Curvas Afins como Interseções Completas como Conjuntos

Pedro de Paula Lemos Teixeira

DISSERTAÇÃO APRESENTADA AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA UNIVERSIDADE DE SÃO PAULO
PARA A OBTENÇÃO DO GRAU DE
MESTRE EM MATEMÁTICA

Área de Concentração: Álgebra
Orientador: Prof. Dr. Daniel Levcovitz

Durante a elaboração deste trabalho o autor recebeu apoio financeiro da FAPESP.

—São Paulo, julho de 1996—

Curvas Afins

como

Interseções Completas como Conjuntos

Este exemplar corresponde à redação final da dissertação apresentada por Pedro de Paula Lemos Teixeira, devidamente corrigida e aprovada pela Comissão Julgadora.

São Paulo, julho de 1996.

Banca Examinadora:

- Prof. Dr. Daniel Levcovitz (Orientador) — IME-USP
- Prof. Dr. Paulo Agozzini Martin — IME-USP
- Prof. Dr. Arnaldo Garcia — IMPA

“Penso, logo penso que existo.”
— Níquel Náusea

Agradecimentos

Ao meu orientador, Daniel Levcovitz, pelo excelente trabalho de orientação e pelo apoio e incentivo constantes.

Ao colega Carlos Juiti Watanabe, pela constante ajuda com computadores, editores de texto, $\text{\LaTeX}$ e afins.

Ao colega Luís Renato Abib Finotti, que inúmeras vezes me salvou, com suas excelentes notas de aula.

Ao meu irmão, Henrique, pelo auxílio na revisão ortográfica.

À FAPESP, pelo apoio financeiro durante a elaboração desta dissertação.

Pedro de Paula Lemos Teixeira.

Resumo

Este texto tem como objetivo a exposição de demonstrações detalhadas dos seguintes teoremas:

Teorema 1 *Curvas afins que são localmente interseções completas são interseções completas como conjuntos* (N. Mohan Kumar, 1978, [MK78]).

Teorema 2 *Curvas afins irredutíveis definidas sobre corpos infinitos de característica $p > 0$ são interseções completas como conjuntos* (Cowsik-Nori, 1978, [CN78]).

Abstract

This text has the aim of presenting detailed proofs of the following theorems:

Theorem 1 *Affine curves that are locally complete intersections are set-theoretic complete intersections* (N. Mohan Kumar, 1978, [MK78]).

Theorem 2 *Irreducible affine curves defined over infinite fields of characteristic $p > 0$ are set-theoretic complete intersections* (Cowsik-Nori, 1978, [CN78]).

Conteúdo

1	Introdução	1
1.1	Interseções Completas - Definições e Exemplos	2
1.2	O Teorema de Mohan Kumar	5
1.3	O Teorema de Cowsik-Nori	6
2	Preliminares	7
2.1	Alguns Resultados Gerais	7
2.2	Resultados de Álgebra Homológica	12
2.3	Seqüências Regulares, Anéis de Cohen-Macaulay	15
2.4	O Complexo de Koszul	20
2.5	O “Splitting-off” de Serre. O Teorema de Quillen-Suslin	24
3	O Teorema de Szpiro	26
3.1	Preliminares	26
3.2	Os Métodos de Szpiro	30
3.3	O Teorema de Szpiro	33
4	O Teorema de Mohan Kumar	37
4.1	Preliminares	37
4.2	Demonstração	40
5	O Teorema de Cowsik-Nori	45
5.1	Preliminares	45
5.2	Demonstração	47
	Índice de Notações	54
	Bibliografia	57

Convenções e Definições

Todos os anéis serão supostos comutativos, com elemento unidade.

Diremos que um ideal I de um anel Noetheriano A tem **codimensão pura** r se todo divisor primo minimal de I tiver altura r ou, equivalentemente, se $h(I_{\mathfrak{p}}) = r$, $\forall \mathfrak{p} \in V(I) \subseteq \text{Spec}(A)$.

Nas condições acima diremos que I tem **dimensão pura** r se $\dim(A/\mathfrak{p}) = \dim(A/I) = r$, para todo ideal primo $\mathfrak{p}$ minimal sobre I . Se $A = k[X_1, \dots, X_n]$ ou, mais geralmente, se A for uma k -álgebra finitamente gerada de dimensão n que é um domínio de integridade, então

$$I \text{ tem codimensão pura } r \iff I \text{ tem dimensão pura } n - r.$$

Estaremos trabalhando com conjuntos algébricos afins definidos sobre um corpo k (*corpo de definição*) em espaços afins sobre uma extensão algebricamente fechada L (*corpo de coordenadas*). Chamaremos estes conjuntos de **k -variedades afins**, ou simplesmente **k -variedades**. Estendemos as definições acima para variedades, dizendo que uma k -variedade de $\mathbb{A}^n(L)$ tem dimensão (resp. codimensão) pura r se seu ideal de definição tiver dimensão (resp. codimensão) pura r em $k[X_1, \dots, X_n]$ ou, equivalentemente, se todas suas componentes irredutíveis relativas à k -topologia de Zariski em $\mathbb{A}^n(L)$ forem de dimensão (resp. codimensão) r .

Chamaremos de **k -curva** (resp. **k -hipersuperfície**) uma k -variedade de dimensão (resp. codimensão) pura 1. Frequentemente falaremos simplesmente em *curvas*, *variedades* ou *hipersuperfícies*, assumindo que o corpo de definição é o próprio corpo de coordenadas.

Estaremos sempre assumindo que L é um corpo algebricamente fechado.

Capítulo 1

Introdução

Dado um ideal I de um anel Noetheriano A , dizemos que I é gerado *a menos de radical* por r elementos se existem $f_1, \dots, f_r \in A$ tais que $\text{Rad}(I) = \text{Rad}(f_1, \dots, f_r)$. O que podemos afirmar sobre o número mínimo de elementos necessários para gerar I a menos de radical? Ou, num contexto um tanto mais forte, o que sabemos sobre o número mínimo de geradores de I , $\mu(I)$?

Apesar das formulações simples, tratam-se de questões altamente complexas e que muitas vezes trazem resultados realmente surpreendentes. Por exemplo, a intuição nos leva a crer que o conjunto $\{\mu(I) \mid I \leq A\}$ é limitado superiormente por uma função da dimensão do anel. Isto é *falso*, mesmo se nos restringirmos a ideais primos e anéis “bem comportados”, como $A := k[X_1, \dots, X_n]$. Um exemplo construído por Macaulay mostra a existência de curvas irredutíveis em $\mathbb{A}^3(L)$ — L algebricamente fechado, conforme estabelecido em ‘Convenções e Definições’ — cujos ideais de definição requerem números arbitrariamente grandes de geradores (exemplo 1.5). Estas curvas apresentam, no entanto, singularidades na origem e poderíamos especular que este comportamento “patológico” se deve a existência destas singularidades. Isto de fato faz uma grande diferença, pois no caso de ideais de definição de variedades irredutíveis *não singulares* em $\mathbb{A}^n(L)$ mostra-se que o número mínimo de geradores é $\leq n + 1$.

A simplicidade dos enunciados, as técnicas sofisticadas empregadas, resultados surpreendentes como os citados acima e a existência de diversos problemas ainda abertos de certo modo justificam o interesse nesta linha de investigação. Nesta dissertação nos concentraremos em resultados direcionados à solução de um destes problemas em aberto: *seriam todos os ideais*

de definição de k -curvas em $\mathbb{A}^n(L)$ gerados a menos de radical por $n - 1$ elementos? Ou, equivalentemente, poderiam as k -curvas em $\mathbb{A}^n(L)$ serem escritas como interseções de $n - 1$ k -hipersuperfícies? Veremos que a resposta é afirmativa quando k tem característica positiva.

1.1 Interseções Completas - Definições e Exemplos

Dado um ideal próprio I de um anel Noetheriano, o *Hauptidealsatz* de Krull garante que o número mínimo de geradores de I é maior ou igual a altura de I . É natural, então, perguntar quando a igualdade é estabelecida, e procurar condições que a garantam. Neste caso dizemos que I é uma **interseção completa**. Transportando esta idéia para a Geometria, dizemos que uma k -variedade afim V de $\mathbb{A}^n := \mathbb{A}^n(L)$ é uma interseção completa quando seu ideal de definição $I(V)$ é uma interseção completa em $k[X_1, \dots, X_n]$, isto é, $\mu(I(V)) = h(I(V)) = \text{codim}(V)$.

Observação Conforme mencionado em ‘Convenções e Definições’, estamos sempre assumindo que L é um corpo algebricamente fechado. Nos exemplos abaixo estaremos sempre trabalhando com L -variedades em $\mathbb{A}^n(L)$.

Exemplo 1.1 A curva C_1 em $\mathbb{A}^3$ dada parametricamente por $x = t$, $y = t^2$ e $z = t^3$ é uma interseção completa: $I(C_1) = (X^2 - Y, X^3 - Z)$, e portanto $\mu(I(C_1)) = 2 = \text{codim}(C_1)$.

Exemplo 1.2 Toda hipersuperfície $H \subseteq \mathbb{A}^n$ é uma interseção completa. De fato, todo ideal primo de altura 1 em um domínio fatorial é principal, gerado por um elemento irredutível, e $I(H)$ é uma interseção de um número finito de tais ideais, correspondentes às componentes irredutíveis de H . Logo $I(H)$ é principal e $\mu(I(H)) = 1 = \text{codim}(H)$.

Exemplo 1.3 Toda variedade linear $V \subseteq \mathbb{A}^n$ é uma interseção completa: após uma mudança afim de variáveis podemos supor que V é determinada pelo sistema $X_1 = \dots = X_r = 0$, para algum r , e assim $I(V) = (X_1, \dots, X_r)$, uma interseção completa.

