Hom}_R(R/I,M/\underline{x}M) \simeq \mathrm{Ext}_R^n(R/I,M)$.

Por indução sobre n, naturalmente. Para $n = 0$, resulta de que Ext_R^o coincide com Hom_R. Suponhamos $n \geq 1$. Consideremos a sequência longa dos Ext correspondente à sequência curta $0 \to M \xrightarrow{x_1} M \to M/x_1M \to 0$ (multiplicação por x_1 em M):

$$\mathrm{Ext}^{n-1}(R/I,M) \to \mathrm{Ext}^{n-1}(R/I,M/x_1M) \to \mathrm{Ext}^n(R/I,M) \xrightarrow{x_1} \mathrm{Ext}^n(R/I,M).$$

Precisamos saber que I anula $\mathrm{Ext}^n(R/I,M)$, o que segue facilmente da definição de Ext via resolução injetiva da segunda variável. Assim, o último homomorfismo é nulo. Por outro lado, pela hipótese de indução,

$$\begin{aligned}\mathrm{Ext}^{n-1}(R/I,M) &\simeq \mathrm{Hom}(R/I,\ M/(x_1,\ldots,x_{n-1})M)\\ &\simeq ((x_1,\ldots,x_{n-1})M \underset{M}{:} I)/(x_1,\ldots,x_{n-1})M\\ &\subset ((x_1,\ldots,x_{n-1})M \underset{M}{:} x_n)/(x_1,\ldots,x_{n-1})M\\ &= (0).\end{aligned}$$

Obtemos, desta maneira, um isomorfismo

$$\mathrm{Ext}^n(R/I,M) \simeq \mathrm{Ext}^{n-1}(R/I,M/x_1M).$$

Novamente, pela hipótese de indução aplicada ao módulo M/x_1M e à (M/x_1M)-sequência $x_2,\dots,x_n$, tem-se, finalmente, $\mathrm{Ext}^n(R/I,M) \simeq \mathrm{Hom}(R/I,M/\underline{x}M)$. //

<u>Corolário II.4</u> - <u>Se</u> $IM \neq M$, <u>então</u> $\mathrm{prof}_I(M)$ <u>é o menor inteiro</u> $k \geq 0$ <u>tal que</u> $\mathrm{Ext}^k(R/I,M) \neq (0)$.

Existem várias notações diferentes para designar a profundidade de um módulo. Para evitar confusões, manteremos, sistematicamente, as seguintes convenções:

- $\mathrm{prof}_I(R)$ será substituida por $\mathrm{prof}(I)$, para indicar que há uma mudança de atitude ao considerar $\mathrm{prof}_I(R)$ como um invariante de I e não de R;
- se $R,\underline{m}$ é local, $\mathrm{prof}_{\underline{m}}(R)$ cederá lugar à notação $\mathrm{prof}(R)$ (assim, de acordo com a primeira convenção, $\mathrm{prof}(R) = \mathrm{prof}(\underline{m})$). Se R não é local, $\mathrm{prof}(R)$ carecerá de qualquer sentido.

<u>Exemplo</u>. Seja M um módulo e $\underline{x} = x_1,\dots,x_n$ uma M-sequência. Ponhamos $I = (\underline{x})$. Então, tem-se:

(i) $\mathrm{prof}_I(M) = n$

(ii) $\mathrm{prof}_P(M) = n$, para todo $P \in \mathrm{Ass}(M/\underline{x}M) \cap \mathrm{Sup}(M)$.

Com efeito, primeiramente, $IM \neq M$ por definição de M-sequência. Logo, toda M-sequência máxima em I tem mesmo comprimento. Mas, $x_1,\dots,x_n$ é obviamente uma M-sequência máxima em I já que $x_1,\dots,x_n$ geram I. Segue que $\mathrm{prof}_I(M) = n$. Seja, agora, $P \in \mathrm{Ass}(M/\underline{x}M)$. Então, $P \subset Z(M/\underline{x}M)$, logo $x_1,\dots,x_n$ é uma M-sequência máxima em P também. Por outro lado, $P \in \mathrm{Sup}(M) \Rightarrow PM \neq M$, logo $\mathrm{prof}_P(M) = n$ novamente.

Aplicando este exemplo ao caso $M = R$, obtemos que se $I \subset R$ é um ideal gerado por uma R-sequência de comprimento n, então ($\operatorname{prof}(I) = n$ e além disso) $\operatorname{prof}(P) = n$ para todo $P \in \operatorname{Ass}(R/I)$.

Em geral, a situação não é tão favorável. De qualquer modo, tem-se ao menos:

<u>Proposição II.5</u> - <u>Seja</u> M <u>um módulo</u>, $I \subset R$ <u>um ideal tal que</u> $IM \neq M$. <u>Então</u> $\operatorname{prof}_I(M) = \inf_{P \in \operatorname{Ass}(M/IM)} \{\operatorname{prof}_P(M)\}$.

<u>Demonstração</u>: $P \in \operatorname{Ass}(M/IM) \Rightarrow P \supset (0): M/IM \supset I$, logo $\operatorname{prof}_I(M) \leq \operatorname{prof}_P(M)$ para todo $P \in \operatorname{Ass}(M/IM)$. Basta, então, mostrar que $\operatorname{prof}_I(M) = \operatorname{prof}_P(M)$ para algum $P \in \operatorname{Ass}(M/IM)$. Ora, seja $n = \operatorname{prof}_I(M)$ ($<\infty$ pois $IM \neq M$), e $\underline{x} = x_1,\ldots,x_n$ uma M-sequência máxima em I. Então, $I \subset Z(M/\underline{x}M)$, logo $I \subset P'$ para algum $P' \in \operatorname{Ass}(M/\underline{x}M)$. Mas, $P' \supset (0): M/\underline{x}M \supset (0):M$. Assim, $P' \supset I + ((0):M)$. Como $\sqrt{(0):M/IM} = \sqrt{I+(0:M)}$ (vide Exercício 9 do Cap.I), resulta $P' \supset 0:M/IM$, logo P' contém um $P \in \operatorname{Ass}(R/(0:M/IM)) = \operatorname{Ass}(M/IM)$. Finalmente, $\operatorname{prof}_P(M) \leq \operatorname{prof}_{P'}(M) = n$ (a útlima igualdade pelo exemplo acima). //

Esta proposição e o exemplo de ideais gerados por M-sequências sugerem a seguinte definição.

Um ideal $I \subsetneq R$ é <u>equiprofundo</u> (ou <u>puro relativamente à profundidade</u>) se para todo $P \in \operatorname{Ass}(R/I)$ tem-se $\operatorname{prof}(P) = \operatorname{prof}(I)$.

<u>Observação</u>. Equiprofundidade é uma noção absoluta, isto é, depende só de I como ideal de R. Poderíamos definir "equiprofundi-

dade relativa" de I (relativa a um módulo M), mas a literatura corrente não consagrou esta terminologia.

Recordamos que um ideal $I \subset R$ é dito <u>equidimensional</u> (ou <u>puro</u>) se $\mathrm{alt}(P) = \mathrm{alt}(I)$ para todo $P \in \mathrm{Ass}(R/I)$. Em seguida, queremos relacionar estas duas noções. Para tal, observemos as seguintes desigualdades:

$\mathrm{prof}_I(M) \leq \mathrm{prof}_{I_P}(M_P)$,	para todo primo $P \supset I$ e todo módulo M
$\mathrm{prof}_{\underline{m}}(M) \leq \dim(M)$,	para todo módulo M sobre um anel local $R,\underline{m}$.

A primeira destas desigualdades é uma decorrência direta das definições, enquanto que a segunda já foi anunciada no exemplo após a Definição II.1. Usando estas desigualdades, obtemos, para todo ideal primo P num anel (não necessariamente local):

$$\mathrm{prof}(P) = \mathrm{prof}_P(R) \leq \mathrm{prof}_{P_P}(R_P) \leq \dim(R_P) = \mathrm{alt}(P).$$

Segue, usando a Proposição II.5, que $\mathrm{prof}(I) \leq \mathrm{alt}(I)$ para todo ideal $I \subset R$. Na próxima seção, estudaremos os anéis para os quais vale sempre a igualdade.

Em seguida, queremos examinar o comportamento da profundidade sob um homomorfismo de anéis. Contentar-nos-emos com um caso, já suficiente para muitas aplicações.

<u>Proposição II.6</u> - <u>Seja</u> $(R,\underline{m}) \xrightarrow{\varphi} (S,\underline{n})$ <u>um homomorfismo de anéis locais tal que</u> S <u>seja, por este homomorfismo, um</u> R-<u>módulo finitamente gerado</u>. <u>Se</u> N <u>é um</u> S-<u>módulo</u> (<u>finitamente gerado</u>), <u>tem-se</u> $\mathrm{prof}_{\underline{m}}(N) = \mathrm{prof}_{\underline{n}}(N)$.

<u>Demonstração</u>: A hipótese de que S é finitamente gerado como R-módulo implica em que $\varphi(\underline{m}) \subset \underline{n}$ (isto resulta da propriedade de "lying over" para extensões inteiras).

Seja $\underline{x} = x_1,\ldots,x_n \in \underline{m}$ uma N-sequência máxima, considerando N como R-módulo via $R \xrightarrow{\varphi} S$. É então evidente que $\varphi(x_1),\ldots,\varphi(x_n) \in \underline{n}$ é ainda N-sequência (N como S-módulo). Por outro lado, $\underline{m} \in \mathrm{Ass}_R(N/\underline{x}N)$. Logo, $N/\underline{x}N$ contém um R-submódulo $L \simeq R/\underline{m}$. Estendemos o R-homomorfismo $R \to L \subset N/\underline{x}N$ para um S-homomorfismo $S \to S\cdot L \subset N/\varphi(\underline{x})N$ da maneira óbvia (enviando $1 \in S$ no gerador cíclico de L). O núcelo deste S-homomorfismo é um ideal J de S, contendo $\varphi(\underline{m})S$. Como $\underline{n} = \sqrt{\varphi(\underline{m})S}$ (por que?), resulta $\sqrt{J} = \underline{n}$, isto é, J é $\underline{n}$-primário. Em outras palavras, $S\cdot L \simeq S/J$ é um módulo $\underline{n}$-primário, o que mostra que $\underline{n} \in \mathrm{Ass}_S(N/\varphi(\underline{x})N)$. Logo, $\varphi(\underline{x})$ é uma N-sequência máxima em $\underline{n}$. //

<u>Observação</u>. A proposição acima é usada, principalmente, no caso em que $S = R/I$, para algum ideal $I \subset R$ (<u>N.B</u>. Não exigimos que $\varphi: R \to S$ seja injetor na proposição).

Para terminar esta seção, examinaremos o comportamento da profundidade numa sequência exata de módulos.

<u>Proposição II.6 (bis)</u>. (R <u>noetheriano</u>) - <u>Seja</u> $0 \to N \to M \to K \to 0$ <u>uma sequência exata de módulos</u> (<u>isto é</u>, $N \subset M$ e $M/N \simeq K$). <u>Se</u> $I \subset R$ <u>é um ideal tal que</u> $IN \neq N$, $IM \neq M$ <u>e</u> $IK \neq K$, <u>então</u> <u>tem-se</u>:

(1) $\mathrm{prof}_I(M) > \mathrm{prof}_I(K) \Rightarrow \mathrm{prof}_I(N) = \mathrm{prof}_I(K) + 1$

(2) $\mathrm{prof}_I(M) < \mathrm{prof}_I(K) \Rightarrow \mathrm{prof}_I(N) = \mathrm{prof}_I(M)$

(3) $\mathrm{prof}_I(M) = \mathrm{prof}_I(K) \Rightarrow \mathrm{prof}_I(N) \geq \mathrm{prof}_I(M)$.

Demonstração: Podemos supor $\text{prof}_I(M) = 0$ ou $\text{prof}_I(K) = 0$, pois, do contrário, escolhemos um $x \in I$ tal que $x \notin Z(M)$ e $x \notin Z(K)$; neste caso, obtemos nova sequência exata

$$0 \to N/xN \to M/xM \to K/xK \to 0$$

(vide demonstração do Lema III.17, Cap.III!), onde as profundidades baixaram de uma unidade.

Primeiro, $\text{prof}_I(M) = 0$. Então, $\text{prof}_I(M) \leq \text{prof}_I(K)$, isto é, estamos no caso (2) ou (3). Basta verificar que se $\text{prof}_I(K) > 0$, então $\text{prof}_I(N) = 0$. Ora, seja $a \in M$ tal que $Ia = 0$. Como $\text{prof}_I(K) > 0$, $a \in N$. Logo, $I \subset Z(N)$.

Em seguida, o caso $\text{prof}_I(K) = 0$. Então, estamos em (1) ou (3). Basta, então, verificar que $\text{prof}_I(M) > 0 \Rightarrow \text{prof}_I(N) = 1$. É claro que $\text{prof}_I(M) > 0 \Rightarrow \text{prof}_I(N) > 0$. Seja $x \notin Z(M)$ e escolhamos um $a \in M$ tal que $Ia \subset N$ ($\text{prof}_I(K) = 0$ por hipótese). Então $xa \notin xN$, já que $x \notin Z(M)$, e, além disso, $I.xa = x \cdot Ia \subset \subset xN$. Isto mostra que $\{x\}$ é uma N-sequência máxima em I. //

Observação. A proposição acima é de grande utilidade técnica, principalmente em argumentos indutivos. Pode-se ter, tipicamente, a seguinte situação (para simplificar, suporemos $R, \underline{m}$ local). M é um R-módulo, munido de uma "apresentação" $0 \to Z \to F \to M \to 0$, com F um módulo livre (vide Cap.III, §1, para maiores detalhes sobre apresentações). Ora, $\text{prof}(F) = \text{prof}(R)$ (isto é uma consequência imediata da proposição acima, mas pode ser visto diretamente). Assim, se tivermos $\text{prof}(M) < \text{prof}(R)$, concluiremos pela Proposição II.6 (bis) que $\text{prof}(Z) = \text{prof}(M) + 1$. Isto permite obter módulos de profundidades crescentes até atingir $\text{prof}(R)$, que funciona como uma barreira natural. Isto não significa, é claro, que $\operatorname{prof}(M) \leq \operatorname{prof}(R)$ para todo módulo M. Mas, se $\operatorname{prof}(M) \leq \operatorname{prof}(R)$ (que é sempre o caso se a dimensão homológica de M é finita; vide Cap.III, §3), então, pelo processo acima, chega-se a um módulo M' tal que $\operatorname{prof}(M') = \operatorname{prof}(R)$. Se, além disso, R é um anel de Cohen-Macaulay, então M' é um módulo de Cohen-Macaulay (vide seção seguinte).

Este processo permite, grosso modo, transferir propriedades de um módulo qualquer a um módulo "aproximadamente" livre.

§2. Módulos de Cohen-Macaulay

Na seção anterior vimos que, dados um módulo M e um ideal I tais que $IM \neq M$, existe um primo $P \supset \operatorname{Ass}(M/IM)$ tal que $\operatorname{prof}_I(M) = \operatorname{prof}_P(M)$ (vide demonstração da Prop.II.5). Em verdade, uma análise cuidadosa mostra que existe um primo satisfazendo $\operatorname{prof}_I(M) = \operatorname{prof}_{I_P}(M_P)$ (o primo P encontrado na demonstração da Prop.II.5 já serve). Destacaremos este fato como um lema.

<u>Lema II.7</u> - <u>Para todo módulo</u> M <u>e todo ideal</u> I <u>tais que</u> $IM \neq M$, <u>existe um primo</u> $P \in \operatorname{Ass}(M/IM)$ <u>tal que</u> $\operatorname{prof}_I(M) = \operatorname{prof}_{I_P}(M_P)$.

O segundo resultado técnico de que faremos uso é um lema sobre o crescimento da profundidade mediante adjunção de novos elementos. Poderíamos dar uma prova elementar deste resultado, mas optaremos por remeter o leitor ao Capítulo III, §4, Proposição III.34, onde uma prova elegante é dada.

Lema II.8 - Seja M um módulo e $I \subset R$, um ideal, tais que $IM \neq M$. Se $a \in R$ é um elemento pertencente ao radical de Jacobson de R, tem-se:

$$\mathrm{prof}_{(I,a)}(M) \leq 1 + \mathrm{prof}_I(M).$$

Queremos destacar os anéis para os quais $\mathrm{prof}(I) = \mathrm{alt}(I)$ para todo ideal $I \subset R$. Pomos, mais geralmente:

Definição e Proposição II.9 - Um módulo M é chamado módulo de Cohen-Macaulay (abrev.: C-M) se satisfaz a uma das condições equivalentes seguintes:

(M_1) $\mathrm{prof}_{P_P}(M_P) = \dim(M_P)$, para todo $P \in \mathrm{Sup}(M)$.

(M_2) $\mathrm{prof}_{\underline{m}_{\underline{m}}}(M_{\underline{m}}) = \dim(M_{\underline{m}})$, para todo $\underline{m} \in \mathrm{Sup}(M)$ com $\underline{m}$ ideal máximo.

(M_3) $\mathrm{prof}_{\underline{m}}(M) = \mathrm{alt}(\underline{m}/(0:M))$, para todo $\underline{m} \in \mathrm{Sup}(M)$ com $\underline{m}$ ideal máximo.

(M_4) $\mathrm{prof}_P(M) = \mathrm{alt}(P/(0:M))$, para todo $P \in \mathrm{Sup}(M)$.

(M_5) $\mathrm{prof}_I(M) = \mathrm{alt}(I/(0:M))$, para todo ideal $I \supset 0:M$.

Observação. (M_1) e (M_2) são condições locais; (M_3)-(M_5) são condições globais - a altura sendo calculada no anel $R/(0:M)$.

Demonstração: $(M_1) \Rightarrow (M_2)$. Trivial.

$(M_2) \Rightarrow (M_3)$. Com $\underline{m} \in \mathrm{Sup}(M)$ tem-se $\underline{m}M \neq M$. Logo, pelo Lema II.7, $\mathrm{prof}_{\underline{m}}(M) = \mathrm{prof}_{\underline{m}_{\underline{m}}}(M_{\underline{m}})$. Por outro lado, $\dim(M_{\underline{m}}) = \dim(R_{\underline{m}}/(0:M_{\underline{m}})) = \mathrm{alt}(\underline{m}_{\underline{m}}/(0:M_{\underline{m}})) = \mathrm{alt}(\underline{m}/(0:M))_{\underline{m}} = \mathrm{alt}(\underline{m}/(0:M))$.

Assim, $\mathrm{prof}_{\underline{m}}(M) = \mathrm{alt}(\underline{m}/(0:M))$.

$(M_3) \Rightarrow (M_4)$. Pelo Lema II.7 e pela invariância da altura de um idéal primo por localização noutro primo maior, podemos supor que $R,\underline{m}$ é local. Suponhamos a existência de um infrator P, que já pode ser escolhido máximo possível com respeito à infração. Por hipótese, $P/(0:M) \neq \underline{m}/(0:M)$; logo, $P \neq \underline{m}$. Seja $a \in \underline{m} \setminus P$. Pelo Lema II.8, $\mathrm{prof}_{(P,a)}(M) \leq 1 + \mathrm{prof}_P(M)$. Por outro lado, temos $\mathrm{alt}((P,a)/0:M) \geq 1 + \mathrm{alt}(P/0:M)$. Segue que

$$\mathrm{prof}_{(P,a)}(M) \lneq \mathrm{alt}((P,a)/0:M),$$

logo $(P,a) \supsetneq P$ é um infrator maior; contradição.

$(M_4) \Rightarrow (M_5)$. Resulta da Proposição II.5 e da propriedade análoga para a altura.

$(M_5) \Rightarrow (M_1)$. Como vimos antes, dado $P \in \mathrm{Sup}(M)$, tem-se

$$\mathrm{prof}_P(M) \leq \mathrm{prof}_{P_P}(M_P) \leq \dim(M_P) = \dim(R_P/(0:M_P)) = \mathrm{alt}(P/(0:M)).$$

A igualdade dos extremos acarreta a igualdade de todos os termos intermediários. //

A condição (M_1) (ou (M_2)) implica em que toda localização de um módulo C-M é C-M.

Um anel R é dito de Cohen-Macaulay se o for como R-módulo. Além disso, se $R,\underline{m}$ é um anel local, dizer que M é C-M significa que $\mathrm{prof}_{\underline{m}}(M) = \dim(M)$.

Módulos C-M admitem propriedades bastante especiais. Comecemos por analisar os primos associados de um tal módulo. Para isto, usaremos o seguinte resultado geral.

<u>Proposição II.10 - Seja</u> $R,\underline{m}$ <u>um anel local</u>, $M \neq (0)$ <u>um</u> R-<u>módulo</u>. <u>Então</u>, $\text{prof}_{\underline{m}}(M) \leq \dim(R/P)$ <u>para todo</u> $P \in \text{Ass}(M)$.

<u>Demonstração</u>: Procedamos por indução sobre $\dim(R/P)$ (que é $<\infty$ pelo Cap.I). Se $\dim(R/P) = 0$, $P = \underline{m}$. Mas, $\underline{m} \in \text{Ass}(M) \Rightarrow$ $\Rightarrow \text{prof}_{\underline{m}}(M) = 0$. Suponhamos $\dim(R/P) \geq 1$. Podemos supor $\text{prof}_{\underline{m}}(M) \geq 1$, do contrário não há nada a provar. Seja $x \in \underline{m}$ tal que $x \notin Z(M)$. Em particular, $x \notin P$. Afirmamos a existência de um primo $P' \in \text{Ass}(M/xM)$ tal que $(P,x) \subset P'$. Com efeito, $P = (0):a$, para algum $a \in M\setminus\{0\}$. Como $\bigcap_{n\geq 0} x^n M = (0)$ (vide Exercício 10 do cap.I), existe um $r \geq 0$ tal que $a \in x^r M \setminus x^{r+1}M$. Digamos, $a = x^r b$, com $b \in M\setminus xM$. Ora, como $x \notin Z(M)$, resulta $Pb = (0)$. Assim, $(P,x)\cdot b \subset xM$, logo $(P,x) \subset P'$, para algum $P' \in \text{Ass}(M/xM)$.

Voltando à demonstração propriamente, tem-se $\dim(R/P') \lneqq$ $\lneqq \dim(R/P)$. Pela hipótese indutiva, temos

$$\begin{aligned}\text{prof}_{\underline{m}}(M) &= \text{prof}_{\underline{m}}(M/xM)+1 \leq \dim(R/P')+1 \\ &\leq \dim(R/P) - 1+1 = \dim(R/P).\end{aligned}$$

//

<u>Observação</u>. A proposição acima admite a seguinte versão global: (R noetheriano) Se $P \in \text{Ass}(M)$ e se $\underline{m} \supset P$, então $\text{prof}_{\underline{m}}(M) \leq$ $\leq \dim(R/P)$.

Aplicando a proposição a um módulo C-M, obtemos:

<u>Corolário II.11 - Seja</u> $R,\underline{m}$ <u>um anel local e</u> M <u>um</u> R-<u>módulo</u> C-M. <u>Então</u>, $\dim(R/P) = \dim(M)$ <u>para todo</u> $P \in \text{Ass}(M)$. <u>Consequentemente, para um tal módulo</u>, $\text{Ass}(M) = \text{Min}(M)$.

Demonstração: Resulta das desigualdades

$$\operatorname{prof}_{\underline{m}}(M) \leq \dim(R/P) \leq \dim(M). \quad //$$

Observação. O corolário pode ser globalizado nos seguintes termos: (R noetheriano). Se M é um R-módulo C-M tal que $\dim(M) = \dim(M_{\underline{m}})$ para todo ideal máximo $\underline{m} \in \operatorname{Sup}(M)$, então $\dim(R/P) = \dim(M)$ para todo $P \in \operatorname{Ass}(M)$ (consequentemente, $\operatorname{Ass}(M) = \operatorname{Min}(M)$ para um tal módulo).

Corolário II.12 - Seja $R,\underline{m}$ um anel local e M, um módulo C-M. Tem-se:

(i) Todo sistema de parâmetros de M é uma M-sequência.

(ii) Se $\underline{x} = x_1,\ldots,x_k$ é parte de um sistema de parâmetros de M, então $M/\underline{x}M$ é C-M e $\dim(M/\underline{x}M) = \dim(M)-k$.

Demonstração: É evidente por indução sobre o comprimento de um subsistema de parâmetros e usando as igualdades seguintes para um módulo N:

$\dim(N/xN) = \dim(N) - 1$, se x é um parâmetro em N;

$\operatorname{prof}_{\underline{m}}(N/xN) = \operatorname{prof}_{\underline{m}}(N) - 1$, se $x \notin Z(N)$. //

Uma das propriedades básicas de um módulo C-M está contida no próximo resultado.

Teorema II.13 ("Codimensão e dimensão complementares") - Seja R um anel noetheriano e M, um R-módulo de Cohen-Macaulay tal que $\dim(M) = \dim(M_{\underline{m}})$, para todo ideal máximo $\underline{m} \in \operatorname{Sup}(M)$. Então, para todo primo $P \in \operatorname{Sup}(M)$,

$$\dim(M) = \dim(M_P) + \dim(M/PM).$$

<u>Demonstração</u>: A desigualdade $\dim(M) \geq \dim(M_P) + \dim(M/PM)$ vale para qualquer módulo M e qualquer primo P (em caso de hesitação, passe aos anuladores!). Em seguida, tomemos um ideal máximo $\underline{m} \supset P$ e suponhamos o resultado válido para $M_{\underline{m}}$. Tem-se, por hipótese:

$$\begin{aligned}\dim(M) = \dim(M_{\underline{m}}) &= \dim(M_{P_{\underline{m}}}) + \dim(M_{\underline{m}}/PM_{\underline{m}}) \\ &= \dim(M_P) + \dim(M/PM)_{\underline{m}} \\ &\leq \dim(M_P) + \dim(M/PM).\end{aligned}$$

Logo, podemos supor R local, com ideal máximo $\underline{m}$.

O plano é mostrar que existe um subsistema de parâmetros $\underline{x} = x_1,\dots,x_r$ de M tal que $\dim(M_P) = r$ e tal que $P \in \mathrm{Ass}(M/\underline{x}M)$.

Para tal, tomamos $\underline{x} = x_1,\dots,x_r$ um subsistema de parâmetros de M (= M-sequência) contido em P e máximo com respeito a esta inclusão. Segue que P está contido em algum primo associado de $M/\underline{x}M$. Por outro lado, $P \in \mathrm{Sup}(M) \cap \mathrm{Sup}(R/(\underline{x})) = \mathrm{Sup}(M/\underline{x}M)$, logo P contém algum primo associado de $M/\underline{x}M$. Mas, como os primos em $\mathrm{Ass}(M/\underline{x}M)$ são todos mínimos (Cor.II.11 e Cor.II.12 (ii)), resulta que $P \in \mathrm{Ass}(M/\underline{x}M)$ e, portanto, $\dim(M/PM) = \dim(R/P) = \dim(M/\underline{x}M) = \dim(M)-r$.

Finalmente, como $x_1,\dots,x_r$ é uma M-sequência em P e M é C-M, resulta $\dim(M_P) = \mathrm{prof}_P(M) \geq r$. Consequentemente, $\dim(M) = r + \dim(M/PM) \leq \dim(M_P) + \dim(M/PM)$, que é a desigualdade (decisiva) procurada.

//

<u>Corolário II.14</u> (R noetheriano) - <u>Se</u> M <u>é um módulo</u> C-M <u>tal que</u> $\dim(M) = \dim(M_{\underline{m}})$ <u>para todo ideal máximo</u> $\underline{m} \in \mathrm{Sup}(M)$, <u>então o anel</u> $S = R/(0{:}M)$ <u>satisfaz a igualdade</u>

$$\dim(S) = \mathrm{alt}(P) + \dim(S/P),$$

<u>para todo primo</u> $P \subset S$.

<u>Demonstração</u>: Trata-se de mera reformulação do resultado anterior.
//

<u>Importante</u>! (Digamos, R local). Se M é um módulo C-M fiel (isto é, $(0){:}M = (0)$), resulta que em R vale

$$\dim(R) = \mathrm{alt}(P) + \dim(R/P)$$

para todo primo $P \subset R$. Em algumas situações, isto é quase tão bom quanto saber que o próprio R é Cohen-Macaulay. Por outro lado, existem anéis locais (domínios, de dimensão 2 e profundidade 1) que não admitem módulos C-M fiéis. O problema da existência de tais módulos é conhecido como questão dos "módulos C-M máximos" (vide Cap.IV).

Para concluir a lista de propriedades de módulos C-M, arquivaremos o seguinte resultado.

<u>Corolário II.15</u> - <u>Seja</u> R <u>um anel</u> C-M <u>equicodimensional</u> (<u>isto significa que todos os ideais máximos têm mesma altura</u>). <u>Se</u> $I \subset R$ <u>é tal que</u> R/I <u>é</u> C-M, <u>então</u> I <u>é um ideal equidimensional</u> (= <u>puro</u>).

<u>Demonstração</u>: Segue facilmente dos resultados precedentes.
//

Em seguida, alguns exemplos para ilustrar a teoria.

Exemplos. (1) Todo anel de dimensão 0 é C-M; todo domínio de dimensão 1 é um anel C-M.

(2) Todo domínio local normal (= inteiramente fechado) de dimensão 2 é um anel C-M (o ponto determinante aqui é que os ideais principais num domínio normal são puros).

(3) Dados inteiros $0 \leq r \leq d$, existe um anel local de dimensão d e profundidade r. Por exemplo, podemos tomar

$$R = (k[X_o,\ldots,X_r,\ldots,X_d]/(X_r^2,X_rX_{r+1},\ldots,X_rX_d))_{(X_o,\ldots,X_d)}.$$

Assim, existem anéis que são "arbitrariamente" não C-M.

(4) Se R é um anel C-M, então $R[X]$ é C-M.

(Demonstração: Se $P \subset R[X]$ é um primo, $R[X]_P$ é uma localização de $R_{P\cap R}[X]$. Logo, podemos supor R local, de ideal máximo $\underline{m} = P \cap R$. Neste caso, tem-se $R[X]/\underline{m}R[X] \simeq R/\underline{m}[X]$, um anel de polinômios sobre um corpo. Logo, $P = \underline{m}R[X]$ ou $P = (\underline{m},f(X))$, com $f(X) \in R[X]$ mônico de grau >0. Por hipótese, $\mathrm{prof}_{\underline{m}}(R) = \dim(R)$. Seja $\underline{x} = x_1,\ldots,x_d$ uma R-sequência máxima em $\underline{m}$. É fácil ver que $x_1,\ldots,x_d$ é uma $R[X]$-sequência: para mostrar que $x_i \notin Z(R[X]/(x_1,\ldots,x_{i-1})R[X])$, usamos o isomorfismo $R[X]/(x_1,\ldots,x_{i-1})R[X] \simeq (R/(x_1,\ldots,x_{i-1}))[X]$ e reduzimos o problema a mostrar que, dado um anel S e um $a \in S$ tal que $a \in Z(S[X])$, então $a \in Z(S)$, o que é imediato.

Segue que $\underline{x}$ é $R[X]_P$-sequência e, portanto, $\mathrm{prof}_{PR[X]_P}(R[X]_P) \geq d$. Analisemos os casos $P = \underline{m}R[X]$ e $P = (\underline{m},f)$ separadamente. Se $P = \underline{m}R[X]$, basta mostrar que $\dim(R[X]_{\underline{m}[X]}) \leq$

$\leq \dim(R)$, já que acabamos de ver que $\mathrm{prof}(R[X]_{\underline{m}[X]}) \geq d = \dim(R)$. Ora, sabemos da teoria de anéis de polinômios que $\mathrm{alt}(\underline{m}[X]) =$ $= \mathrm{alt}(\underline{m})$. Logo $\dim(R[X]_{\underline{m}[X]}) = \mathrm{alt}(\underline{m}[X]_{\underline{m}[X]}) = \mathrm{alt}(\underline{m}[X]) = \dim(R)$.

No segundo caso, como f é mônico, $f \notin Z(R[X]_{p}/\underline{x}R[X]_{p})$. Logo, $\mathrm{prof}_{PR[X]_p}(R[X]_p) \geq d+1 = \dim(R)+1 = \dim(R[X]) \geq \dim(R[X]_p)$, como queríamos).

(5) (<u>Teorema de Macaulay</u>). <u>Se</u> k <u>é um corpo</u>, $k[X_1,\ldots,X_n]$ <u>é</u> C-M.

Isto resulta, imediatamente, de (4). Este resultado tornou-se célebre mais pelo método usado por Macaulay, do que pelo que afirma. Macaulay provou, em verdade, que $k[X_1,\ldots,X_n]$ satisfaz a seguinte propriedade: se $I \subset k[X_1,\ldots,X_n]$ é um ideal tal que $\dim(k[X_1,\ldots,X_n]/I) = n-h$ e tal que $\mu(I) \leq h$ (lembre: μ = número mínimo de geradores) então I é puro.

Este resultado compõe-se, no fundo, de dois resultados:

(i) $\dim(k[X_1,\ldots,X_n]/I) = \dim(k[X_1,\ldots,X_n]) - \mathrm{alt}(I)$;

(ii) ("Teorema clássico da pureza"). Se $I \subset k[X_1,\ldots,X_n]$ é tal que $\mu(I) \leq \mathrm{alt}(I)$, então I é puro.