Os exemplos seguintes mostram que nem toda variedade (ou mesmo curva) afim é uma interseção completa.

Exemplo 1.4 A curva C_2 em $\mathbb{A}^3$ dada parametricamente por $x = t^3$, $y = t^4$ e $z = t^5$ não é uma interseção completa: seu ideal de definição $I(C_2) = (Y^2 - XZ, X^3 - YZ, Z^2 - X^2Y)$ não pode ser gerado por dois elementos, nem mesmo localmente na origem, conforme [Gey76].

Exemplo 1.5 (Curvas de Macaulay) Um interessante exemplo dado por Macaulay em [Mac16] mostra a existência de curvas irredutíveis em $\mathbb{A}^3$ cujos ideais de definição exigem (mesmo localmente) números arbitrariamente grandes de geradores. Tratamentos modernos deste exemplo podem ser encontrados em [Gey76, §4] e [Abh73].

Seja I um ideal próprio de um anel Noetheriano A . Dizemos que I é **localmente uma interseção completa** se as localizações $I_{\mathfrak{m}}$ forem interseções completas, para todo ideal maximal $\mathfrak{m}$ com $I \subseteq \mathfrak{m}$, e estendemos da maneira óbvia este conceito para k -variedades de $\mathbb{A}^n$, via ideais de definição. Vemos imediatamente que se I é uma interseção completa então também é localmente uma interseção completa, pois

$$\mu(I_{\mathfrak{m}}) \leq \mu(I) = h(I) \leq h(I_{\mathfrak{m}}), \quad \forall \mathfrak{m} \in V(I) \cap \text{Max}(A).$$

É claro também — pelo mesmo argumento acima — que se I é localmente uma interseção completa então $I_{\mathfrak{p}}$ é interseção completa, para todo $\mathfrak{p} \in V(I)$, uma vez que $I_{\mathfrak{p}}$ é uma localização de $I_{\mathfrak{m}}$, onde $\mathfrak{p} \subseteq \mathfrak{m} \in \text{Max}(A)$.

Exemplo 1.6 Toda variedade não singular em $\mathbb{A}^n$ é localmente uma interseção completa, conforme [Kun85, Cap. VI, Corolário 1.11].

Nas mesmas condições acima, dizemos que I é uma **interseção completa como conjunto** se I for gerado *a menos de radical* por $h(I)$ elementos, ou seja, se existir um ideal J de A com $\text{Rad}(J) = \text{Rad}(I)$ que seja uma interseção completa. Estendendo este conceito para k -variedades de $\mathbb{A}^n$ via ideais de definição vemos que dizer que uma k -variedade V é uma interseção completa como conjunto equivale a dizer que ela pode ser escrita como interseção de $r := \text{codim}(V)$ k -hipersuperfícies.

Exemplo 1.7 A curva C_2 do exemplo 1.4 é uma interseção completa como conjunto, pois se escreve como interseção das hipersuperfícies definidas por $Z^2 - X^2Y$ e $X^4 + Y^3 - 2XYZ$.

Exemplo 1.8 Mais geralmente, as curvas em $\mathbb{A}^3$ dadas parametricamente por $x = t^\alpha$, $y = t^\beta$ e $z = t^\gamma$, com $\text{mdc}(\alpha, \beta, \gamma) = 1$, são determinadas por dois polinômios e portanto são interseções completas como conjuntos. Bresinsky apresenta em [Bre79] uma demonstração elementar e construtiva deste fato, no sentido em que fornece um algoritmo para encontrar as duas superfícies que determinam a curva.

A seguinte analogia mostra um outro contexto onde a codimensão também aparece como o número “certo” de equações definindo uma variedade:

Exemplo 1.9 Seja X uma variedade diferenciável de classe C^k em $\mathbb{R}^n$, de codimensão r . Então X é localmente a imagem inversa de um valor regular de uma função de classe C^k a valores em $\mathbb{R}^r$, ou seja, X se escreve localmente como interseção de r hipersuperfícies. Usando uma terminologia análoga à introduzida acima, diríamos que X é “localmente uma interseção completa como conjunto”.

Mais uma vez, nem toda variedade afim é uma interseção completa como conjunto:

Exemplo 1.10 A superfície em $\mathbb{A}^4(\mathbb{C})$ dada parametricamente por $x_1 = t$, $x_2 = tu$, $x_3 = u(u-1)$ e $x_4 = u^2(u-1)$ não é uma interseção completa como conjunto, conforme [Har62].

No entanto não são conhecidos exemplos de *curvas* afins que não são interseções completas como conjuntos, o que sugere a seguinte conjectura:

Conjectura 1.11 *Toda curva afim é uma interseção completa como conjunto.*

Diversos resultados vêm sendo obtidos nesta direção, especialmente após a demonstração da Conjectura de Serre por Quillen e Suslin. Entre estes, podemos citar dois teoremas centrais neste sentido:

Teorema 1.12 *Toda curva afim que é localmente uma interseção completa é uma interseção completa como conjunto (Mohan Kumar [MK78]).*

Teorema 1.13 *Toda curva afim em característica $p > 0$ é uma interseção completa como conjunto (Cowsik-Nori [CN78]).*

Este texto tem como objetivo apresentar, de modo claro e sistemático, as demonstrações dos teoremas de Mohan Kumar e de Cowsik-Nori — este último apenas no caso particular de curvas *irredutíveis* definidas sobre corpos *infinitos*.

Procuraremos sempre enunciar os resultados utilizados e demonstrar aqueles que não representem um grande desvio de nossos objetivos, de modo a tornar o texto acessível a um leitor com conhecimentos básicos de Álgebra Comutativa e Geometria Algébrica e com alguma familiaridade com as técnicas de Álgebra Homológica.

Nas próximas sessões faremos um rápido esboço das demonstrações que serão apresentadas.

1.2 O Teorema de Mohan Kumar

A demonstração do teorema de Mohan Kumar (1.12) será feita essencialmente em duas etapas. Na primeira delas, descrita no Capítulo 3, mostraremos que se um ideal I de um anel de Cohen-Macaulay A de dimensão $n \geq 3$ é localmente uma interseção completa, com codimensão pura $n - 1$, então existe um ideal J de A , também interseção completa local, com $\text{Rad}(J) = \text{Rad}(I)$ e $\omega_J := \text{Ext}_A^{n-1}(A/J, A)$ livre, de posto 1, como A/J -módulo. Como consequência veremos que o módulo conormal J/J^2 será livre, de posto $n - 1$, sobre A/J . Os métodos usados nesta etapa são devidos a Szpiro ([Szp79]). Provaremos, então, o teorema no caso particular de curvas em $\mathbb{A}^3$: se $I < A := k[X, Y, Z]$ tem dimensão pura 1 e é localmente interseção completa, construindo um ideal J como acima teremos $\text{Ext}_A^1(J, A) \cong \omega_J$ cíclico e, por um resultado de Serre e pelo teorema de Quillen-Suslin, J será gerado por dois elementos.

Na etapa seguinte, descrita no Capítulo 4, demonstraremos o teorema no caso geral, conforme [MK78]. Mostraremos que se I é um ideal de $k[X_1, \dots, X_n]$ com $\mu(I/I^2) \geq \dim k[X_1, \dots, X_n]/I + 2$, então $\mu(I) = \mu(I/I^2)$. Seja então $I < k[X_1, \dots, X_n]$ um ideal de dimensão pura 1 que é localmente uma interseção completa. Suponhamos $n \geq 4$. Pelos métodos descritos no Capítulo 3, existe um ideal $J < k[X_1, \dots, X_n]$ com $\text{Rad}(J) = \text{Rad}(I)$ tal que J/J^2 é livre, de posto $n - 1$, como $k[X_1, \dots, X_n]/J$ -módulo. Temos assim $\mu(J/J^2) = n - 1 \geq 3 = \dim k[X_1, \dots, X_n]/J + 2$ e portanto

$$\mu(J) = \mu(J/J^2) = n - 1 = h(J).$$

1.3 O Teorema de Cowsik-Nori

Provaremos o teorema de Cowsik-Nori (1.13) — no caso particular de curvas *irredutíveis* definidas sobre corpos *infinitos* — seguindo a demonstração apresentada por Lyubeznik em [Lyu89]. Sejam k um corpo infinito de característica $p > 0$ e $\mathfrak{P} < R := k[X_1, \dots, X_n]$ ($n \geq 3$) um ideal primo de dimensão 1. Mostraremos inicialmente que, após algumas reduções, podemos assumir k perfeito, $B := R/\mathfrak{P} = k[x_1, \dots, x_n]$ inteiro sobre $A := k[x_1, x_2]$ e os corpos de frações $k(x_1, \dots, x_n)$ e $k(x_1, x_2)$ *iguais*. Nestas condições, o condutor C de B em A é não nulo; logo B/C é Artiniano e, sendo uma k -álgebra finitamente gerada, é um k -espaço vetorial de dimensão finita. Como consequência desta k -dimensão finita, representando por $\bar{x}_i$ a imagem da indeterminada X_i em B/C obteremos, para $i = 3, \dots, n$, equações

$$\bar{x}_i^{p^r} + a_{i,1} \bar{x}_i^{p^{r+1}} + a_{i,2} \bar{x}_i^{p^{r+2}} + \dots + a_{i,t_i} \bar{x}_i^{p^{r+t_i}} = 0,$$

onde $a_{i,j} \in k$, e levantando estas equações para $R = k[X_1, \dots, X_n]$ teremos

$$X_i^{p^r} + a_{i,1} X_i^{p^{r+1}} + a_{i,2} X_i^{p^{r+2}} + \dots + a_{i,t_i} X_i^{p^{r+t_i}} + c_i = f_i \in \mathfrak{P},$$

onde $c_i \in k[X_1, X_2]$.

Introduzimos, então, novas variáveis $Y_i := X_i^{p^r}$ ($i = 3, \dots, n$) e definimos $R' := k[X_1, X_2, Y_3, \dots, Y_n]$. Como a extensão $R|R'$ é inteira, $\mathfrak{P}' := \mathfrak{P} \cap R'$ também tem dimensão 1. Como

$$\frac{\partial f_i}{\partial Y_j} = \delta_{ij}, \quad \forall i, j \geq 3,$$

pelo Critério do Jacobiano verificamos que $R'' := R'/(f_3, \dots, f_n)$ é um anel regular e $(f_3, \dots, f_n)$ tem dimensão pura 2. $\mathfrak{P}'' := \mathfrak{P}'/(f_3, \dots, f_n)$ é, então, um ideal primo de codimensão 1 em R'' e portanto é gerado localmente por 1 elemento, uma vez que, sendo R'' regular, suas localizações são domínios fatoriais. Assim $\mathfrak{P}'$ é localmente gerado por $n - 1$ elementos e, pelo Teorema de Mohan Kumar, é gerado a menos de radical por $n - 1$ elementos. Se $\mathfrak{P}' = \text{Rad}((g_1, \dots, g_{n-1})R')$, concluiremos a demonstração mostrando que $\mathfrak{P} = \text{Rad}((g_1, \dots, g_{n-1})R)$.

Capítulo 2

Preliminares

Apresentaremos aqui alguns resultados que serão utilizados ao longo dos demais capítulos. Procuraremos incluir (breves) provas dos resultados mais simples e citar referências para os demais, de modo que o leitor possa encontrar facilmente tais demonstrações na literatura.

2.1 Alguns Resultados Gerais

Começaremos esta sessão descrevendo um processo de passagem de informação local para global que usaremos no próximo capítulo. Dada uma cobertura finita $(D(f))_{f \in \Gamma}$ de $\text{Spec}(A)$, A -módulos M e N e uma família de morfismos $N_f \rightarrow M_f$ ($f \in \Gamma$) compatíveis — num sentido que logo tornaremos preciso —, queremos definir uma aplicação “global” $N \rightarrow M$ que “estenda” as aplicações dadas, isto é, quando localizada em cada $f \in \Gamma$ seja igual ao homomorfismo $N_f \rightarrow M_f$ dado.

Dados $f, g \in A$, existe um homomorfismo canônico

$$\begin{aligned} M_f &\longrightarrow M_{fg} \\ \frac{m}{f^k} &\longmapsto \frac{m}{f^k}|_{D(fg)} := \frac{g^k m}{(fg)^k} \end{aligned}$$

que chamaremos de **aplicação de restrição** a $D(fg)$. Suponhamos então, nas condições do parágrafo anterior, dados elementos $\alpha_f \in M_f$ ($f \in \Gamma$) tais que, para todo f e $g \in \Gamma$, α_f e α_g são iguais quando restritos a $D(fg) = D(f) \cap D(g)$, isto é, $\alpha_f|_{D(fg)} = \alpha_g|_{D(fg)}$, $\forall f, g \in \Gamma$. Então existe um único $\alpha \in M = M_1$ tal que $\alpha|_{D(f)} = \alpha_f$, para todo $f \in \Gamma$:

Unicidade. Sejam $\alpha, \beta \in M$ tais que $\alpha|_{D(f)} = \alpha_f = \beta|_{D(f)}, \forall f \in \Gamma$. Temos $\langle \alpha - \beta \rangle_f = 0, \forall f \in \Gamma$, e assim $\langle \alpha - \beta \rangle_{\mathfrak{p}} = 0, \forall \mathfrak{p} \in \text{Spec}(A)$, uma vez que $\text{Spec}(A) = \bigcup_{f \in \Gamma} D(f)$. Logo $\alpha = \beta$.

Existência. Para todo $f \in \Gamma$ podemos escrever $\alpha_f = m_f/f^k$, onde $m_f \in M$ e k independe de f , e por hipótese temos

$$\frac{g^k m_f}{(fg)^k} = \frac{f^k m_g}{(fg)^k}, \quad \forall f, g \in \Gamma.$$

Logo existe r (independente de f e g) tal que

$$(fg)^r (g^k m_f - f^k m_g) = 0, \quad \forall f, g \in \Gamma.$$

Como $\text{Spec}(A) = \bigcup_{f \in \Gamma} D(f) = \bigcup_{f \in \Gamma} D(f^{k+r})$, temos $(f^{k+r} \mid f \in \Gamma) = (1)$ e podemos, então, tomar elementos $h_f \in A$ com $\sum_{f \in \Gamma} h_f f^{k+r} = 1$. Tomamos então $\alpha := \sum_{f \in \Gamma} h_f f^r m_f$ e temos, para todo $g \in \Gamma$,

$$g^{k+r} \alpha = \sum_{f \in \Gamma} h_f f^r g^{k+r} m_f = \sum_{f \in \Gamma} h_f f^{k+r} g^r m_g = g^r m_g.$$

Logo $\alpha|_{D(g)} = m_g/g^k = \alpha_g, \forall g \in \Gamma$.

Fica imediata, portanto, a demonstração da seguinte proposição:

Proposição 2.1 *Sejam A um anel, M e N A -módulos e $\Gamma \subseteq A$ finito, tal que $\text{Spec}(A) = \bigcup_{f \in \Gamma} D(f)$. Então, dada uma família de morfismos*

$$N_f \xrightarrow{\alpha(f)} M_f \quad (f \in \Gamma)$$

tal que

$$\alpha_{(f)}(x/1)|_{D(fg)} = \alpha_{(g)}(x/1)|_{D(fg)}$$

para todo x em N e todo f e g em Γ , existe um único A -homomorfismo $N \xrightarrow{\alpha} M$ tal que $\alpha_f = \alpha_{(f)}$, para todo f .

Demonstração: Vimos acima que, para todo $x \in N$, existe um único elemento $\alpha(x) \in M$ tal que $\alpha(x)|_{D(f)} = \alpha_{(f)}(x/1), \forall f \in \Gamma$. É claro que a função $N \xrightarrow{\alpha} M$ assim definida é A -linear e que $\alpha_f = \alpha_{(f)}$, para todo f . $\square$

Observação 1 Se cada $\alpha_{(f)}$ for um isomorfismo, a aplicação α também o será. A verificação é local, usando a hipótese $\text{Spec}(A) = \bigcup_{f \in \Gamma} D(f)$.

Observação 2 Por fim, representando por $[\cdot]_{\mathfrak{p}}$ as imagens de elementos de M_f , M_g e M_{fg} em $M_{\mathfrak{p}}$ ($\mathfrak{p} \in D(fg)$) temos $[\alpha_f|_{D(fg)}]_{\mathfrak{p}} = [\alpha_f]_{\mathfrak{p}}$, e portanto

$$\begin{aligned} \alpha_f|_{D(fg)} = \alpha_g|_{D(fg)} &\iff [\alpha_f|_{D(fg)}]_{\mathfrak{p}} = [\alpha_g|_{D(fg)}]_{\mathfrak{p}}, \forall \mathfrak{p} \in D(fg) \\ &\iff [\alpha_f]_{\mathfrak{p}} = [\alpha_g]_{\mathfrak{p}}, \forall \mathfrak{p} \in D(fg). \end{aligned}$$

À luz desta equivalência, podemos reescrever a proposição 2.1 de um modo mais simples:

Proposição 2.2 *Sejam A um anel, M e N A -módulos e $\Gamma \subseteq A$ finito, tal que $\text{Spec}(A) = \bigcup_{f \in \Gamma} D(f)$. Então, dada uma família de morfismos*

$$N_f \xrightarrow{\alpha_f} M_f \quad (f \in \Gamma)$$

tal que

$$(\alpha_f)_{\mathfrak{p}} = (\alpha_g)_{\mathfrak{p}}, \quad \forall \mathfrak{p} \in D(fg)$$

para todo f e g em Γ , existe um único A -homomorfismo $N \xrightarrow{\alpha} M$ tal que $\alpha_f = \alpha|_{N_f}$, para todo f . $\square$

Lema 2.3 (“Lema da Cobra”) *Seja dado o seguinte diagrama comutativo de A -módulos, com linhas e colunas exatas:*

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & K' & & K & & K'' \\ & & \downarrow & & \downarrow & & \downarrow \varphi \\ 0 & \longrightarrow & M' & \xrightarrow{\alpha_1} & M & \xrightarrow{\alpha_2} & M'' \longrightarrow 0 \\ & & \downarrow \gamma' & & \downarrow \gamma & & \downarrow \gamma'' \\ 0 & \longrightarrow & N' & \xrightarrow{\beta_1} & N & \xrightarrow{\beta_2} & N'' \longrightarrow 0 \\ & & \downarrow \psi & & \downarrow & & \downarrow \\ & & C' & & C & & C'' \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array}$$

Então existe uma seqüência exata

$$0 \longrightarrow K' \xrightarrow{\overline{\alpha}_1} K \xrightarrow{\overline{\alpha}_2} K'' \xrightarrow{\delta} C' \xrightarrow{\overline{\beta}_1} C \xrightarrow{\overline{\beta}_2} C'' \longrightarrow 0$$

onde as aplicações $\overline{\alpha}_1$, $\overline{\alpha}_2$, $\overline{\beta}_1$ e $\overline{\beta}_2$ são as induzidas por α_1 , α_2 , β_1 e β_2 , respectivamente.

Demonstração:

Construção do homomorfismo de conexão δ :

Seja $x \in K''$. Então existe $y \in M$ tal que $\alpha_2(y) = \varphi(x)$, e $\gamma(y) \in \text{Ker } \beta_2 = \text{Im } \beta_1$, pela comutatividade do diagrama dado. Logo existe $z \in N'$ tal que $\beta_1(z) = \gamma(y)$. Definimos então $\delta(x) := \psi(z)$.