Ideais satisfazendo $\mu(I) \leq \mathrm{alt}(I)$ (log, $=$) são chamados classicamente de <u>ideais da classe principal</u>. No início do século, mostrar que um ideal da classe principal em $k[X_1,\ldots,X_n]$ era puro, certamente tratava-se de um feito. Hoje, a maneira mais elegante de demonstrar o teorema de Macaulay da pureza é "fatorá-la" pelo Exemplo dado após o Corolário II.4, reduzindo-a às etapas seguintes: (1) $k[X_1,\ldots,X_n]$ é C-M, como no Exemplo (4) acima; (2) Logo, $\mathrm{prof}(I) = \mathrm{alt}(I)$; (3) $\mathrm{prof}(I) = \mu(I) \Rightarrow I$ gerado por

R-sequência; (4) Usar o resultado do Exemplo após o Corolário II.4. Destas etapas, a única estranha à presente teoria é (3); mas isto pode ser demonstrado de maneira razoavelmente elementar usando as chamadas transformações elementares, aplicadas a um conjunto de geradores de I, e um "lema de esquiva" popularíssimo (vide Exercício 2 do Cap.I).

Finalmente, apontemos o fato de que um anel satisfazendo o teorema "abstrato" da pureza (isto é, todo ideal da classe principal é puro) já é C-M. Assim, o teorema "abstrato" da pureza é equivalente à propriedade de C-M!

(6) Módulos perfeitos.

Esta é a principal classe de módulos C-M (por exemplo, todo módulo C-M sobre $R = k[X_1,\dots,X_n]$ - mais geralmente, R regular, cf. Capítulo III, §1 - é um módulo perfeito). Estudaremos tais módulos no Capítulo III, §3. O exemplo primordial de um módulo perfeito é um módulo R/I, onde I é o ideal das relações dos invariantes fundamentais pela ação de um grupo. Quase todos estes ideais são de tipo "determinantal" e têm sido objeto de intenso estudo, tanto no século passado como mais recentemente.

(7) C-M sob passagem mediante um homomorfismo $R \to S$.

Seja $(R,\underline{m}) \xrightarrow{\varphi} (S,\underline{n})$ um homomorfismo de anéis locais tais que S é R-módulo finitamente gerado. Se N é um S-módulo (f.g.), então N é C-M como S-módulo $\Leftrightarrow$ N é C-M como R-módulo.

Com efeito, pela Proposição II.6, $\mathrm{prof}_{\underline{m}}(N) = \mathrm{prof}_{\underline{n}}(N)$. Por outro lado, é fácil ver que $\dim_S(N) = \dim_R(N)$ (Sugestão: mostre que $R/(0:_R N) \hookrightarrow S/(0:_S N)$ e que $R/(0:_S N)$ é finitamente gerado sobre $R/(0:_R N)$, por consideração da fatoração $R/(0:_R N) \to S/(0:_R N)\cdot S \to S/(0:_S N))$.

§3. Interpretação geométrica.

1. M-sequências versus interseções completas.

A noção geométrica por trás de M-sequência é a de interseção completa, em suas diversas variações. A importância (ou o reconhecimento da importância) deste conceito remonta, provavelmente, a M. Nöther [Nö] que introduziu o estudo das "interseções residuais".

Após alguma controvérsia, causada pelo tom obscuro dos argumentos geométricos em voga no século passado, presentemente reconhecemos a existência de dois conceitos diferentes:

(i) Uma variedade algébrica $V \subset k^n$ (resp. $\subset \mathbb{P}^n(k)$) de dimensão d é uma interseção completa como conjunto se existem polinômios (resp. polinômios homogêneos) $f_1,\ldots,f_{n-d} \in k[X_1,\ldots,X_n]$ (resp. $\in k[X_0,X_1,\ldots,X_n]$) tais que V é o conjunto dos zeros simultâneos destes polinômios.

(ii) Uma variedade algébrica $V \subset k^n$ (resp. $\subset \mathbb{P}^n(k)$) é uma interseção completa no sentido estrito (ou de ideais) se o ideal dos polinômios que se anulam sobre V é gerado por $n-d$ polinômios (resp. $n-d$ polinômios homogêneos).

Existe vasta literatura sobre o assunto (vide [Ge], [Oh] e [Va_2]).

<u>Exemplo</u>. Considere a variedade afim $V \subset k^3$ dada pelos zeros simultâneos de $Y-X^2$ e $Z-X^3$. Temos diante dos olhos um objeto bastante concreto: V é a curva espacial com equações paramétricas $x = t$, $y = t^2$, $z = t^3$.

É fácil ver que $k[X,Y,Z]/(Y-X^2,Z-X^3) \simeq k[X]$, pelo homomorfismo $k[X,Y,Z] \to k[X]$ tal que $X \mapsto X$, $Y \mapsto X^2$, $Z \mapsto X^3$ (isto é a contrapartida algébrica da afirmação "paramétrica" anterior). Segue que $(Y-X^2,Z-X^3)$ é um ideal primo e coincide, portanto, com o ideal dos polinômios se anulando em V. Como $\dim(V)$ $(= \dim(k[X,Y,Z]/(Y-X^2,Z-X^3)) = \dim(k[X])) = 1$, resulta que V é uma interseção completa no sentido estrito.

Queremos deixar claro que a passagem à curva projetiva associada $\bar{V} \subset \mathbb{P}^3(k)$ é um processo sutil, ainda que $\bar{V} \setminus V$ seja um conjunto <u>finito</u> de pontos ("os pontos no infinito"). Assim, no exemplo anterior, $\bar{V}$ <u>não é</u> interseção completa no sentido estrito mas <u>é</u> interseção completa como conjunto.

Para verificar este fato, é preciso manipular um pouco as equações de V. Começamos, ingenuamente, por homogeneizar, individualmente, os polinômios $Y-X^2$, $Z-X^3$ (topologicamente, estamos compactificando, separadamente, as superfícies cuja interseção é V). Assim procedendo, obtemos $YW-X^2$, ZW^2-X^3, cujos zeros admitem $X = W = 0$ como componente extra. Isto estava fora dos nossos planos, de modo que devemos esforçar-nos um pouco mais.

Ponhamos $J = (YW-X^2, ZW^2-X^3) \subset R = k[X,Y,Z,W]$. Verifica-se, por manipulação, que $W(XY-ZW) \in J$ e $W(XZ-Y^2) \in (J, XY-ZW)$.

Logo, $I = (XY-ZW, XZ-Y^2, YW-X^2) \subset J:W^2$. Como $W^2 \notin J$, I está contido num primo associado P de R/J; P é, então, o candidato para o ideal de $\bar{V}$.

Mas, a situação é um pouco melhor. Mostraremos, em verdade, que $I = P$. (Como primeira aproximação, é fácil ver que R/I admite como primo associado o núcleo do homomorfismo $k[X,Y,Z,W] \to k[T,U]$, $X \mapsto T^2U$, $Y \mapsto TU^2$, $W \mapsto T^3$, $Z \mapsto U^3$; esta é a "parametrização" do cone projetante de $\bar{V}$).

Isto decorre das seguintes observações:

(i) Em $\bar{R} = R/(W-1)$, $\bar{I} = (I,W-1)/(W-1)$ é primo.

Com efeito, tem-se $(I,W-1) = (XY-Z, Y-X^2, W-1) = $
$= (Z-X^3, Y-X^2, W-1)$. Logo, $(I,W-1)$ é um ideal primo em R e, como contém $W-1$, sua imagem $\bar{I}$ em $\bar{R}$ é um ideal primo.

(ii) $W \notin Z(R/I)$.

De fato, seja $F \in I:W$. Reduzindo módulo $(W-1)$, encontramos $\bar{F} \in \bar{I}$, logo $F \in (I,W-1)$. Seja $F = F_1 + F_2(W-1)$, com $F_1 \in I$. Como $FW \in I$, vem $F_2(W-1)W \in I$. Mas $W-1$ não pertence a nenhum dos primos associados de R/I, já que estes são homogêneos (vide Exercício 9). Então, $F_2W \in I$. Repetimos o argumento anterior para F_2, etc. Desta forma, obtemos que $F \in \bigcap_{n\geq 1} (I,(W-1)^n)$, o que é impossível a menos que $F \in I$.

(iii) Seja $R_W = k[X,Y,Z,W][\frac{1}{W}]$. Então IR_W é primo.

Isto resulta de (i). Com efeito, usando o isomorfismo $\bar{R} \xrightarrow{\sim} k[\frac{X}{W},\frac{Y}{W},\frac{Z}{W}] \subset k(X,Y,Z,W)$ = corpo de frações de R, vemos que $\bar{R}$ identifica-se com um subanel de R_W. Mais precisamente, como

$R_W = k[\frac{X}{W},\frac{Y}{W},\frac{Z}{W}][W][\frac{1}{W}]$ e W é transcendente sobre $k[\frac{X}{W},\frac{Y}{W},\frac{Z}{W}]$ (por que?), resulta que R_W é a localização $\bar{R}[W]_W$ do anel de polinômios $\bar{R}[W]$ (a uma variável, sobre $\bar{R}$). Das propriedades usuais de anéis de polinômios, $I\bar{R}[W]$ é primo. Como $W \notin \bar{I}$, $\bar{I}R_W$ é primo em R_W. Por outro lado, é imediato verificar que $\tilde{I}R_W = IR_W$, como queríamos.

(iv) Conclusão: de (ii) e (iii) resulta que I é primo.

Os primos associados de R/J são (X,W) e I. Os zeros de I constituem a variedade $\bar{V}$ procurada e, como I é primo, resulta que I é o ideal de $\bar{V}$. Como $XY-ZW$, $XZ-Y^2$, $YW-X^2$ constituem, claramente, um sistema mínimo de geradores de I, $\bar{V}$ não é interseção completa no sentido estrito.

Finalmente, pode-se verificar que $I^2 \subset I'$, onde $I' = (XZ-Y^2, X(YW-X^2)-W(ZW-XY))$, por exemplo. Então, $\sqrt{I'} = I$ e, portanto, $\bar{V}$ é uma interseção completa como conjunto.

<u>Observação</u>. O anel R/I acima é C-M. De fato, se $P \supset I$ é um primo $\neq (X,Y,Z,W)$, então alguma variável $\notin P$. Localizando em P, vê-se então diretamente que $\mu(I_P) \leq 2$, e que I_P é gerado por uma R_P-sequência. Como R_P é C-M, R_P/I_P é então C-M (Cor.II.12). Assim, o único problema é a localização em (X,Y,Z,W). Queremos $\text{prof}(R/I)_{(X,Y,Z,W)} = 2$. Ora, por exemplo, $W \notin I_{(X,Y,Z,W)}$. Deixamos como exercício a verificação de que $(X,Y,Z,W) \notin$ $\notin \text{Ass}(R_{(X,Y,Z,W)}/(W,I)_{(X,Y,Z,W)})$.

No Capítulo III, §3, veremos que R/I é um módulo perfeito. Disso segue-se, em geral, que R/I é C-M.

2. A propriedade de C-M versus normalidade.

Suponhamos, para simplificar as idéias, que R é um domínio local, com ideal máximo $\underline{m}$ (ou graduado, com radical graduado $\underline{m}$). Vimos que se R é normal e de dimensão 2, então R é C-M (Cap.II, §2, Exemplo (2)). A recíproca é falsa, o que se vê facilmente com $R = S[X]_{\underline{m}}$, onde $\underline{m} = (\underline{n}, X)$, com $S, \underline{n}$ domínio local de dimensão 1 não normal (por exemplo, S = anel local de um ponto singular de uma curva). A recíproca falha simplesmente pela existência de "singularidade em codimensão 1". Em verdade, por um teorema popular [Se]), sabe-se que R é normal se e só se têm lugar as condições seguintes:

(S_2) $\quad \mathrm{alt}(P) \geq 2 \Rightarrow \mathrm{prof}_{P_P}(R_P) \geq 2$

(R_1) $\quad \mathrm{alt}(P) \leq 1 \Rightarrow R_P$ é regular (vide Cap.III, §1).

Disso concluimos facilmente que:

Se R é um domínio, então "C-M" + "(R_1)" $\Rightarrow$ "normal".

Se $\dim(R) = 2$, "C-M" + (R_1) $\Leftrightarrow$ "normal".

A importância geométrica destes fatos decorre do seguinte resultado (vide [Mu]): Se $V \subset \mathbb{P}^n$ é uma variedade projetiva não singular, as seguintes condições são equivalentes:

(i) Para toda aplicação biregular

$$\begin{array}{ccc} W & \subset & \mathbb{P}^m(k) \\ \downarrow & & \vdots \\ V & \subset & \mathbb{P}^n(k) \end{array} \qquad (W \not\subset \mathbb{P}^r(k) \subset \mathbb{P}^m(k), \quad r \lneq m)$$

induzida por uma projeção linear de $\mathbb{P}^m$ em $\mathbb{P}^n$, tem-se $m = n$.*

(ii) O anel de coordenadas homogêneas de V é normal (diz-se, neste caso, que V é <u>aritmeticamente normal</u>).

Usando a caracterização anterior, temos assim que uma curva não singular $V \subset \mathbb{P}^3$ não pode ser obtida como projeção linear biregular de uma curva num espaço projetivo $\mathbb{P}^m$, $m \geq 4$, se e só se o anel do cone projetante de V, localizado na origem, é C-M.

<u>Exemplo</u>. Consideremos a quártica projetiva $W \subset \mathbb{P}^4$, imagem biregular de $\mathbb{P}^2$ pela aplicação

$$(t:u) \longmapsto (\underset{X_o}{t^4} : \underset{X_1}{t^3u} : \underset{X_2}{t^2u^2} : \underset{X_3}{tu^3} : \underset{X_4}{u^4})$$

Projetando $\mathbb{P}^4$ em $\mathbb{P}^3$ (identificado com o hiperplano $X_2 = 0$, a restrição a W é uma aplicação biregular sobre a curva $V \subset \mathbb{P}^3$ parametrizada por $(t^4:t^3u:tu^3:u^4)$. Segue que o anel do cone projetante de V, localizado na origem, é não C-M. Explicitamente, este anel é $R = k[X,Y,Z,W]_{(X,Y,Z,W)}/(XW-YZ, Y^3-X^2Z, Z^3-W^2Y, Y^2W-Z^2X)$. É um exercício fácil verificar, diretamente, que $\mathrm{prof}(R) = 1$.

3. <u>A propriedade de C-M versus interseções residuais</u> ("<u>liaison</u>")

Vimos que ideais gerados por R-sequências correspondem, geometricamente, a variedades interseções completas. Pode-se perguntar se as variedades cujos anéis de coordenadas são C-M estão "ligadas" a variedades interseções completas. Assim, no Exemplo do nº 1, a curva $V \subset \mathbb{P}^3$, cujo anel de coordenadas homogêneas R/I é C-M, satisfaz a igualdade $C = V \cup V'$, com $V' = \{X=W=0\}$

e $C = \{XY-ZW = YW-X^2 = 0\}$. Ou, algebricamente:

$$(XY-ZW, YW-X^2) = I \cap (X,W).$$

Dizemos que V' é "interseção residual de C", ou que V' e V são "residuais relativamente a C". Precisamente, sejam $V, V' \subset \mathbb{P}^n$ variedades projetivas; dizemos que V e V' são <u>(geometricamente) residuais</u> - ou <u>(geometricamente) ligadas</u> - se têm lugar as condições:

(i) V, V' são equidimensionais e sem componentes imersas;

(ii) V e V' não tem componentes irredutíveis comuns;

(iii) $V \cup V'$ é uma interseção completa no sentido estrito.

Em terminologia de anéis, dois quocientes R/I e R/J de um anel local regular são <u>(geometricamente) ligados</u> se:

(i)bis I e J são equidimensionais

(ii)bis $\mathrm{Ass}(R/I) \cap \mathrm{Ass}(R/J) = \emptyset$

(iii)bis $I \cap J$ é gerado por uma R-sequência.

<u>Observação</u>. Se R/I e R/J são geometricamente ligados, verifica-se facilmente que $I = (I \cap J):J$ e $J = (I \cap J):I$. Além disso I_P (resp. J_P) é gerado por uma R_P-sequência para todo $P \in \mathrm{Ass}(R/I)$ (resp. $P \in \mathrm{Ass}(R/J)$).

Os resultados centrais que demonstram a importância da noção de profundidade e de C-M para interseções residuais são os seguintes:

<u>Teorema</u> - Seja R um anel local regular e R/I, R/J quocientes (geometricamente) ligados. Se J é gerado por uma R-sequência, então R/I é C-M.

Teorema - Seja R um anel local regular, $I \subset R$ um ideal e $\underline{x} \subset I$ uma R-sequência máxima em I. As seguintes condições são equivalentes:

(i) R/I é C-M

(ii) $R/(\underline{x}:I)$ é C-M e I é puro.

(Além disso, nestas condições, necessariamente $\underline{x}:(\underline{x}:I) = I$).

Teorema ("de residução") - Seja R um anel local regular e $I \subset R$ um ideal de altura 2 tal que I_P seja gerado por uma R_P-sequência para todo $P \in \mathrm{Ass}(R/I)$. As condições seguintes são equivalentes:

(i) R/I é C-M

(ii) Existem ideais $I_1 = I, I_2, \ldots, I_s$ de R tais que R/I_i e R/I_{i+1} são (geometricamente) residuais e I_s é gerado por uma R-sequência (de comprimento 2, necessariamente).

Deixaremos, como exercício, a tarefa de enunciar os análogos geométricos dos teoremas acima.

Estes resultados estão ligados a Dubreil, Gaeta, Pesquine-Szpiro, Artin-Nagata. Dubreil introduziu a noção de variedade projetiva de "primeira espécie", que é exatamente uma variedade cujo cone projetante tem um anel (na origem) de profundidade ≥ 2.

A principal questão é: quais as propriedades que se mantêm na passagem por residuação? Pode-se mostrar que a profundidade (do anel na origem do cone projetante) não se mantém invariante a menos que seja ≤ 2. O que se pode mostrar é que a profundidade se mantém "alternadamente", isto é, se R/I e R/J

são residuais e se R/J e R/L são residuais, então $\text{prof}(R/I) = \text{prof}(R/L)$. Assim, numa "cadeia" de residuações $R/I_1, R/I_2, \ldots$, tem-se $\text{prof}(R/I_i) = \text{prof}(R/I_{i+2})$, $i = 1, \ldots$.

Existem várias outras propriedades que se mantêm por residuação alternada. A existência de cadeias longas de residuação se impõe precisamente pelo fato de que residuação não é uma relação transitiva.

Como leitura recomendamos [$(P-S)_1$], [A-N], [Du], [Gae].

Exercícios

1. Seja $R = k[X,Y,Z]$. Mostre que $X(Y-1)$, Y, $Z(X-1)$ é uma R-sequência, mas $X(Y-1)$, $Z(X-1)$, Y não o é. Isto pode acontecer com polinômios homogêneos de grau >0?

2. Seja $R = k[X_1,\ldots,X_6]_{(X_1,\ldots,X_6)}$. Estenda as seguintes R-sequências a R-sequências máximas em $(X_1,\ldots,X_6)R$:

   a) X_1X_2, X_1+X_3, X_4, X_5, X_6

   (Sugestão: reduza módulo (X_4,X_5,X_6))

   b) $X_1X_4 - X_2X_3$, $X_1X_6 - X_2X_5$

   (Sugestão: os primos associados de $(X_1X_4-X_2X_3, X_1X_6-X_2X_5)$ são (X_1,X_2) e o ideal dos determinantes 2×2 da matriz genérica $\begin{pmatrix} X_1 & X_3 & X_5 \\ X_2 & X_4 & X_6 \end{pmatrix}$).

3. Para cada um dos módulos do Exercício 3, Cap.I, determine sua profundidade e decida se é ou não um módulo de C-M.

4. Seja R um anel (noetheriano) e $I \subset R$ um ideal tal que $\mu(I) = \mathrm{alt}(I)$. Mostre:

a) Se $\mathrm{alt}(I) = \mathrm{prof}(I)$ (em particular, se R é C-M), I pode ser gerado por uma R-sequência.

b) Se $\mu = \mu(I)$ e R é S_μ (isto é, $\mathrm{prof}(R_P) \geq \min\{\mu, \mathrm{alt}(P)\}$ para todo primo $P \subset R$), então I pode ser gerado por uma R-sequência e é equidimensional. (Sugestão: esquiva (Exercício 2, Cap.I).

5. Seja $R,\underline{m}$ um anel, $J \subset I$ ideais contidos em $\underline{m}$. Mostre:

a) Se $x_1,\ldots,x_r \in I$ são tais que suas imagens em R/J formam um sistema mínimo de geradores do módulo I/J, então $\{x_1,\ldots,x_r\}$ pode ser estendido a um sistema mínimo de geradores de I. Generalize.

b) As seguintes condições são equivalentes:

(i) Todo sistema mínimo de geradores de J pode ser estendido a um de I

(ii) $\underline{m}I \cap J = \underline{m}J$

(iii) $\mu(I) = \mu(J) + \mu(I/J)$.

(Sugestão: considere a sequência exata deduzida da sequência exata $0 \to J \to I \to I/J \to 0$ por redução módulo $\underline{m}$).

6. Seja $R,\underline{m}$ um anel local, $J \subset I \subset \underline{m}$ ideais. Mostre que se I/J é gerado por uma R/J-sequência, então $I^t \cap J = I^{t-1}J$, para todo $t \geq 1$. (Sugestão: seja $\underline{x} = x_1,\ldots,x_n \in I$ uma R/J-sequência cuja imagem em R/J gera I/J; então $I = (\underline{x},J)$. Mostre que $(\underline{x})^t \cap J = (\underline{x})^{t-1}\cdot J$, usando o fato de que $(\underline{x})^t/(\underline{x})^{t+1}$ é um módulo livre sobre $R^*/(\underline{x}^*)$, onde $R^* = R/J$ e $\underline{x}^*$ é a imagem de $\underline{x}$ em R^* (vide Exercício 9).

7. Seja A um anel (noetheriano) de dimensão finita e $\underline{x} = x_1,\ldots,x_n \in A$ uma A-sequência. Mostre:

(a) $(n=2)$ $\dim(A[T]/(x_2-x_1T)) = \dim(A)$.

(b) Deduza de (a): $\dim(A[T_2,\ldots,T_n]/(x_2-x_1T_2,\ldots,x_n-x_1T_n))$ $= \dim(A)$.

(c) Deduza de (b): $\dim(A[T_1,\ldots,T_n]/(x_iT_j-x_jT_i)_{1\leq i<j\leq n}) =$ $= \dim(A)+1$.

(d) Suponha $A,\underline{m}$ local regular, $\underline{m} = (\underline{x})$ e admita que A contém um corpo infinito $k \simeq A/\underline{m}$. Mostre que o anel local

$$R = A[T_1,\ldots,T_n]_{(\underline{m},T_1,\ldots,T_n)}/(x_iT_j-x_jT_i)_{1\leq i<j\leq n}$$

é C-M exibindo um sistema de parâmetros de comprimento $n+1$. (Sugestão: escolha elementos $\alpha_i \in k\setminus\{0\}$, $\alpha_i \neq \alpha_j$ se $i \neq j$, $i = 1,\ldots,n$ e seja t_i a imagem de T_i módulo $(x_iT_j-x_jT_i)_{1\leq i<j\leq n}$. Então, $x_1-\alpha_1t_1,\ldots,x_n-\alpha_nt_n$, $t_1+\ldots+t_n$ é um sistema de parâmetros de R - a verificação de que $x_1-\alpha_1t_1,\ldots,x_n-\alpha_nt_n$ é uma R-sequência resulta facilmente; é mais penoso verificar que $t_1+\ldots+t_n \notin$ $\notin Z(R/(x_i-\alpha_it_i))_{1\leq i\leq n}$, fato que decorre essencialmente de que

$T_1+\dots+T_n$ não está contido em qualquer dos primos associados de $k[T_1,\dots,T_n]/(T_iT_j)_{1\le i<j\le n})$.

<u>Observação</u>: O ideal $(x_iT_j-x_jT_i)$ é gerado pelos determinantes 2x2 da matriz "semi-genérica" $\begin{pmatrix} x_1 \dots x_n \\ T_1 \dots T_n \end{pmatrix}$, logo, pelos resultados do Capítulo III, R é um módulo perfeito sobre $A[T_1,\dots,T_n]_{(\underline{m},T_1,\dots,T_n)}$. Isto mostra que R é C-M.

8. Seja R um anel local C-M. Mostre:

   (a) Se $P \subsetneqq Q$ são ideais primos tais que $\mathrm{alt}(Q/P) = 1$, então $\mathrm{prof}(Q) = \mathrm{prof}(P)+1$.

   (b) Deduza de (a) que toda cadeia saturada entre primos P e Q tem comprimento $= \mathrm{alt}(Q) - \mathrm{alt}(P)$.

<u>Observação</u>: Uma cadeia $P = P_o \subseteq \dots \subset P_n = Q$ é saturada se $\mathrm{alt}(P_i/P_{i-1}) = 1$, $i = 1,\dots,n$.

9. Seja $R = k[X_1,\dots,X_n]$ e $I \subset R$ um ideal homogêneo. Mostre:

   (a) $P \in \mathrm{Ass}(R/I) \Rightarrow P$ é homogêneo e $P = I:(f)$ para algum polinômio homogêneo $f \in R$.

   (b) Se P é um ideal primo homogêneo e Q um ideal P-primário, então o subideal Q' de Q gerado pelos polinômios homogêneos de Q é P-primário. Deduza que I admite uma decomposição primária cujas componentes primárias são ideais homogêneos. (Sugestão: se $P' \in \mathrm{Ass}(R/Q')$ então P' é homogêneo pelo item (a); $P = P' \Leftrightarrow P \cap H = P' \cap H$, onde $H \subset R$ é o conjunto dos polinômios homogêneos de R).

10. Seja R um anel e $\underline{x} = x_1,\ldots,x_n$ uma R-sequência. Ponhamos $I = (\underline{x})$. Mostre:

(a) Para todo $t \geq 0$, I^t/I^{t+1} é um R/I-módulo livre.

(b) Se $R,\underline{m}$ é local, deduza de (a): todo polinômio homogêneo $F \in R[X_1,\ldots,X_n]$ de grau t tal que $F(x_1,\ldots,x_n) \in I^t\underline{m}$, pertence a $\underline{m}R[X_1,\ldots,X_n]$. Obs.: em outras palavras, uma R-sequência é analiticamente independente.

(d) Se k é um corpo e $f_1,\ldots,f_n \in k[X_1,\ldots,X_n]$ são polinômios homogêneos constituindo $k[X_1,\ldots,X_n]$-sequência, então eles são algebricamente independentes sobre k.

11. Se R é um anel e $I \subset R$ um ideal gerado por uma R-sequência, então I^t é equiprofundo, $t \geq 1$ (isto é, $\text{prof}(P) = \text{prof}(I^t)$ para todo $P \in \text{Ass}(R/I^t)$).
(Sugestão: use 9(a), procedendo por indução ao longo das sequências exatas $0 \to I^t/I^{t+1} \to R/I^{t+1} \to R/I^t \to 0$).

12. Seja R um anel e M um R-módulo. Dados $x_1,\ldots,x_n \in R$ e inteiros positivos $d_1,\ldots,d_n$, tem-se:

$$x_1,\ldots,x_n \text{ é M-sequência} \Leftrightarrow x_1^{d_1},\ldots,x_n^{d_n} \text{ é M-sequência.}$$

(Sugestão: mostre que dada uma sequência de elementos $x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n$ em R, com $x_i = ab$ e tal que $(x_1,\ldots,x_{i-1},a,x_{i+1},\ldots,x_n)M \neq M$, $(x_1,\ldots,x_{i-1},b,x_{i+1},\ldots,x_n)M \neq M$ então

$\{x_1,\ldots,x_{i-1},x_i,x_{i+1},\ldots,x_n\}$ é M-sequência $\Leftrightarrow$

$\{x_1,\ldots,x_{i-1},a,x_{i+1},\ldots,x_n)$ e $\{x_1,\ldots,x_{i-1},b,x_{i+1},\ldots,x_n\}$

são M-sequências).

Capítulo III

Métodos homológicos

§1. Anéis regulares; o teorema de Serre-Auslander-Buchsbaum.

Seja R um anel (noetheriano) e $I \subset R$ um ideal. Lembremos algumas das notações anteriores:

$\mu(I)$ = número mínimo possível de geradores de I

$\mathrm{alt}(I)$ = altura de I $(= \min\{\mathrm{alt}(P) \mid P \in \mathrm{Min}(R/I)\})$

$\mathrm{prof}(I)$ = profundidade de I $(= \mathrm{prof}_I(R)$ = comprimento de uma R-sequência máxima contida em I).

Sabemos que

$$\mathrm{prof}(I) \underset{\substack{\uparrow \\ \text{Cap.II},\S 1}}{\leq} \mathrm{alt}(I) \underset{\substack{\uparrow \\ \text{Cor.I.12 ("Primidealsatz")}}}{\leq} \mu(I)$$

Particularizemos ao caso $I = \underline{m}$, ideal máximo de um anel local R. Neste caso:

$\mathrm{prof}(\underline{m}) = \mathrm{alt}(\underline{m}) \Leftrightarrow R$ é C-M (Cap.II, §2)

$\mathrm{prof}(\underline{m}) = \mu(\underline{m}) \Leftrightarrow \underline{m}$ é gerado por uma R-sequência (Cap.II,§2, Exemplo (5) e Exercício 4, Cap.II).

O que se pode afirmar quando $\mathrm{alt}(\underline{m}) = \mu(\underline{m})$? Surpreendentemente, esta igualdade acarreta a igualdade dos dois extremos, como veremos.

<u>Proposição III.1</u> - <u>Seja</u> R,$\underline{m}$ <u>um anel local</u>. <u>Se</u> alt(m) $= \mu$(m), <u>então</u> $\underline{m}$ <u>é gerado por uma</u> R-<u>sequência</u>.

<u>Demonstração</u>: Procedemos por indução sobre o valor comum $n = \mathrm{alt}(\underline{m}) = \mu(\underline{m})$. Podemos iniciar de $n = 0$, desde que aceitemos que o conjunto vazio é uma R-sequência (de comprimento 0...). Suponhamos, agora, $n \geq 1$. Tomemos $x \in \underline{m} \setminus \underline{m}^2$ ($\underline{m} = \underline{m}^2 \Rightarrow \underline{m} = (0)$, como se vê facilmente). Então:

$$\dim(R/(x)) \geq \dim(R) - 1 \qquad \text{(Prop.I.13)}$$

$$\mu(\underline{m}/(x)) = \mu(\underline{m}) - 1$$

Para verificar a segunda relação, observemos que se $\bar{y}_1,\ldots,\bar{y}_r$ geram $\underline{m}/(x)$, então $(x,y_1,\ldots,y_r) = \underline{m}$. Isto significa que $\mu(\underline{m}) \leq \mu(\underline{m}/(x)) + 1$. Por outro lado, se $\bar{y}_1,\ldots,\bar{y}_r$ é um conjunto mínimo de geradores, então $x,y_1,\ldots,y_r$ geram $\underline{m}$ minimamente; com efeito, se $x \in (y_1,\ldots,y_r)$ então $x = \lambda_1 y_1 + \ldots + \lambda_r y_r$, com (digamos) λ_1 inversível (já que $x \notin \underline{m}^2$ por hipótese). Neste caso, $\bar{y}_1 \in (\bar{y}_2,\ldots,\bar{y}_r)$. Isto mostra que $\mu(\underline{m}) \geq \mu(\underline{m}/(x)) + 1$.

Assim, $\dim(R/(x)) = \mathrm{alt}(\underline{m}/(x)) \leq \mu(\underline{m}/(x)) =$

$$= \mu(\underline{m}) - 1 = \dim(R) - 1.$$

Pela hipótese relativa à indução, $\underline{m}/(x)$ é gerado por uma $R/(x)$-sequência $\bar{x}_2,\ldots,\bar{x}_n$. É imediato verificar que $x_i \notin Z(R/(x,x_2,\ldots,x_{i-1}))$, $i = 2,\ldots,n$. Desta forma, se tivéssemos sido afortunados na escolha inicial de x, a ponto de $x \notin Z(R)$, $x,x_2,\ldots,x_n$ seria uma R-sequência gerando $\underline{m}$.

Sucede que qualquer escolha de $x \in \underline{m} \setminus m^2$ é boa!

Com efeito, temos:

Lema III.2 - Se $R,\underline{m}$ é um anel local tal que $\mathrm{alt}(\underline{m}) = \mu(\underline{m})$, então R é um domínio.

Demonstração: Procedemos por indução sobre $n = \mathrm{alt}(\underline{m}) = \mu(\underline{m})$, como acima. Assim, por hipótese, se $x \in \underline{m}\setminus\underline{m}^2$, $R/(x)$ é um domínio e, portanto, (x) é um ideal primo. Afirmamos que $(x) \in \mathrm{Min}(R)$ a menos que R seja domínio. De fato, seja $P \subsetneq (x)$ um primo. Dado $p \in P$, temos $p = xp_1$. Como $x \notin P$, necessariamente tem-se $p_1 \in P$, etc., de modo que $P \subseteq \bigcap_{n\geq 0} (x)^n$. Disso resulta que $P = (0)$ (vide Exercício 10(c) do Cap.I).

Refazendo: mostramos que todo $x \in \underline{m}\setminus\underline{m}^2$ gera um primo de $\mathrm{Min}(R) = \{P_1,\ldots,P_t\}$. Isto é, $\underline{m} \subset \underline{m}^2 \cup P_1 \cup\ldots\cup P_t$. Então $\underline{m} \subset P_i$, para algum i (Exercício 1, Cap.I), logo $\dim(R) = 0$; contradição. Logo, $(x) \notin \mathrm{Min}(R)$ e, portanto, R é um domínio. //

Observemos que a recíproca da Proposição III.1 é trivial já que a igualdade $\mathrm{prof}(\underline{m}) = \mu(\underline{m})$ força $\mathrm{alt}(\underline{m}) = \mu(\underline{m})$. Isto motiva a seguinte noção:

Definição III.3 - Um anel local $R,\underline{m}$ é regular se, equivalentemente:

(i) $\dim(R) = \mu(\underline{m})$ (i.e., $\underline{m}$ é da classe principal).