A verificação de que δ está bem definida, é A -linear, e que a seqüência resultante é exata é simples e pode ser encontrada em [Kun85, Cap. VII, Lema 1.9]. $\square$

Proposição 2.4 *Sejam A um anel Noetheriano, M e N A -módulos, M finitamente gerado. Então para todo sistema multiplicativo $S \subseteq A$ existe um isomorfismo natural de A_S -módulos*

$$\Phi : \text{Hom}_A(M, N)_S \xrightarrow{\sim} \text{Hom}_{A_S}(M_S, N_S)$$

$$\frac{f}{s} \longmapsto \frac{1}{s} f_S$$

Demonstração: Seja $\{m_1, \dots, m_r\}$ um sistema de geradores de M e consideremos a seqüência exata

$$0 \longrightarrow K \longrightarrow A^r \xrightarrow{\alpha} M \longrightarrow 0,$$

onde $\alpha(e_j) := m_j$ e $K := \text{Ker } \alpha$.

(i) Φ é injetora:

Seja $f/s \in \text{Ker } \Phi$. Então $f(m_j)/s = 0$ ($j = 1, \dots, r$) e portanto existe $s' \in S$ tal que $s'f(m_j) = 0$ para todo j . Logo $s'f = 0$, e assim $f/s = 0$.

(ii) Φ é sobrejetora:

Seja $g \in \text{Hom}_{A_S}(M_S, N_S)$. Tomemos $s \in S$ tal que, para todo j , os elementos $s \cdot g(m_j/1)$ sejam imagens de elementos de N , digamos $s \cdot g(m_j/1) = n_j/1$. Definindo $A^r \xrightarrow{\beta} N$ por $\beta(e_j) := n_j$ temos um diagrama comutativo

$$\begin{array}{ccc} A^r & \xrightarrow{\beta} & N \\ \downarrow \phi_M \circ \alpha & & \downarrow \phi_N \\ M_S & \xrightarrow{sg} & N_S \end{array}$$

onde $M \xrightarrow{\phi_M} M_S$ e $N \xrightarrow{\phi_N} N_S$ são as aplicações canônicas.

Do diagrama acima segue que $\phi_N(\beta(K)) = 0$ e, como $\beta(K)$ é finitamente gerado, existe $s' \in S$ tal que $s'\beta(K) = 0$. Então existe uma (única) aplicação A -linear $f : M \rightarrow N$ que torna o diagrama abaixo comutativo.

$$\begin{array}{ccc} & A^r & \\ \alpha \swarrow & & \searrow s'\beta \\ M & \xrightarrow{f} & N \end{array}$$

Temos então

$$f_S\left(\frac{m_j}{1}\right) = \frac{f(m_j)}{1} = \frac{s'\beta(e_j)}{1} = \frac{s'n_j}{1} = s's \cdot g\left(\frac{m_j}{1}\right)$$

e portanto, como os elementos $m_j/1$ geram M_S ,

$$g = \frac{1}{s's} f_S = \Phi\left(\frac{f}{s's}\right).$$

□

Corolário 2.5 *Sob as mesmas hipóteses da proposição anterior temos*

$$\text{Ext}_A^k(M, N)_S \cong \text{Ext}_{A_S}^k(M_S, N_S), \quad \forall k \geq 0.$$

Demonstração: Como M é finitamente gerado e A é Noetheriano, podemos tomar uma resolução projetiva $\mathcal{P}_M$ de M com módulos finitamente gerados, apenas. Pela proposição 2.4, existe um isomorfismo *de complexos*

$$\text{Hom}_A(\mathcal{P}_M, N)_S \cong \text{Hom}_{A_S}((\mathcal{P}_M)_S, N_S)$$

e portanto

$$\begin{aligned}
 \text{Ext}_A^k(M, N)_S &= \left(H^k(\text{Hom}_A(\mathcal{P}_M, N)) \right)_S \\
 &\cong H^k(\text{Hom}_A(\mathcal{P}_M, N)_S) \\
 &\cong H^k(\text{Hom}_{A_S}((\mathcal{P}_M)_S, N_S)) \\
 &= \text{Ext}_{A_S}^k(M_S, N_S).
 \end{aligned}$$

□

Corolário 2.6 *Sejam A um anel Noetheriano e P um A -módulo projetivo, finitamente gerado. Então o dual P^* é projetivo, finitamente gerado, e a aplicação canônica $P \rightarrow P^{**}$ é um isomorfismo.*

Demonstração: Se P é um somando direto de um A -módulo livre F , de posto r , então P^* será um somando direto de $F^* \cong A^r$ e portanto projetivo, finitamente gerado. Como P é localmente livre, verificamos facilmente, com a ajuda de (2.4), que a aplicação canônica $P \rightarrow P^{**}$ é localmente um isomorfismo. □

2.2 Resultados de Álgebra Homológica

Estamos admitindo que o leitor está familiarizado com algumas técnicas de Álgebra Homológica como, por exemplo, a definição e propriedades do funtor Ext . Mesmo assim, listaremos a seguir algumas proposições simples que serão utilizadas posteriormente, pois não gostaríamos de interromper o curso de demonstrações de teoremas mais profundos, nos próximos capítulos, com verificações deste tipo.

Proposição 2.7 *Dada uma sequência exata de A -módulos*

$$0 \rightarrow K \rightarrow P_1 \rightarrow \cdots \rightarrow P_t \rightarrow M \rightarrow 0 \quad (*)$$

com módulos P_j projetivos, existem, para todo A -módulo N , isomorfismos

$$\text{Ext}_A^i(K, N) \cong \text{Ext}_A^{i+t}(M, N), \quad \forall i \geq 1.$$

Demonstração: Para todo A -módulo N , a aplicação do funtor $\text{Hom}_A(\cdot, N)$ a uma seqüência exata de A -módulos

$$0 \longrightarrow M_1 \longrightarrow P \longrightarrow M_2 \longrightarrow 0$$

com P projetivo leva a isomorfismos $\text{Ext}_A^i(M_1, N) \cong \text{Ext}_A^{i+1}(M_2, N)$, para todo $i \geq 1$, uma vez que $\text{Ext}_A^i(P, N) = 0$, $\forall i \geq 1$. No nosso caso, quebramos a seqüência $(*)$ em seqüências curtas e aplicamos este resultado a cada uma destas. $\square$

Proposição 2.8 *Sejam A um anel e M um A -módulo. São equivalentes:*

1. $\dim \text{proj}_A(M) \leq t$;
2. $\text{Ext}_A^k(M, N) = 0$, $\forall k > t$, para todo A -módulo N ;
3. $\text{Ext}_A^{t+1}(M, N) = 0$, para todo A -módulo N .

Demonstração:

$(1) \Rightarrow (2)$ É consequência imediata da definição do funtor Ext via resolução projetiva da primeira variável.

$(3) \Rightarrow (1)$ Tomamos uma seqüência exata

$$0 \rightarrow K \rightarrow P_{t-1} \rightarrow \cdots \rightarrow P_0 \rightarrow M \rightarrow 0$$

onde os P_j são A -módulos projetivos. Pela proposição 2.7, temos

$$\text{Ext}_A^1(K, N) \cong \text{Ext}_A^{t+1}(M, N) = 0$$

para todo A -módulo N , ou seja, K é projetivo. $\square$

Observação Fica claro, da demonstração acima, que se A é Noetheriano e M um A -módulo finitamente gerado, de dimensão projetiva finita, então sempre existe uma resolução projetiva de comprimento mínimo envolvendo apenas módulos finitamente gerados.

Proposição 2.9 *Se A é um anel Noetheriano e M um A -módulo finitamente gerado, então:*

$$\dim \text{proj}_A(M) = t := \sup\{\dim \text{proj}_{A_{\mathfrak{m}}}(M_{\mathfrak{m}}) \mid \mathfrak{m} \in \text{Max}(A)\}.$$

Demonstração: É claro que $\dim \operatorname{proj}_{A_{\mathfrak{m}}}(M_{\mathfrak{m}}) \leq \dim \operatorname{proj}_A(M)$, para todo $\mathfrak{m} \in \operatorname{Max}(A)$, e portanto $t \leq \dim \operatorname{proj}_A(M)$. Se $t = \infty$, acabou. Senão, vemos que $\operatorname{Ext}_A^{t+1}(M, N) = 0$, para todo A -módulo N , pois este módulo se anula localmente em todo $\mathfrak{m} \in \operatorname{Max}(A)$, por (2.5) e (2.8). O resultado segue, então, da proposição 2.8. $\square$

Proposição 2.10

1. Se dois dos módulos envolvidos na sequência exata de A -módulos

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \quad (*)$$

tiverem dimensões projetivas finitas, o terceiro também terá.

2. Neste caso, teremos

$$\dim \operatorname{proj}_A(M_2) \leq t := \max\{\dim \operatorname{proj}_A(M_1), \dim \operatorname{proj}_A(M_3)\}.$$

3. Se $\dim \operatorname{proj}_A(M_2) < t$, então $\dim \operatorname{proj}_A(M_3) = \dim \operatorname{proj}_A(M_1) + 1$.

Demonstração: Para todo A -módulo N a aplicação do funtor $\operatorname{Hom}_A(\cdot, N)$ à sequência $(*)$ leva a uma sequência exata longa

$$\begin{aligned} \cdots \longrightarrow \operatorname{Ext}_A^r(M_3, N) \longrightarrow \operatorname{Ext}_A^r(M_2, N) \longrightarrow \operatorname{Ext}_A^r(M_1, N) \longrightarrow \\ \longrightarrow \operatorname{Ext}_A^{r+1}(M_3, N) \longrightarrow \operatorname{Ext}_A^{r+1}(M_2, N) \longrightarrow \operatorname{Ext}_A^{r+1}(M_1, N) \longrightarrow \cdots \quad (**) \end{aligned}$$

de onde tiraremos facilmente as informações procuradas, com o auxílio da proposição 2.8.