(ii) $\underline{m}$ é gerado por uma R-sequência (um tal conjunto de geradores é chamado sistema regular de parâmetros).

Observações. (1) O termo "regular" tem conotações geométricas, correspondendo à situação de um ponto regular (= não-singular) de uma variedade algébrica V: tais são os pontos pelos quais passam $n = \dim V$ hipersuperfícies em posição transversal.

(2) Com relação à Proposição III.1, existe o seguinte resultado mais geral [Da]: se $P \subset R$ é um ideal primo (R noetheriano) da classe principal, então P é gerado por uma R-sequência. Isto é claramente falso para ideais quaisquer (por exemplo, sejam $P_1,\ldots,P_t$ os primos de altura 0 de um anel R e suponhamos que $P \in \mathrm{Ass}(R)$ é um primo imerso; tome-se $I = (a)$, com $a \in P \setminus \bigcup_{i=1}^{t} P_i$).

Queremos enfatizar algumas das propriedades fortes a que satisfaz um anel local regular R:

$\mathcal{R}_1$: R é um domínio

$\mathcal{R}_2$: R é C-M

$\mathcal{R}_3$: R é normal

$\mathcal{R}_4$: Um quociente R/I é regular $\Leftrightarrow$ I é gerado por um subsitema de parâmetros regulares de R.

Vejamos o que se tem até agora. $\mathcal{R}_1$ é o Lema III.2. $\mathcal{R}_2$ é imediata. Quanto a $\mathcal{R}_3$, usando a caracterização de Krull-Serre de anéis normais (vide Cap.II, §3, Nº 2), e $\mathcal{R}_2$ acima, basta verificar que se $P \subset R$ é um primo de altura 1, então R_P é novamente regular. Em vez de fazê-lo a esta altura, seremos pacientes e aguardaremos um resultado mais geral que nos diz que R_P é regular para <u>todo</u> primo P (vide Cor.III.8 adiante).

Finalmente, $\mathcal{R}_4$ pode ser verificada facilmente. Primeiro, suponhamos que $I = (x_1,\ldots,x_d)$, com $\underline{m} = (x_1,\ldots,x_d, x_{d+1},\ldots,x_n)$ uma R-sequência. Como $\underline{m}/(x_1,\ldots,x_d)$ é gerado pelas imagens de $\bar{x}_{d+1},\ldots,\bar{x}_n$, que constituem por sua vez R/I-sequência, resulta que R/I é regular. Reciprocamente, suponhamos

R/I regular. Seja $\bar{x}_{d+1},\dots,\bar{x}_n$ um sistema regular de parâmetros de R/I. Escolhamos $x_1,\dots,x_d \in I$ tais que $\underline{m} = (x_1,\dots,x_d,x_{d+1},\dots,x_n)$ e tais que $n = \dim(R)$ (por que isto é possível?). Segue que $x_1,\dots,x_n$ é uma R-sequência (vide Exercício 6). Pela primeira implicação, $P = (x_1,\dots,x_d)$ é primo e, evidentemente, $\mathrm{alt}(P) = d$. Mas, I também é primo por $\mathfrak{R}_1$ e, por $\mathfrak{R}_2$, $\mathrm{alt}(I) = \dim(R) - \dim(R/I) = n-(n-d) = d$. Logo, $I = P = (x_1,\dots,x_d)$, como queríamos.

Observação. Uma das implicações contidas na propriedade $\mathfrak{R}_4$ é análoga ao resultado descrito no Corolário II.12(ii) para anéis de C-M. A implicação inversa, contudo, não tem análogo no caso C-M (vide Cap.II, §3, Nº 1, Exemplo). Isto indica que a classe de anéis regulares obtidos como quocientes de um anel regular R fixo, é bem restrita (isto pode servir como razão filosófica porque, para "resolver singularidades", precisa-se considerar extensões sucessivas do anel inicial R ...).

Exemplo. Seja R um anel (noetheriano) tal que R_P é regular para todo primo $P \subset R$. Então $R[X]$ tem também esta propriedade.

(Sugestão: Proceder como no Exemplo (4), Cap.II, §2, fazendo as adaptações necessárias).

Disso segue-se o "milagre de Hilbert":

(k = corpo) $k[X_1,\dots,X_n]_P$ é regular para todo primo P.

(A maneira clássica - isto é, E. Noether e sucessores - de mostrar isto era reduzir ao caso em que P é um ideal máximo, por um processo de "uniformização" - vide Exercício 1).

A bem da honestidade, não devíamos invocar o nome de Hilbert em vão. De fato, Hilbert foi responsável por uma descoberta bem mais profunda - o popular "teorema do syzygy" - e sequer conhecia o formalismo de anéis regulares conforme expusemos. De modo que, a fazer justiça com o trabalho de Hilbert ([Hi], 1890 - gulp!), deveríamos explicar o que a afirmação "$k[X_1,\ldots,X_n]_p$ é regular" tem a ver com o "teorema do syzygy".

Esta é a nossa próxima tarefa.

Suporemos, como sempre, que R é um anel noetheriano e que "R-módulo" significa "R-módulo finitamente gerado".

Se M é um R-módulo podemos, escolhendo um conjunto finito $x_1,\ldots,x_m$ de geradores de M, definir um R-homomorfismo sobrejetor $F \xrightarrow{\varphi_o} M$, onde F é um R-módulo livre de posto m; φ_o tem um núcleo Z. Indicaremos esta construção, brevemente, pondo

$$0 \to Z \to F \to M \to 0,$$

que é chamada uma <u>sequência exata curta</u> (ou uma <u>apresentação de M</u>). O módulo Z é o "módulo de relações" dos geradores $x_1,\ldots,x_m$, já que por definição, seus elementos são m-uplas $a_1,\ldots,a_m \in R$ tais que $a_1x_1 + \ldots + a_mx_m = 0$.

Como Z é finitamente gerado, podemos iterar este processo, o que será indicado por

$$\ldots \to F_n \xrightarrow{\varphi_n} F_{n-1} \xrightarrow{\varphi_{n-1}} \ldots \to F_1 \xrightarrow{\varphi_1} \overset{\displaystyle F}{\overset{\shortparallel}{F_o}} \xrightarrow{\varphi_o} M \to 0,$$

onde entende-se que $\text{núcl}(\varphi_i) = \text{im}(\varphi_{i+1})$, $i = -1,0,\ldots$ $(\varphi_{-1}=0)$. Designaremos uma tal sequência de homomorfismos por <u>sequência exata longa de módulos livres</u> ou, mais brevemente, <u>resolução livre</u>

(do módulo M). Uma tal sequência é "infinita", em princípio. Podemos truncá-la em qualquer etapa, tornando-a finita:

$$0 \to Z_n \to F_{n-1} \to \cdots \to F_1 \to F_o \to M \to 0.$$

Mas, neste caso, não se trata mais de uma resolução livre, a menos que Z_n seja um módulo livre.

O módulos $Z_n = \text{núcl}(\varphi_{n-1})$ são chamados <u>módulos de xyzygys</u> ou, simplesmente, <u>syzygys</u>.

Se suceder que Z_n é livre, então temos uma <u>resolução livre finita</u>, de <u>comprimento</u> n. (N.B. n = número de módulos livres -1).

Isto motiva:

<u>Definição III.4</u> - Se M é um R-módulo, a <u>dimensão homológica de</u> M é o comprimento de uma resolução livre finita de M de menor comprimento possível.

<u>Notação</u>: $d.h._R(M)$ ou $d.h.(M)$ (se R é fixo no contexto).

Se M não admitir resolução livre finita, poremos $d.h.(M) = \infty$.

<u>Exemplos</u>. (1) (Este é o padrão de módulo de $d.h. < \infty$). Seja $\underline{x} = x_1,\ldots,x_n \in R$ uma R-sequência. Então, $d.h._R(R/(\underline{x})) = n$. Assim, para $n = 1$, uma resolução é

$$0 \to R \xrightarrow{.x} R \to R/(x) \to 0,$$

onde $.x$ é o homomorfismo "multiplicação por x". Para $n = 2$, uma resolução é

$$0 \to R \xrightarrow[\binom{-x_2}{x_1}]{} R^2 \xrightarrow[(x_1,x_2)]{} R \to R/(x_1,x_2) \to 0$$

(escrevendo os homomorfismo sob forma matricial).

Para $n=3$, ainda é fácil calcular uma resolução:

$$0 \quad R \xrightarrow[\begin{pmatrix} x_3 \\ -x_2 \\ x_1 \end{pmatrix}]{} R^3 \xrightarrow[\begin{pmatrix} -x_2 & -x_3 & 0 \\ x_1 & 0 & -x_3 \\ 0 & x_1 & x_2 \end{pmatrix}]{} R^3 \xrightarrow[(x_1\ x_2\ x_3)]{} R \to R/(x_1,x_2,x_3) \to 0$$

O princípio começa a ficar claro e é possível calcular "na mão" o caso geral, sem que isto seja terrivelmente recompensador. No §4 veremos como obter uma tal resolução, com várias informações adicionais (complexo de Koszul).

(2) (Um módulo de d.h. $= \infty$)

Seja $R = k[X,Y]/(XY) = k[x,y]$ e $I = (x,y)$. Então, I admite resolução livre infinita

$$\cdots \to R^2 \xrightarrow[\begin{pmatrix} y & 0 \\ 0 & x \end{pmatrix}]{} R^2 \xrightarrow[\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}]{} R^2 \xrightarrow[\begin{pmatrix} y & 0 \\ 0 & x \end{pmatrix}]{} R^2 \to I \to 0$$

(Note-se a "periodicidade" de período 2 desta resolução). Em verdade, $\text{d.h.}_R(I) = \infty$, o que será uma consequência do teorema de Serre-Auslander-Buchsbaum (Teor.III.7).

Nosso primeiro objetivo é mostrar que a teoria da dimensão homológica é "razoável". Com isto queremos dizer que se M é tal que $\text{d.h.}(M) < \infty$, então não é preciso testar todas as resoluções livres finitas de M a fim de tropeçar numa de comprimento mínimo. Mais precisamente, queremos mostrar que se $\text{d.h.}(M) < < \infty$, então de qualquer resolução livre é possível extrair uma cujo comprimento é igual a d.h.(M).

Para que isto funcione de fato, já veremos que é preciso fazer concessões na definição de dimensão homológica. O resultado seguinte não só resolve o problema acima, como permite-nos ver quais concessões devem ser feitas.

Proposição III.5 ("Lema de Schanuel") - Dadas duas resoluções "livres" de um mesmo módulo M,

$$0 \to Z_n \to F_{n-1} \to F_{n-2} \to \cdots \to F_o \xrightarrow{\varphi_o} M \to 0$$

$$0 \to Z'_n \to F'_{n-1} \to F'_{n-2} \to \cdots \to F'_o \xrightarrow{\varphi'_o} M \to 0$$

(Z_n e Z'_n não necessariamente livres), tem-se

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

Demonstração: Consideramos as resoluções truncadas

$$0 \to Z_n \to F_{n-1} \to \cdots \to F_1 \xrightarrow{\varphi_1} Z_1 \to 0$$

e

$$0 \to Z'_n \to F'_{n-1} \to \cdots \to F'_1 \xrightarrow{\varphi'_1} Z'_1 \to 0 ,$$

onde $Z_1 = \text{núcl}(\varphi_o)$, $Z'_1 = \text{núcl}(\varphi'_o)$.

É fácil ver que as sequências seguintes ainda são exatas (apenas "insuflmaos" o início das sequências acima):

$$0 \to Z_n \to F_{n-1} \to \cdots \to F_2 \to F_1 \oplus F'_o \xrightarrow{(\varphi_1, 1_{F'_o})} Z_1 \oplus F'_o \to 0$$

$$0 \to Z'_n \to F'_{n-1} \to \cdots \to F'_2 \to F'_1 \oplus F_o \xrightarrow{(\varphi'_1, 1_{F_o})} Z'_1 \oplus F_o \to 0$$

(onde 1_N = aplicação identidade do módulo N).

Assim, procedendo por indução sobre n, basta mostrar que $Z_1 \oplus F'_0 \simeq Z'_1 \oplus F_0$ (este resultado é o "lema de Schanuel curto").

Para isto, usamos um argumento típico de "inflação" de geradores de M, de tal modo que reduzimos o problema ao seguinte, mais simples:

Se $0 \to Z \to F \xrightarrow{\varphi} M \to 0$ é <u>uma apresentação de</u> M <u>e se</u> $F \oplus R \xrightarrow{\psi} M$ <u>é qualquer homomorfismo tal que</u> $\psi|_F = \varphi$, <u>então</u> $Z \oplus (F \oplus R) \simeq \text{núcl}(\psi) \oplus F$. Mostraremos, mais precisamente, que $\text{núcl}(\psi) \simeq Z \oplus R$ (atenção: não é verdade que $\text{núcl}(\psi) = Z \oplus R$; o isomorfismo é "torcido"). É necessário precisar a notação: $F = \sum_{i=1}^{m} Re_i$, $F' = \sum_{i=1}^{m} Re_i + Re$ (bases de F e F', respectivamente). Denotemos $x_i = \varphi(e_i) = \psi(e_i)$, $x = \psi(e)$. Como φ é sobrejetor por hipótese, tem-se $x = \sum_{i=1}^{m} \alpha_i x_i$ para certos $\alpha_i \in R$. Ponhamos $e' = e - \sum_{i=1}^{m} \alpha_i e_i$ e mostremos que $\text{núcl}(\psi) = Z + Re'$. A inclusão $\text{núcl}(\psi) \supset Z + Re'$ é imediata uma vez que $\psi(e) = x = \Sigma\, \alpha_i x_i = \Sigma\, \alpha_i\, \psi(e_i) = \psi(\Sigma \alpha_i e_i)$ e, portanto, $\psi(e') = 0$. Inversamente, se $\Sigma\, \lambda_i e_i + \lambda e \in \text{núcl}(\psi)$, um cálculo direto mostra que $\Sigma(\lambda_i + \lambda\alpha_i)e_i \in Z$. Daí que $\Sigma\, \lambda_i e_i + \lambda e = \Sigma(\lambda_i + \lambda\alpha_i)e_i - \lambda(\Sigma\, \alpha_i e_i - e) \in Z + Re'$, como queríamos.

Para concluir, basta notar que $\{e_1, \ldots, e_n, e'\}$ é ainda uma base de F' (apenas efetuamos uma transformação elementar da base original). //

Usemos, momentaneamente, a seguinte definição: um módulo N é <u>estavelmente livre</u> se existem módulos livres F e F' tais que $N \oplus F' \simeq F$.

<u>Corolário III.6</u> - <u>Seja</u> R <u>um anel tal que todo módulo estavelmente livre é livre</u>. <u>Se</u> M <u>é um módulo tal que</u> d.h.(M) $< \infty$, <u>então de toda resolução livre</u> (<u>possivelmente infinita</u>) <u>de</u> M <u>é possível extrair uma resolução livre de comprimento</u> = d.h.(M).

<u>Demonstração</u>: É evidente: comparamos a resolução dada

$$\ldots \to F_i \to F_{i-1} \to \ldots \to F_o \to M \to 0$$

(tomando o cuidado de truncá-la na etapa n = d.h.(M)) com uma resolução livre de comprimento n, utilizando o lema de Schanuel e a hipótese sobre os módulos estavelmente livres. //

Assim, a concessão a ser feita na definição de dimensão homológica é clara: ou consideramos permissíveis resoluções a módulos estavelmente livres ou, alternativamente, aplicamos a teoria das resoluções livres apenas a anéis que satisfazem a hipótese do corolário.

A maneira de escapar a uma tal decisão é usar "resoluções projetivas" (isto é, resoluções a "módulos projetivos"). Este é um conceito a um passo apenas das resoluções livres, mas estas últimas se impõem tão naturalmente - além da sua importância na teoria dos complexos livres - que preferimos mantê-los como pedra de toque.

De qualquer modo, teremos liquidez já que os anéis locais são exemplos de anéis satisfazendo a hipótese do corolário (em verdade, um pouco mais do que isto vale para um anel local, a saber, que todo módulo projetivo é livre).

<u>Suporemos que</u> R <u>é local sempre que falarmos em dimensão homológica</u>.

Entrementes, voltemos ao nosso motivo original, que era a relação entre o conceito de anel local regular e o "teorema do syzygy".

Hilbert mostrou o seguinte, na nossa linguagem.

<u>Teorema de Syzygy</u> - <u>Se</u> I <u>é um ideal homogêneo num anel de polinômios</u> $R = k[X_1,\dots,X_n]$, <u>então</u> $d.h._R(R/I) \le n$.

Este resultado, como o vemos hoje, é consequência do resultado local seguinte: <u>se</u> $I \subset R = k[X_1,\dots,X_n]_{(X_1,\dots,X_n)}$ <u>é um ideal, então</u> $d.h._R(R/I) \le n$. (Por esta razão é que Hilbert obteve um módulo <u>livre</u> na etapa n-ésima e não apenas <u>estavelmente</u> livre; em verdade, as resoluções que considerou eram por homomorfismos homogêneos, obtendo como n-ésimo syzygy um módulo estavelmente livre "graduado" que é, como nos ensinou Eilenber [Ei], livre).

Sabemos que $k[X_1,\dots,X_n]_{(X_1,\dots,X_n)}$ é regular. Surge, portanto, a questão de se esta é exatamente a razão para $d.h.(R/I) < \infty$. A resposta é afirmativa e, com precisão suplementar, é o conteúdo do célebre

<u>Teorema III.7</u> (Serre-Auslander-Buchsbaum) - <u>Seja</u> $R,\underline{m}$ <u>um anel local. As seguintes condições são equivalentes:</u>

(i) R <u>é regular</u>

(ii) $d.h._R(\underline{m}) = \dim(R)-1$

(iii) $d.h._R(\underline{m}) < \infty$

(iv) $\sup\{d.h._R(M) \mid M \text{ R-módulo}\} < \infty$

(<u>necessariamente, este</u> "<u>sup</u>" <u>é igual a</u> $d.h.(\underline{m})+1$).

As demais seções deste capítulo serão, grosso modo, organizadas em torno do teorema acima. Ao cabo, teremos toda a ferramenta para demonstrar este teorema (e, evidentemente, outros). Para já gostaríamos de arquivar uma consequência importante do teorema.

<u>Corolário III.8</u> - <u>Se</u> R <u>é um anel local regular, então</u> R_P <u>é regular para todo primo</u> $P \subset R$.

<u>Demonstração</u>: Tem-se $d.h._{R_P}(P_P) \leq d.h._R(P)$ (mais geralmente, $d.h._{R_S}(M_S) \leq d.h._R(M)$ para todo R-módulo M e todo conjunto multiplicativo $S \subset R$: localização preserva sequências exatas). O resultado segue então do teorema. //

<u>Observação</u>. O valor $\sup\{d.h._R(M) \mid M \text{ R-módulo}\}$ é chamado a <u>dimensão global</u> (<u>homológica</u>) de R.

Notação: $d.gl.(R)$.

Pode-se mostrar que $d.gl.(R) = \sup\limits_{P \text{ primo}} \{d.gl.(R_P)\}$.

(Isto é óbvio se R é local, mas não é óbvio se R é apenas noetheriano - com as necessárias adaptações na definição de d.h., conforme mencionamos antes. Neste caso, resulta do seguinte fato: $d.h._R(M) = \sup\limits_{P \text{ primo}} \{d.h._{R_P}(M_P)\}$ para todo R-módulo M).

§2. <u>A ferramenta homológica</u>.

Nesta seção desenvolveremos algumas técnicas básicas de homologia. Um estudo exaustivo dos preliminares homológicos, com vistas a aplicações em álgebra comutativa, é algo que costuma variar desde o "prolixo" até o "entediante". Embora cobrindo a maioria dos detalhes de demonstração, esta seção é mais propriamente um arquivo dos principais resultados homológicos a serem utilizados neste livro.

A) Dimensão homológica versus sequências exatas curtas.

Aqui, ficará patente a importância do lema de Schanuel (na forma do Cor.III.6).

Lema III.9 (Suponhamos R local) - Seja $0 \to Z \to F \to M \to 0$ uma apresentação do módulo M (lembremos: F é livre). Então uma (e uma só) das seguintes condições tem lugar:

(1) $d.h.(M) = d.h.(Z) = \infty$

(2) M é livre (logo, Z é livre)

(3) $d.h.(M) = d.h.(Z) + 1 < \infty$.

Observação: (3) é realmente o caso fundamental nas aplicações, enquanto que (1) e (2) devem ser vistos como casos "degenerados".

Demonstração: Seja

$$\cdots \to F_1 \to F_o \to Z \to 0$$

uma resolução livre de Z (finita ou infinita). Então

$$\begin{tikzcd}
\cdots \arrow[r] & F_1 \arrow[r] & F_o \arrow[dr] & & F \arrow[r] & M \arrow[r] & 0 \\
& & & Z \arrow[ur] \arrow[dr] & & & \\
& & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

é uma resolução livre de M. Pelo Corolário III.6, resulta que

$d.h.(M) = \infty \Leftrightarrow d.h.(Z) = \infty$ e, além disso, $d.h.(M) \leq d.h.(Z) + 1$. Forcemos o argumento um pouco mais: seja

$$0 \to F_n \to \ldots \to F_1 \to F_o \to Z \to 0$$

uma resolução livre de Z, com $n = d.h.(Z) < \infty$. Novamente, da resolução $0 \to F_n \to \ldots \to F_o \to F \to M \to 0$ podemos extrair uma de comprimento $= d.h.(M)$. Isto força $d.h.(M) = d.h.(Z)+1$, a menos que Z e M sejam livres (isto é, de $d.h. = 0$). //

O lema acima será utilizado na demonstração (e é um caso particular) da seguinte proposição.

Proposição III.10 - Seja $0 \to N \to M \to K \to 0$ uma sequência exata de módulos. Então

(i) Se dois quaisquer dos módulos N, M, K têm dimensão homológica finita, o terceiro também a tem.

(ii) $d.h.(M) < d.h.(N) \Rightarrow d.h.(K) = d.h.(N) + 1$

$d.h.(M) > d.h.(N) \Rightarrow d.h.(K) = d.h.(M)$

$d.h.(M) = d.h.(N) \Rightarrow d.h.(K) \leq d.h.(M)+1$ (caso "indeterminado")

Demonstração: A idéia é construir resoluções livres simultâneas dos 3 módulos (suporemos R local, pelas razões técnicas anteriormente mencionadas).

Tomemos um conjunto de geradores de M, $x_1,\ldots,x_r$, $y_1,\ldots,y_s$, tais que $x_1,\ldots,x_r$ geram N e $\bar{y}_1,\ldots,\bar{y}_s$ geram $M/N = K$. Usando estes geradores, construimos apresentações

$$0 \to Z' \to F' \xrightarrow{\partial'} N \to 0, \qquad 0 \to Z'' \to F'' \xrightarrow{\partial''} K \to 0$$

e

$$0 \to Z \to F' \oplus F'' \to M \to 0.$$

Deixaremos como exercício verificar a existência de homomorfismos $Z \to Z$ e $Z \to Z''$ tais que o diagrama abaixo admite todas (colunas e) linhas exatas e comuta no sentido usual

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & Z' \arrow[r] \arrow[d] & Z \arrow[r] \arrow[d] & Z'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & F' \arrow[r] \arrow[d, "\partial'"] & F' \oplus F'' \arrow[r] \arrow[d, dashed, "\partial"] & F'' \arrow[r] \arrow[d, dashed, "\partial''"] & 0 \\
0 \arrow[r] & N \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & K \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Repetindo este processo para a sequência $0 \to Z' \to Z \to Z'' \to 0$, e assim, sucessivamente, obtemos resoluções livres "simultâneas" de N, M, K.

O item (i) segue, por uma análise deste processo, utilizando-se o Corolário III.6.

Passemos a (ii). Suporemos que M, N, K têm $\text{d.h.} < \infty$ (ainda que ao resultado possa-se atribuir um sentido em geral), e procederemos por indução sobre $\text{d.h.}(N) + \text{d.h.}(M) + \text{d.h.}(K)$. Finalmente, consideraremos apenas o caso $\text{d.h.}(M) < \text{d.h.}(N)$ como típico, deixando os demais como exercícios.

Há dois casos possíveis:

1) M é livre.

Neste caso, K não é livre. Com efeito, K livre acarretaria a existência de um homomorfismo $K \to M$ tal que a composta $K \to M \to K$ é a identidade, logo K identificar-se-ia, por meio deste homomorfismo, com um somando direto de M cujo complemento é N. Assim, N seria estavelmente livre, logo, livre (R é local). Mas, isto é impossível já que, por hipótese, d.h.(N) > > d.h.(M) = 0.

Assim, K não é livre. Pelo Lema III.9, d.h.(K) = = d.h.(N)+1, como queríamos.

2) M não é livre.

Se K não é livre, pelo Lema III.9, d.h.(Z″) = d.h.(K)-1. Por hipótese (e ainda pelo Lema III.9), d.h.(Z) = d.h.(M)-1. Temos d.h.(Z′) + d.h.(Z) + d.h.(Z″) $\lneq$ d.h.(N) + d.h.(M) + d.h.(K) (até com certa folga), logo podemos aplicar a hipótese de indução. Em qual dos casos estamos na sequência $0 \to Z' \to Z \to Z'' \to 0$? Ora, lembremos que N não é livre, pois d.h.(N) > d.h.(M) > 0 por hipótese. Então, d.h.(Z′) = d.h.(N)-1 e, portanto, permanece a condição d.h.(Z) < d.h.(Z′). Por indução, d.h.(Z″) = d.h.(Z′)+1 e, voltando, obtemos d.h.(K) = d.h.(Z″)+1 = d.h.(Z′)+2 = = d.h.(N)-1+2 = d.h.(N)+1, conforme queríamos.

Se K é livre, Z″ também o é (mesmo argumento usado acima, no caso 1)). Como M e N não são livres, segue do Lema III.9 que d.h.(Z) < d.h.(Z′). Por indução, d.h.(Z) < d.h.(Z′) $\Rightarrow$ d.h.(Z″) = d.h.(Z′)+1, o que é impossível pois d.h.(Z″) = 0.

Assim, K não pode ser livre neste caso.

B) <u>A homologia de um complexo</u>.

Noção subjacente à de resolução livre é a de complexo (de módulos), a qual deve ser introduzida o quanto antes.

Uma sequência de R-módulos e R-homomorfismos

$$\cdots \to C_{i+1} \xrightarrow{d_{i+1}} C_i \xrightarrow{d_i} C_{i-1} \to \cdots \qquad (i \in \mathbb{Z})$$

é um <u>complexo</u> se $d_i \cdot d_{i+1} = 0$, $i \in \mathbb{Z}$. Os homomorfismos d_i são as <u>diferenciais</u> do complexo.

Parte substancial da teoria reduz-se ao estudo de complexos "à esquerda", i.e., tais que $C_i = (0)$ para $i < 0$. "Complexo" neste livro significará, salvo menção explícita em contrário, "complexo à esquerda". Uma notação corrente para designar um complexo é $C_\bullet$ $(= (C_i)_{i\geq 0})$ e será usada tanto quanto possível neste texto. C_i é denominado a <u>componente</u> (ou <u>o termo</u>) de grau i de $C_\bullet$.

Existem, para cada $i \geq 0$, dois módulos notáveis:

$$Z_i(C_\bullet) = \text{núcl}(d_i) \qquad (= \text{ciclos de grau } i)$$

$$B_i(C_\bullet) = \text{im}(d_{i+1}) \qquad (= \text{bordos de grau } i).$$

A definição de complexo traduz-se pela inclusão $B_i(C_\bullet) \subseteq Z_i(C_\bullet)$, $i \geq 0$.

Se $B_i(C_\bullet) = Z_i(C_\bullet)$, dizemos que $C_\bullet$ é exato em grau i; $C_\bullet$ é dito <u>exato</u> (ou <u>acíclico</u>) se for exato em grau i, para todo $i \geq 0$.

Em geral, medimos a inexatidão de um complexo através do quociente $Z_i(C_\bullet)/B_i(C_\bullet)$, que é chamado o módulo <u>de homologia de grau</u> i (ou, simplesmente, a <u>homologia em grau</u> i) de $C_\bullet$. A notação usual é $H_i(C_\bullet)$.

Se os termos C_i pertencem a determinada categoria de módulos, dizemos que $C_\bullet$ é um complexo de módulos nesta categoria. Por exemplo, temos complexos de módulos livres, projetivos, injetivos, etc. Neste sentido, uma resolução livre é um complexo exato de módulos livres finitamente gerados.

Em verdade, pode-se até mesmo falar na categoria de complexos, etc. Para nós, será suficiente saber o que se entende por uma aplicação (ou morfismo) de complexos: dados complexos $C_\bullet$ e $C'_\bullet$, com morfismo $C_\bullet \xrightarrow{f} C'_\bullet$ é uma coleção $f = (f_i)_{i\geq 0}$ de R-homomorfismos $f_i: C_i \to C'_i$ tais que o diagrama abaixo é comutativo:

$$\begin{array}{ccccccc} \cdots \to C_{i+1} & \xrightarrow{d_{i+1}} & C_i & \xrightarrow{d_i} & C_{i-1} \to \cdots \\ \downarrow f_{i+1} & & \downarrow f_i & & \downarrow f_{i-1} \\ \cdots \to C'_{i+1} & \xrightarrow{d'_{i+1}} & C'_i & \xrightarrow{d'_i} & C'_{i-1} \to \cdots \end{array}$$

Podemos, então, definir isomorfismo de complexos na maneira óbvia.

Mais precisamente, o que acabamos de definir é um morfismo de grau 0. Se existir um k (fixo) tal que $f_i: C_i \to C_{k+i}$, $i \geq 0$, o morfismo é de grau k.

Passar de um complexo à sua homologia é um processo funtorial. Assim, dado um morfismo $C_\bullet \xrightarrow{f} C'_\bullet$ de complexos, obtemos ao menos um punhado de R-homomorfismos $H_\bullet(f) = (H_i(f))_{i\geq 0}$,

$$H_i(f): H_i(C_\bullet) \to H_i(C'_\bullet).$$

Deixamos ao leitor a tarefa de constatar a existência de tais homomorfismos.

Por uma "sequência exata" de complexos,

$$0 \to C'_\bullet \xrightarrow{f} C_\bullet \xrightarrow{g} C''_\bullet \to 0,$$

entendemos um par de morfismos $f: C'_\bullet \to C_\bullet$, $g: C_\bullet \to C''_\bullet$ de complexos tais que, para todo $i \geq 0$, a sequência

$$0 \to C'_i \xrightarrow{f_i} C_i \xrightarrow{g_i} C''_i \to 0$$

é uma sequência exata curta de módulos.

Em virtude do caráter funtorial da homologia, deduzimos uma família

$$H_i(C'_\bullet) \xrightarrow{H_i(f)} H_i(C_\bullet) \xrightarrow{H_i(g)} H_i(C''_\bullet), \qquad i \geq 0$$

de sequências de R-homomorfismos.

Trata-se de um punhado de sequências desencontradas ou existe um fio comum que as conecte? A resposta está contida na festejada

<u>Proposição III.11</u> ("Sequência exata longa de homologia") - *Seja $0 \to C'_\bullet \xrightarrow{f} C_\bullet \xrightarrow{g} C''_\bullet \to 0$ uma sequência exata de complexos. Então, para todo $i \geq 1$, existe um R-homomorfismo $\delta_i: H_i(C''_\bullet) \to H_{i-1}(C'_\bullet)$* (chamado homomorfismo de conexão) *tal que a sequência*

$$\cdots \to H_i(C'_\bullet) \xrightarrow{H_i(f)} H_i(C_\bullet) \xrightarrow{H_i(g)} H_i(C''_1) \xrightarrow{\delta_i}$$

$$\xrightarrow{\delta_i} H_{i-1}(C'_\bullet) \xrightarrow{H_{i-1}(f)} H_{i-1}(C_\bullet) \xrightarrow{H_{i-1}(g)} H_{i-1}(C''_\bullet) \xrightarrow{\delta_{i-1}}$$

$$\longrightarrow \cdots$$

é um complexo exato.

<u>Demonstração</u>: Daremos a receita para obter δ_i, deixando a verificação dos detalhes como exercício.

Para tanto, focalizemos uma fatia da sequência dada:

$$\begin{tikzcd}
0 \arrow[r] & C'_i \arrow[r, "f_i"] \arrow[d, "d'_i"] & C_i \arrow[r, "g_i"] \arrow[d, "d_i"] & C''_i \arrow[r] \arrow[d, "d''_i"] & 0 \\
0 \arrow[r] & C'_{i-1} \arrow[r, "f_{i-1}"] \arrow[d, "d'_{i-1}"] & C_{i-1} \arrow[r, "g_{i-1}"] \arrow[d, "d_{i-1}"] & C''_{i-1} \arrow[r] \arrow[d, "d''_{i-1}"] & 0 \\
0 \arrow[r] & C'_{i-2} \arrow[r, "f_{i-2}"] & C_{i-2} \arrow[r, "g_{i-2}"] & C''_{i-2} \arrow[r] & 0
\end{tikzcd}$$

Dado um ciclo de grau i de $C''_\bullet$, $z''_i \in Z_i(C''_\bullet)$, queremos antes de mais nada associar a este ciclo um ciclo de grau $i-1$ de $C'_\bullet$. Ora, por hipótese, existe $c_i \in C_i$ tal que $g_i(c_i) = z''_i$. Por outro lado, $g_{i-1}(d_i(c_i)) = d''_i(g_i(c_i)) = d''_i(z''_i) = 0$ já que $z''_i \in Z_i(C''_\bullet)$. Desta maneira, obtemos um elemento $d_i(c_i) \in C_{i-1}$ que é levado no 0 por g_{i-1}, isto é, $d_i(c_i) = f_{i-1}(c'_{i-1})$ para algum $c'_{i-1} \in C'_{i-1}$.

Resta verificar que $c'_{i-1} \in Z_{i-1}(C'_\bullet)$. Mas, temos $f_{i-2}(d'_{i-1}(c'_{i-1})) = d_{i-1}(f_{i-1}(c'_{i-1})) = (d_{i-1} \cdot d_i)(c_i) = 0$ e como f_{i-2} é injetora, resulta $d'_{i-1}(c'_{i-1}) = 0$.

Para completar a receita, é preciso analisar a dependência de $c'_{i-1} \in Z_{i-1}(C'_\bullet)$ do elemento $c_i \in C_i$ selecionado a esmo. Mas se $e_i \in C_i$ é outra escolha permissível com resultado $e'_{i-1} \in C'_{i-1}$, então $g_i(e_i - c_i) = z''_i - z''_i = 0$, de modo que $e_i - c_i \in \operatorname{im}(f_i)$. Neste caso, tem-se $d_i(e_i) - d_i(c_i) \in \operatorname{im}(d_i \cdot f_i)$, logo $d_i(e_i) - d_i(c_i) = f_{i-1}(d'_i(a'_i))$, para certo $a'_i \in C'_i$. Como f_{i-1} é injetor, $e'_{i-1} - c'_{i-1} \in B_{i-1}(C'_\bullet)$. Assim, obtivemos que a <u>classe</u> de c'_{i-1} (módulo bordos) não depende da escolha de c_i, mas tão somente do ciclo inicial $z''_i \in C''_i$. Isto significa que, até agora, inventamos um R-homomorfismo $Z_i(C''_\bullet) \to Z_{i-1}(C'_\bullet)/B_{i-1}(C'_\bullet)$.

Resta mostrar que este induz, por sua vez, o desejado homomorfismo de conexão

$$Z_i(C''_\bullet)/B_i(C''_\bullet) \xrightarrow{\delta_i} Z_{i-1}(C'_\bullet)/B_{i-1}(C'_\bullet) \ .$$

Deixaremos esta tarefa como exercício, bem como a de verificar que os homomorfismos de conexão encaixam sob medida para formar uma sequência exata (longa). //

<u>Observação</u>. Em situações concretas, tem interesse explicitar os homomorfismos de conexão. Na seção 4, veremos um exemplo em que se pode descrever facilmente estes homomorfismos (sequência longa da homologia de Koszul).

C) <u>Os módulos</u> $\mathrm{Tor}_i^R(M,N)$; "<u>décalage</u>".

A construção depende do conceito de produto tensorial de módulos, conceito este totalmente análogo ao de produto tensorial de espaços vetoriais.

Dado R-módulos M e N, escolhemos uma resolução livre de M,

$$\cdots \to F_1 \xrightarrow{d_1} F_o \xrightarrow{d_o} M \to 0,$$

a qual multiplicamos tensorialmente pelo módulo N. Resulta uma sequência de R-homomorfismos

$$\cdots \to F_1 \otimes N \xrightarrow{d_1 \otimes 1_N} F_o \otimes N \xrightarrow{d_o \otimes 1_N} M \otimes N \to 0,$$

que é, de fato, um complexo como se pode verificar facilmente.
(<u>N.B</u>. - Por definição, $(d_i \otimes 1_N)(e_i \otimes n) = d_i(e_i) \otimes n$, onde $e_i \in F_i$ e $n \in N$).

Consideremos, finalmente, o complexo truncado

$$\ldots \to F_1 \otimes N \to F_o \otimes N \to 0.$$

O i-ésimo módulo de homologia deste complexo é denotado por $\mathrm{Tor}_i^R(M,N)$ (ou $\mathrm{Tor}_i(M,N)$). Pode ser demonstrado que tais módulos dependem apenas de M e N e não de uma resolução particular de M.

A sequência longa dos Tor_i é obtida da seguinte maneira. Como dado inicial, temos uma sequência exata de R-módulos

$$0 \to M'' \to M \to M' \to 0$$

e um R-módulo N. Pelo processo usado na demonstração da Proposição III.10, podemos construir resoluções livres simultâneas de M'', M e M', resultando um diagrama cujas sequências horizontais são todas exatas:

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & F''_1 \arrow[r] \arrow[d] & F_1 \arrow[r] \arrow[d] & F'_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & F''_o \arrow[r] \arrow[d] & F_o \arrow[r] \arrow[d] & F'_o \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M'' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Em seguida, multiplicamos tensorialmente por N tudo que está à vista. Resulta um diagrama análogo, cujas sequências horizontais de módulos livres são ainda exatas (uma vez que são cindidas, isto é, $F_i \simeq F''_i \oplus F'_i$). Consideramos, então, o diagrama associado truncado na sequência $0 \to M''\otimes N \to M\otimes N \to M'\otimes N \to 0$. Tal diagrama é, então, uma sequência exata de complexos (verticais), de modo que resulta uma sequência exata longa em homologia:

$$\begin{aligned} \ldots &\to \mathrm{Tor}_i(M'',N) \to \mathrm{Tor}_i(M,N) \to \mathrm{Tor}_i(M',N) \xrightarrow{\delta_i} \\ &\to \mathrm{Tor}_{i-1}(M'',N) \to \ldots\ldots \to \mathrm{Tor}_1(M',N) \xrightarrow{\delta_1} \\ &\to \mathrm{Tor}_o(M'',N) \to \mathrm{Tor}_o(M,N) \to \mathrm{Tor}_o(M',N) \to 0. \end{aligned}$$

Observemos que, como se verifica facilmente, para dois módulos M, N tem-se sempre $\mathrm{Tor}_o(M,N) \simeq M\otimes N$. Assim, a sequência exata dos Tor_i é a sequência apropriada que estende a sequência $M''\otimes N \to M\otimes N \to M'\otimes N \to 0$.

O que dizer dos δ_i? Em alguns casos, os δ_i assumem uma forma particularmente simples (vide o caso da sequência longa da homologia de Koszul, §4). Na situação presente, os homomorfismos de conexão são um pouco intrincados e dependem, para sua explicitação, da natureza dos módulos Tor_i. Em verdade, a estrutura de tais módulos é pouco conhecida (cf. Cap.IV, §1). Por tal, contentamo-nos em tratar um caso especial.

Nomeadamente, seja $I \subset R$ um ideal e consideremos a sequência exata estrutural

$$0 \to I \to R \to R/I \to 0.$$

Aplicando $\mathrm{Tor}_i(-,I)$, obtemos a sequência

$$\begin{aligned} \ldots &\to \mathrm{Tor}_i(I,I) \to \mathrm{Tor}_i(R,I) \to \mathrm{Tor}_i(R/I,I) \\ &\to \mathrm{Tor}_{i-1}(I,I) \to \ldots\ldots\ldots \to \mathrm{Tor}_1(R/I,I) \\ &\to I \otimes I \to I \to I/I^2 \to 0. \end{aligned}$$

Mas, como R é R-livre, $\mathrm{Tor}_i(R,I) = (0)$ para $i \geq 1$ (vide Exercício 4). Da sequência acima resultam, então, as seguintes informações:

$$\mathrm{Tor}_i(R/I,I) \xrightarrow[\sim]{\delta_i} \mathrm{Tor}_{i-1}(I,I), \quad i \geq 2 \quad (\text{"décalage"})$$

$$0 \to \mathrm{Tor}_1(R/I,I) \xrightarrow{\delta_1} I\otimes I \to I^2 \to 0 \quad (\text{"sequência de torção de } I\otimes I\text{"})$$

<u>Obs</u>.: Obtemos resultado análogo de "décalage" com $\mathrm{Tor}_i(-,N)$.

Assim, todos os homomorfismos de conexão são isomorfismos, exceto δ_1 que injeta $\mathrm{Tor}_1(R/I,I)$ no produto tensorial $I\otimes I$, como núcleo do homomorfismo canônico $I\otimes I \to I^2$ tal que $a\otimes b \mapsto ab$. Isto fornece uma descrição implícita (isto é, que depende só de $I\subset R$) de $\mathrm{Tor}_1(R/I,I)$.

Podemos obter $\mathrm{Tor}_1(R/I,I)$ mais explicitamente, usando a própria definição. Seja

$$\begin{array}{ccccccccccc}
\cdots \to & F_1 & & \to & & F_o & \to & R & \to & R/I & \to 0 \\
& & \searrow & & \nearrow & & & & & & \\
& & & Z & & & & & & & \\
& & \nearrow & & \searrow & & & & & & \\
& 0 & & & & 0 & & & & &
\end{array}$$

uma resolução de R/I. Então:

$$\begin{aligned}
\mathrm{Tor}_1(R/I,I) &= \mathrm{nucl}(F_o\otimes I \to R\otimes I)/\mathrm{im}(Z\otimes I) \\
&\simeq \mathrm{nucl}(IF_o \to I)/IZ \\
&\simeq Z \cap IF_o/IZ.
\end{aligned}$$

Observemos, finalmente, que para calcular $\mathrm{Tor}_1(I,R/I)$ podemos usar a mesma resolução para I (truncando em $R \to R/I \to 0$ e aumentando de $I \to 0$). A sequência longa associada a $0 \to Z \to F_o \to I \to 0$ fornece então a sequência exata

$$0 \to \mathrm{Tor}_1(I,R/I) \to Z/IZ \to F_o/IF_o \to I/I^2 \to 0.$$

Por outro lado, é claro que $\ker(Z/IZ \to F_o/IF_o) = (Z\cap IF_o)/IZ$. Resulta que $\mathrm{Tor}_1(I,R/I) \simeq \mathrm{Tor}_1(R/I,I)$.

Na verdade, pode-se mostrar que, <u>quaisquer que sejam os módulos</u> M, N, <u>tem-se</u> $\mathrm{Tor}_i(M,N) \simeq \mathrm{Tor}_i(N,M)$, $i \geq 0$.

Uma última palavra sobre os R-módulos $\mathrm{Tor}_i(I,R/I)$. Das considerações acima ("décalage" + comutatividade), segue que

$$\mathrm{Tor}_i(R/I,R/I) \simeq \mathrm{Tor}_{i-2}(I,I), \quad i \geq 3$$

$$\mathrm{Tor}_2(R/I,R/I) \simeq \mathrm{Tor}_1(I,R/I) \hookrightarrow I \otimes I.$$

Além disso, aplicando $\mathrm{Tor}_1(-,R/I)$ à sequência $0 \to I \to R \to R/I \to \to 0$, resulta que $\mathrm{Tor}_1(R/I,R/I) \simeq I/I^2$.

Consideremos o R-módulo

$$\mathrm{Tor}(R/I,R/I) \overset{\text{def.}}{=} \oplus\, \mathrm{Tor}_i(R/I,R/I) \simeq R/I \oplus I/I^2 \oplus \mathrm{Tor}_1(I,R/I) \oplus \oplus\, \mathrm{Tor}_1(I,I) \oplus \ldots .$$

Por um resultado de Tate [Ta], R/I admite uma resolução livre (infinita, em geral) $\ldots \to F_2 \to F_1 \to F_o \to R/I \to 0$, $F_o = R$, tal que o R-módulo $\bigoplus_{i\geq 0} F_i$ pode ser munido de uma estrutura de R-álgebra diferencial graduada, anti-comutativa. Segue (vide ainda loc.cit.) que $\mathrm{Tor}(R/I,R/I)$ acima definido herda uma estrutura análoga. A importância de tal estrutura é evidente em vários contextos (cf. [G-L],[Ta]).

Em especial, se R é local e $k = R/m$, temos a R-álgebra $\mathrm{Tor}(k,k)$. Os R-módulos $\mathrm{Tor}_i(k,k)$ são k-espaços vetoriais de dimensão finita $b_i = b_i(R)$ (<u>números de Betti</u> de R). O estudo da série $\sum_{i=0}^{\infty} b_i t^i$ (<u>série de Poincaré</u> de R) é um tema central em Álgebra Comutativa (vide "Rebobinando" para outras informações sobre $\mathrm{Tor}_i^R(k,k)$).

D) Dimensão homológica em termos dos $\mathrm{Tor}_i^R(M,N)$.

Queremos dar uma caracterização de d.h.(M) em termos do anulamento dos módulos $\mathrm{Tor}_i^R(M,-)$. Suporemos, para todos efeitos, que $R,\underline{m}$ é local. Pomos $k = R/\underline{m}$.

Proposição III.12 - Seja M um R-módulo. Então, tem-se:

$$\mathrm{d.h.}(M) \leq n \Leftrightarrow \mathrm{Tor}_{n+1}^R(M,k) = (0).$$

Demonstração: ($\Rightarrow$) Pelo processo de "décalage", obtemos

$$\mathrm{Tor}_{n+1}(M,k) \simeq \mathrm{Tor}_n(Z_1,k) \simeq \ldots \simeq \mathrm{Tor}_1(Z_n,k)$$

(precisamente, fracionamos uma resolução livre de comprimento n de M nas sequências curtas de syzygys,

$$\begin{tikzcd}[column sep=small]
0 \arrow[r] & F_n \arrow[r] \arrow[dr, equal] & & F_{n-1} \arrow[r] \arrow[dr] & \ldots \arrow[r] & F_1 \arrow[r] \arrow[dr] & & F_o \arrow[r] & M \arrow[r] & 0 \\
& & Z_n \arrow[ur] & & Z_{n-1} \arrow[ur] & & Z_1 \arrow[ur] & & &
\end{tikzcd}$$

e aplicamos a sequência longa dos Tor a cada uma dessas sequências, sucessivamente).

Como $Z_n = F_n$ é livre, $\mathrm{Tor}_1(Z_n,k) = (0)$. Logo, $\mathrm{Tor}_{n+1}(M,k) = (0)$.

($\Leftarrow$) Seja $\ldots \to F_n \to \ldots \to F_1 \to F_o \to M \to 0$ uma resolução livre (possivelmente infinita) de M. Como acima, por "décalage", temos

$$\mathrm{Tor}_{n+1}(M,k) \simeq \mathrm{Tor}_1(Z_n,k).$$

Mostraremos que $\mathrm{Tor}_1(Z_n,k) = (0) \Rightarrow Z_n$ livre, o que é suficiente para concluir que d.h.$(M) \leq n$. Ora, seja $0 \to Z \to F \to Z_n \to 0$ uma apresentação de Z_n tal que $Z \subset \underline{m}F$ (isto é sempre possível?) e apliquemos a sequência longa dos Tor's a esta sequência. Resulta a sequência exata

$$0 \to \mathrm{Tor}_1(Z_n,k) \to Z/\underline{m}Z \to F/\underline{m}F \to Z_n/\underline{m}Z_n \to 0,$$

logo, por hipótese, a sequência exata

$$0 \to Z/\underline{m}Z \to F/\underline{m}F \to Z_n/\underline{m}Z_n \to 0.$$

Mas, o núcleo de $Z/\underline{m}Z \to F/\underline{m}F$ é $Z \cap \underline{m}F/\underline{m}Z$, como se verifica imediatamente. Assim, $Z \cap \underline{m}F = \underline{m}Z$. Por outro lado, por construção, $Z \subset \underline{m}F$. Segue que $Z/\underline{m}Z = (0)$ e, pelo lema de Nakayama (Exercício 10(b) do Cap.I), $Z = (0)$. Assim, $Z_n \simeq F$ é livre. //

<u>Corolário III.13</u> - <u>Seja</u> $R,\underline{m}$ <u>local</u>, $k = R/\underline{m}$. <u>Tem-se</u>:

$$\mathrm{d.gl.}(R) \leq n \Leftrightarrow \mathrm{Tor}_{n+1}(k,k) = (0).$$

<u>Em particular</u>, $\mathrm{d.gl.}(R) = \mathrm{d.h.}_R(k)$.

<u>Demonstração</u>: $(\Rightarrow)$ Resulta da Proposição III.12.

$(\Leftarrow)$ Pela Proposição III.12, temos $\mathrm{d.h.}_R(k) \leq n$. Novamente, por "décalage", $\mathrm{Tor}_{n+1}(M,k) = (0)$ para qualquer módulo M. Ainda pela Proposição III.12, resulta d.h.$(M) \leq n$ para todo módulo M. Consequentemente, $\mathrm{d.gl.}(R) \leq n$. //

<u>Observação</u>. O corolário mostra, em particular, que (iii) e (iv) do Teorema III.7 são equivalentes. Isto responde por uma grande simplificação na teoria dos anéis regulares.

E) <u>Dimensão homológica na passagem</u> $R \to R/(x)$.

Como antes, $R, \underline{m}$ é um anel local e $x \in \underline{m}$.

Dado um R-módulo M, temos três dimensões homológicas em cena: $d.h._R(M)$, $d.h._R(M/xM)$ e $d.h._{R/(x)}(M/xM)$. Neste parágrafo, queremos comparar estas dimensões, para o que necessitaremos fazer hipóteses sobre a natureza "aritmética" de x. Assim, os resultados a seguir devem ser vistos como primeiros resultados ligando o aspecto aritmético (isto é, divisores de zero, etc.) com o homológico. Eles foram popularizados por Kaplansky [Ka_1] como "teoremas de mudança de anel".

Começaremos com uma desigualdade que vale para homomorfismos arbitrários.

<u>Proposição III.14</u> (Cartan-Eilenberg) - <u>Seja</u> $R \to S$ <u>um homomorfismo de anéis locais</u>. <u>Para todo</u> S-<u>módulo</u> N, <u>que é finitamente gerado sobre</u> R, <u>tem-se</u>

$$d.h._R(N) \le d.h._S(N) + d.h._R(S).$$

(<u>N.B.</u> Um módulo sobre S é naturalmente um módulo sobre R através do homomorfismo $R \to S$).

<u>Demonstração</u>: Se $d.h._S(N) = \infty$ ou $d.h._R(S) = \infty$, não há nada a mostrar. Logo, suporemos ambas finitas. Por indução sobre $d.h._S(N)$.

$d.h._S(N) = 0 \Rightarrow N$ é S-livre $\Rightarrow N \simeq S^d$, algum $d \ge 1$

$\Rightarrow d.h._R(N) = d.h._R(S^d) = d.h._R(S)$ (por que?).

$d.h._S(N) \ge 1 \Rightarrow$ apresentação $0 \to Z \to G \to N \to 0$ de S-módulos, com $d.h._S(Z) = d.h._S(N)-1$

$$\underset{\text{(indução)}}{\Rightarrow} \quad d.h._R(Z) \le d.h._S(Z) + d.h._R(S)$$
$$= d.h._S(N) + d.h._R(S)-1.$$

Agora, examinamos as dimensões homológicas, como R-módulos, dos termos da sequência $0 \to Z \to G \to N \to 0$, usando a Preposição III.10. Primeiro, se $d.h._R(G) \le d.h._R(Z)$ então $d.h._R(N) \le d.h._R(Z)+1$. Levando na desigualdade acima, obtemos, efetivamente, $d.h._R(N) \le d.h._S(N) + d.h._R(S)$. Resta o caso $d.h._R(G) > d.h._R(Z)$, quando então tem-se $d.h._R(N) = d.h._R(G) = d.h._R(S)$, logo, por maior razão, $d.h._R(N) \le d.h._S(N) + d.h._R(S)$. //

Observações. (1) A hipótese de N ser finitamente gerado como R-módulo entra apenas para asseguar que $d.h._R(N)$ tem sentido, dentro do contexto da definição dada neste livro. Com a definição de $d.h.(M)$, para M não finitamente gerado, esta hipótese é supérflua. Por outro lado, ela é sempre satisfeita se o próprio S for finitamente gerado como R-módulo, o que é suficiente para muitas aplicações.

(2) Em geral, não pode-se esperar a igualdade na proposição acima. E a razão é simples: tomemos R um anel regular (pressuporemos o Teorema de Serre-Auslander-Buchsbaum) e R/I um quociente não regular. Então, existe um R/I-módulo N (por exemplo, $N = \underline{m}/I$) tal que $d.h._{R/I}(N) = \infty$. Mas, $d.h._R(N) < \infty$ e $d.h._R(R/I) < \infty$ já que R é regular. Logo, não há igualdade. Mas, o mal está todo presente neste exemplo. Em verdade, supondo sempre que S é finitamente gerado como R-módulo, se tivermos $d.h._R(S) < \infty$ e $d.h._S(N) < \infty$, então vale a igualdade. Este resultado, devido a

Auslander-Buchsbaum $[(A-B)_2]$, será obtido como consequência da igualdade de Auslander-Buchsbaum (neste capítulo, §3).

Em seguida, especializaremos a situação acima, pondo $S = R/(x)$, $x \in \underline{m}$. A primeira proposição é uma consequência imediata do caso da igualdade na Proposição III.14, conforme obtido por Auslander-Buchsbaum (vide Obs.2 acima). Como ela se insere naturalmente no contexto desta seção, daremos seu enunciado, sugerindo uma demonstração alternativa.

<u>Proposição III.15</u> - <u>Seja</u> $R,\underline{m}$ <u>local</u>, $x \in \underline{m}$ <u>tal que</u> $x \notin Z(R)$ <u>e</u> N, <u>um</u> $R/(x)$-<u>módulo tal que</u> $d.h._{R/(x)}(N) < \infty$. <u>Então</u>

$$d.h._R(N) = d.h._{R/(x)}(N) + 1.$$

<u>Demonstração</u>: Como $x \notin Z(R)$, $0 \to R \xrightarrow{x} R \to R/(x) \to$ é uma resolução livre de $R/(x)$. Consequentemente, pela Proposição III.14, tem-se $d.h._R(N) \leq d.h._{R/(x)}(N) + 1$.

Por outro lado, um exame cuidadoso da demonstração da Proposição III.14, com $S = R/(x)$, põe em evidência o fato seguinte: se $d.h._S(N) < \infty$, a igualdade $d.h._R(N) = d.h._S(N) + d.h._R(S)$ tem lugar a menos, possivelmente, que $d.h._S(N) \leq 1$. Assim, para terminar a proposição, temos apenas de verificar o caso $d.h._{R/(x)}(N) \leq 1$ diretamente, o que será deixado como exercício. //

<u>Proposição III.16</u> - <u>Seja</u> $R,\underline{m}$ <u>local e</u> $x \in \underline{m}$ <u>tal que</u> $x \notin Z(R)$. <u>Se</u> M <u>é um</u> R-<u>módulo tal que</u> $x \notin Z(M)$, <u>então</u>

$$d.h._{R/(x)}(M/xM) = d.h._R(M).$$

Faremos uso do seguinte lema.

<u>Lema III.17</u> - <u>Seja</u> N <u>um</u> R-<u>módulo e</u> $x \in \underline{m}$ <u>tal que</u> $x \notin Z(N)$. <u>Então</u> N/xN $R/(x)$-<u>livre</u> $\Rightarrow$ N R-<u>livre</u>.

<u>Demonstração</u>: Seja $0 \to Z \to F \xrightarrow{\varphi} N \to 0$ uma apresentação de N tal que $Z \subset \underline{m}F$. Mediante multiplicação tensorial por $R/(x)$, obtemos a sequência exata

$$0 \to (Z \cap xF)/xZ \to Z/xZ \to F/xF \to N/xN \to 0.$$

Por outro lado, existe um homomorfismo sobrejetor

$$\psi\colon (0):_N x \to (Z \cap xF)/xZ,$$

definido da seguinte maneira: se $a \in (0):_N x$, tomamos qualquer $b \in F$ tal que $\varphi(b) = a$ e pomos $\psi(a) = xb$. Deixaremos como exercício a verificação de que ψ está bem definido e é um homomorfismo sobrejetor.

Por hipótese, $(0):_N x = (0)$. Resulta, então, uma sequência exata

$$0 \to Z/xZ \to F/xF \to N/xN \to 0,$$

com a propriedade adicional de que $Z/xZ \subset \underline{m}\cdot F/xF$. Por hipótese, N/xN é $R/(x)$-livre. Logo $F/xF \simeq (Z/xZ) \oplus (N/xN)$. Necessariamente, $Z/xZ = (0)$. Novamente, pelo lema de Nakayama, $Z = (0)$. //

Voltemos à proposição.

<u>Demonstração</u> (da Prop.III.16): Primeiramente, vejamos que $d.h._{R/(x)}(M/xM) < \infty \Rightarrow d.h._R(M) < \infty$. De fato, seja

$$\cdots \to F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

uma resolução livre (possivelmente infinita) de M. Aplicando "décalage" ou, diretamente, como na demonstração do lema, obtemos uma sequência exata

$$\cdots \to F_n/xF_n \to F_{n-1}/xF_{n-1} \to \cdots \to F_1/xF_1 \to F_o/xF_o \to M/xM \to 0.$$

(N.B. Precisamos $x \notin Z(M)$ para a sequência $0 \to Z_1 \to F \to M \to 0$ e $x \notin Z(R)$ ($\Rightarrow x \in Z(Z_i)$) para a sequência de syzygys $0 \to Z_{i+1} \to F_i \to Z_i \to 0$).

Pelo Corolário III.6, Z_n/xZ_n é $R/(x)$-livre, para algum n. Pelo lema anterior, Z_n é R-livre. Logo, $d.h._R(M) < \infty$.

Finalmente, se $d.h._R(M) = n$, repetimos o argumento acima para uma resolução livre de M, de comprimento n. //

Como consequência, obtemos a última igualdade de "mudança de anel".

Corolário III.18 - R,m local, $x \in m$ tal que $x \notin Z(R)$ e tal que $x \notin Z(M)$ (M um R-módulo). Então, se $d.h._R(M) < \infty$, tem-se:

$$d.h._R(M/xM) = d.h._R(M) + 1.$$

Observação. Em ambos Proposição III.16 e Corolário III.18, as hipóteses de que $x \notin Z(R)$ e $x \notin Z(M)$ são exigidas simultaneamente. É natural perguntar se uma implica na outra. Ora, é claro que $x \notin Z(R) \underset{\forall x}{\Longrightarrow} x \notin Z(M)$ significa que M é livre de torção (vide Cap.I, §1, Exemplo (6)). Quanto à implicação $x \notin Z(M) \Rightarrow$ $\Rightarrow x \notin Z(R)$ é falsa, em geral. Mas, os contra-exemplos que se sabe escrever são todos com $d.h._R(M) = \infty$. Se $d.h._R(M) < \infty$, trata-se de um problema aberto, conhecido como a "conjectura do divisor de zero". Trataremos deste problema no Capítulo IV.

§3. A igualdade de Auslander-Buchsbaum. Módulos perfeitos.

Nesta seção, demonstraremos uma igualdade fundamental, que pode ser considerada como um dos vértices da Álgebra Comutativa. A demonstração propriamente dita, após o aparato que vimos desenvolvendo nas seções anteriores, adquire bastante simplicidade. A igualdade relaciona os dois invariantes centrais deste curso, profundidade e dimensão homológica, de uma maneira surpreendente. As aplicações, por outro lado, poder-se-ia dizer que são tantas quanto se queira; daremos algumas mais típicas.

Teorema III.19 (Auslander-Buchsbaum [(A-B)$_1$]) - Seja $R,\underline{m}$ um anel local. Se $M \neq (0)$ é um R-módulo tal que $d.h._R(M) < \infty$, então

$$d.h._R(M) + \mathrm{prof}_{\underline{m}}(M) = \mathrm{prof}_{\underline{m}}(R).$$

Demonstração: Distinguiremos três casos.

1) $\mathrm{prof}(R) = 0$.

Neste caso, veremos que, necessariamente M é livre e, consequentemente, $d.h.(M) = 0$ e $\mathrm{prof}(M) = \mathrm{prof}(R) = 0$.

Ora, se $d.h.(M) = n > 0$, o syzygy Z_{n-1} de uma resolução livre de M (de comprimento n) tem $d.h. = 1$. Logo, podemos supor de entrada que o próprio M tem $d.h. = 1$. Neste caso, seja $0 \to F_1 \to F_o \to M \to 0$ uma resolução livre de M tal que $F_1 \subset \underline{m}F_o$. Por hipótese, $\underline{m} \in \mathrm{Ass}(R)$. Logo, $\underline{m} = (0):r$, para algum $r \in R$, $r \neq 0$. Segue que $rF_1 \subset r\cdot\underline{m}F_o = (0)$. Mas, F_1 é livre; logo, $r = 0$: contradição.

2) $\text{prof}(R) > 0$ e $\text{prof}(M) = 0$.

Procedemos por indução sobre $\text{prof}(R)$. Para isto, tomemos $x \notin Z(R)$. Então, $\text{prof}(R/(x)) = \text{prof}(R)-1$ (Cap.II, §1). Precisamos também de um $R/(x)$-módulo para aplicar a hipótese de indução. O candidato é Z/xZ, onde $0 \to Z \to F \to M \to 0$ é uma apresentação de M. Devemos verificar duas coisas: $\text{d.h.}_{R/(x)}(Z/xZ) < \infty$ e $\text{prof}_{R/(x)}(Z/xZ) = 0$. A primeira resulta imediatamente da Proposição III.16 já que $x \notin Z(Z)$ (notação, quantos crimes...). Quanto à segunda, precisamos calcular um pouco. Por hipótese, $\underline{m} \in \text{Ass}(M)$: seja $0 \neq a \in M$ tal que $a\underline{m} = 0$. Escolhamos uma pre-imagem e de a em F. Como $a \neq 0$, $e \notin Z$; segue que $xe \notin xZ$ (F é livre!). Por outro lado, $e\underline{m} \subset Z$, logo $xe \cdot \underline{m} \subset xZ$. Assim, $\underline{m}$ está contido num primo associado de Z/xZ, logo é um tal primo (não faz diferença considerar Z/xZ como R-módulo ou $R/(x)$-módulo no que toca à profundidade, cf. Prop.II.6, Cap.II).

Estamos, agora, prontos para aplicar a hipótese de indução, e o fazemos:

$$\text{d.h.}_{R/(x)}(Z/xZ) = \text{prof}_{\underline{m}/(x)}(R/(x)).$$

Mas, temos: $\text{d.h.}_{R/(x)}(Z/xZ) = \text{d.h.}_R(Z)$ (Prop.III.16)

$= \text{d.h.}_R(M) - 1$ (Lema III.9),

e $\text{prof}(R/(x)) = \text{prof}(R) - 1.$

Consequentemente, $\text{d.h.}_R(M) = \text{prof}(R)$, como queríamos.

3) $\text{prof}(R) > 0$ e $\text{prof}(M) > 0$.

Neste, podemos escolher $x \in \underline{m}$ tal que $x \notin Z(R)$ e $x \notin Z(M)$

(por que?). Como antes, temos:

$$d.h._{R/(x)}(M/xM) = d.h._R(M) \qquad \text{(Prop.III.16)}$$

$$prof(R/(x)) = prof(R)-1$$

$$prof_{\underline{m}/(x)}(M/xM) = prof_{\underline{m}}(M/xM) \qquad \text{(vide Prop.II.6,Cap.II)}$$

$$= prof_{\underline{m}}(M)-1 \qquad \text{(Cap.II,§1).}$$

Então, pela hipótese indutiva ou pelos casos 1 e 2, e usando as igualdades acima, obtemos a igualdade procurada. //

Em seguida, consideraremos algumas aplicações da igualdade de Auslander-Buchsbaum. A primeira delas é para a obtenção de uma igualdade entre dimensões homológicas na passagem por um homomorfismo (vide Prop.III.14,§2).

<u>Corolário III.20</u> (Auslander-Buchsbaum [$(A-B)_2$]) - <u>Seja</u> $(R,\underline{m}) \to (S,\underline{n})$ <u>um homomorfismo de anéis locais tais que</u> S <u>seja finitamente gerado como</u> R-<u>módulo</u>. <u>Seja</u> N <u>um</u> S-<u>módulo finitamente gerado</u>. <u>Então</u>

$$\left.\begin{array}{l} d.h._R(S) < \infty \\ d.h._S(N) < \infty \end{array}\right\} \Rightarrow d.h._R(N) = d.h._S(N) + d.h._R(S).$$

<u>Demonstração</u>: Pela Proposição III.14, temos a desigualdade $d.h._R(N) \leq d.h._S(N) + d.h._R(S)$. Logo, $d.h._R(N) < \infty$. Pelo Teorema III.19 e pelo Exemplo (7), Capítulo II, §2, temos:

$$d.h._R(N) = prof_{\underline{m}}(R) - prof_{\underline{m}}(N)$$

$$d.h._R(S) = prof_{\underline{m}}(R) - prof_{\underline{m}}(S)$$

$$d.h._S(N) = prof_{\underline{n}}(S) - prof_{\underline{n}}(N) = prof_{\underline{m}}(S) - prof_{\underline{m}}(N).$$

Disso segue o resultado procurado. //

Corolário III.21 - Seja $R \to S$ um homomorfismo injetor de anéis locais tal que S é finitamente gerado como R-módulo. Então:

$$\begin{cases} \mathrm{d.h.}_R(S) < \infty \\ S \quad \text{C-M} \end{cases} \iff \begin{cases} S \quad \text{é } R\text{-livre} \\ R \quad \text{C-M} \end{cases}$$

Demonstração: A implicação " $\Leftarrow$ " é imediata. Reciprocamente, as condições $\mathrm{d.h.}_R(S) < \infty$ e S C-M implicam:

$$\begin{aligned} \mathrm{prof}(S) &\le \mathrm{prof}(S) + \mathrm{d.h.}_R(S) = \mathrm{prof}(R), && \text{(Teor.III.19)} \\ &\le \dim(R) = \dim(S), && \text{(propriedade das extensões inteiras)} \\ &= \mathrm{prof}(S). \end{aligned}$$

Logo, $\mathrm{d.h.}_R(S) = 0$ e $\mathrm{prof}(R) = \dim(R)$, como queríamos. //

(Exercício. Uma formulação análoga do último corolário é possível, com "regular" substituindo "C-M". Qual?)