1. Se as dimensões projetivas de M_i e M_j são finitas e $\{i, j, k\} = \{1, 2, 3\}$, observamos que os módulos $\operatorname{Ext}_A^r(M_k, N)$ aparecem entre zeros na sequência $(**)$, para $r > \max\{\dim \operatorname{proj}_A(M_i), \dim \operatorname{proj}_A(M_j)\} + 1$. Temos, portanto, $\dim \operatorname{proj}_A(M_k) < \infty$.

2. Basta notar que $\operatorname{Ext}_A^{t+1}(M_2, N)$ aparece entre zeros na sequência $(**)$.

3. Teremos, da sequência $(**)$, isomorfismos $\operatorname{Ext}_A^r(M_1, N) \cong \operatorname{Ext}_A^{r+1}(M_3, N)$, para todo $r > \dim \operatorname{proj}_A(M_2)$. O resultado segue da proposição 2.8. $\square$

2.3 Seqüências Regulares, Anéis de Cohen-Macaulay

Definição 2.11 *Dados um anel A , um A -módulo M e uma seqüência de elementos $x_1, \dots, x_r$ de A , dizemos que esta é uma **seqüência M -regular** se $M \neq (x_1, \dots, x_r)M$ e x_{i+1} não é divisor de zero em $M/(x_1, \dots, x_i)M$, para $i = 0, \dots, r-1$. Se $M = A$ dizemos simplesmente que esta é uma **seqüência regular**.*

Proposição 2.12 *Seja A um anel e I um ideal de A gerado por uma seqüência regular $x_1, \dots, x_r$. Então o módulo conormal I/I^2 é livre, de posto r , como A/I -módulo.*

Demonstração: Demonstraremos, por indução sobre r , que $\overline{x_1}, \dots, \overline{x_r}$, imagens de $x_1, \dots, x_r$ em I/I^2 , formam uma base deste A/I -módulo. Se $r = 1$, seja $\overline{a} \in A/I$ tal que $\overline{a} \overline{x_1} = 0$ em I/I^2 . Então existe $b \in A$ com $ax_1 = bx_1^2$ e, como x_1 não é divisor de zero, temos $a = bx_1 \in I$, isto é, $\overline{a} = 0$.

Suponhamos agora $r > 1$ e a proposição válida para seqüências regulares de comprimento $r-1$. Sejam $\overline{a_1}, \dots, \overline{a_r} \in A/I$ tais que

$$\sum_{i=1}^r \overline{a_i} \overline{x_i} = 0.$$

Então existem $y_1, \dots, y_r \in I$ tais que

$$\sum_{i=1}^r a_i x_i = \sum_{i=1}^r y_i x_i,$$

e fazendo $b_i := a_i - y_i$ temos $\sum b_i x_i = 0$. Assim $b_r x_r \in I' := (x_1, \dots, x_{r-1})$ e, como x_r não é divisor de zero em A/I' , existem $c_1, \dots, c_{r-1} \in A$ com

$$b_r = \sum_{i=1}^{r-1} c_i x_i.$$

Temos assim

$$\sum_{i=1}^{r-1} (b_i + c_i x_r) x_i = 0$$

e, pela hipótese de indução aplicada à seqüência $x_1, \dots, x_{r-1}$, temos $b_i + c_i x_r \in I'$. Logo $b_i \in I$ e $\overline{a_i} = \overline{b_i} = 0$, $\forall i$, o que conclui a proposição. $\square$

Proposição 2.13 *Seja A um anel Noetheriano e I um ideal próprio de A . Se I for gerado por uma seqüência regular de comprimento r , então*

$$\dim \operatorname{proj}_A(A/I) = r.$$

Demonstração: Demonstraremos, por indução sobre r , apenas uma desigualdade — $\dim \operatorname{proj}_A(A/I) \leq r$ —, que será suficiente para quase todas as nossas aplicações (embora sempre escreveremos a igualdade).

Se $r = 0$, não há o que provar. Suponhamos $r > 0$ e a proposição válida para seqüências de comprimento $r - 1$. Se I é gerado pela seqüência regular $x_1, \dots, x_r$, então $\dim \operatorname{proj}_A(A/(x_1, \dots, x_{r-1})) \leq r - 1$, pela hipótese de indução, e aplicando a proposição 2.10 à seqüência exata

$$0 \longrightarrow A/(x_1, \dots, x_{r-1}) \xrightarrow{x_r} A/(x_1, \dots, x_{r-1}) \longrightarrow A/I \longrightarrow 0$$

concluimos que $\dim \operatorname{proj}_A(A/I) \leq r$.

Para a demonstração completa, ver [Kun85, Cap. VII, Teorema 2.1]. $\square$

Sejam A um anel Noetheriano, I um ideal de A e M um A -módulo finitamente gerado com $M \neq IM$. Como M é Noetheriano, é fácil ver que toda seqüência M -regular em I pode ser estendida a uma *maximal*. O que é notável é que todas estas seqüências maximais têm o mesmo comprimento, que chamaremos de *I -profundidade de M* (notação: $d(I, M)$), como veremos na nossa próxima proposição.

Proposição 2.14 *Sejam A um anel Noetheriano, I um ideal de A e M um A -módulo finitamente gerado com $M \neq IM$. Então a I -profundidade de M está bem definida e vale:*

$$d(I, M) = \min\{i \mid \operatorname{Ext}_A^i(A/I, M) \neq 0\}.$$

Demonstração: Seja $\underline{x} := x_1, \dots, x_r$ uma seqüência M -regular em I . Observamos inicialmente que

$$\operatorname{Hom}_A(A/I, M/\underline{x}M) \neq 0 \iff \underline{x} \text{ é maximal em } I.$$

De fato:

- Se $\underline{x}$ não é maximal em I , então existe $x_{r+1} \in I$ que não é divisor de zero em $M/\underline{x}M$. Assim, se $f \in \operatorname{Hom}_A(A/I, M/\underline{x}M)$ então $x_{r+1}f = 0$, pois $x_{r+1} \in I$, e portanto $f = 0$, uma vez que $x_{r+1} \notin Z(M/\underline{x}M)$.

- Se $\underline{x}$ é maximal em I , temos

$$I \subseteq Z(M/\underline{x}M) = \bigcup \text{Ass}(M/\underline{x}M)$$

e, como a união acima é uma união finita de ideais primos, temos

$$I \subseteq \mathfrak{p} \in \text{Ass}(M/\underline{x}M).$$

Assim, existe uma imersão de $A/\mathfrak{p}$ em $M/\underline{x}M$ e a composta desta com a aplicação canônica $A/I \rightarrow A/\mathfrak{p}$ nos dá um elemento não nulo de $\text{Hom}_A(A/I, M/\underline{x}M)$.

Tendo em vista a equivalência acima, a proposição segue facilmente se provarmos que

$$\text{Ext}_A^r(A/I, M) \cong \text{Hom}_A(A/I, M/\underline{x}M)$$

para qualquer $\underline{x}$ M -regular em I , de comprimento r . Prosseguimos por indução em r . Para $r = 0$, não há o que provar. Suponhamos $r > 0$. Aplicando o funtor $\text{Hom}_A(A/I, \cdot)$ à sequência exata

$$0 \longrightarrow M \xrightarrow{x_1} M \longrightarrow M/x_1M \longrightarrow 0$$

obtemos a sequência exata

$$0 \longrightarrow \text{Ext}_A^{r-1}(A/I, M/x_1M) \longrightarrow \text{Ext}_A^r(A/I, M) \xrightarrow{x_1} \text{Ext}_A^r(A/I, M),$$

uma vez que $\text{Ext}_A^{r-1}(A/I, M) \cong \text{Hom}_A(A/I, M/(x_1, \dots, x_{r-1})M) = 0$, pela hipótese de indução e pela equivalência acima. Mas, como a multiplicação por x_1 é a aplicação nula em $\text{Ext}_A^r(A/I, M)$ (ver observação após a definição 3.3), temos

$$\text{Ext}_A^r(A/I, M) \cong \text{Ext}_A^{r-1}(A/I, M/x_1M) \cong \text{Hom}_A(A/I, M/\underline{x}M),$$

novamente pela hipótese de indução, aplicada à sequência M/x_1M -regular $x_2, \dots, x_r$. $\square$

Se $(A, \mathfrak{m})$ é um anel Noetheriano local e $M \neq 0$ um A -módulo finitamente gerado, chamaremos a $\mathfrak{m}$ -profundidade de M simplesmente de **profundidade de M** (notação: $d(M)$). Observamos que temos sempre $d(M) \leq \dim(M) := \dim(A/\text{Ann}M)$, conforme [Kun85, Cap.VI, Prop. 3.9], e a igualdade nos traz uma série de consequências importantes. Neste caso, dizemos que M é **de Cohen-Macaulay** ou, abreviando, **C-M**.

Definição 2.15 Dizemos que um anel Noetheriano local $(A, \mathfrak{m})$ é de Cohen-Macaulay se ele for um A -módulo C-M, isto é, $d(A) = \dim(A)$. Mais geralmente, dizemos que um anel Noetheriano qualquer é de Cohen-Macaulay se todas as localizações em ideais maximais o forem.

Dentre as diversas propriedades “boas” dos anéis C-M, estaremos particularmente interessados naquela que garante que ideais que são interseções completas são gerados por seqüências regulares, de comprimento igual a altura do ideal:

Teorema 2.16 Seja A um anel C-M e I um ideal próprio de A . Então:

- $d(I, A) = h(I)$;
- I é uma interseção completa se, e somente se, for gerado por uma seqüência regular.

Demonstração: [Kun85, Cap. VI, Teorema 3.14] □

Proposição 2.17 Se A é C-M e S um sistema multiplicativo de A , então A_S também é C-M.

Demonstração: [Kun85, Cap. VI, Corolário 3.16] □

Assim, se um ideal de um anel de Cohen-Macaulay é localmente uma interseção completa, então ele é gerado localmente por seqüências regulares. Se assumirmos que este ideal tem codimensão pura r , então todas estas seqüências terão comprimento r . Isto será extremamente importante no próximo capítulo.

Definição 2.18 Dizemos que um anel Noetheriano local $(A, \mathfrak{m})$ é regular se $\mathfrak{m}$ for uma interseção completa, isto é,

$$\mu(\mathfrak{m}) = h(\mathfrak{m}) = \dim(A).$$

Mais geralmente, dizemos que um anel Noetheriano qualquer é regular se todas as localizações em ideais maximais forem regulares.

Exemplo 2.19 O anel de polinômios $k[X_1, \dots, X_n]$ é regular ([Kun85, Cap. VI, Corolário 1.8]).

A regularidade é preservada por localizações:

Proposição 2.20 *Se A é regular e S um sistema multiplicativo de A , então A_S também é regular.*

Demonstração: [Kun85, Cap. VII, Corolário 2.6] □

Proposição 2.21 *Todo anel regular é de Cohen-Macaulay.*

Demonstração: [Kun85, Cap. VI, §3] □

Em particular, o anel de polinômios $k[X_1, \dots, X_n]$ é de Cohen-Macaulay. Teremos isto sempre em mente quando, nos capítulos seguintes, aplicarmos teoremas provados para anéis C-M em situações geométricas.

Para finalizar esta sessão, incluímos dois teoremas relacionados a anéis regulares que serão utilizados no Capítulo 5.

Teorema 2.22 (Critério do Jacobiano) *Sejam dados um anel de polinômios $A := k[X_1, \dots, X_n]$ e um ideal $I = (f_1, \dots, f_s) \leq A$. Então:*

- *para todo $\mathfrak{p} \in V(I)$, a redução módulo $\mathfrak{p}$ da matriz Jacobiana*

$$\mathcal{J} := \left(\frac{\partial f_i}{\partial X_j} \right)$$

tem posto $\leq h(I_{\mathfrak{p}})$;

- *se k for perfeito e I tiver codimensão pura c , seja J o ideal de $B := A/I$ gerado pelas imagens dos menores $c \times c$ da matriz Jacobiana $\mathcal{J}$. Então para $\mathfrak{p} \in \text{Spec}(B)$ temos $\mathfrak{p} \in V(J) \iff B_{\mathfrak{p}}$ não é regular.*

Demonstração: [Eis94, Teorema 16.19, Corolário 16.20] □

Teorema 2.23 *Todo anel local regular é um domínio fatorial.*

Demonstração: [Eis94, Teorema 19.19], [ZS60, Apêndice 7] □

2.4 O Complexo de Koszul

Dada uma seqüência $\underline{x} := x_1, \dots, x_r$ de elementos de um anel A , construímos o **complexo de Koszul** $\mathcal{K}(\underline{x})$ fazendo

$$\mathcal{K}_0(\underline{x}) := A$$

$$\mathcal{K}_1(\underline{x}) := A\text{-módulo livre } F \text{ com base } \{e_1, \dots, e_r\}$$

$$\mathcal{K}_p(\underline{x}) := A\text{-módulo livre } \wedge^p F \text{ com base } \{e_{i_1} \wedge \dots \wedge e_{i_p} \mid i_1 < \dots < i_p\}$$

$$\mathcal{K}_r(\underline{x}) := A\text{-módulo livre } \wedge^r F \text{ com base } \{e_1 \wedge \dots \wedge e_r\}$$

e definindo as **aplicações de fronteira** $\mathcal{K}_p(\underline{x}) \xrightarrow{d} \mathcal{K}_{p-1}(\underline{x})$ por

$$d(e_{i_1} \wedge \dots \wedge e_{i_p}) := \sum_{j=1}^p (-1)^{j-1} x_{i_j} e_{i_1} \wedge \dots \wedge \widehat{e_{i_j}} \wedge \dots \wedge e_{i_p},$$

onde o símbolo $\widehat{}$ indica a omissão de um elemento. Temos então, para elementos $\alpha_1, \dots, \alpha_p \in F$ arbitrários,

$$d(\alpha_1 \wedge \dots \wedge \alpha_p) = \sum_{j=1}^p (-1)^{j-1} d(\alpha_j) \alpha_1 \wedge \dots \wedge \widehat{\alpha_j} \wedge \dots \wedge \alpha_p.$$

Com efeito, basta observarmos que a aplicação

$$(\alpha_1, \dots, \alpha_p) \mapsto \sum_{j=1}^p (-1)^{j-1} d(\alpha_j) \alpha_1 \wedge \dots \wedge \widehat{\alpha_j} \wedge \dots \wedge \alpha_p$$

é multilinear alternada e portanto induz uma aplicação linear em $\mathcal{K}_p(\underline{x})$ que coincide com d na base.

Uma verificação direta mostra que $d^2 = 0$ e temos assim o complexo

$$0 \rightarrow \mathcal{K}_r(\underline{x}) \rightarrow \dots \rightarrow \mathcal{K}_p(\underline{x}) \rightarrow \dots \rightarrow \mathcal{K}_1(\underline{x}) \rightarrow A \rightarrow 0.$$

Mais geralmente, para qualquer A -módulo M definimos o **complexo de Koszul de M** por $\mathcal{K}(\underline{x}; M) := \mathcal{K}(\underline{x}) \otimes_A M$.

Teorema 2.24 *Sejam A um anel, M um A -módulo, $\underline{x} := x_1, \dots, x_r$ uma seqüência de elementos de A e $I := (x_1, \dots, x_r)$.*

- *Se $\underline{x}$ é M -regular, então o complexo de Koszul $\mathcal{K}(\underline{x}; M)$ é uma resolução de M/IM , ou seja, $H_0 \mathcal{K}(\underline{x}; M) \cong M/IM$ e $H_i \mathcal{K}(\underline{x}; M) = 0$, $\forall i > 0$.*

- Reciprocamente, suponhamos que A seja local e $\underline{x}$ esteja contida no ideal maximal de A . Suponhamos ainda que M seja finitamente gerado e que a homologia $H_1 \mathcal{K}(\underline{x}; M)$ seja nula. Então a seqüência $\underline{x}$ é M -regular.

Demonstração: [Lan93, Cap. XXI, Teorema 4.6] $\square$

Teorema 2.25 *Sejam A um anel, M um A -módulo, $\underline{x} := x_1, \dots, x_r$ uma seqüência de elementos de A e $I := (x_1, \dots, x_r)$. Suponhamos que o complexo de Koszul $\mathcal{K}(\underline{x})$ seja uma resolução de A/I . Então existe um isomorfismo*

$$\varphi_{\underline{x}, M} : \text{Ext}_A^r(A/I, M) \longrightarrow M/IM.$$

Demonstração: $\mathcal{K}(\underline{x})$ é, por hipótese, uma resolução livre de A/I , e portanto

$$\text{Ext}_A^r(A/I, M) = H^r(\text{Hom}_A(\mathcal{K}(\underline{x}), M)).$$

Escrevendo explicitamente os últimos termos do complexo $\text{Hom}_A(\mathcal{K}(\underline{x}), M)$ temos

$$\text{Hom}_A(\mathcal{K}_{r-1}(\underline{x}), M) \xrightarrow{\bar{d}} \text{Hom}_A(\mathcal{K}_r(\underline{x}), M) \longrightarrow 0$$

$$\text{e } \text{Ext}_A^r(A/I, M) = \text{Hom}_A(\mathcal{K}_r(\underline{x}), M) / \bar{d}(\text{Hom}_A(\mathcal{K}_{r-1}(\underline{x}), M)).$$

Como $\mathcal{K}_r(\underline{x})$ é livre, com base $e_1 \wedge \dots \wedge e_r$, temos um isomorfismo

$$\phi : \text{Hom}_A(\mathcal{K}_r(\underline{x}), M) \longrightarrow M$$

definido por $\phi(f) := f(e_1 \wedge \dots \wedge e_r)$ e verificaremos sem dificuldade que a imagem de $\bar{d}(\text{Hom}_A(\mathcal{K}_{r-1}(\underline{x}), M))$ por este isomorfismo é exatamente IM , de modo que ϕ induz um isomorfismo $\varphi_{\underline{x}, M}$ entre $\text{Ext}_A^r(A/I, M)$ e M/IM . De fato, para todo $m \in M$ e todo $i = 1, \dots, r$, podemos definir $f \in \text{Hom}_A(\mathcal{K}_{r-1}(\underline{x}), M)$ fazendo $f(e_1 \wedge \dots \wedge \hat{e}_i \wedge \dots \wedge e_r) := \delta_{ij} m$ e, como

$$d(e_1 \wedge \dots \wedge e_r) = \sum_{j=1}^r (-1)^{j-1} x_j e_1 \wedge \dots \wedge \hat{e}_j \wedge \dots \wedge e_r,$$

temos

$$\phi(\bar{d}(f)) = \bar{d}(f)(e_1 \wedge \dots \wedge e_r) = f \circ d(e_1 \wedge \dots \wedge e_r) = (-1)^{i-1} x_i m.$$

Isto mostra que a imagem de $\bar{d}(\text{Hom}_A(\mathcal{K}_{r-1}(\underline{x}), M))$ por ϕ contém IM . A outra inclusão é imediata. $\square$