A próxima consequência é conhecida como Teorema de Rees (publicado por este matemático em 1957, portanto simultaneamente - mas, de forma independente - com a publicação da igualdade de Auslander-Buchsbaum). A demonstração (!) abaixo é, paradoxalmente, atribuida a Chase no livro de Kaplansky [Ka_2].

Corolário III.22 (Rees [Re]) - Seja R um anel noetheriano e $M \neq (0)$ um R-módulo. Então:

$$\mathrm{prof}(P) \le \mathrm{d.h.}_R(M), \quad \text{para todo} \quad P \in \mathrm{Ass}(M).$$

Demonstração: Só interessa o caso em que $d.h._R(M) < \infty$. Seja $P \in Ass(M)$. Então:

$$\begin{aligned} prof(P) &\leq prof(P_P) = prof_{P_P}(R_P) \\ &= d.h._{R_P}(M_P) + prof_{P_P}(M_P) \qquad \text{(Teorema III.19)} \\ &= d.h._{R_P}(M_P) + 0 \\ &\leq d.h._R(M). \end{aligned}$$

//

(N.B. A rigor, como só definimos d.h. com precisão no caso de um anel local, só temos o teorema acima neste caso. Contamos com a indulgência do leitor neste ponto de menor importância).

Em particular, como $Ass(M) = Ass(R/(0:M))$ (em verdade, muito menos do que isto é suficiente), resulta do corolário que $prof(0:M) \leq d.h._R(M)$. Aproveitamos, então, esta ocasião para inserir um conceito importante.

Definição III.23 (R noetheriano) - Um R-módulo M é perfeito se $prof(0:M) = d.h._R(M)$.

Esta terminologia remonta a Macaulay [Mac].

A igualdade de Auslander-Buchsbaum intervem, ainda desta vez, para relacionar módulos perfeitos com módulos C-M.

Corolário III.24 (Macaulay-Gröbner-Rees) - Seja R um anel local C-M e $I \subseteq R$ um ideal tal que $d.h.(R/I) < \infty$. Então

$$R/I \text{ é perfeito} \Leftrightarrow R/I \text{ é C-M}.$$

Demonstração: ($\Rightarrow$) Temos

$$\begin{aligned} \mathrm{prof}(R/I) &= \mathrm{prof}(R) - \mathrm{d.h.}_R(R/I), && \text{pelo Teorema III.19} \\ &= \mathrm{prof}(R) - \mathrm{prof}(I), && \text{porque } R/I \text{ é perfeito} \\ &= \dim(R) - \mathrm{alt}(I), && \text{porque } R \text{ é C-M} \\ &= \dim(R/I), && \text{pelo Teorema II.13.} \end{aligned}$$

($\Leftarrow$) É análoga:

$$\begin{aligned} \mathrm{d.h.}_R(R/I) &= \mathrm{prof}(R) - \mathrm{prof}(R/I), && \text{pelo Teorema III.19} \\ &= \mathrm{prof}(R) - \dim(R/I), && \text{porque } R/I \text{ é C-M} \\ &= \mathrm{prof}(R) - (\dim R - \mathrm{alt}(I)), && \text{pelo Teorema II.13} \\ &= \mathrm{prof}(I), && \text{porque } R \text{ é C-M.} \end{aligned}$$

//

No que segue, daremos alguns exemplos não triviais de módulos perfeitos. Parece ser esta uma boa oportunidade para enfatizar dois aspectos: primeiro, <u>os módulos perfeitos constituem os módulos de dimensão homológica finita</u> "<u>par excellence</u>", <u>no sentido de que existem de maneira mais ou menos universal, independente do anel</u>; segundo, <u>a principal fonte de módulos perfeitos é a clássica Teoria dos Invariantes de Cayley, Silvester et al, se bem que o pleno reconhecimento disto apenas tenha se dado nas últimas décadas</u>.

<u>Exemplos</u>. (1) Seja $R,\underline{m}$ um anel local e seja $I = (\underline{x}) \subset R$, com $\underline{x} = x_1,\dots,x_n \in \underline{m}$ uma R-sequência. Então, R/I é perfeito.

Há várias maneiras de verificar este fato. Eis uma extremamente simples, usando a igualdade do Corolário III.20. Como $\mathrm{prof}(I) = n$, devemos verificar que $\mathrm{d.h.}_R(R/I) = n$. Isto é claro se $n = 1$, pois $0 \to R \xrightarrow{x} R \to R/(x) \to 0$ é uma resolução livre. Por indução, $\text{d.h.}_R(R/(x_1,\dots,x_{n-1})) = n-1$. Agora aplicamos o Corolário III.20 com $S = R/(x_1,\dots,x_{n-1})$ e $N = R/I$.

Observação. O fato acima de que $\text{d.h.}(R/I) = n$ também é uma consequência imediata da Proposição III.15. Em verdade, para qualquer anel R, R/I (I gerado por R-sequência) é um módulo perfeito, já que $\text{d.h.}_R(R/I) = n$ vale em geral e pode-se até construir uma resolução livre "universal" de R/I (vide a seção seguinte, sobre complexos de Koszul).

(2) Seja $R,\underline{m}$ um anel local e seja M um módulo $\underline{m}$-primário (isto é, $\text{Ass}(M) = \{\underline{m}\}$) tal que $\text{d.h.}(M) < \infty$. Então M é perfeito.

Isto é fácil: como $(0:M)$ é $\underline{m}$-primário (vide Cap.I, §2), temos $\text{prof}(0:M) = \text{prof}(R)$. Pela igualdade de Auslander-Buchsbaum, $\text{d.h.}(M) = \text{prof}(R)$.

Neste exemplo vemos a extraordinária força da teoria, especialmente da igualdade de Auslander-Buchsbaum, já que na prática é difícil explicitar uma resolução livre de um ideal $\underline{m}$ primário.

Contudo, a teoria dos módulos perfeitos não se justificaria apenas pelos exemplos acima. O joio é algo no estilo do próximo exemplo.

(3) Seja $R = \mathbb{Z}[X_{ij}]$ (anel de polinômios), $1 \le i \le m$, $1 \le j \le n$. Seja $I_t \subset R$ o ideal gerado pelos determinantes $t \times t$ da matriz "genérica" (X_{ij}). Então R/I_t é um módulo perfeito e $\text{prof}(I_t) = (m-t+1)(n-t+1)$.

Agora, sim, temos dificuldades! Este fato (ou a sua de monstração) tem sido objeto desde Macaulay. A palavra definitiva é de Hochster-Eagon-Northcott ([(EN_1)],[H-E]). É importante salientar que este exemplo é substancialmente diferente dos anteriores, já que se deseja um módulo perfeito sem se saber, a priori, a profundidade do anulador.

Se, digamos, $m \geq n$ e $t = n$, então existe uma resolução livre explícita de R/I_t (o complexo de Eagon-Northcott); vide [$(E\text{-}N)_1$]. No caso $t < n$, existe evidência de que se pode escrever explicitamente resoluções livres ([La],[Ni]).

Não demonstraremos nenhum destes fatos (precisaríamos outros Colóquios!). Gostaríamos, contudo, de por em relevo um aspecto fundamental destes módulos, a saber, o da sua "perfeição genérica". Precisamente, mostraremos:

<u>Proposição III.25</u> - <u>Seja</u> S <u>um anel noetheriano</u>, (s_{ij}), $1 \leq i \leq m$, $1 \leq j \leq n$, <u>uma matriz a coeficientes em</u> S <u>e</u> $I_t = I_t(s_{ij}) \subset S$ <u>o ideal gerado pelos determinantes</u> $t \times t$ <u>de</u> (s_{ij}). <u>Se</u> $I_t \neq S$ <u>e</u> $\operatorname{prof}(I_t) \geq (m-t+1)(n-t+1)$, <u>então</u> S/I_t <u>é um módulo perfeito</u> <u>e</u> $\operatorname{prof}(I_t) = (m-t+1)(n-t+1)$.

Evidentemente, demonstraremos esta proposição pressupondo o Exemplo (3) acima[1]. Desta maneira, consideraremos o homomorfismo "especialização" $R = \mathbb{Z}[X_{ij}] \to S$ tal que $X_{ij} \mapsto s_{ij}$. É claro que $I_t(s_{ij}) = I_t(X_{ij}) \cdot S$. A proposição segue, então, do seguinte resultado, que nos presenteia com um bonus extra.

(1) Incidentalmente, a proposição mostra que, no caso genérico, poderíamos ter começado com $A[X_{ij}]$ em vez de $Z[X_{ij}]$, onde A é um anel noetheriano qualquer.

Proposição III.26 ("Estabilidade dos módulos perfeitos") - Seja $R \to S$ um homomorfismo de anéis (noetherianos) e seja $I \subset R$ um ideal tal que $IS \neq S$. Então:

$$\begin{cases} R/I \text{ perfeito} \\ \quad e \\ \operatorname{prof}(IS) \geq \operatorname{prof}(I) \end{cases} \Rightarrow \begin{cases} S/IS \text{ perfeito} \\ \quad e \\ d.h._S(S/IS) = d.h._R(R/I) \end{cases}$$

Além disso, se $0 \to F_n \to \ldots \to F_1 \to F_o \to R/I \to 0$ é uma resolução de R/I, de comprimento $= d.h.(R/I)$, então

$$0 \to F_n \otimes_R S \to \ldots \to F_o \otimes_R S \to S/IS \to 0$$

é uma resolução de S/IS.

Demonstração: Seja d o maior inteiro tal que $\operatorname{Tor}_d^R(R/I,S) \neq (0)$. Suponhamos, por um momento, que $\operatorname{prof}(IS) + d \leq d.h.(R/I)$. Neste caso, como $\operatorname{prof}(IS) \geq \operatorname{prof}(I) = d.h.(R/I)$ por hipótese, resulta $d = 0$. Isto implica em que, se $F_{\bullet} \to R/I \to 0$ é uma resolução de R/I, então $F_{\bullet} \otimes_R S \to S/IS \to 0$ é uma resolução de S/IS. Assim, $d.h._S(S/IS) \leq d.h._R(R/I) = \operatorname{prof}(I) \leq \operatorname{prof}(IS)$ e como $\operatorname{prof}(IS) \leq$ $\leq d.h._S(S/IS)$ (Cor.III.22), resulta a igualdade $\operatorname{prof}(IS) =$ $= d.h._S(S/IS)$, como queríamos.

Desta forma, a demonstração depende agora do seguinte resultado.

Proposição III.27 ("Sensibilidade à profundidade"; forma fraca) Seja R um anel noetheriano, M, N dois R-módulos e $\underline{x} = x_1,\ldots,x_n$ $\in 0{:}M$. Seja d o maior inteiro para o qual $\operatorname{Tor}_d(M,N) \neq (0)$. Então:

$$\underline{x} \text{ N-sequência} \Rightarrow d+n \leq d.h.(M).$$

(Para completar a demonstração anterior, aplicamos esta última proposição com $N = S$, $M = R/I$).

Demonstração: Por indução sobre n.

Se $n = 0$, queremos $d \leq d.h.(M)$. (Suponhamos $R,\underline{m}$ local, por simplicidade). Ora, sabemos que $d.h.(M) \leq d-1 \Leftrightarrow$ $\Leftrightarrow \mathrm{Tor}_d(M,N') = (0)$ para todo módulo N'. Como $\mathrm{Tor}_d(M,N) \neq (0)$, tem-se $d.h.(M) \geq d$.

Suponhamos, então, $n > 0$. Pondo $x = x_1$, temos a sequência exata $0 \to N \xrightarrow{x} N \to N/xN \to 0$, que fornece uma sequência longa de Tor's:

$$\begin{aligned} \cdots \to \mathrm{Tor}_i(M,N) &\xrightarrow{x} \mathrm{Tor}_i(M,N) \to \mathrm{Tor}_i(M,N/xN) \\ \to \mathrm{Tor}_{i-1}(M,N) &\xrightarrow{x} \mathrm{Tor}_{i-1}(M,N) \to \mathrm{Tor}_{i-1}(M,N/xN) \to \cdots \end{aligned}$$

Como $x \in 0:M$, é fácil ver que $\mathrm{Tor}_i(M,N) \xrightarrow{x} \mathrm{Tor}_i(M,N)$ é a aplicação nula, para todo i. Obtemos, assim, sequências curtas

$$0 \to \mathrm{Tor}_i(M,N) \to \mathrm{Tor}_i(M,N/xN) \to \mathrm{Tor}_{i-1}(M,N) \to 0.$$

Por hipótese, $\mathrm{Tor}_{d+1}(M,N) = (0)$. Logo,

$$\mathrm{Tor}_{d+1}(M,N/xN) \simeq \mathrm{Tor}_d(M,N) \neq (0).$$

Analogamente, $\mathrm{Tor}_{d+2}(M,N) = (0)$ implica $\mathrm{Tor}_{d+2}(M,N/xN) = (0)$. Por indução, temos $(d+1)+(n-1) \leq d.h.(M)$, logo $d+n \leq d.h.(M)$. //

<u>Rebobinando</u>: <u>demonstração do Teorema de Serre-Auslander-Buchsbaum</u>

A esta altura, tendo desenvolvido uma teoria motivada, por assim dizer, pelo teorema de Serre-Auslander-Buchsbaum, nada mais justo do que usar esta teoria para demonstrar o teorema.

Remetemos o leitor de volta ao Teorema III.7, onde se afirmava a equivalência de quatro condições.

(i) $\Rightarrow$ (ii) ($R,\underline{m}$ regular $\Rightarrow$ $d.h._R(R/\underline{m}) = \dim(R)$)

Por hipótese, $\underline{m}$ é gerado por uma R-sequência. Logo, $R/\underline{m}$ é um módulo perfeito (Exemplo (1), §3).

(ii) $\Rightarrow$ (iii) ($d.h.(R/\underline{m}) = \dim(R) \Rightarrow d.h.(R/\underline{m}) < \infty$). Trivial.

(iii) $\Leftrightarrow$ (iv) ($d.h.(R/\underline{m}) < \infty \Leftrightarrow d.gl.(R) < \infty$). É o Corolário III.13.

(iii) $\Rightarrow$ (i) ($d.h.(R/\underline{m}) < \infty \Rightarrow R,\underline{m}$ regular). Esta implicação é o núcleo do teorema.

Ponhamos $d.h.(R/\underline{m}) = h$. Como, além disso, $\text{prof}(R/\underline{m}) = 0$, resulta da igualdade de Auslander-Buchsbaum que $d.h.(R/\underline{m}) = \text{prof}(R)$. Queremos mostrar, portanto, que $\mu(\underline{m}) = d.h.(R/\underline{m})$. Seja $\mu(\underline{m}) = s$. O resultado segue dos dois fatos seguintes:

(a) $\text{Tor}_s^R(k,k) \neq (0)$, $k = R/\underline{m}$.

(b) $\dim_k \text{Tor}_i^R(k,k) = \dim_k F_i/\underline{m}F_i$, $i \geq 0$, onde

$$\cdots \to F_i \to F_{i-1} \to \cdots \to F_o \to R/\underline{m} \to 0$$

é uma resolução <u>mínima</u> (isto é, $\text{im}(F_i) \subset \underline{m}F_{i-1}$, $i \geq 1$) de $R/\underline{m}$.

Com efeito, de (a) e (b) segue que $F_s/\underline{m}F_s \neq (0)$, logo

$F_s \neq (0)$. Como $s \geq \text{prof}(R) = \text{d.h.}(R/\underline{m})$, forçosamente $s = \text{prof}(R)$, como queríamos.

Resta-nos mostrar os fatos (a) e (b) acima.

Quanto a (b), mais geralmente, seja

$$\cdots \to F_i \xrightarrow{d_i} F_{i-1} \to \cdots \to F_o \to M \to 0$$

uma resolução mínima de um módulo M (sempre existe; por que?), possivelmente infinita. Tensorizando com $R/\underline{m}$, obtemos um complexo

$$\bar{F}_{\bullet}: \quad \cdots \to F_i/\underline{m}F_i \xrightarrow{\bar{d}_i} F_{i-1}/\underline{m}F_{i-1} \to \cdots \to F_o/\underline{m}F_o \to 0$$

cujas diferenciais $\bar{d}_i$ são triviais (isto é, $=0$). Logo, $H_i(\bar{F}_{\bullet}) = F_i/\underline{m}F_i$, $i \geq 0$. Mas, por definição, $\text{Tor}_i^R(M,k) \simeq H_i(\bar{F}_{\bullet})$, donde o resultado.

A demonstração de (a) é menos simples. Em verdade, (a) é apenas uma pequena faceta do seguinte resultado mais geral:

(Tate [Ta]) - Se $R,\underline{m}$ é um anel local com $k = R/\underline{m}$, a aplicação k-linear canônica $\Lambda(\underline{m}/\underline{m}^2) \to \text{Tor}^R(k,k) = \sum_{i\geq 0} \text{Tor}_i^R(k,k)$ é injetora.

A aplicação canônica $\Lambda(\underline{m}/\underline{m})^2 \to \text{Tor}^R(k,k)$ resulta da propriedade universal da álgebra exterior, já que existe de saida um k-isomorfismo $\underline{m}/\underline{m}^2 \simeq \text{Tor}_1^R(k,k)$ (vide "décalage" dos Tor's, §2, C.) e que $\text{Tor}^R(k,k)$ é uma álgebra diferencial graduada, anticomutativa, etc. (Cartan-Eilenberg). O problema é a injetividade.

Existe uma outra demonstração, de autoria de Serre [Se], usando diretamente técnicas de resoluções mínimas.

Não demonstraremos o resultado acima, mas o leitor interessado deveria ler uma das (ou ambas!) memórias acima mencionadas.

Finalmente, uma demonstração diferente da implicação (iii) ⇒ (i) é indicada em "Presto" (Corolário do Teorema V-F).

§4. O método do complexo de Koszul.

Na seção anterior, relacionamos, através da igualdade de Auslander-Buchsbaum, dois invariantes importantes de um módulo: a profundidade e a dimensão homológica. Sempre que se obtém um teorema deste tipo, pode-se esperar muitas aplicações. Imbuidos deste espírito, introduziremos agora um complexo cuja homologia "mede" a diferença entre a profundidade e o número de geradores (de um ideal).

Faremos uso de propriedades da álgebra exterior de um módulo.

O complexo de Koszul (ou complexo da álgebra exterior) depende de uma sequência $x_1,\ldots,x_n \in R$ (R pode ser qualquer anel comutativo). Fixada uma base $e_1,\ldots,e_n$ de R^n, existe um único homomorfismo $R^n \xrightarrow{\varphi} R$ tal que $e_i \mapsto x_i$, $i=1,\ldots,n$. Este homomorfismo induz outros:

$$\Lambda^r R^n \xrightarrow{d_r} \Lambda^{r-1} R^n, \qquad r \geq 1$$

$$e_{i_1} \wedge \ldots \wedge e_{i_r} \mapsto \sum_{t=1}^{r} (-1)^t \, x_{i_t} \, e_{i_1} \wedge \ldots \wedge \hat{e}_{i_t} \wedge \ldots \wedge e_{i_r}$$

(onde "∧" sobre um elemento indica a supressão deste elemento).

Evidentemente, $d_1 = \varphi$ desde que façamos as identificações usuais $\Lambda^1 R^n = R^n$ e $\Lambda^o R^n = R$.

Verifica-se, diretamente, que $d_r \cdot d_{r+1} = 0$, $r \geq 1$. Logo, obtemos um complexo

$$0 \to \Lambda^n R^n \xrightarrow{d_n} \Lambda^{n-1} R^n \to \ldots \to \Lambda^2 R^n \xrightarrow{d_2} \Lambda^1 R^n \xrightarrow{d_1} \Lambda^o R^n \to 0$$

de módulos livres. Usaremos a notação $K_{\bullet}(\underline{x};R)$ para o complexo de Koszul (K = Koszul, $\underline{x}$ para enfatizar a dependência nos elementos $x_1,\ldots,x_n$). Insistimos em que os termos do complexo não dependem de $\underline{x} = x_1,\ldots,x_n$; as diferenciais d_r, sim.

O complexo será usado para testar $\underline{x}$ quanto a R-sequências. Se quisermos testar $\underline{x}$ quanto a M-sequências (M um R-módulo), usaremos o complexo $K_{\bullet}(\underline{x};R) \otimes_R M$, que será designado por $K_{\bullet}(\underline{x};M)$. Assim, estendemos o complexo de Koszul à categoria de todos os módulos e logo veremos que $K_{\bullet}(\underline{x};M)$ tem boas propriedades funtoriais.

Há duas maneiras adicionais de ver o complexo $K_{\bullet}(\underline{x};R)$:

(1) <u>Como álgebra associativa</u>.

Consideramos a álgebra exterior $\Lambda R^n = \sum\limits_r \Lambda^r R^n$. Trata-se de uma R-álgebra associativa, graduada ($\Lambda^r R^n$ é a parte de grau r) tal que

$$v \wedge w = (-1)^{rs}\, w \wedge v \quad , \quad \text{se} \quad v \in \Lambda^r R^n, \quad w \in \Lambda^s R^n$$

e

$$v \wedge v = 0 \quad , \quad \text{se} \quad v \in \Lambda^r R^n, \quad r \text{ ímpar}.$$

Além disso, as diferenciais d_r fornecem, de maneira óbvia, um R-homomorfismo $d\colon \Lambda R^n \to \Lambda R^n$ (de grau -1, pois vem das diferenciais d_r) tal que

$$d \cdot d = 0$$

e $\quad d(v \wedge w) = d(v) \wedge w + (-1)^r v \wedge d(w), \quad v \in \Lambda^r R^n, \quad w \in \Lambda^s R^n.$

Deixaremos a verificação destas propriedades como exercício.

Assim, é indiferente falar no complexo de Koszul ou na álgebra acima, munida da "derivação" d. Uma vantagem deste segundo ponto de vista é que obtemos, imediatamente, os seguintes fatos:

(i) $Z(K_\bullet(\underline{x};R)) = \sum_r Z_r(K_\bullet(\underline{x};R))$ é uma R-subálgebra da álgebra $K_\bullet(\underline{x};R)$ e $B(K_\bullet(\underline{x};R)) = \sum_r B_r(K_\bullet(\underline{x};R))$ é um ideal em $Z(K_\bullet(\underline{x};R))$.

($Z_r(K_\bullet(\underline{x};R))$ e $B_r(K_\bullet(\underline{x};R))$ denotam, respectivamente, o módulo dos r-ciclos e o módulo dos r-bordos; vide §2, B.)

(ii) Se $I = (\underline{x}) \subset R$, então $I \cdot H(K_\bullet(\underline{x};R)) = (0)$, onde $H(K_\bullet(\underline{x};R)) = \sum_r H_r(K_\bullet(\underline{x};R))$ é a álgebra quociente $Z(K_\bullet(\underline{x};R))/B(K_\bullet(\underline{x};R))$ (chamada álgebra de homologia do complexo de Koszul).

Sempre que o contexto não deixar lugar a confusões, usaremos as notações $Z(K_\bullet)$, $B(K_\bullet)$, $H(K_\bullet)$, $Z_r(K_\bullet)$, etc.

Para verificar (i) e (ii), usamos a propriedade fundamental da derivação d, conforme explicamos acima. Assim, se $v \in Z_r(K_\bullet)$, $w \in Z_s(K_\bullet)$ então $d(v \wedge w) = 0 \wedge w + (-1)^r v \wedge 0 = 0$, logo $v \wedge w \in Z_{r+s}(K_\bullet)$. Isto é suficiente para concluir que $Z(K_\bullet)$ é subálgebra de $K_\bullet$, as outras verificações sendo triviais. De maneira análoga, se $v \in Z_r(K_\bullet)$ e $w = d(w') \in B_s(K_\bullet)$ então

$d(v \wedge w') = 0 \wedge w' + (-1)^r\, v \wedge d(w') = (-1)^r\, v \wedge w$, o que mostra que $v \wedge w \in B_{r+s}(K_\bullet)$. Logo, $B(K_\bullet)$ é um ideal (bilateral) de $Z(K_\bullet)$.

Finalmente, se $x \in I = (\underline{x}) \subset K_o = \Lambda^o R^n$, tomamos $v \in K_1 = \Lambda^1 R^n$ tal que $d(v) = d_1(v) = x$. Se $w \in Z_r(K_\bullet)$, temos $d(v \wedge w) = xw$, o que mostra que $x \cdot Z_r(K_\bullet) \subset B_r(K_\bullet)$.

O outro ponto de vista é:

(2) <u>Como produto tensorial de complexos</u>

Dados dois complexos

$$X_\bullet: \qquad \cdots \to X_n \xrightarrow{\partial_n} X_{n-1} \to \cdots$$

$$X'_\bullet: \qquad \cdots \to X'_n \xrightarrow{\partial'_n} X'_{n-1} \to \cdots \quad ,$$

o seu <u>produto tensorial</u>, denotado $(X \otimes X')_\bullet$, é um novo complexo, definido da seguinte maneira:

$$(X \otimes X')_n = \sum_{i=0}^{n} (X_{n-1} \otimes X'_i) \qquad \text{(soma direta)}$$

e d_n: $(X \otimes X')_n \to (X \otimes X')_{n-1}$ é tal que

$$d_r(x_{n-i} \otimes x'_i) = \partial_{n-i}(x_{n-1}) \otimes x'_i + (-1)^{n-i}\, x_{n-i} \otimes \partial'_i(x'_i).$$

(Note-se a semelhança com a propriedade fundamental da derivação d de $K_\bullet$).

Deixamos os detalhes da verificação (de que $(X \otimes X')_\bullet$ é efetivamente um complexo) como exercício.

Por iteração, definimos o produto tensorial de vários complexos (é tedioso, porém direto, verificar que o produto tensorial de complexos é comutativo e associativo).

Aplicando ao presente contexto, temos:

Lema III.28 - Sejam $\underline{x} = x_1,\ldots,x_n \in R$ e M um R-módulo. Então $K_\bullet(\underline{x};M) \simeq K_\bullet(x_1;R) \otimes \ldots \otimes K_\bullet(x_n;R) \otimes M$ como complexos.

(N.B. M designa um módulo ou o complexo "concentrado em grau 0" com M como termo de grau 0).

Demonstração: É suficiente mostrar que $K_\bullet(\underline{x};R) \simeq K_\bullet(x_1;R)\otimes\ldots\otimes$ $\otimes K_\bullet(x_n;R)$. Por indução sobre n. Para $n=1$, o isomorfismo é a identidade. Para $n > 1$, escolhemos um isomorfismo $\Lambda^r R^n \simeq$ $\simeq \Lambda^r R^{n-1} \oplus \Lambda^{r-1} R^{n-1}$. Usando a hipótese de indução, resulta um isomorfismo

$$((K_\bullet(x_1;R) \otimes\ldots\otimes K_\bullet(x_{n-1};R)) \otimes K_\bullet(x_n;R))_r =$$

$$= \sum_{i=0}^{r} (K_\bullet(x_1;R)\otimes\ldots\otimes K_\bullet(x_{n-1};R))_{r-i} \otimes K_\bullet(x_n,R)_i \simeq \sum_{i=0}^{r} (\Lambda^{r-i}R^{n-1} \otimes K_\bullet(x_n;R)_i)$$

$$\simeq (\Lambda^r R^{n-1} \otimes R) \oplus (\Lambda^{r-1}R^{n-1} \otimes R) \simeq \Lambda^r R^{n-1} \oplus \Lambda^{r-1}R^{n-1} \simeq \Lambda^r R^n.$$

Deixaremos como exercício a verificação de que tais isomorfismos comutam com as diferenciais dos dois complexos (é um bom treino para entender como age a diferencial num produto tensorial de complexos). //

Utilizando esta segunda interpretação do complexo de Koszul, desenvolveremos algumas de suas propriedades técnicas.

K_1. Se $I = (\underline{x}) \subset R$, então $I \cdot H(K_\bullet(\underline{x};M)) = (0)$.

Interpretando $K_\bullet(\underline{x};R)$ como álgebra anticomutativa, etc., vimos que $I \cdot H(K_\bullet(\underline{x};R)) = (0)$. Contudo, não se pode concluir, imediatamente, que $I \cdot H(K_\bullet(\underline{x};M)) = (0)$ para um módulo M qualquer (apesar de $K_\bullet(\underline{x};M) = K_\bullet(\underline{x};R) \otimes M$ por definição, não vale em geral $H(K_\bullet(\underline{x};M)) \simeq H(K_\bullet(\underline{x};R)) \otimes M$; vide demonstração da Prop.IV.5, §1, Cap.IV). Precisamos de um estratagema diferente.

<u>Lema III.29</u> - <u>Seja</u> $x \in R$ <u>e</u> $C_\bullet$ <u>um complexo</u>. <u>Seja</u>

$$f: K_\bullet(x;R) \otimes C_\bullet \to (K_\bullet(x;R) \otimes C_\bullet) \otimes (K_\bullet(x;R) \otimes C_\bullet)$$

<u>o morfismo de complexos "inclusão no primeiro fator"</u>. <u>Então, existe um morfismo</u> $g: (K_\bullet(x;R) \otimes C_\bullet) \otimes (K_\bullet(x;R) \otimes C_\bullet) \to$ $\to K_\bullet(x;R) \otimes C_\bullet$ <u>tal que</u> $gf = 1$.

<u>Demonstração</u>: Basta mostrar para $K_\bullet(x;R)$. Definimos $g(a,b) =$ $= a+b$, em grau 1, e g = identidade, em grau 0. //

Para aplicar o lema é conveniente, primeiramente, fixar a seguinte notação: se $C_\bullet$ é um complexo e d um inteiro, $C_\bullet(-d)$ denota o complexo original "trasladado de d graus", quer dizer, $C(-d)_r = C_{r-d}$.

Consideremos, entrementes, a seguinte sequência exata de complexos:

$$0 \to K_\bullet(x;R) \to K_\bullet(x;R) \otimes K_\bullet(x;R) \to K_\bullet(x;R)(-1) \to 0.$$

Tensorizando com um complexo $C_\bullet$, obtemos ainda uma sequência exata (por que?) de complexos

$$\begin{array}{ccccccccc} 0 \to & K_\bullet(x;R)\otimes C_\bullet & \xrightarrow{f} & (K_\bullet(x;R)\otimes C_\bullet)\otimes(K_\bullet(x;R)\otimes C_\bullet) & \to & (K_\bullet(x;R)\otimes C_\bullet)(-1) & \to 0, \\ & \parallel & & \parallel & & \parallel & \\ & C_x & & C_x \otimes C_x & & C_x(-1) & \end{array}$$

da qual deduzimos uma sequência de homologia

$$\begin{array}{c}
\cdots \to H_{n+1}(C_x) \xrightarrow{H_{n+1}(f)} H_{n+1}(C_x \otimes C_x) \to \underset{}{\overset{\displaystyle H_n(C_x)}{\overset{\Vert}{H_{n+1}(C_x(-1))}}} \xrightarrow{\delta_n} \\
\to H_n(C_x) \xrightarrow{H_n(f)} H_n(C_x \otimes C_x) \to \underset{\displaystyle H_{n-1}(C_x)}{\underset{\Vert}{H_n(C_x(-1))}} \to \cdots
\end{array}$$

Observemos, agora, dois fatos cruciais:

(i) $H_n(f)$ <u>é injetora, para todo</u> n.

Segue do Lema III.29, já que f é cindida.

(ii) $\delta_n = (-1)^n x$ (<u>multiplicação por</u> x).

O que afirmamos aqui é algo bem geral: seja $D_\bullet$ um complexo arbitrário e consideremos a sequência exata de complexos

$$0 \to D_\bullet \to K_\bullet(x;R) \underset{}{\overset{\overset{\displaystyle D_x}{\Vert}}{\otimes}} D_\bullet \to D_\bullet(-1) \to 0$$

obtida da sequência "fundamental"

$$0 \to R \to K_\bullet(x;R) \to R(-1) \to 0$$

por tensorização com $D_\bullet$. Então, na sequência longa associada, os homomorfismos de conexão são, a menos de sinal, multiplicação por x.

Para constatar este fato, visualizemos uma fatia da sequência original. Temos, após as identificação ordinárias:

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & & \vdots & \\
 & & \downarrow & & \downarrow & & & \downarrow & \\
0 & \to & D_n & \to & D_n \oplus D_{n-1} & \to & D_n(-1) & = D_{n-1} & \to 0 \\
 & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle \partial_n} & & & \downarrow{\scriptstyle d_{n-1}} & \\
0 & \to & D_{n-1} & \to & D_{n-1} \oplus D_{n-2} & \to & D_{n-1}(-1) & = D_{n-2} & \to 0 \\
 & & \downarrow & & \downarrow & & & \downarrow & \\
 & & \vdots & & \vdots & & & \vdots &
\end{array}$$

onde, em notação matricial óbiva, $\partial_n = \begin{pmatrix} d_n & (-1)_x^{n-1} \\ 0 & d_{n-1} \end{pmatrix}$. Lembremos como age o homomorfismo de conexão: começamos com $z_{n-1} \in Z_{n-1}(D_.) \subset D_{n-1}$ (no complexo quociente) e tomamos qualquer imagem inversa de z_{n-1} em $D_n \oplus D_{n-1}$, por exemplo, o vetor $(0,z_{n-1})$. Então, $\partial_n(0,z_{n-1}) = ((-1)^{n-1}\, xz_{n-1},\ d_{n-1}(z_{n-1}))$. Por outro lado, como $z_{n-1} \in Z_{n-1}(D_.)$, tem-se $d_{n-1}(z_{n-1}) = 0$. Segue que $\partial_n(0,z_{n-1}) = ((-1)^{n-1}\, xz_{n-1},0)$, que é imagem de $(-1)^{n-1}\, xz_{n-1} \in D_{n-1}$ pela aplicação $0 \to D_{n-1} \to D_{n-1} \oplus D_{n-2}$. Isto mostra que o homomorfismo de conexão é multiplicação por x, como queríamos.