Se I é gerado por uma seqüência regular então temos o isomorfismo acima, mas este *depende* da escolha da seqüência regular geradora de I usada na construção do complexo de Koszul. Com efeito, sejam $\underline{x} := x_1, \dots, x_r$ e $\underline{y}$ duas tais seqüências. Então $\underline{y}$ tem comprimento r (por 2.12, digamos). Façamos $\underline{y} = y_1, \dots, y_r$ e suponhamos $y_i = \sum c_{ij} x_j$ ($c_{ij} \in A$). Construimos o complexo de Koszul $\mathcal{K}(\underline{y})$ a partir de um módulo livre F' de base $\{e'_1, \dots, e'_r\}$, chamando as aplicações de fronteira de d' . Definimos uma aplicação

$$\Psi : \mathcal{K}(\underline{y}) \longrightarrow \mathcal{K}(\underline{x})$$

fazendo

$$\begin{aligned} \Psi_0 &:= \text{id} \\ \Psi_1(e'_i) &:= \sum c_{ij} e_j, \quad \forall i = 1, \dots, r \\ &\vdots \\ \Psi_p &:= \underbrace{\Psi_1 \wedge \dots \wedge \Psi_1}_{p \text{ vezes}}. \end{aligned}$$

Em particular, fazendo $D := \det(c_{ij})$ vemos que

$$\Psi_r(e'_1 \wedge \dots \wedge e'_r) = D e_1 \wedge \dots \wedge e_r.$$

Ψ é um morfismo de complexos, pois

$$\begin{aligned} \Psi_{p-1} \circ d'(\epsilon'_{i_1} \wedge \dots \wedge \epsilon'_{i_p}) &= \Psi_{p-1} \left(\sum_{k=1}^p (-1)^{k-1} y_{i_k} \epsilon'_{i_1} \wedge \dots \wedge \widehat{\epsilon'_{i_k}} \wedge \dots \wedge \epsilon'_{i_p} \right) \\ &= \sum_{k=1}^p (-1)^{k-1} y_{i_k} \Psi_1(\epsilon'_{i_1}) \wedge \dots \wedge \widehat{\Psi_1(\epsilon'_{i_k})} \wedge \dots \wedge \Psi_1(\epsilon'_{i_p}) \\ &= \sum_{k=1}^p (-1)^{k-1} \left(\sum c_{i_k j} x_j \right) \Psi_1(\epsilon'_{i_1}) \wedge \dots \wedge \widehat{\Psi_1(\epsilon'_{i_k})} \wedge \dots \wedge \Psi_1(\epsilon'_{i_p}) \\ &= \sum_{k=1}^p (-1)^{k-1} d(\Psi_1(\epsilon'_{i_k})) \Psi_1(\epsilon'_{i_1}) \wedge \dots \wedge \widehat{\Psi_1(\epsilon'_{i_k})} \wedge \dots \wedge \Psi_1(\epsilon'_{i_p}) \\ &= d \circ \Psi_p(\epsilon'_{i_1} \wedge \dots \wedge \epsilon'_{i_p}) \end{aligned}$$

e portanto $\Psi_{p-1} \circ d' = d \circ \Psi_p$. Aplicando o funtor $\text{Hom}_A(\cdot, M)$ obtemos o morfismo de complexos

$$\overline{\Psi} : \text{Hom}_A(\mathcal{K}(\underline{x}), M) \longrightarrow \text{Hom}_A(\mathcal{K}(\underline{y}), M)$$

que induz nas homologias de nível r a aplicação

$$\Phi : H^r(\text{Hom}_A(\mathcal{K}(\underline{x}), M)) \longrightarrow H^r(\text{Hom}_A(\mathcal{K}(\underline{y}), M)).$$

Para $f \in \text{Hom}_A(\mathcal{K}_r(\underline{x}), M)$ com $f(e_1 \wedge \cdots \wedge e_r) := m$ temos

$$\bar{\Psi}_r(f)(e'_1 \wedge \cdots \wedge e'_r) = f \circ \Psi_r(e'_1 \wedge \cdots \wedge e'_r) = f(D e_1 \wedge \cdots \wedge e_r) = Dm.$$

Assim, revendo a construção das aplicações $\varphi_{\underline{x}, M}$ e $\varphi_{\underline{y}, M}$ vemos que o diagrama

$$\begin{array}{ccc} H^r(\text{Hom}_A(\mathcal{K}(\underline{x}), M)) & \xrightarrow{\varphi_{\underline{x}, M}} & M/IM \\ \downarrow \Phi & & \downarrow D \\ H^r(\text{Hom}_A(\mathcal{K}(\underline{y}), M)) & \xrightarrow{\varphi_{\underline{y}, M}} & M/IM \end{array}$$

comuta. Observamos que todas as aplicações do diagrama acima são isomorfismos — Φ é exatamente o isomorfismo construído em Álgebra Homológica na demonstração de que a definição do funtor $\text{Ext}_A^r(A/I, \cdot)$ independe da escolha da resolução projetiva de A/I . De outro modo, poderíamos observar que

$$M/IM \xrightarrow{D} M/IM$$

é um isomorfismo, uma vez que, como a redução de (c_{ij}) módulo I é uma matriz de mudança de base do A/I -módulo livre I/I^2 (conforme 2.12), $D = \det(c_{ij})$ é uma unidade módulo I .

Identificando $H^r(\text{Hom}_A(\mathcal{K}(\underline{x}), M))$ e $H^r(\text{Hom}_A(\mathcal{K}(\underline{y}), M))$ através de Φ obtemos o diagrama comutativo

$$\begin{array}{ccc} & \text{Ext}_A^r(A/I, M) & \\ \varphi_{\underline{x}, M} \swarrow & & \searrow \varphi_{\underline{y}, M} \\ M/IM & \xrightarrow{D} & M/IM \end{array}$$

Sabemos, pela proposição 2.12, que I/I^2 é um A/I -módulo livre, com base $\{\bar{x}_1, \dots, \bar{x}_r\}$, e portanto $\bigwedge^r(I/I^2)$ é livre, com base $\bar{x}_1 \wedge \cdots \wedge \bar{x}_r$. Tomando agora o dual de $\bigwedge^r(I/I^2)$ (como A/I -módulo), temos o isomorfismo

$$\psi_{\underline{x}, M} : M/IM \longrightarrow M/IM \otimes_{A/I} \left(\bigwedge^r(I/I^2) \right)^*$$

definido por $\psi_{\underline{x},M}(\overline{m}) := \overline{m} \otimes (\overline{x_1} \wedge \cdots \wedge \overline{x_r})^*$. Mas $\overline{y_1} \wedge \cdots \wedge \overline{y_r} = D \overline{x_1} \wedge \cdots \wedge \overline{x_r}$ e portanto $D(\overline{y_1} \wedge \cdots \wedge \overline{y_r})^* = (\overline{x_1} \wedge \cdots \wedge \overline{x_r})^*$. Assim, definindo $\psi_{\underline{y},M}$ de modo análogo obtemos o diagrama comutativo

$$\begin{array}{ccccc} \mathrm{Ext}_A^r(A/I, M) & \xrightarrow{\varphi_{\underline{x},M}} & M/IM & \xrightarrow{\psi_{\underline{x},M}} & M/IM \otimes (\wedge^r(I/I^2))^* \\ \parallel & & \downarrow D & & \parallel \\ \mathrm{Ext}_A^r(A/I, M) & \xrightarrow{\varphi_{\underline{y},M}} & M/IM & \xrightarrow{\psi_{\underline{y},M}} & M/IM \otimes (\wedge^r(I/I^2))^* \end{array}$$

e portanto a composta das aplicações $\psi_{\underline{x},M}$ e $\varphi_{\underline{x},M}$ nos dá um isomorfismo

$$\varphi_M : \mathrm{Ext}_A^r(A/I, M) \longrightarrow M/IM \otimes_{A/I} (\wedge^r(I/I^2))^*$$

que independe da escolha da seqüência, isto é, é intrínseco ao ideal. Destacamos este resultado abaixo:

Teorema 2.26 *Sejam A um anel, M um A -módulo e I um ideal de A gerado por uma seqüência regular de comprimento r . Então existe um isomorfismo de A/I -módulos*

$$\varphi_M : \mathrm{Ext}_A^r(A/I, M) \longrightarrow M/IM \otimes_{A/I} (\wedge^r(I/I^2))^*$$

que só depende do ideal I , e não da escolha da seqüência regular geradora deste ideal.

2.5 O “Splitting-off” de Serre. O Teorema de Quillen-Suslin

Teorema 2.27 (“Splitting-off Theorem”) *Seja A um anel Noetheriano de dimensão finita. Sejam P e P_0 A -módulos projetivos, finitamente gerados, e suponhamos P_0 de posto 1 e*

$$\mu_{\mathfrak{p}}(P) > \dim A$$

para todo $\mathfrak{p} \in \mathrm{Spec}(A)$. Então $P \cong P_0 \oplus P'$ para algum A -módulo P' .

Demonstração: [Kun85, Cap. IV, Teorema 3.18]

□

Teorema 2.28 (Quillen-Suslin) *Se M é um $A[X]$ -módulo projetivo finitamente gerado e $f \in A[X]$ um polinômio mônico tal que M_f é livre sobre $A[X]_f$, então M é livre.*

Demonstração: [Kun85, Cap IV, Teorema 3.14] □

Teorema 2.29 (Quillen-Suslin, “Conjectura de Serre”) *Todo módulo projetivo, finitamente gerado, sobre $k[X_1, \dots, X_n]$ é livre.*

Demonstração: Provas detalhadas podem ser encontradas em [Lan93, Cap. XXI, Teorema 3.7], [Kun85, Cap. IV, Teorema 3.15] ou [Lam78], este último uma referência obrigatória, quer seja pelas diversas provas apresentadas (duas provas elementares e a demonstração de Quillen [Qui76]), quer pela apresentação de diversas motivações, da ligação com o problema das interseções completas e de um histórico da evolução do problema desde sua formulação em 1955 por Serre até sua resolução por Quillen e Suslin, em 1976. □

Capítulo 3

O Teorema de Szpiro

Provaremos neste capítulo que curvas em $\mathbb{A}^3$ que são localmente interseções completas são interseções completas como conjuntos, resultado que será generalizado posteriormente para dimensões arbitrárias.