Para terminar o argumento inicial, aplicamos os fatos (i) e (ii) à sequência longa em questão: como $\delta_n = (-1)^n x$ e $\mathrm{im}(\delta_n) = \mathrm{núcl}(H_n(f)) = 0$, temos $x \cdot H_n(C_x) = (0)$. Agora, usamos este resultado com $x = x_i$ e $C_. = K_.(x_1,\ldots,\hat{x}_i,\ldots,x_n;M)$, $i=1,\ldots,n$. Isto fornece, finalmente, $(x_1,\ldots,x_n)\cdot H(K_.(\underline{x};M)) = (0)$.

$\underline{K}_2$. $K_.(\underline{x};-)$ <u>é um funtor exato na categoria dos</u> R-<u>módulos</u>.

Trocando em miúdos, se $0 \to M' \to M \to M'' \to 0$ é uma sequência exata de módulos, então existe uma sequência exata de complexos

$$0 \to K_\bullet(\underline{x};M') \to K_\bullet(\underline{x};M) \to K_\bullet(\underline{x};M'') \to 0.$$

Isto é fácil: tensorizamos a sequência de módulos com $K_r(\underline{x};R) = \Lambda^r R^n$ e como este é um módulo livre, a sequência resultante

$$0 \to K_r(\underline{x};R)\otimes M' \to K_r(\underline{x};R)\otimes M \to K_r(\underline{x};R)\otimes M'' \to 0$$

é exata. É claro que estas sequências, uma para cada r, compõem uma sequência exata de complexos.

Em particular, temos um sequência longa de homologia

$$\ldots \to H_r(\underline{x};M') \to H_r(\underline{x};M) \to H_r(\underline{x};M'') \to \ldots$$

$\underline{K}_3$. <u>Para todo módulo</u> M, <u>existe uma sequência exata longa</u>

$$\ldots \to H_{r+1}(x_1,\ldots,x_n;M) \to H_r(x_1,\ldots,x_{n-1};M) \xrightarrow{(-1)^r x_n}$$
$$H_r(x_1,\ldots,x_{n-1};M) \to H_r(x_1,\ldots,x_n;M) \to \ldots$$
$$\ldots \to H_1(x_1,\ldots,x_n;M) \to H_o(x_1,\ldots,x_{n-1};M) \xrightarrow{x_n} H_o(x_1,\ldots,x_{n-1};M).$$

(Note-se que, como $H_o(x_1,\ldots,x_{n-1};M) \simeq M/(x_1,\ldots,x_{n-1})M$, a sequência acima pode ser aumentada com o módulo $M/(x_1,\ldots,x_n)M \simeq H_o(x_1,\ldots,x_n;M)$).

A demonstração disto já foi essencialmente feita na propriedade K_1: tensorizamos com $K_\bullet(x_1,\ldots,x_{n-1};M)$ a sequência fundamental $0 \to R \to K_\bullet(x_n;R) \to R(-1) \to 0$, etc.

As propriedades acima são extremamente importantes, mas a "raison d'être" dos complexos $K_\bullet(\underline{x};M)$ é o seguinte resultado.

<u>Teorema III.30</u> ("Sensibilidade à profundidade") - <u>Seja</u> R <u>um anel noetheriano</u>, $\underline{x} = x_1,\ldots,x_n \in R$ <u>uma sequência de elementos e</u> M <u>um</u> R-<u>módulo tal que</u> $M/\underline{x}M \neq (0)$. <u>Então</u>:

$$n - \mathrm{prof}_{(\underline{x})}(M) = q,$$

<u>onde</u> $q \geq 0$ <u>é o maior inteiro tal que</u> $H_q(K_{.}(\underline{x};M)) \neq (0)$.

(Compare-se este resultado com a Prop.III.27 do §3).

<u>Demonstração</u>: Procedemos por indução decrescente sobre o inteiro $q = \sup\{r \mid H_r(K_{.}(\underline{x};M)) \neq (0)\}$ (isto faz sentido, pois $H_{n+1}(K_{.}(\underline{x};M)) = H_{n+2}(K_{.}(\underline{x};M)) = \ldots = (0)$ e $H_o(K_{.}(\underline{x};M)) = M/\underline{x}M \neq (0)$ por hipótese).

Se $q = n$, $H_q(K_{.}(\underline{x};M)) = (0):_M(x)$ (por que?). Neste caso, $(\underline{x}) \subset Z(M)$ (divisores de zero, não ciclos!), de modo que $\mathrm{prof}_{(\underline{x})}(M) = 0$.

Suponhamos $q \lneq n$. Então $H_n(K_{.}(\underline{x};M)) = (0):_M(\underline{x}) = (0)$, de maneira que existe $a \in (\underline{x})$ tal que $a \notin Z(M)$. Consideremos a sequência longa de homologia associada à sequência exata

$$0 \to M \xrightarrow{a} M \to M/aM \to 0$$

(vide propriedade $\underline{K}_2$), que toma a forma

$$\ldots \to \underset{\substack{\parallel \\ 0}}{H_{q+1}(K_{.}(\underline{x};M))} \to H_{q+1}(K_{.}(\underline{x};M/aM)) \to H_q(K_{.}(x;M) \xrightarrow{a} H_q(K_{.}(\underline{x};M)) \to \ldots$$

Por hipótese, $H_i(K_{.}(\underline{x};M)) = (0)$ para $i \geq q+1$. Segue então que $H_i(K_{.}(\underline{x};M/aM)) = (0)$ para $i \geq q+2$. Por outro lado, pela propriedade $\underline{K}_1$, $a \cdot H_q(K_{.}(\underline{x};M)) = (0)$. Então, ainda da sequência acima, tiramos

$$H_{q+1}(K_{\bullet}(\underline{x};M/aM)) \simeq H_q(K_{\bullet}(\underline{x};M)) \neq (0).$$

Por indução, $\text{prof}_{(\underline{x})}(M/aM) = n-(q+1)$. Mas, $\text{prof}_{(\underline{x})}(M) =$ $= \text{prof}_{(\underline{x})}(M/aM) + 1$. Segue então a igualdade procurada. //

Corolário III.31 - Se $\underline{x} = x_1,\ldots,x_n$ é uma M-sequência, então $H_r(K_{\bullet}(\underline{x};M)) = (0)$ para $r \geq 1$.

Demonstração: É uma consequência instantânea do teorema anterior (é também consequência imediata da propriedade $\underline{K}_3$, utilizando indução). //

Observação. A recíproca do corolário acima é falsa. A razão é simplesmente de que o complexo de Koszul $K_{\bullet}(\underline{x};M)$ independe da ordem dos elementos na sequência $x_1,\ldots,x_n$, enquanto que a noção de M-sequência depende da ordem destes elementos. Para um contra-exemplo explícito, vide Exercício 1, Cap. II.

A recíproca vale em "situações locais". Precisamente:

Proposição III.32 - Seja $R,\underline{m}$ um anel local, $\underline{x} = x_1,\ldots,x_n \in \underline{m}$ e M um R-módulo. Então:

(i) ("Rigidez") Se $H_r(K_{\bullet}(\underline{x};M)) = (0)$ para algum $r \geq 0$, então $H_s(K(x_1,\ldots,x_i;M)) = (0)$ para todo $s \geq r$ e para todo $1 \leq i \leq n$.

(ii) $H_1(K_{\bullet}(\underline{x};M)) = (0) \Rightarrow x_1,\ldots,x_n$ é M-sequência.

Corolário III.33 - $R,\underline{m}$ local, $x_1,\ldots,x_n \in \underline{m}$. Se $x_1,\ldots,x_n$ é M-sequência, então $x_{\pi(1)},\ldots,x_{\pi(n)}$ é M-sequência para toda permutação π de $\{1,\ldots,n\}$.

Demonstração (da proposição): (i) Da longa sequência de homologia na propriedade $\underline{K}_3$, tiramos, em particular

$$0 \to H_r(x_1,\ldots,x_{n-1};M)/x_n \cdot H_r(x_1,\ldots,x_{n-1};M) \to H_r(\underline{x};M),$$

onde $H_r(K_.(-;M)) = H_r(-;M)$ por simplicidade. Logo, pelo lema de Nakayama, $H_r(x_1,\ldots,x_{n-1};M) = (0)$. Por indução (sobre n), $H_s(x_1,\ldots,x_i;M) = (0)$ para todo $s \geq r$ e todo $1 \leq i \leq n-1$. Resulta, então

$$\cdots \to \underset{\substack{\parallel \\ 0}}{H_{r+1}(x_1,\ldots,x_{n-1};M)} \to H_{r+1}(\underline{x};M) \to \underset{\substack{\parallel \\ 0}}{H_r(x_1,\ldots,x_{n-1};M)}$$

Logo, $H_{r+1}(\underline{x};M) = (0)$, etc.

(ii) (Por indução sobre n). Óbvio se $n=1$. Suponhamos $n \geq 2$. Pela parte (i), temos $H_1(x_1,\ldots,x_{n-1};M) = (0)$. Logo, pela hipótese de indução, $x_1,\ldots,x_{n-1}$ é M-sequência. Mas $H_1(\underline{x};M) = (0)$ implica ainda que

$$0 \to \underset{\substack{\parallel \\ M/(x_1,\ldots,x_{n-1})M}}{H_o(x_1,\ldots,x_{n-1};M)} \xrightarrow{x_n} \underset{\substack{\parallel \\ M/(x_1,\ldots,x_{n-1})M}}{H_o(x_1,\ldots,x_{n-1};M)}$$

Logo, $x_n \notin Z(M/(x_1,\ldots,x_{n-1})M)$. //

No mesmo espírito, podemos usar o método desta seção para obter um resultado sobre o crescimento da profundidade por adjunção de elementos. Este resultado foi enunciado no Cap.II como Lema II.8, mas não vemos danos em repetí-lo no presente contexto.

<u>Proposição III.34</u> - <u>Seja</u> R <u>um anel noetheriano</u>, $I \subset R$ <u>um ideal e</u> M <u>um</u> R-<u>módulo tal que</u> $IM \neq M$. <u>Se</u> $a \in R$ <u>é um elemento no radical de Jacobson de</u> R, <u>tem-se</u>:

$$\text{prof}_{(I,a)}(M) \leq 1 + \text{prof}_I(M).$$

<u>Demonstração</u>: Seja $\underline{x} = x_1,\ldots,x_{n-1}$ um sistema de geradores de I. Como antes, da sequência longa de homologia, tiramos

$$0 \to H_q(\underline{x};M)/aH_q(\underline{x};M) \to H_q(\underline{x},a;M).$$

Como $a \in$ radical de Jacobson, pelo lema de Nakayama vem:

$$H_q(\underline{x},a;M) = (0) \Rightarrow H_q(\underline{x};M) = (0).$$

Logo, pela sensibilidade à profundidade (Teor. III.30):

$$n - \text{prof}_{(I,a)}(M) \geq (n-1) - \text{prof}_I(M).$$

Segue $\text{prof}_{(I,a)}(M) \leq 1 + \text{prof}_I(M)$, como queríamos. //

<u>Observação</u>. Note-se que não é preciso supor $I \subset$ radical de Jacobson. Para aplicar o Teorema III.30 precisamos $(I,a)M \neq M$ também; mas isto vale pois, do contrário, $a(M/IM) = M/IM$ e, pelo lema de Nakayama, $IM = M$.

"<u>Presto</u>": <u>quando é gerado por</u> R-<u>sequência</u>?

Neste pequeno desfecho, queremos indicar alguns testes que permitam averiguar quando um ideal é gerado por uma R-sequência. Advertimos, contudo, para o significado da palavra "teste" aqui empregado: não temos em mente critérios suficientes de fácil improvisação; antes, tratam-se de condições <u>necessárias</u> e <u>suficientes</u> de grande sofisticação (polimento, diríamos), situados a uma boa distância do alvo em teste.

Estes testes são, em verdade, teoremas (de atribuição bem definida). Existem três ou quatro tais teoremas que gozam de popularidade. Um deles é o item (ii) da Proposição III.32, §4. Daremos mais três destes testes, mas só faremos a demonstração de um deles, remetendo o leitor às fontes apropriadas.

Começamos com

Teorema V-F (Vasconcelos [Va_1]-Ferrand [Fe]) - Seja $R, \underline{m}$ um anel local, $I \subset \underline{m}$ um ideal. São equivalentes:

(i) I é gerado por R-sequência

(ii) $d.h.(I) < \infty$ e I/I^2 é um R/I-módulo livre.

Para a demonstração, usaremos um resultado auxiliar, devido a Auslander-Buchsbaum, que por sua vez, pode ser visto como um primeiro teste não trivial para existência de elementos regulares (isto é, não divisores de zero).

Lema A-B (Auslander-Buchsbaum [$(A\text{-}B)_2$]) - Seja R um anel noetheriano e M um módulo admitindo uma resolução livre finita. São equivalentes:

(i) $0:M \neq (0)$

(ii) $\text{prof}(0:M) \geq 1$.

Demonstração: (ii) $\Rightarrow$ (i). Óbvio.

(i) $\Rightarrow$ (ii). Ponhamos $I = 0:M \neq (0)$. Temos:

$$\begin{aligned}\text{prof}(I) = 0 &\Rightarrow I \subset Z(R) \Rightarrow I \subset P, \quad \text{algum} \quad P \in \text{Ass}(R)\\ &\Rightarrow P \in \text{Sup}(M) \Leftrightarrow M_P \neq (0).\end{aligned}$$

Por outro lado, para todo $Q \in \text{Ass}(R)$, $\text{prof}(R_Q) = 0$. Logo, pelo caso fácil da igualdade de Auslander-Buchsbaum, M_Q é R_Q-livre para todo $Q \in \text{Ass}(R)$. Além disso M_P é R_P livre de posto $\neq 0$ para um $P \in \text{Ass}(R)$ (como acima) contendo I.

(Ainda não sabemos que $M_Q \neq (0)$ para os outros primos $Q \in \mathrm{Ass}(R)$; este é o ponto por excelência).

Localizando uma resolução livre finita

$$0 \to F_n \to \cdots \to F_o \to M \to 0$$

em um $Q \in \mathrm{Ass}(R)$, obtemos uma sequência exata longa de módulos livres sobre um anel local. Logo, posto $(M_Q) = \sum_{i=0}^{n} (-1)^i \cdot \mathrm{posto}(F_i)_Q$ (por que?). Mas, $(F_i)_Q$ e $(F_i)_{Q'}$ têm o mesmo posto, para dois primos quaisquer Q, Q'. Fazendo $Q' = P$, temos então que M_Q é R_Q-livre de posto $\neq 0$, para todo $Q \in \mathrm{Ass}(R)$. Como $I_Q = 0:M_Q$, resulta $I_Q = (0)$ para todo $Q \in \mathrm{Ass}(R)$. Em outras palavras, $I_S = (0)$ onde $S = R \setminus \bigcup_{Q \in \mathrm{Ass}(R)} Q$. Mas $I \subset I_S$, logo $I = (0)$; contradição. //

Voltemos, entrementes, à

<u>Demonstração</u> (do Teorema V-F): (i) $\Rightarrow$ (ii). d.h.$(I) < \infty$ já foi mostrado em, pelo menos, três formas diferentes. Quanto à segunda condição, seja $x_1,\ldots,x_n$ uma R-sequência que gera I. Evidentemente, as imagens de $x_1,\ldots,x_n$ módulo I^2 geram I/I^2 como R/I-módulo. Independência linear destes geradores significa: $\sum_{i=1}^{n} \lambda_i x_i \in I^2 \Rightarrow \lambda_i \in I$, para todo i. Isto segue da definição de R-sequência. Com efeito, escrevemos

$$\sum_{i=1}^{n} \lambda_i x_i = \sum_{j,k} \mu_{jk} x_j x_k, \quad \text{ou} \quad (\lambda_n - \Sigma\, \mu_{jn} x_j) x_n \in (x_1,\ldots,x_{n-1}).$$

Segue $\lambda_n - \sum_j \mu_{jn} x_j \in (x_1,\ldots,x_{n-1})$, logo $\lambda_n \in I$. Digamos $\lambda_n = \alpha_1 x_1 + \cdots + \alpha_n x_n$ com $\alpha_n = \mu_{nn}$. Então, $\sum_{i=1}^{n} \lambda_i x_i - \alpha_n x_n^2 = \sum_{i=1}^{n-1} (\lambda_i + \alpha_i x_n) x_i \in (x_1,\ldots,x_{n-1})I$. Repetimos o argumento acima, obtendo $\lambda_{n-1} \in I$, etc.

(ii) $\Rightarrow$ (i) (Esta implicação é o núcleo do teorema). Primeiramente, observemos que $I/I^2 \otimes R/\underline{m} \simeq I/\underline{m}I$. Pelo lema de Nakayama, então, podemos iniciar um sistema mínimo de geradores de I/I^2 com qualquer $x_1 \in I \setminus \underline{m}I$. Como I/I^2 é R/I-livre, um tal sistema - vê-se facilmente - já é uma base de I/I^2. Mais ainda: podemos escolher $x_1 \notin Z(R)$. Com efeito, queremos $I \not\subset \underline{m}I \cup P_1 \cup \ldots \cup P_m$, onde $P_1,\ldots,P_m$ são os primos associados de R. Isto resulta da "esquiva" (vide Exercício 2, Cap.I) e do Lema A-B já que $d.h.I < \infty$.

Procedemos por indução sobre o cardinal s de uma base de I/I^2. Escolhamos, de uma vez por todas, uma base $x_1,x_2,\ldots,x_s$ de I/I^2 (2), tal que $x_1 \in I \setminus Z(R)$.

Verifiquemos a hipótese de indução para $\bar{I}/\bar{I}^2$, onde $\bar{R} = R/(x_1)$, $\bar{I} = I/(x_1)$.

(1) $\bar{I}/\bar{I}^2$ é $\bar{R}/\bar{I}$-livre, de posto $s-1$.

Observemos que $\bar{R}/\bar{I} = R/(x_1)/I/(x_1) \simeq R/I$ e que $\bar{I}/\bar{I}^2 = (I/(x_1))/(I^2+(x_1)/(x_1)) \simeq I/(I^2+(x_1))$. Por outro lado, temos a sequência exata natural

$$0 \to I^2+(x_1)/I^2 \to I/I^2 \to I/I^2+(x_1) \to 0,$$

onde $I^2+(x_1)/I^2 \simeq (x_1)/(x_1) \cap I^2 \simeq (x_1)/x_1 I \simeq R/I \otimes (x_1)$. Até agora, todos os homomorfismos e isomorfismos são naturais. Finalmente, como x_1 é parte de uma base de I/I^2, $R/I \otimes (x_1)$ é isomorfo a um somando direto $(R/I)\, x_1$ de I/I^2. Resulta que o

---

(2) Estamos, deliberamente, confundindo uma base de I/I^2 com uma imagem inversa desta base em I.

quociente de I/I^2 pelo submódulo $I^2+(x_1)/I^2$ é isomorfo ao submódulo livre complementar, $(R/I)x_2 \oplus \ldots \oplus (R/I)x_s$. Mas, este quociente é $I/I^2+(x_1)$ pela sequência exata acima; donde segue o resultado.

(2) $d.h._{\bar{R}}(\bar{I}) < \infty$.

Esta parte não é difícil, mas é certamente atrevida! (vide Observação abaixo).

Pomos $J = (x_1 I, x_2, \ldots, x_s)$. É claro que $I = (x_1)+J$. Afirmamos que $(x_1) \cap J = x_1 I$. Com efeito, seja $y \in (x_1) \cap J$, digamos, $y = r_1 x_1 = x_1 a + \sum_{i>1} r_i x_i$, $a \in I$. Então, tem-se $r_1 x_1 - \sum_{i>1} r_i x_i = x_1 a \in I^2$ e como $x_1, \ldots, x_s$ é uma base de I/I^2, $r_1 \in I$. Assim, $y \in x_1 I$.

Disto resulta que $I/x_1 I \simeq x_1/x_1 I \oplus J/x_1 I$.

Por outro lado, $d.h._{R/(x_1)}(I/x_1 I) = d.h._R(I) < \infty$ (vide Prop. III.16,§3). Segue que $d.h._{R/(x_1)}(x_1/x_1 I) < \infty$. Mas, como vimos na verificação (1), $x_1/x_1 I \simeq R/I \simeq \bar{R}/\bar{I}$. Consequentemente, $d.h._{\bar{R}}(\bar{I}) < \infty$.

Pela hipótese indutiva $\bar{I}$ é gerado por uma $\bar{R}$-sequência, logo I é gerado por uma R-sequência. //

<u>Observação</u>. A razão pela qual a parte (2) acima é um tanto quanto inesperada é que , em verdade, provou-se que $d.h._{\bar{R}}(R/I) < \infty$, $\bar{R} = R/(x_1)$, ao passo que, guiados pelos teoremas de mudança de anel do §3, esperaríamos um resultado assim para um módulo M precisamente no outro extremo do espectro (isto é, $x \notin Z(M)$) .

Naturalmente, aí reside a beleza e a simplicidade do teorema. É um bom exercício (ginasiano) "jogralizar" com as condições do teorema, a priori, isto é, antes de concluir por indução que $\{x_1, x_2, \ldots\}$ pode ser adaptada (= transformada por matrizes elementares) a uma R-sequência. Por exemplo, se $\underline{x} = (x_2, \ldots, x_s)$, então $J/x_1 I \simeq \underline{x}/\underline{x}I$ e a sequência cindida da parte (2) se torna:

$$0 \to \underline{x}/\underline{x}I \to I/x_1 I \to x_1/x_1 I \to 0.$$

Pode-se perguntar: se $I' \subset R$ é um ideal qualquer e $x \in R$ um elemento do anel, em que condições tem-se (com $I = (x, I')$):

$$0 \to I'/I'I \to I/xI \to x/xI \to 0 \;?$$

Etc., etc.

O impacto do Teorema V-F, anterior à avalanche dos resultados sobre interseções completas, é este:

<u>Corolário</u> - <u>Se</u> $R, \underline{m}$ <u>é um anel local tal que</u> $\mathrm{d.h.}_R(R/\underline{m}) < \infty$, <u>então</u> R <u>é regular</u>.

(Isto é a implicação (iii) $\Rightarrow$ (i) no teorema de Serre-Auslander-Buchsbaum!).

Examinemos a condição (ii) do Teorema V-F mais detidamente. O módulo I/I^2 pode ser explicado, geometricamente, em termos do "fibrado conormal à variedade R/I imersa em R". A condição (ii) diz que este fibrado é "trivial" e que uma condição adicional é satisfeita ($\mathrm{d.h.}_R < \infty$ só pode ser explicada, geometricamente, em termos de certa regularidade do "espaço ambiente" R). A conclusão é, então, que a "variedade" R/I é, geometricamente, "trivial".

Ora, $I/I^2 = I \otimes R/I$ é apenas o fibrado conormal de "primeira ordem". Há fibrados conormais de ordem superior: $I^r \otimes R/I \simeq I^r/I^{r+1}$, $r \geq 1$. Surpreendente é que ainda se pode deduzir a "trivialidade" de R/I a partir da trivialidade de I^r/I^{r+1}, qualquer que seja r (fixo). A demonstração consiste em reduzir às condições do Teorema V-F [Va_2, Th.4.3].

O que dizer da condição $d.h._R(I) < \infty$? Evidentemente, ela é necessária para I ser gerado por R-sequência, mas, frequentemente, não é óbvia do contexto. Ora, existe uma maneira de "colar" os fibrados I^r/I^{r+1}, $r \geq 0$, de maneira a obter uma nova variedade. Chamamos este processo do <u>método do anel graduado</u> (ou do <u>divisor excecional</u>). Eis a receita, em breves pinceladas.

Formamos a soma direta dos R/I-módulos I^r/I^{r+1},

$$gr_I(R) = \sum_{r=0}^{\infty} I^r/I^{r+1},$$

e nela definimos uma multiplicação: se $\bar{a} \in I^r/I^{r+1}$ e $\bar{b} \in I^s/I^{s+1}$ então $\bar{a}\cdot\bar{b} = \overline{ab} \in I^{r+s}/I^{r+s+1}$.

O anel (graduado) $gr_I(R)$ assim obtido é o <u>anel graduado do ideal</u> I. Pode-se ver que $gr_I(R)$ é uma álgebra sobre R/I, gerada por elementos de grau 1 por exemplo pelas imagens, módulo I^2, de geradores $x_1,\ldots,x_n$ de I. Assim, obtemos um homomorfismo de R/I-álgebras, que é sobrejetor:

$$\begin{aligned} R/I[T_1,\ldots,T_n] &\to gr_I(R) \\ T_i &\longmapsto x_i \pmod{I^2}. \end{aligned}$$

O segundo teste da trivialidade homológica de I vem neste contexto.

<u>Teorema R</u> (Rees [Re]) - <u>Se</u> $R, \underline{m}$ <u>é local e</u> $I \subset \underline{m}$ <u>um ideal tal que o homomorfismo acima definido é injetor, então</u> I <u>é gerado por</u> R-<u>sequência</u>.

<u>Observação</u>. A recíproca do Teorema R é verdadeira e vale, mais geralmente, para qualquer anel. Deve-se mostrar que se $F(T_1,\ldots,T_n)$ é uma forma de grau r tal que $F(x_1,\ldots,x_n) \in I^{r+1}$, então $F(T_1,\ldots,T_n) \in IR[T_1,\ldots,T_n]$. Para $r=1$, é a propriedade usada na demonstração do Teorema V-F: $\Sigma \lambda_i x_i \in I^2 \Rightarrow \lambda_i \in I$, para todo i.

Insistimos: não é suficiente que todos os módulos conormais I^r/I^{r+1}, $r \geq 0$, sejam livres sobre R/I para concluir que I é gerado por R-sequência. É preciso que $\langle x_1,\ldots,x_n\rangle$ base de $I/I^2 \Rightarrow \langle x_1^{i_1}\ldots x_n^{i_n} \mid i_1+\ldots+i_n=r\rangle$ base de I^r/I^{r+1}, para todo $r \geq 0$.

Para terminar, daremos um teste para decidir se I é gerado por R-sequência, em termos da homologia do complexo de Koszul. Trata-se de uma generalização não trivial (e, frequentemente, útil) da Proposição III.32 (ii), §4.

<u>Teorema G</u> (Gulliksen [G-L]) - <u>Seja</u> $R, \underline{m}$ <u>um anel local</u>, $\underline{x} = x_1,\ldots,x_n \in \underline{m}$ <u>e</u> $I = (\underline{x}) \subset R$. <u>Se</u> $H_1(\underline{x};R)$ <u>é um</u> R/I-<u>módulo livre, então</u> I <u>é gerado por uma</u> R-<u>sequência</u>.

(<u>N.B</u>. O teorema não diz que os próprios $x_1,\ldots,x_n$ formam uma R-sequência. A hipótese de $H_1(\underline{x};R)$ ser livre é natural a fortiori, isto é, se $x_1,\ldots,x_r,\ldots,x_n$ geram um ideal I de profundidade r, com $x_1,\ldots,x_r$ R-sequência, então $H_1(\underline{x};R) \simeq (R/I)^{n-r}$ como R/I-módulos).

A demonstração do Teorema G depende da teoria das resoluções livres que admitem estrutura de álgebra graduada anticomutativa. Isto foge, por conseguinte, aos objetivos deste livro. Gostaríamos, contudo, de explicar como se relacionam os Teoremas V-F e G.

Suponhamos dada uma apresentação

$$0 \to Z \to R^n \to I \to 0.$$

Tensorizando por R/I, encontramos a sequência exata

$$0 \to Z \cap IR^n/IZ \to Z/IZ \to (R/I)^n \to I/I^2 \to 0,$$

ou

$$0 \to Z/Z \cap IR^n \to (R/I)^n \to I/I^2 \to 0,$$

que é uma apresentação de I/I^2 como R/I-módulo.

Consideremos, agora, o complexo $K_{\bullet}(\underline{x};R)$, onde $\underline{x}$ é o sistema de geradores de I usado para confeccionar a apresentação inicial. Então, $Z = Z_1(\underline{x};R)$, de modo que a apresentação acima de I/I^2 pode ser prolongada uma etapa:

$$0 \to Z_1(\underline{x};R) \cap IR^n/B_1(\underline{x};R) \to H_1(\underline{x};R) \to (R/I)^n \to I/I^2 \to 0.$$

Supondo, por um momento, que o último termo à esquerda é nulo - em cujo caso, dizemos que I é um <u>ideal syzygético</u> - obtemos a apresentação

$$0 \to H_1(\underline{x};R) \to (R/I)^n \to I/I^2 \to 0.$$

Nestas condições, obtemos: Teorema G $\Rightarrow$ Teorema V-F (porque I/I^2 livre $\Rightarrow$ a sequência acima é cindida $\Rightarrow$ $H_1(\underline{x};R)$ livre).
Na verdade, obtemos a seguinte forma do Teorema V-F.

<u>Teorema V-F</u> (bis) - $R,\underline{m}$ <u>local</u>, $I \subset \underline{m}$. <u>As seguintes condições são equivalentes</u>:

(i) I é gerado por R-sequência.

(ii) I é syzygético e I/I^2 é R/I-livre.

Pode-se mostrar que $Z_1(\underline{x};R) \cap IR^n/B_1(\underline{x};R)$ independe do sistema de geradores [$(S-V)_1$]. Logo, a noção de syzygetismo é invariante do ideal I. Isto torna a forma acima do Teorema V-F quase tão boa quanto a original. Ainda: ela põe em relevo que syzygetismo responde por propriedades homológicas profundas do ideal I.

<u>Exercício</u>. Provar o Teorema V-F (bis) sem recorrer ao Teorema G. (Sugestão: pressupondo que syzygetismo não depende de geradores, escolha um sistema mínimo de geradores de I. Prove que $H_1(\underline{x};R) =$ $= (0)$ para tais geradores. Atenção: vai precisar mostar que $\mu(I) = \mu(I/I^2)$).

<u>Questão</u>. Suponha $I = (\underline{x})$ syzygético. Mostrar diretamente (isto é, sem recorrer ao Teorema G) que $H_1(\underline{x};R)$ livre $\Rightarrow 0 \to H_1(\underline{x};R)$ $\to (R/I)^n \to I/I^2 \to 0$ é cindida.

<u>Exercícios</u>

1. Considere o anel de polinômios $k[X_1,\ldots,X_n]$ (k um corpo). Mostre:

(a) Se $\underline{m} \subset k[X_1,\ldots,X_n]$ é um ideal máximo, $\underline{m} \cap k[X_1,\ldots,X_{n-1}]$ é um ideal máximo.

(Sugestão: pela forma de Zariski do teorema dos zeros - vide sugestão para o Exercício 5, Cap.I - o corpo $k[X_1,\ldots,X_n]/\underline{m}$ é uma extensão algébrica de k; mas, $k[X_1,\ldots,X_{n-1}]/\underline{m} \cap k[X_1,\ldots,X_{n-1}] \subset k[X_1,\ldots,X_n]/\underline{m}$, etc.)

(b) Deduza de (a): todo ideal máximo $\underline{m}$ de $k[X_1,\ldots,X_n]$ é gera do por n polinômios e, consequentemente, $k[X_1,\ldots,X_n]_{\underline{m}}$ é um anel regular.

(c) Se $P \subset k[X_1,\ldots,X_n]$ é um ideal primo, $k[X_1,\ldots,X_n]_P$ é regular.

(Sugestão: seja $d = \dim(k[X_1,\ldots,X_n]/P)$ = grau de transcendência do corpo de frações de $k[X_1,\ldots,X_n]/P$ sobre k. Pode-se supor que $X_1,\ldots,X_d$ são algebricamente independente módulo P, isto é $k[X_1,\ldots,X_d] \cap P = (0)$. Neste caso, se $S = k[X_1,\ldots,X_d] \setminus (0)$, então $k[X_1,\ldots,X_n]_S = k(X_1,\ldots,X_d)[X_{d+1},\ldots,X_n]$ e P_S é um ideal primo deste anel. Mas, $\mathrm{alt}(P_S) = \mathrm{alt}(P) = n-d =$ $= \dim k(X_1,\ldots,X_d)[X_{d+1},\ldots,X_n]$. Logo, P_S é máximo e estamos na situação acima (item (a))).

(d) Aplique a vários ideais primos de $k[X_1,\ldots,X_n]$ a sugestão do item (c), a fim de determinar geradores mínimos de P_P. Por exemplo, $P = (Y^2-XZ,\ Z^2-X^2Y,\ X^3-YZ)$ (Exercício 4, Cap.I), $P = (XY-ZW,\ XZ-Y^2,\ YW-X^2)$ (Cap.II,§3,Nº 1), $P = (XW-YZ,\ Y^3-X^2Z,\ Z^3-W^2Y,\ Y^2W-Z^2X)$ (Cap.II, §3, Nº 2). Verifique também se P_Q é gerado por R_Q-sequência, para primos $Q \supsetneqq P$, onde $R = k[X_1,\ldots,X_n]$. (<u>Atenção</u>: na prática, buscamos variáveis $X_1,\ldots,X_d$ que não pertençam a P (ou Q), sem passar explicitamente pelo anel de frações intermediário R_S).

2. (a) Para cada um dos ideais abaixo determine uma resolução livre explícita (isto é, sua resposta deve conter os postos dos módulos livres e as diferenciais em forma matricial).

$I = (X^2, XY, Y^2) \subset k[X,Y]_{(X,Y)}$

$I = (XY, XZ, YZ) \subset k[X,Y,Z]_{(X,Y,Z)}$

$I = (Y^2-XZ, Z^2-X^2Y, X^3-YZ) \subset k[X,Y,Z]_{(X,Y,Z)}$

$I = (XY-ZW, XZ-Y^2, YW-X^2) \subset k[X,Y,Z,W]_{(X,Y,Z,W)}$

$I = (X_i(Y_jZ_k-Z_jY_k) - Y_i(X_jZ_k-Z_jX_k) + Z_i(X_jY_k-Y_jX_k))_{1\leq i<j<k\leq 4} \subset$
$\subset k[X_\ell, Y_\ell, Z_\ell]_{(X_\ell, Y_\ell, Z_\ell)} \quad (1 \leq \ell \leq 4).$

(b) É capaz de extrair um comportamento uniforme nos exemplos acima? Dependendo da resposta, você pode estar próximo de formular o teorema de Hilbert-Burch ...

(c) Verifique se $I = (XW-YZ, Y^3-X^2Z, Z^3-W^2Y, Y^2W-Z^2X) \subset R =$ $k[X,Y,Z,W]_{(X,Y,Z,W)}$ obedece ao mesmo comportamento dos ideais em (a). Determine $d.h._R(R/I)$. É capaz de escrever uma resolução livre explicitamente?

3. Escreva uma resolução livre (necessariamente infinita) para cada um dos ideais abaixo (k um corpo).

$I = (x,y) \subset k[x,y]_{(x,y)} = k[X,Y]_{(X,Y)}/(Y^2-X^3)$

$I = (x,z) \subset k[x,y,z]_{(x,y,z)} = k[X,Y,Z]_{(X,Y,Z)}/(Z^2-XY)$

$I = (x,y,z) \subset k[x,y,z]_{(x,y,z)} = k[X,Y,Z]_{(X,Y,Z)}/(XY,XZ,YZ)$.

4. Seja M um R-módulo (digamos, R local). Mostre que para todo R-módulo N tem-se $\mathrm{Tor}_i^R(M,N) = (0)$ para $i > \mathrm{d.h.}(M)$.

5. Seja $f\colon C_\bullet \to C'_\bullet$ um morfismo de complexo (de módulos). Ponhamos $\mathbb{M}(f)_i = C'_i \oplus C_{i-1}$ e $\partial_i = \begin{pmatrix} d'_i & (-1)^i f_{i-1} \\ 0 & d_{i-1} \end{pmatrix}\colon \mathbb{M}(f)_i \to$ $\to \mathbb{M}(f)_{i-1}$ onde d_i (resp. d'_i) são as diferenciais de $C_\bullet$ (resp. $C'_\bullet$). Mostre:

(a) $\mathbb{M}(f)_\bullet = (\mathbb{M}(f)_i, \partial_i)$ é um complexo (o <u>cilindro de</u> f).

(b) $\mathbb{M}(f)_\bullet$ é acíclico $\Leftrightarrow$ $H(f)\colon H(C_\bullet) \to H(C'_\bullet)$ é um isomorfismo (em cada componente).

(Sugestão: considere a sequência longa de homologia derivada da sequência exata $0 \to C_\bullet \to \mathbb{M}(f)_\bullet \to C'_\bullet(-1) \to 0$).

(c) Se $C'_\bullet = C_\bullet$, f = multiplicação por $x \in R$ e se $K_\bullet(x;R)$ é o complexo de Koszul associado a x, então $\mathbb{M}(f) \simeq C_\bullet \otimes K_\bullet(x;R)$ como complexos.

(d) Deduza algumas das propriedades do complexo de Koszul usando a técnica acima do cilindro.

6. Seja R um anel (noetheriano), $\underline{x} = x_1,\ldots,x_n \in$ radical de Jacobson de R e M um R-módulo $\neq (0)$. Mostre que se $I = (\underline{x})$, então $\mathrm{prof}_I(M) = n \Leftrightarrow \underline{x}$ é M-sequência.
(Sugestão: por indução sobre n; seja $J = (x_1,\ldots,x_{n-1})$. Pela Propo.III.34, $\mathrm{prof}_J(M) \geq n-1$. Mas, $\mathrm{prof}_J(M) \leq$ $\leq \mathrm{alt}((J + (0:M))/(0:M)) \leq \mathrm{alt}(J) \leq n-1$. Aplique a hipótese indutiva).

7. Seja R um anel local, $\underline{x} = x_1,\dots,x_n \in R$ e $I = (\underline{x}) \neq R$. Mostre:

(a) $\sqrt{0:H_i(\underline{x};R)} \subset \sqrt{0:H_{i+1}(\underline{x};R)}$ para todo $i \geq 0$.

(Sugestão: use a rigidez do complexo de Koszul (Prop.III.32)).

(b) Se $q = n\text{-prof}_I(M)$ então $H_q(\underline{x};R) \simeq (\underline{y}:I)/(\underline{y})$, onde $\underline{y}$ é uma R-sequência máxima em I.

(Sugestão: é capaz de demonstrar isto sem apelo a Ext?)

(c) Deduza: $\dim(R/I) \geq \dim H_i(\underline{x};R) \geq \dim(R/(\underline{y}:(\underline{y}:I)))$, onde $\underline{y}$ é uma R-sequência máxima em I.

(Sugestão: $0:(\underline{y}:I)/(\underline{y}) = \underline{y}:(\underline{y}:I)$).

(d) (R C-M) Mostre que $\dim H_i(\underline{x};R) = \dim(R/I)$, $i \geq 0$.

(Sugestão: com a notação de (c), basta mostrar que $\dim(R/I) \leq \dim(R/(\underline{y}:(\underline{y}:I)))$ ou, passando ao quociente por $\underline{y}$, que se R é C-M e $I \subset R$, um ideal de profundidade 0, então $\dim(R/I) = \dim(R/(0:(0:I)))$. Para isto, mostre que se $P \supset I$ é um primo tal que $\dim(R/P) = \dim(R/I)$, então $(0:(0:I)) \subset P$).

Capítulo IV

Conjecturas homológicas

Explicação. Neste capítulo teremos como objeto aprofundar algumas das questões apenas mencionadas nos capítulos anteriores. Estas questões agrupam-se, grosso modo, sob o título geral de "conjecturas homológicas".

Examinamos, primeiramente, a "conjectura do divisor de zero", atribuida a Auslander. Este mostrou que a conjectura é verdadeira em presença da validade da "rigidez" dos módulos Tor_i^R. (Em geral, dizemos que um complexo $C_\bullet$ é *rígido* se $H_i(C_\bullet) = (0) \Rightarrow H_j(C_\bullet) = (0)$, $j \geq i$; daqui passa-se, facilmente, à noção de rigidez dos Tor_i^R). Malgrado o avanço que se fêz em relação a outras conjecturas homológicas importantes, a questão da rigidez dos Tor_i^R permanece como um ponto isolado, de misterioso acesso. O que se sabe, até agora, foi essencialmente estabelecido pelo próprio Auslander (para anéis regulares não ramificados) há 20 anos atrás, e por Lichtenbaum (para anéis regulares arbitrários) alguns anos depois. As técnicas usadas por estes autores são essencialmente baseadas na análise de sequências espectrais convenientes que "degeneram". É possível, contudo, que o problema esteja à caça de métodos diferentes, tais como a defrontação dos Tor_i^R com a homologia de outros complexos, rígidos a priori.

Em seguida, tocamos de leve o trabalho de Pesquine-

Szpiro, notadamente a observação de que a "conjectura da interseção" implica formalmente na conjectura do divisor de zero. Isto tem interesse, uma vez que estes autores demonstram a validade de sua conjectura para anéis de "igual característica" (isto é, anéis que contêm um corpo). É, talvez, instrutivo mencionar que a conjectura da interseção emana do "teorema de interseção" de Serre, motivado por sua vez por problemas de interseção de subvariedades de uma variedade algébrica. Pareceu-nos natural, por conseguinte, iniciar a seção por algumas implicações formais do teorema da interseção.

A seção seguinte é dedicada à conjectura (da existência) de módulos de C-M "máximos" ou "infinitamente gerados". A importância desta conjectura, devida a Hochster, deriva de que ela implica formalmente em muitas outras conjecturas homológicas, incluindo a do divisor de zero. A contribuição de Hochster é a de ter estabelecido a validade da conjectura no caso de anéis que contêm um corpo ($\operatorname{car} k = 0$ e $\operatorname{car} k > 0$ requerem demonstrações diferentes).

Concluimos com uma aplicação da existência de módulos de C-M para o "problema do syzygy", estudado principalmente por Evans e Griffith.

Várias conjecturas interessantes, agrupadas sob o título geral de "teoremas do ideal principal", foram deixadas de lado por falta de espaço (e energia dos autores). Tratam-se de conjecturas bastante concretas e atraentes que podem, em princípio, ser atacadas sem muita sofisticação homológica.

§1. A conjectura do divisor de zero e o problema da rigidez dos Tor_i^R (Auslander); a conjectura da interseção (Pesquine-Szpiro).

Seja $R,\underline{m}$ um anel local e M um R-módulo tal que d.h. $M < \infty$. Vimos (Cap.III, §3) que

$$\text{d.h. } M + \text{prof}(M) = \text{prof}(R).$$

Em vista desta igualdade, é talvez natural perguntar se uma R-sequência de comprimento máximo pode ser obtida por prolongamento de uma M-sequência. Formulamos esta pergunta sob a forma de conjectura.

Conjectura 1. ("do divisor de zero", Auslander) - *Seja $R,\underline{m}$ um anel local e M um R-módulo tal que d.h. $M < \infty$. Então, toda M-sequência é uma R-sequência.*

Observação. A hipótese d.h. $M < \infty$ é essencial. Com efeito, seja $R = k[x,y]_{(x,y)} = k[X,Y]_{(X,Y)}/(X^2,XY)$ e $M = R/(x)$. Da sequência exata $0 \to (x,y) \to R \to (x) \to 0$ segue que d.h.$(x) = \infty$ - co contrário, d.h.$(x,y) < \infty$, logo R seria um anel regular. Assim, d.h. $M = \infty$. É imediato, por outro lado, que y é não divisor de zero em M.

Que importância tem a conjectura acima? Afinal, pode-se sempre selecionar uma sequência $x_1,\ldots,x_n$ que é *a priori* M-sequência e R-sequência (vide, por exemplo, a demonstração do teorema de Auslander-Buchsbaum).

Ora, anotemos primeiramente o seguinte fato.

Proposição IV.1 - Seja $R, \underline{m}$ um anel local. As seguintes condições são equivalentes:

(i) Dados R-módulos M e N tais que $\mathrm{Sup}(M) \cap \mathrm{Sup}(N) = \{\underline{m}\}$, então $\dim M + \dim N \leq \dim R$.

(ii) Dado um R-módulo M, todo sistema de parâmetros de M se prolonga em um sistema de parâmetros de R.

Demonstração: (i) $\Rightarrow$ (ii). Seja $\underline{x} = x_1, \ldots, x_s$ um sistema de parâmetros de M. Por definição, $M/\underline{x}M$ é $\underline{m}$-primário. Por hipótese, então, $\dim M + \dim R/(\underline{x}) \leq \dim R$. Digamos, $\dim R = d$. Assim, $\dim R/(\underline{x}) \leq d-s$. Mas, $\dim R/(\underline{x}) \geq \dim R - s = d-s$ sempre vale, logo $\dim R/(\underline{x}) = d-s$. Se, agora, $\bar{x}_{s+1}, \ldots, \bar{x}_d$ geram um ideal $\underline{m}/(\underline{x})$-primário em $R/(\underline{x})$, é claro que $x_1, \ldots, x_s, x_{s+1}, \ldots, x_d$ é um sistema de parâmetros de R.

(ii) $\Rightarrow$ (i). Sejam M e N tais que $\mathrm{Sup}(M) \cap \mathrm{Sup}(N) = \{\underline{m}\}$. Então, é claro que $\mathrm{Sup}(M/\underline{a}M) = \mathrm{Sup}(M) \cap \mathrm{Sup}(R/\underline{a}) = \{\underline{m}\}$, onde $\underline{a} = 0{:}N$. Assim, $M/\underline{a}M$ é $\underline{m}$-primário, logo $\underline{a}$ contém um sistema de parâmetros de M, digamos, $\underline{x} = x_1, \ldots, x_s$. Por hipótese, tal sistema pode ser prolongado em um sistema de parâmetros de R. Logo, $\dim R/(\underline{x}) = \dim R - s$. Daqui resulta que $\dim N$ $(= \dim R/\underline{a})$ $\leq \dim R/(\underline{x}) = \dim R - s$, como queríamos. //

Corolário IV.2 - Seja $R, \underline{m}$ um anel local. Consideremos as seguintes condições:

(i) Dados móudlos M e N tais que $\mathrm{Sup}(M) \cap \mathrm{Sup}(N) = \{\underline{m}\}$, *tem-se* $\dim M + \dim N \leq \dim R$.

(ii) *Dado um módulo* M, *toda* M-*sequência é uma* R-*sequência*.

Se R *é Cohen-Macaulay*, (i) $\Rightarrow$ (ii). *Se um pelo menos dos módulos* M *e* N *é Cohen-Macaulay*, (ii) $\Rightarrow$ (i).

Estes resultados põem em relevo a importância da Conjectura 1, devido ao seguinte resultado.

Teorema (Serre [Se]) - *Seja* R *um anel local regular*. *Então a condição* (i) *tem lugar*.

Corolário (do teorema) - *Sejam* V *e* W *subvariedades* (*não necessariamente irredutíveis*) *do espaço afim* k^n. *Se* V *e* W *não admitem componente comuns, tem-se*

$$\operatorname{codim}(V \cap W) \leq \operatorname{codim}(V) + \operatorname{codim}(W).$$

Demonstração: Traduzindo em linguagem algébrica, é suficiente mostrar que para todo primo mínimo P do ideal $I+J$ (onde $I = \mathcal{I}(V)$ e $J = \mathcal{I}(W)$) tal que $\operatorname{alt}(P) = \operatorname{alt}(I+J)$, tem-se:

$$\operatorname{alt}(P) \leq \operatorname{alt}(I) + \operatorname{alt}(J).$$

Ora, podemos evidentemente localizar em P sem alterar hipóteses ou teses. Temos então a nova situação seguinte:

R $(= S_P,\ S = k[X_1, \ldots, X_n])$ um anel local regular e $I, J \subset R$ ideais tais que $I + J$ é $\underline{m}$-primário. Aplicando o teorema acima, resulta $\operatorname{coalt}(I) + \operatorname{coalt}(J) \leq \dim R$ ou, como R é Cohen-Macaulay $2 \dim R - (\operatorname{alt}(I) + \operatorname{alt}(J)) \leq \dim R$. Daqui que $\operatorname{alt}(I+J)$ $(= \dim R) \leq \operatorname{alt}(I) + \operatorname{alt}(J)$, como queríamos.

A seguir, faremos algumas observações sobre a Conjectura 1, exibindo alguns casos em que é válida.

Uma forma preliminar da Conjectura 1 é a seguinte: "se $x \in R$ é não divisor de zero em M com d.h.$M < \infty$, então x é não divisor de zero em R." É fácil ver, por um argumento indutivo, que se esta versão da Conjectura 1 é válida para todo módulo M tal que d.h. $M < \infty$ e para todo anel local pertencente a uma classe de anéis locais R fechada sob a operação de passar ao quociente por um não divisor de zero em R, então a Conjectura 1 é válida também nestas circunstâncias.

Infelizmente, classes interessantes de anéis locais não são fechadas sob tal operação, por exemplo, a classe de todos os anéis regulares, a classe de todos os domínios. Por outro lado, a classe dos anéis de Cohen-Macaulay é fechada sob esta operação. Isto nos permite concluir:

("<u>Princípio indutivo da Conjectura 1</u>") - <u>Se</u> R <u>é um anel de Cohen-Macaulay e se</u> d.h. $M < \infty$, <u>então toda</u> M-<u>sequência é uma</u> R-<u>sequência se e só se todo</u> $x \in R$ M-<u>regular é</u> R-<u>regular</u>.

Uma consequência deste princípio é que o análogo do Teorema de Serre, para R Cohen-Macaulay e um dos módulos M, N Cohen-Macaulay, é equivalente à seguinte forma fraca da Conjectura 1: "Se R é Cohen-Macaulay e M é Cohen-Macaulay tal que d.h. $M < \infty$, então todo elemento $x \in R$ M-regular é R-regular".

As dificuldades técnicas mencionadas na observação acima indicam que é preferível restringir a classe dos módulos e não a dos anéis. Neste espírito, tem-se:

Proposição IV.3 (R um anel local) - Seja M um R-módulo tal que d.h. $M \leq 1$. Então, toda M-sequência é uma R-sequência.

Demonstração: O resultado é trivial se d.h. $M = 0$ (M é livre). De acordo com as observações anteriores, basta mostrar que se d.h. $M = 1$ então todo $x \in R$ M-regular é R-regular.[3] Seja, então

$$0 \to G \xrightarrow{\varphi} F \to M \to 0$$

uma resolução livre de M. A partir desta, obtemos uma sequência longa de homologia (Koszul)

$$\dots \to \underset{\overset{\|}{(0)}}{H_2(x;M)} \to H_1(x;G) \xrightarrow{H_1(\varphi)} H_1(x;F) \to H_1(x;M).$$

Por hipótese, $H_1(x;M) = (0)$. Resulta que a aplicação $H_1(\varphi)$ é um isomorfismo. Mas, como F (resp. G) é um módulo livre, temos $H_1(x;F) \simeq H_1(x;R) \otimes F$ (resp. $H_1(x;G) \simeq H_1(x;R) \otimes G$). Além disso, um momento de reflexão nos convencerá de que $H_1(\varphi)$ é efetivamente $1_{H_1(x;R)} \otimes \varphi$. Logo, $H_1(x;R) \otimes M = (0)$ e, portanto, $H_1(x;R) = (0)$, como queremos. //

Não é possível aplicar o método de demonstração da Proposição IV.3 a um módulo de d.h. ≥ 2. Somos levados a procurar algum critério mediante o qual possamos testar a validade da Conjectura 1. Comecemos, então, por examinar o Corolário IV.2 mais detidamente. Lá tínhamos (i) $\Rightarrow$ (ii) (isto é, (i) $\Rightarrow$ Conjectura 1)

---

(3) Aplicamos o princípio indutivo antes mencionado, em relação ao módulo. Assim, se $x \notin Z(M)$ e $x \notin Z(R)$, temos $d.h._{R/(x)}(M/xM) = d.h._R(M) \leq 1$ (Prop.III.16,§3,Cap.III).

sob a hipótese de R ser C-M. Mas, qual a propriedade essencial de um R C-M que realmente provoca a implicação (i) $\Rightarrow$ (ii)?

No Capítulo II, §2, insistimos na propriedade de complementaridade de codimensão e dimensão para um módulo de C-M (Teor.II.13), como sendo um substituto quase tão bom quanto a propriedade original de C-M (vide "Importante", loc.cit.). Reformulemos aquela propriedade: se R é C-M local e $M \neq 0$ um R-módulo, então

$$\begin{array}{ccc} \dim(M) & + \ \operatorname{prof}(0:M) & = \dim(R) \\ \| & \| & \\ \dim(R/0:M) & \operatorname{alt}(0:M) & \end{array}$$

Se R não é C-M e ainda temos esperança de que valha esta igualdade, precisamos impor alguma condição de "regularidade" em M. Isto nos leva à <u>conjectura da codimensão</u>:

<u>Conjectura 2</u> (M. Auslander) - <u>Se</u> R <u>é um anel local e</u> $M \neq 0$ <u>um módulo tal que</u> $\mathrm{d.h.}(M) < \infty$, <u>então</u>

$$\dim(M) + \operatorname{prof}(0:M) = \dim(R).$$

O fato de que esta igualdade é suficiente, juntamente com a condição (i) da Proposição IV.1, para obter a conjectura foi percebido por Pesquine e Szpiro. Para escrever este resultado na forma de "conjectura $\Rightarrow$ conjectura", reenunciemos a condição (i) da Proposição IV.1 como

<u>Conjectura 3</u> (Serre [Se], Pesquine-Szpiro [$(P\text{-}S)_1$]) - <u>Seja</u> $R,\underline{m}$ <u>um anel local</u>, M <u>e</u> N <u>módulos tais que</u>:

1) $\mathrm{d.h.}(M) < \infty$

2) $\operatorname{Sup}(M) \cap \operatorname{Sup}(N) = \{\underline{m}\}$.

Então $\dim(M) + \dim(N) \leq \dim(R)$.

O resultado de Pesquine-Szpiro é, então, este:

Proposição IV.4 - Conjectura 2 + Conjectura 3 $\Rightarrow$ Conjectura 1.

Demonstração: Afirmamos, primeiramente, que as Conjecturas 2 e 3, juntas, implicam o seguinte:

$(*)_M$ ($R,\underline{m}$ local, M e N módulos) Se $d.h.(M) < \infty$ e se $\mathrm{Sup}(M) \cap \mathrm{Sup}(N) = \{\underline{m}\}$, então $\dim(N) \leq d.h.(M)$.

Com efeito, tem-se
$$\begin{aligned}\dim(N) &\leq \dim(R) - \dim(M)\\ &= \dim(R)-(\dim(R)-\mathrm{prof}(0{:}M))\\ &= \mathrm{prof}(0{:}M) \leq d.h.(M),\end{aligned}$$

a última desigualdade pelo Teorema de Rees (Cor.III.22, §3 do Cap.III).

Em seguida, mostremos que este último estado de coisas, $(*)_M$ acarreta a validade da Conjectura 1. Primeiramente, vejamos que nas condições de $(*)_M$, o princípio indutivo da Conjectura 1 vale (vide observações que precedem a Prop.IV.3).

Temos de verificar: dado um módulo $M \neq (0)$ tal que $d.h.(M) < \infty$ e um elemento $x \in R$ tal que $x \notin Z(R)$ e $x \notin Z(M)$, então $(*)_M \Rightarrow (*)_{M/xM}$.

Isto é fácil: para começar, temos a igualdade $d.h._R(M) = d.h._{R/(x)}(M/xM)$ (Prop.III.16,§2). Ora, seja N um $R/(x)$-módulo tal que $\mathrm{Sup}(M/xM) \cap \mathrm{Sup}(N) = \{\underline{m}/(x)\}$. Como $\mathfrak{a}_{R/(x)}N = (0{:}N)/(x)$ (das definições!), vê-se que $\mathrm{Sup}(M) \cap \mathrm{Sup}(N) = \{\underline{m}\}$ (considerando N como R-módulo via $R \to R/(x)$). Pela hipótese $(*)_M$, temos $\dim(N) \leq d.h.(M)$. Consequentemente, $\dim(N)$

$\leq \text{d.h.}_{R/(x)}(M/xM)$, como queríamos.

Sendo válido o princípio indutivo, o problema fica reduzido a mostrar que, se $(*)_M$ <u>vale para todo anel local e todo módulo</u> M <u>tal que</u> $\text{d.h.}(M) < \infty$, <u>então vale também a seguinte propriedade, para todo anel local</u> R <u>e todo módulo</u> M <u>tal que</u> $\text{d.h.}(M) < \infty$: $P \in \text{Ass}(R) \Rightarrow P \subset Q$, <u>para algum</u> $Q \in \text{Ass}(M)$.

Mostramos esta última implicação por indução sobre $\dim(M)$. Se $\dim(M) = 0$, $\text{Sup}(M) = \{\underline{m}\}$; é claro, neste caso, que todo $P \in \text{Ass}(R)$ está contido em um primo associado de M.

Seja $\dim(M) > 0$ e $P \in \text{Ass}(R)$. Há duas possibilidades. Primeiro, o único primo do $\text{Sup}(M)$ contendo P é $\underline{m}$. Neste caso, $\text{Sup}(M) \cap \text{Sup}(R/P) = \{\underline{m}\}$, logo $(*)_M$ diz que $\dim(R/P) \leq$ $\leq \text{d.h.}(M)$. Mas, $\text{prof}(R) \leq \dim(R/P)$ (Prop.II,10,§2,Cap.II) e, portanto, pela igualdade de Auslander-Buchsbaum, $\text{prof}(M) = 0$. Em outras palavras, $\underline{m} \in \text{Ass}(M)$.

A outra possibilidade é que exista $Q \in \text{Sup}(M)$ tal que $Q \supset P$ e $Q \neq \underline{m}$. Neste caso, podemos aplicar a hipótese indutiva a M_Q já que $\dim(M_Q) \lneq \dim(M)$. Como $\text{d.h.}_{R_Q}(M_Q) \leq \text{d.h.}(M) < \infty$, $(*)_{M_Q}$ vale e, por conseguinte, existe $Q'R_Q \in \text{Ass}(M_Q)$ tal que $PR_Q \subset Q'R_Q$. Deduzimos que $P \subset Q'$, $Q' \in \text{Ass}(M)$, como queríamos. //

<u>Observação</u>. Analisando a demonstração da última implicação acima, vemos que não é preciso supor $(*)_M$ para todos anéis locais e todos módulos de dimensão homológica finita. Podemos mostrar a implicação para um módulo fixo M (de $\text{d.h.} < \infty$) contanto que $(*)_M \Rightarrow (*)_{M_Q}$ para todo $Q \in \text{Sup}(M)$. Mais precisamente, o que a Proposição IV.4 contém é a afirmação de que, <u>numa classe de anéis</u>

locais fechada sob as operações de localização (em primos) e passagem ao quociente por um não divisor de zero, as Conjecturas 2 e 3, em conjunto, implicam a Conjectura 1.

$(*)_M$ é chamada conjectura da interseção.

Assim, reformulando:

Proposição IV.4 (bis) - Seja $\mathcal{L}$ uma classe de anéis locais tais que: (i) Se $R \in \mathcal{L}$ e $P \subset R$ é um primo, então $R_P \in \mathcal{L}$; (ii) Se $R \in \mathcal{L}$ e $x \notin Z(R)$, então $R/(x) \in \mathcal{L}$. Então, para módulos sobre anéis de $\mathcal{L}$, tem-se: conjectura da interseção $\Rightarrow$ $\Rightarrow$ conjectura do divisor de zero.

É claro que o interesse da Proposição IV.4 (bis) depende da validade da conjectura da interseção. Eis uma das contribuições centrais de Pesquine-Szpiro:

Teorema P-S (Pesquine-Szpiro [$(P\text{-}S)_1$, Th.2.1,Ch.II]) - Seja R um anel local satisfazendo uma das condições seguintes: (i) R é de característica $p > 0$; (ii) R é a localização de uma álgebra finitamente gerado sobre um corpo de característica 0. Neste caso, a conjectura da interseção é válida.

Trata-se de um resultado difícil, cuja demonstração não cabe aqui (mesmo no sentido físico!).

Como consequência deste teorema, a conjectura do divisor de zero vale sob as mesmas hipóteses para R. Contudo, é algo que incomoda pensar que uma questão básica de divisores de zero e dimensão homológica dependa de uma hipótese bastante "geométrica", como o é a de que o anel contenha um corpo. Por exemplo, esta situação exclui certas álgebras bastante concretas tais como quocientes de $Z[X_1,\ldots,X_n]_p$. Este estado de coisas, misterioso, lembra o período em que os anéis locais de "característica desigual" esperneavam teimosamente nas mãos dos especialistas, antes das contribuições homológicas decisivas dos anos 50.

Queremos, em seguida, indicar um outro método para decidir a validade da conjectura do divisor de zero. Este método depende da chamada <u>conjectura da rigidez dos</u> Tor_i e foi imaginado pelo próprio Auslander [Au].

<u>Conjectura 4</u> ("Rigidez dos Tor_i", Auslander) - <u>Seja</u> $R,\underline{m}$ <u>um anel local e</u> M <u>um módulo tal que</u> $d.h.(M) < \infty$. <u>Para todo módulo</u> N, $\mathrm{Tor}_i(M,N) = (0) \Rightarrow \mathrm{Tor}_j(M,N) = (0)$ <u>para todo</u> $j \geq i$.

Pela "décalage" dos Tor (vide §2, Cap.III), vê-se sem dificuldade que a conjectura acima é equivalente à conjectura análoga com $i = 1$. (Além disso, por localização, etc., podemos até supor que $\mathrm{Tor}_j(M,N)$ é $\underline{m}$-primário, $j \geq 1$; não insistiremos nisto, contudo). Esta equivalência diz respeito à <u>toda</u> a classe dos módulos de $d.h. < \infty$; ela não faz muito sentido para <u>um</u> módulo (fixo).

De maneira provisória, chamaremos Tor^R-<u>rígido</u> um R-módulo M tal que $\mathrm{Tor}_1^R(M,N) = (0) \Rightarrow \mathrm{Tor}_i^R(M,N) = (0)$ para todo $i \geq 1$ e para todo R-módulo N.

Antes de enunciar a próxima proposição, observemos o seguinte fato simples: se um R-módulo M é Tor^R-rígido e se $I \subset R$ é um ideal, então M/IM é um R/I-módulo $\mathrm{Tor}^{R/I}$-rígido. Isto resulta de que todo R/I-módulo é (evidentemente) redução, "módulo" I,

de um R-módulo e da propriedade $\mathrm{Tor}_i^R(M,N) \otimes_R R/I \simeq$
$\simeq \mathrm{Tor}_i^{R/I}(M/IM,\ N/IN)$.

<u>Proposição IV.5</u> (Auslander [Au]) - <u>Para todo anel local</u> R <u>e todo</u> R-<u>módulo</u> $M \neq (0)$, <u>tem-se</u>:

M Tor^R-<u>rígido</u> $\Rightarrow$ <u>toda</u> M-<u>sequência é</u> R-<u>sequência</u>.

<u>Demonstração</u>: A afirmação é no sentido de que a Conjectura 4 acarreta a Conjectura 1. Assim, procederemos por indução sobre o cardinal da M-sequência e para todos os anéis locais e módulos! Seja, então, $\underline{x} = x_1,\ldots,x_n$ uma M-sequência.

Suponhamos $n = 1$, $x = x_1$. A observação chave é a de que existe o diagrama comutativo seguinte:

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & & \mathrm{Tor}_1^R((x),M) \arrow[d] \arrow[dl, dashed] & & \\
0 \arrow[r] & \mathrm{Núc}(\varphi) \arrow[r] & Z_1(x;R)\otimes M \arrow[r, "\varphi"] \arrow[d] & Z_1(x;M) & \\
 & & K_1(x;R)\otimes M \arrow[r, Rightarrow] \arrow[d] & K_1(x;M) & \\
0 \arrow[r] & \mathrm{Tor}_1^R(R/(x),M) \arrow[r] & (x)\otimes M \arrow[r] & (x)\cdot M \arrow[r] & 0
\end{tikzcd}$$

Disso, segue facilmente (há aqui coisas do "lema da serpente", mas é tudo tão direto!...) que

$$\mathrm{conúc}(\varphi) \simeq \mathrm{núc}((x)\otimes M \to (x)M) = \mathrm{Tor}_1^R(R/(x),M)$$

e, além disso, existe uma sobrejeção

$$\mathrm{Tor}_1^R((x),M) \to \mathrm{Núc}(\varphi) \to 0$$

(seta pontilhada no diagrama). Em suma, obtemos uma sequência exata

$$\begin{array}{ccccccc} \mathrm{Tor}_2^R(R/(x),M) \to & Z_1(x;R)\otimes M & \to & Z_1(x;M) & \to \mathrm{Tor}_1^R(R/(x),M) \to 0 \\ & \| & & \| & \\ & H_1(x;R)\otimes M & & H_1(x;M) & \\ & \| & & \| & \\ & (0:_R x)\otimes M & & (0):_M x & \end{array}$$

(observemos que a sobrejeção da direita foi descrita também na demonstração do Lema III.17, §2, Cap.III).

A conclusão, neste caso, é agora imediata. Com efeito, por hipótese $x \notin Z(M)$, logo $(0):_M x = (0)$. Isto implica $\mathrm{Tor}_1^R(M,R/(x)) = (0)$. Como M é Tor^R-rígido, $\mathrm{Tor}_2^R(M,R/(x)) = (0)$. Consequentemente, $(0:_R x)\otimes M = (0)$, donde $(0):_R x = (0)$ pois R é local e $M \neq (0)$.

Suponhamos, agora, $n > 1$. Ponhamos $\bar{R} = R/(x_1)$, $\bar{M} = M/x_1 M$. Pela observação feita antes da proposição $\bar{M}$ é $\mathrm{Tor}^{\bar{R}}$-rígido e $x_2,\dots,x_n$ é $\bar{M}$-sequência. Pela hipótese indutiva, $x_2,\dots,x_n$ é $\bar{R}$-sequência. Pelo caso $n = 1$, segue então a conclusão. //

<u>Questão</u>. Para todo anel local R e todo R-módulo $M \neq (0)$, tem-se: M Tor^R-rígido $\Rightarrow$ toda sequencia $\underline{x} \in R$ tal que $H_q(\underline{x};M) = (0)$ para todo $q \geq q_o$ (fixo), satisfaz $H_q(\underline{x};R) = 0$, $q \geq q_o$. (Equivalentemente: M Tor^R-rígido $\Rightarrow$ $\mathrm{prof}_{(\underline{x})}(R) \geq \mathrm{prof}_{(\underline{x})}(M)$ para todo ideal $(\underline{x})$).

Para responder esta questão (que pode se tornar um exercício!), é conveniente escrever diagramas parecidos ao que usamos na proposição, envolvendo Tor_i de ordem superior, etc.

O principal resultado sobre a rigidez dos Tor_i é devido a Auslander, em um caso particular, e a Lichtenbaum, em sua forma final.

<u>Teorema A-L</u> (Auslander [Au], Lichtenbaum [Li]) - <u>Se</u> R <u>é um anel local regular, todo</u> R-<u>módulo é</u> Tor^R-<u>rígido</u>.

Não daremos a demonstração deste teorema, a qual depende de técnicas de sequências espectrais (dos módulos Tor_i) e de produtos tensoriais "completados".

<u>Questão</u>. Dar uma demonstração do Teorema A-L sem recorrer às técnicas "extra-terrenas" mencionadas.

(O projeto pode ser interessante e não totalmente impossível; vide, por exemplo, [$(S\text{-}V)_2$, Ch.I,§b], onde se demonstra, por via elementar, um resultado obtido em [Li] sobre características de Euler-Poincaré).

Uma consequência do Teorema A-L é que a conjectura do divisor de zero é válida para anéis regulares. É claro, como já vimos, que para anéis regulares a conjectura é uma consequência do resultado de Serre (vide Cor.IV.2). Aproveitamos para lembrar, mais uma vez, que não há princípio indutivo imediato para anéis regulares, assim que efetivamente faz-se necessário algo como a rigidez dos Tor_i ou o resultado de Serre.

§2. Módulos de Cohen-Macaylay máximos (conjectura de Hochster); o problema do syzygy (G. Evans).

Definição IV.6 - Seja $R,\underline{m}$ um anel local. Um R-módulo M é chamado módulo de C-M máximo se:

(i) M é (finitamente gerado) C-M;

(ii) $\text{prof}_{\underline{m}}(M) = \dim(R)$.

(N.B. $\text{prof}_{\underline{m}}(M) \leq \dim(M) = \dim(R/0:M) \leq \dim(R)$, de modo que $\dim(R)$ é um limite superior para profundidade e a condição (i) já é consequência de (ii)).

A pergunta é: o que tem de especial um módulo de C-M máximo? Primeiramente, observemos que se um tal módulo tem d.h. $< \infty$, então ele é de fato um módulo livre e o anel R é C-M (igualdade de Auslander-Buchsbaum). Assim, devemos esquecer a condição d.h. $< \infty$ para tais módulos. Neste caso, a pergunta é se tais módulos existem (com R não C-M).

A importância da existência de módulos de C-M máximos se explica, em parte, pelo seguinte resultado.

Proposição IV.7 (Hochster [Ho_2]) - *Seja $\mathcal{L}$ uma classe de anéis locais satisfazendo as seguintes condições:*

(i) $R \in \mathcal{L} \Rightarrow R$ *admite um módulo de C-M máximo;*

(ii) $R \in \mathcal{L}$ *e* $P \subset R$ *primo* $\Rightarrow R/P \in \mathcal{L}$.

Então para todo $R \in \mathcal{L}$, *a conjectura da interseção é verdadeira.*

Demonstração: (Depende de um resultado de sensibilidade à profundidade demonstrado no Cap.III). Primeiramente, podemos supor, sem perda de generalidade, que são dados um ideal $J \subset R$ e um R-módulo M tais que $d.h._R(M) < \infty$ e $Sup(M/JM) = \{\underline{m}\}$, e quer-se provar que $\dim(R/J) \leq d.h.(M)$.

Seja $P \subset R$ um primo tal que $J \subset P$ e $\dim(R/P) = \dim(R/J)$. Pelas hipóteses (i) e (ii), R/P admite um R/P-módulo E de C-M máximo. Escolhemos um sistema de parâmetros $\bar{y}_1,\ldots,\bar{y}_k \in R/P$ de E. Como E é C-M máximo, resulta que $\bar{y}_1,\ldots,\bar{y}_k$ é uma E-sequência e é um sistema de parâmetros (de $R/(P+0:E)$, isto é) de R/P.

Em seguida, entramos com a hipótese $Sup(M/JM) = \{\underline{m}\}$. Pondo $I = 0:M$, $I+J$ é $\underline{m}$-primário. Logo, substituindo $y_1,\ldots,y_k$ por suas potências suficientemente altas, podemos supor que $y_1,\ldots,y_k \in I+J \subset I+P$ (vide Exercício 11, Cap.II). Neste caso, escrevendo $y_i = x_i+z_i$, $x_i \in I$, $z_i \in J$, vemos que $\bar{y}_i = \bar{x}_i$. Logo, $\bar{x}_1,\ldots,\bar{x}_k$ e, consequentemente, $x_1,\ldots,x_k$, formam ainda uma E-sequência.

Estamos agora em posição de aplicar a Proposição III.27, Capítulo III, §3, com $N = E$. Obtemos $d+k \leq d.h.(M)$, onde $d \geq 0$ é definido de certa maneira (irrelevante neste momento). Em particular, $\dim(R/J) = \dim(R/P) = k \leq d.h.(M)$, como queríamos. //

Coletando os resultados da Proposição IV.4 (bis) e da última proposição, obtemos:

Proposição IV.8 - Seja $\mathcal{L}$ uma classe de anéis locais satisfazendo as seguintes condições:

(i) $R \in \mathcal{L}$, $P \subset R$ primo $\Rightarrow R_P \in \mathcal{L}$ e $R/P \in \mathcal{L}$;

(ii) $R \in \mathcal{L}$, $x \notin Z(R) \Rightarrow R/(x) \in \mathcal{L}$.

(iii) $R \in \mathcal{L} \Rightarrow R$ admite um módulo de C-M máximo.

Então, para todo $R \in \mathcal{L}$, a conjectura do divisor de zero é verdadeira.

Uma formulação monemônica, ainda que imprecisa, do resultado acima é: numa classe de anéis locais fechada sob localização e passagem ao quociente, a existência de módulos de C-M máximos implica a validade da conjectura do divisor de zero.

O problema é: poucas dentre as classes usuais de anéis locais parecem satisfazer as condições (i) e (ii) acima (exceto a classe de todos os anéis locais, evidentemente). Mais sério ainda: (iii) falha para anéis bastante "razoáveis". De fato, existem exemplos de domínios locais R de dimensão 2 (e profundidade 1) tais que nem toda álgebra finitamente gerada sobre R satisfaz a condição das cadeias saturadas de ideais primos. Ora, se um tal R admitisse um módulo E de C-M máximo, teríamos necessariamente $\operatorname{Sup}(E) = \operatorname{Sup}(R)$. Neste caso, o método de demonstração do Teorema II.13, §2, fornece o resultado de que toda álgebra finitamente gerada sobre R satisfaz a condição das cadeias saturadas.

Isto coloca-nos em situação desagradável: não podemos decidir a validade da conjectura do divisor de zero (e, portanto, tampouco a da interseção) nem mesmo para anéis de C-M, já que não formam uma classe $\mathcal{L}$ "decente". É aqui que Hochster dá um passo atrevido: se módulos de C-M máximos inexistem é porque eles são demasiado "pequenos" a priori! Sejamos, então, mais generosos:

Definição IV.9 - Seja $R,\underline{m}$ um anel local. Um R-módulo E, não necessariamente finitamente gerado, é um módulo de C-M grande se existem $x_1,\ldots,x_n \in \underline{m}$ tais que:

(i) $x_1,\ldots,x_n$ é um sistema de parâmetros de R;

(ii) $(x_1,\ldots,x_n)E \neq E$

(iii) $x_i \notin Z(E/(x_1,\ldots,x_{i-1})E)$, $i = 0,\ldots,n$.

(N.B. (ii) e (iii) dizem que $x_1,\ldots,x_n$ é uma E-sequência, mas não podemos aplicar os argumentos usuais empregados quando E é finitamente gerado. Em particular, $(x_1,\ldots,x_n)E \neq E$ não segue somente de que $\underline{x} \in \underline{m}$).

Há dois aspectos importantes que põem em cheque o valor desta noção: primeiro, o da existência de tais módulos; segundo, o do seu comportamento sob as técnicas usuais que vimos funcionar para módulos finitamente gerados.

A contribuição essencial de Hochster é a de ter resolvido ambos os aspectos do problema de maneira satisfatória. Quanto ao segundo, não é difícil mostrar que "sensibilidade à profundidade" mantém-se para módulos de tipo infinito; assim como a Proposição IV.7, que é passível de adaptação. Vários outros resultados técnicos podem ser estendidos ([Ho_1], [Ho_2]). Quanto à existência, tem-se:

Teorema H (Hochster [Ho_2]) - Seja R um anel local contendo um corpo. Então, R admite um módulo de C-M grande.

(Observe-se que este resultado é ligeiramente melhor do que o Teorema P-S. Em particular, para um anel local contendo um corpo, a conjectura do divisor de zero é válida).

Enunciemos formalmente a

<u>Conjectura 5</u> (Hochster) - <u>Todo anel local admite um módulo de C-M grande</u>.

Mais à frente, mencionaremos outras consequências formais da Conjectura 5. Para já, gostaríamos de examinar a relevância desta conjectura para o chamado "problema do syzygy". Seguiremos, de perto, os trabalhos de G. Evans e P. Griffith ([$(E-G)_1$], [$(E-G)_2$]), tornando mais precisas algumas consequências que não aparecem claramente delineadas naqueles trabalhos.(4)

Já deparamo-nos com syzygys no Capítulo III, §1: dizemos que um módulo Z é um <u>syzygy de ordem</u> k se existe um módulo M e uma resolução livre

$$\begin{tikzcd}[column sep=small]
\cdots \arrow[r] & F_k \arrow[rr] \arrow[dr] & & F_{k-1} \arrow[r] & \cdots \arrow[r] & F_1 \arrow[r] & F_o \arrow[r] & M \arrow[r] & 0 \\
& & Z_k \arrow[ur] \arrow[dr] & & & & & & \\
& 0 \arrow[ur] & & 0 & & & & &
\end{tikzcd}$$

tal que $Z \simeq Z_k$.

É evidente que a ordem de um syzygy não está bem definida: se Z é um syzygy de ordem k (Z_k de um módulo M) então ele é um syzygy de ordem $j \leq k$.

---

(4) Em tempo: algumas destas observações já aparecem no artigo recente [Br-E-G].

Deveríamos, talvez, definir "um syzygy de ordem $\leq k$ ". O que realmente interssa é um limite superior - e não inferior - para a ordem de um syzygy.

<u>Exemplo</u>. Seja $\underline{x} = x_1,\dots,x_k \in R$ uma R-sequência. O complexo de Koszul $K_{\bullet}(\underline{x};R)$ mostra que o módulo R é um syzygy de ordem k. Assim, posto(R) = 1 << k. Por outro lado, podemos adicionar um número arbitrário de cópias de R aos dois últimos termos de $K_{\bullet}(\underline{x};R)$ (o mesmo número para os dois termos), sem desfazer a aciclicidade do complexo. Isto mostra que um módulo livre R^r (qualquer) é um syzygy de ordem k. Assim, podemos ter posto >>k.

O comportamento de syzygys que são módulos livres, sendo tão selvagem quanto poderia ser, perguntamos se é possível controlar os syzygys não livres.

O primeiro resultado relevante, nesta linha, é o seguinte.

<u>Proposição B</u> (Bruns [Br]) (R local regular) - Se Z é um syzygy de ordem k e de posto k+s, então Z contém um submódulo livre F tal que Z/F é um syzygy de ordem k e de posto k.

É este o melhor resultado possível? Precisamente, temos o

<u>Problema do Syzygy</u> (R local regular) - Se Z é um syzygy de ordem k, então posto(Z) $\lneq$ k $\Rightarrow$ Z livre.

Antes de comentar sobre o estado atual deste problema, mencionaremos algumas consequências de uma solução afirmativa para o mesmo.

1) <u>Se</u> $I \subset R$ <u>é um ideal tal que</u> $\mu(I) \leq 2$, <u>então</u> $d.h._R(I) \leq 1$.

Suponhamos que $d.h.(I) \geq 2$, isto é, $d.h.(R/I) \geq 3$. Então, R/I admite uma resolução mínima

$$\begin{tikzcd}
\cdots \arrow[r] & F_3 \arrow[rr] \arrow[dr] & & F_2 \arrow[rr] \arrow[dr] & & F_1 \arrow[rr] \arrow[dr] & & F_o \arrow[r] & R/I \arrow[r] & 0 , \\
& & Z_3 \arrow[ur] & & Z_2 \arrow[ur] & & I \arrow[ur] & R \arrow[u, equal] & &
\end{tikzcd}$$

com Z_2 não livre. Pelo "problema" do syzygy, $posto(Z_2) \geq 2$. Resulta $posto(F_1) = posto(Z_2) + posto(I) \geq 2+1 = 3$. Mas, como a resolução é mínima, $posto(F_1) = \mu(I)$; contradição.

<u>Observação</u>. O resultado é verdadeiro, independentemente do probelma do syzygy (atribuido a Mac Rae [McR]). É válido, mais geralmente, para um anel noetheriano - no que é consequência também do problema do syzygy, se resolvido em condições mais gerais: R local e $d.h.(Z) < \infty$. O interesse deste resultado é que permite demonstrar, facilmente, que todo anel local regular é fatorial [B-E].

2) <u>Se</u> $0 \to F_n \to \ldots \to F_o$ <u>é uma resolução livre mínima, tem-se</u>:

$$posto(F_{n-1}) \geq n$$

$$posto(F_i) \geq 2i+1, \quad i = 0,\ldots,n-2.$$

Trata-se de mera estimativa, com o problema do syzygy e a igualdade $posto(F_i) = posto(Z_i) + posto(Z_{i+1})$.

<u>Observação</u>. Estas estimativas dão alguma idéia de como podem ser os postos dos módulos livres numa resolução livre mínima. Há algumas conjecturas informais sobre o crescimento (resp. decrescimento) destes postos, bastante mais audaciosas do que permitem en

trever as estimativas acima - que, a propósito, são equivalentes a uma resposta afirmativa ao problema do syzygy.

3) Se $I \subset R$ é um ideal equidimensional (= puro) e se $\mu(I) \leq 3$, então I é perfeito.

A questão é relevante quando $\mu(I) = 3$, os outros casos podendo ser verificados diretamente ($\mu(I) = 2$ pede o teorema de MacRae acima). O caso $\text{alt}(I) = 3$ é o de um ideal da classe principal, logo perfeito.

Assim, $\mu(I) = 3$, $\text{alt}(I) = 2$. Escrevamos uma apresentação:

$$\begin{tikzcd}[column sep=small] 0 \arrow[r] & Z \arrow[r] & R^3 \arrow[rr] \arrow[dr] & & R \arrow[r] & R/I \arrow[r] & 0 \\ & & & I \arrow[ur] \arrow[dr] & & & \\ & & 0 \arrow[ur] & & 0 & & \end{tikzcd}$$

Evidentemente, $\text{posto}(Z) = \text{posto}(R^3) - \text{posto}(I) = 2$. A idéia é mostrar que, em virtude de I ser equidimensional, Z é um syzygy de ordem 3. Pelo problema do syzygy, Z é então necessariamente livre (consequentemente, R/I é perfeito).

Para isto, usamos o seguinte critério:

Proposição IV.10 (Auslander-Bridger [A-Br]) - Seja R um anel local e Z um R-módulo tal que $\text{d.h.}(Z) < \infty$. As seguintes condições são equivalentes:

(i) Z é um syzygy de ordem k;

(ii) $\text{prof}_{P_P}(Z_P) \geq \min\{k, \text{prof}_{P_P}(R_P)\}$ para todo primo $P \subset R$.

N.B. Se R é C-M, $\text{prof}_{P_P}(R_P) = \text{prof}_P(R) = \text{alt}(P)$. Neste caso, (ii) é exatamente a condição chamada "S_k" para um módulo Z (vide

Cap.II, §3, Nº 2, onde S_2 é mencionada).

<u>Demonstração</u>: (i) ⇒ (ii). Esta implicação é fácil. Consideramos uma sequência exata

$$\begin{tikzcd}[column sep=small] 0 \arrow[r] & Z \arrow[r] & F_{k-1} \arrow[r] \arrow[dr] & \cdots \arrow[r] & F_1 \arrow[r] \arrow[dr] & F_o, \\ & & & Z_{k-1} \arrow[ul, phantom] & Z_2 \arrow[u] & Z_1 \arrow[u] \end{tikzcd} \qquad F_i \text{ livre.}$$

Localizemos em P (primo). Se Z_P é R_P-livre, então $\mathrm{prof}_{P_P}(Z_P) = \mathrm{prof}_{P_P}(R_P)$. Se Z_P não é R_P-livre, então $\mathrm{prof}_{P_P}(Z_P) \lneq \mathrm{prof}_{P_P}(R_P)$ (igualdade de Auslander-Buchsbaum). Neste caso, aplicações sucessivas da Proposição II.6 (bis) fornecem $\mathrm{prof}_{P_P}(Z_P) = \mathrm{prof}_{P_P}((Z_1)_P) + k-1 = \mathrm{prof}_{P_P}(M_P) + k$, onde $M = \mathrm{conúcl}(F_1 \to F_o)$. Logo, $\mathrm{prof}_{P_P}(Z_P) \geq k$.

(ii) ⇒ (i). Esta implicação é mais intricada. Com a desculpa de que sobrecarregaria o texto de tecnicismos, deixamos como pequeno desafio para o leitor (em caso de emergência, vide [A-Br,Th.(4.25)]).

De volta à demonstração da consequência 3): mostremos que $\mathrm{prof}_{P_P}(Z_P) \geq \min\{3,\mathrm{alt}(P)\}$. Se $P \not\supset I$, a afirmação é óbvia pois $I_P = R_P$. Se $P \supset I$, há duas possibilidades: $P \in \mathrm{Ass}(R/I)$ ou $P \notin \mathrm{Ass}(R/I)$. No primeiro caso, como I é equidimensional, $\mathrm{alt}(P) = 2$. Por outro lado, para um tal P, $\mathrm{prof}_{P_P}(R/I)_P = 0$. Logo $\mathrm{prof}_{P_P}(I_P) \geq 1$ por causa da sequência estrutural

$$0 \to I_P \to R_P \to (R/I)_P \to 0.$$

Logo, $\mathrm{prof}_{P_P}(Z_P) \geq 2$, aplicando a Proposição II.6 (bis) à sequência

$$0 \to Z_P \to R_P^3 \to I_P \to 0.$$

O caso $P \notin \mathrm{Ass}(R/I)$ é verificado analogamente ($\mathrm{prof}_{P_P}(R/I)_P \geq 1$, etc.).

Observação. Vê-se que, em verdade, esta consequência do problema do syzygy é equivalente ao mesmo.

Todas as consequências acima são válidas se R contém um corpo (esceto 1), que vale de qualquer maneira), em virtude do

Teorema E-G (Evans-Griffith [$(E-G)_2$]) - *Seja* R *um domínio local de C-M, contendo um corpo. Se* Z *é um syzygy de ordem* k *tal que* $0 \neq \mathrm{d.h.}(Z) < \infty$, *então* $\mathrm{posto}(Z) \geq k$.

A demonstração depende de três ingredientes:

1º) Existência de módulos de C-M grandes.

2º) "Lema de aciclicidade" de Pesquine-Szpiro-Foxby ([$(P-S)_1$], [Fox]):

Seja R *um anel local e seja*

$$C_{\bullet}: \qquad 0 \to C_{\ell} \to C_{\ell-1} \to \dots \to C_0$$

um complexo de R-*módulos* (*não necessariamente de tipo finito*) *tal que*:

(i) $\mathrm{prof}(C_i) = d$ (*constante ao longo do complexo*);

(ii) $H_i(C_{\bullet}) = (0)$ *ou* $\mathrm{prof}\, H_i(C_{\bullet}) = 0$, $i > 0$.

Então, $\ell \leq d \Rightarrow C_{\bullet}$ *acíclico*. *Se, em verdade*, $\ell \lneq d$ *e* $H_0(C_{\bullet}) \neq (0)$, *então* $\mathrm{prof}\, H_0(C_{\bullet}) \gneq 0$.

(Atenção: um pouco de cuidado na definição de $\mathrm{prof}_I(M)$, no caso em que M não é finitamente gerado. Se $IM \neq M$, a defi nição usual funciona bem. Em geral, há alternativas propostas por vários autores ([Bar], [$(E-N)_2$], [Ho_1], [Fox]) e todas parecem coincidir no caso em que $IM \neq M$).

3º) "Teorema do syzygy" de Gröbner, generalizado:

<u>Seja</u> R <u>um domínio local de C-M, contendo um corpo e</u> Z, <u>um syzygy de ordem</u> k <u>tal que</u>:

(i) $d.h.(Z) < \infty$;

(ii) Z_P <u>é</u> R_P-<u>livre para todo</u> $P \neq \underline{m}$.

<u>Então</u>, $x \in Z \setminus \underline{m}Z \Rightarrow alt(Z^*(x)) \geq k$.

<u>N.B</u>. $Z^*(x) = \{f(x) \mid f \in Z^* = Hom_R(Z,R)\}$ é o <u>ideal traço</u> de x. Este ideal desempenha um papel relevante nas questões de escolha de geradores mínimos de um módulo.

<u>Demonstração</u> (do Teorema E-G): Trata-se de uma consequência quase direta dos três ingredientes acima.

Suponhamos, por "reductio ad absurdum", que Z é não livre e $r = posto(Z) \lneq k$. Podemos supor que Z é um contra-exemplo menor possível, isto é, r é mínimo e dim(R) é mínima para este valor do posto. Em particular, Z_P é R_P-livre para todo $P \neq \underline{m}$ (pois $posto(Z_P) = posto(Z)$ e $dim(R_P) \lneq dim(R)$ se $P \neq \underline{m}$).

Seja, agora, $x \in Z\setminus\underline{m}Z$. Mostraremos duas desigualdades:

$$alt(Z^*(x)) \leq r \qquad e \qquad alt(Z^*(x)) \geq k,$$

evidentemente contraditórias.

Primeiro, $alt(Z^*(x)) \leq r$. Isto resulta de uma análise cuidadosa da sequência exata

$$0 \to \underset{\substack{\wr\|\\ R}}{Rx} \to Z \to Z/Rx \to 0,$$

localizada num primo P. Se $P \not\supset Z^*(x)$, a sequência localizada é cindida e, portanto, $\text{prof}(Z/Rx)_P = \text{prof}(Z_P) = \text{prof}(R_P)$, pois $P \neq \underline{m}$. Neste caso, obviamente, $\text{prof}(Z/Rx)_P \geq \min\{r, \text{prof}(R_P)\}$. Se $P \supset Z^*(x)$ e se supuzermos que $\text{alt}(Z^*(x)) \gneq r$, então $\text{prof}(R_P) = \text{alt}(P) \gneq r$. Por outro lado, $\text{prof}(Z/Rx)_P \geq \text{prof}(Z_P)-1$ devido a que Rx é livre (Prop.II.6 (bis)). Assim, $\text{prof}(Z/Rx)_P \geq k-1 \geq r$ e, portanto, $\text{prof}(Z/Rx)_P \geq \min\{r, \text{prof}(R_P)\}$. Pelo critério de Auslander-Bridger (Prop.IV.10), Z/Rx é um syzygy de ordem r; como $\text{posto}(Z/Rx) = r-1$, obtemos um contra-exemplo "menor" do que Z, a contradição tendo resultado de supor $\text{alt}(Z^*(x)) \gneq r$.

A segunda desigualdade é, evidentemente, o próprio teorema de Gröbner generalizado (ingrediente 3º). É na demonstração deste que são usados os dois primeiros ingredientes. Procedemos da seguinte maneira.

Por absurdo, suponhamos $\text{alt}(Z^*(x)) \lneq k$. Como R é C-M e $k \leq \text{prof}(Z)$, a igualdade de Auslander-Buchsbaum fornece $\dim(R/Z^*(x)) \geq \text{d.h.}(Z) = \ell$.

Seja

$$0 \to F_\ell \to \dots \to F_1 \to F_o \to Z \to 0$$

uma resolução livre mínima de Z, e seja E um módulo de C-M grande para o anel $R/Z^*(x)$ (Teorema H). Consideremos o complexo

$$C_\bullet : \qquad 0 \to F_\ell \otimes E \to \dots \to F_o \otimes E \to 0.$$

Como Z é livre em $\text{Sup}(R) \setminus \{\underline{m}\}$, $H_i(C_\bullet) = \text{Tor}_i^R(Z,E)$ tem profundidade 0 (ou é (0)). Por outro lado,

$$\operatorname{prof}(F_i \otimes E) = \operatorname{prof}(\underbrace{E \otimes \ldots \otimes E}_{\text{posto}(F_i) \text{ vezes}}) = \operatorname{prof}(E) = \dim(R/Z^*(x))$$

(pois E é de C-M grande). Resulta $\operatorname{prof}(F_i \otimes E)$ constante ao longo de $C_{\bullet}$ e $> \ell = \mathrm{d.h.}_R(Z)$. Pelo lema de aciclicidade, $C_{\bullet}$ é acíclico e $\operatorname{prof}(Z \otimes E) > 0$, já que $Z \otimes E \neq (0)$ $((Z\otimes E)/\underline{m}(Z\otimes E) \simeq$ $\simeq (Z/\underline{m}Z) \otimes (E/\underline{m}E) \neq (0)$ pois $Z \neq \underline{m}Z$ e $E \neq \underline{m}E)$.

Por outro lado, se provarmos que $x \in Z \setminus \underline{m}Z$ gera um submódulo $\underline{m}$-primário de Z/IZ, com $I = Z^*(x)$, teremos que $Z \otimes E \simeq (Z/IZ) \otimes E$ já contém um submódulo $\underline{m}$-primário. Em outras palavras, $\operatorname{prof}(Z \otimes E) = 0$; contradição! Mas, como $(Z^*(x))_P \simeq$ $\simeq (Z_P)^*(x)$ e Z_P é R_P-livre para todo $P \neq \underline{m}$, vê-se que $\operatorname{Sup}((Rx+IZ)/IZ) = \{\underline{m}\}$, como queríamos. //

<u>Observação</u>. É evidente que o ponto crítico da demonstração acima reside no Teorema de Gröbner generalizado. É possível que existam generalizações do Teorema de Gröbner, sem usar módulos de C-M grandes. Outra alternativa de abordagem do problema do syzygy seria através da análise direta do homomorfismo $Z_k \to F_{k-1}$ numa resolução

$$\begin{tikzcd}[column sep=small] \cdots \arrow[r] & F_k \arrow[rr] \arrow[dr] & & F_{k-1} \arrow[r] & \cdots . \\ & & Z_k \arrow[ur] & & \end{tikzcd}$$

Usando o critério de Buchsbaum-Eisenbud para resoluções livres [B-E], localmente em $P \neq \underline{m}$, a hipótese $\operatorname{posto}(Z_k) \lneq k$ conduziria a informações precisas sobre o comportamento "genérico" de $Z_k \to F_{k-1}$. Em seguida, deveríamos saber controlar a "especialização".

REFERÊNCIAS

[Au] Auslander, M., Modules over unramified local rings, Ill. J. of Math. 5 (1961) 631-645.

[$(A-B)_1$] Auslander, M. e Buchsbaum, D., Homological dimension in local rings, Trans. Amer. Math. Soc. 85 (1957) 390-405.

[$(A-B)_2$] ——————————, Codimension and multiplicity, Ann. of Math. 68 (1958) 625-657.

[A-Br] Auslander, M. e Bridger, M., Stable module theory, Memoirs Amer. Math. Soc. 94 (1969)

[A-N] Artin, M. e Nagata, M., Residual intersections in Cohen-Macaulay rings, J. Math. Kyoto Univ. 12 (1972) 307-323.

[Bar] Barger, S.F., Generic perfection and the theory of grade, Thesis, Univ. of Minnesota, 1970.

[Br] Bruns, W., "Jede" endliche freie Auflösung ist freie Auflösung eines von drei Elementen erzengten Ideals, J. Algebra 39 (1976) 429-439.

[B-E] Buchsbaum, D. e Eisenbud, D., Some structure theorems for finite free resolutions, Adv. in Math. 12 (1974) 84-139.

[Br-E-G] Bruns, W., Evans, E.G. e Griffith, P.A., Syzygies, ideals of height two and vector bundles, J. Algebra 67 (1980) 143-162.

[Da] Davis, E., Ideals of the principal class, R-sequences and a certain monoidal transformation, Pacific J. Math. 20 (1967) 197-205.

[Du] Dubreil, P., Quelques propriétés des variétés algébriques, Act. Sci. Indust. 210. Paris: Hermann 1935.

[$(E-G)_1$] Evans, E.G. e Griffith, P.A., Syzygies, ideals of height two and vector bundles, preprint.

[$(E-G)_2$] ——————————, The syzygy problem, preprint.

[Ei] Eilenberg, S., Homological dimension and syzygies, Ann. of Math. 64 (1956) 328-336.

[$(E-N)_1$] Eagon, J.A. e Northcott, D.G., Ideals defined by matrices and a certain complex associated to them, Proc. Royal Soc. Ser. A 269 (1962) 188-204.

[$(E-N)_2$] ——————————, On the Buchsbaum-Eisenbud theory of finite free resolutions, J. Reine Angew. Math. 262/263 (1973) 205-219.

[Fe] Ferrand, D. Suite régulière et intersection complète, C.R. Acad. Sci. Paris 264 (1967) 427-428.

[Fox] Foxby, H., On the μ^i, in a minimal injective resolution II, Math. Scand. 41 (1977) 19-44.

[Gae] Gaeta, F., Quelques progrès récents dans la classification des variétés algébriques d'un espace projectif. Deuxième Colloque de Géométrie Algébrique, Liège. C.B.R.M. (1952) 145-181.

[Ge] Geyer, W.-D., On the number of equations which are necessary to describe an algebraic set in n-space, Atas III Escola de Álgebra, IMPA-SBM, Rio de Janeiro: 1974.

[G-L] Gulliksen, T. e Levin, G., Homology of local rings, Queen's Papers in Pure and Applied Mathematics, 20 (1969) Queen's University, Kingston.

[Hi] Hilbert, D., Über die Theorie der algebraischen Formen, Math. Ann. 36 (1890) 473-534.

[Ho_1] Hochster, M., Grade-sensitive modules and perfect modules, Proc. London Math. Soc. 29 (1974) 55-76.

[Ho_2] ——————, Topics in the homological theory of modules over commutative rings, RCSM Amer. Math. Soc. 24 (1974).

[H-E] Hochster, M. e Eagon, J.A., Cohen-Macaulay rings, invariant theory and the generic perfection of determinantal loci, Amer. J. Math. 93 (1971) 1020-1058.

[Ka_1] Kaplansky, I., Fields and rings, Chicago: Univ. of Chicago Press, 1969.

[Ka_2] ——————, Commutative rings, Allyn and Bacon, Boston 1970.

[La] Lascoux, A., Syzygies des variétés déterminantales, Adv. in Math. 30 (1978) 202-237.

[Li] Lichtenbaum, S., On the vanishing of Tor in regular local rings, Ill. J. Math. 10 (1966) 220-226.

[Mac] Macaulay, F.S., Algebraic theory of modular systems, Cambridge Tracts Nº 19, Cambridge 1916.

[McR] MacRae, R.E., On an application of Fitting invariants, J. Algebra 2 (1965) 153-169.

[Mu] Mumford, D., Algebraic Geometry I, Complex projective Varieties, Grund. Math. Wiss. Nº. 221, Springer-Verlag, Berlin: 1976.

[Ni] Nielsen, H.A., Tensor functors of complexes, Preprint Series 1977/78, Nº 15, Matematisk Inst. Aarhus Univ. 1978.

[Nö] Nöther, M., Zur Grundlegung der Theorie der algebraischen Raumcurven, Crelle Journale 93 (1882) 271-318.

[Oh] Ohm, J., Space curves as ideal-theoretic complete intersections, Louisiana State University, Baton Rouge 1978.

[$(P-S)_1$] Pesquine, C. e Szpiro, L., Dimension projective finie et cohomologie locale, IHES Publ. Math. 42 (1973) 323-395.

[$(P-S)_2$] ——————————, Liaison des variétés algébriques. I, Inv. Math. 26 (1974) 271-302.

[Re] Rees, D., The grade of an ideal or module, Proc. Camb. Phil. Soc. 53 (1957) 28-42.

[Se] Serre, J.P., Algèbre locale. Multiplicités, Lecture Notes in Mathematics, Nº 11, Springer-Verlag: 1975 (3ème édition).

[$(S-V)_1$] Simis, A. e Vasconcelos, W.V., The conormal module of an ideal, Amer. J. Math., no prelo.

[$(S-V)_2$] Simis, A. e Vasconcelos, W.V., Approximation complexes, a ser publicado nas Atas da VI Escola de Álgebra, Recife 1980.

[Ta] Tate, J., Homology of noetherian rings and local rings, Ill. J. Math. 1 (1957) 14-27.

[Va_1] Vasconcelos, W.V., Ideals generated by R-sequences, J. Algebra 6 (1967) 309-316.

[Va_2] ——————, The conormal bundle of an ideal, Atas da V Escola de Álgebra, IMPA-SBM, Rio de Janeiro: 1978.