3.1 Preliminares

Durante toda esta sessão vamos supor A um anel de Cohen-Macaulay de dimensão $n \geq 3$ e $I < A$ um ideal de codimensão pura $r \geq 2$, *localmente interseção completa* em A . Nestas condições, I será gerado localmente por seqüências regulares de comprimento r (por 2.16) e o módulo conormal I/I^2 será um A/I -módulo localmente livre, de posto r (por 2.12), e portanto projetivo de posto r .

As condições acima são satisfeitas, por exemplo, pelo anel de polinômios $k[X_1, \dots, X_n]$ e o ideal de definição de uma k -variedade de codimensão pura r que seja localmente uma interseção completa.

Apresentaremos nesta sessão alguns resultados que serão usados ao longo deste capítulo.

Lema 3.1 $\text{Ext}_{A_{\mathfrak{p}}}^k(A_{\mathfrak{p}}/I_{\mathfrak{p}}, A_{\mathfrak{p}}) = 0$, para todo $\mathfrak{p} \in \text{Spec}(A)$ e $k \neq r$.

Demonstração: Se $\mathfrak{p} \in \text{Spec}(A) \setminus V(I)$, o resultado é imediato. Caso contrário, temos $\text{Ext}_{A_{\mathfrak{p}}}^k(A_{\mathfrak{p}}/I_{\mathfrak{p}}, A_{\mathfrak{p}}) = 0$ para $k > r$, pois $\dim \text{proj}_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}/I_{\mathfrak{p}}) = r$ (por 2.13), e para $k < r$, pela proposição 2.14. $\square$

Ainda pela proposição 2.14, temos que $\text{Ext}_{A_{\mathfrak{p}}}^r(A_{\mathfrak{p}}/I_{\mathfrak{p}}, A_{\mathfrak{p}}) \neq 0, \forall \mathfrak{p} \in V(I)$. Assim, com a ajuda do corolário 2.5 temos imediatamente:

Proposição 3.2 $\text{Ext}_A^k(A/I, A) \neq 0 \iff k = r.$ $\square$

Definição 3.3 Chamamos $\omega_I := \text{Ext}_A^r(A/I, A)$ de **módulo canônico de A/I** .

Observamos que ω_I tem estrutura natural de A/I -módulo. Isto é imediato da definição do funtor Ext via resolução injetiva: se $\mathcal{I}_A$ é uma resolução injetiva de A , ω_I será a r -ésima homologia do complexo $\text{Hom}_A(A/I, \mathcal{I}_A)$. Mas os módulos $\text{Hom}_A(A/I, \mathcal{I}^k)$ e, *a fortiori*, $\text{Ext}_A^k(A/I, A)$ são anulados por I e portanto podem ser tratados naturalmente como A/I -módulos.

Proposição 3.4 $(\omega_I)_{\mathfrak{p}} \cong A_{\mathfrak{p}}/I_{\mathfrak{p}}, \forall \mathfrak{p} \in \text{Spec}(A)$. Logo ω_I é *projetivo*, de posto 1, como A/I -módulo.

Demonstração: Se $\mathfrak{p} \in \text{Spec}(A) \setminus V(I)$, o resultado é óbvio, pois I anula ω_I . Por outro lado, se $\mathfrak{p} \in V(I)$,

$$\begin{aligned} (\omega_I)_{\mathfrak{p}} &\cong \text{Ext}_{A_{\mathfrak{p}}}^r(A_{\mathfrak{p}}/I_{\mathfrak{p}}, A_{\mathfrak{p}}) && \text{pelo corolário 2.5} \\ &\cong A_{\mathfrak{p}}/I_{\mathfrak{p}} && \text{pelo teorema 2.25.} \end{aligned}$$

$\square$

Teorema 3.5 $\omega_I \cong \text{Hom}_{A/I}(\wedge^r(I/I^2), A/I)$ como A/I -módulos.

Demonstração: Dado $\mathfrak{p} \in V(I) \subseteq \text{Spec}(A)$, sabemos que $I_{\mathfrak{p}}$ é gerado por uma seqüência regular de comprimento r , que podemos assumir ser a imagem de uma seqüência de elementos de I , digamos $\underline{x} := x_1, \dots, x_r$. Logo $(I/(\underline{x}))_{\mathfrak{p}} = 0$, isto é, $\mathfrak{p} \notin \text{Supp}(I/(\underline{x})) = V(\text{Ann}(I/(\underline{x})))$ e, como este é fechado em $\text{Spec}(A)$, existe um aberto básico $D(f) \ni \mathfrak{p}$ tal que $D(f)$ e $\text{Supp}(I/(\underline{x}))$ são disjuntos. Como consequência, temos $I_f = (\underline{x})_f$.

Pelo teorema 2.24 o complexo $\mathcal{K}(\underline{x})_{\mathfrak{p}}$, canonicamente isomorfo ao complexo de Koszul construído a partir das imagens de $x_1, \dots, x_r$ em $A_{\mathfrak{p}}$, é uma resolução de $A_{\mathfrak{p}}/I_{\mathfrak{p}}$ e portanto $\mathfrak{p} \notin \text{Supp}(H_i \mathcal{K}(\underline{x})), \forall i > 0$. Assim, reduzindo $D(f)$ se necessário, podemos assumir $D(f)$ e $\bigcup_{i>0} \text{Supp}(H_i \mathcal{K}(\underline{x}))$ disjuntos, e assim $\mathcal{K}(\underline{x})_f$ é uma resolução de A_f/I_f , conforme podemos verificar localmente, em todo $\mathfrak{q} \in D(f) \cong \text{Spec}(A_f)$. Mais ainda, a seqüência $\underline{x}$ é regular em $A_{\mathfrak{q}}, \forall \mathfrak{q} \in D(f) \cap V(I)$, novamente pelo teorema 2.24.

Conseguimos assim uma cobertura $\{D(f) \mid f \in \Gamma\}$ de $V(I) \cong \text{Spec}(A/I)$ tal que, para todo $f \in \Gamma$, existe uma sequência $\underline{x} := x_1, \dots, x_r$ em I (que *depende* de f) tal que:

- $I_f = (x_1, \dots, x_r)_f$;
- $\mathcal{K}(\underline{x})_f$ é uma resolução de A_f/I_f ;
- a imagem de $\underline{x}$ em $A_{\mathfrak{q}}$ é regular, para todo $\mathfrak{q} \in D(f) \cap V(I)$.

Podemos supor esta cobertura *finita* :

$$\begin{aligned} V(I) \subseteq \cup_{f \in \Gamma} D(f) &\iff (\bar{f} \mid f \in \Gamma) = A/I \\ &\iff \exists \Gamma_0 \subseteq \Gamma \text{ finito com } (\bar{f} \mid f \in \Gamma_0) = A/I \\ &\iff V(I) \subseteq \cup_{f \in \Gamma_0} D(f) \end{aligned}$$

Seja $f \in \Gamma$ e $\underline{x}$ a sequência correspondente. Pelo teorema 2.25, existe um isomorfismo de A_f/I_f -módulos

$$\varphi_{\underline{x},f} : \text{Ext}_{A_f}^r(A_f/I_f, A_f) \longrightarrow A_f/I_f.$$

Observamos que a imagem de $\underline{x}$ em I_f/I_f^2 é uma base deste A_f/I_f -módulo, pois o é localmente, em todo $\mathfrak{p} \in D(f) \cap V(I) \cong \text{Spec}(A_f/I_f)$. Assim, $\text{Hom}_{A_f/I_f}(\bigwedge^r(I_f/I_f^2), A_f/I_f)$ é livre, com base $(\widetilde{x}_1 \wedge \dots \wedge \widetilde{x}_r)^*$, onde o símbolo $\sim$ indica imagem em I_f/I_f^2 . Assim podemos definir o isomorfismo

$$\psi_{\underline{x},f} : A_f/I_f \longrightarrow \text{Hom}_{A_f/I_f}(\bigwedge^r(I_f/I_f^2), A_f/I_f)$$

por $\psi_{\underline{x},f}(\zeta) := \zeta \cdot (\widetilde{x}_1 \wedge \dots \wedge \widetilde{x}_r)^*$. Compondo os isomorfismos $\psi_{\underline{x},f}$ e $\varphi_{\underline{x},f}$ obtemos, após algumas identificações, um isomorfismo de $(A/I)_{\bar{f}}$ -módulos

$$\varphi_{\bar{f}} : \text{Ext}_A^r(A/I, A)_{\bar{f}} \longrightarrow \text{Hom}_{A/I}(\bigwedge^r(I/I^2), A/I)_{\bar{f}}.$$

Para todo $f \in \Gamma$, a localização de $\varphi_{\bar{f}}$ em $\mathfrak{p} \in D(f) \cap V(I) \cong D(\bar{f})$ é, a menos de isomorfismos canônicos, exatamente o isomorfismo construído conforme o teorema 2.26, a partir do complexo de Koszul de $A_{\mathfrak{p}}$ relativo a *qualquer* sequência regular que gera $I_{\mathfrak{p}}$. Assim, a família $(\varphi_{\bar{f}})_{f \in \Gamma}$ satisfaz a condição de compatibilidade da proposição 2.2 e estes isomorfismos se “colam”, dando um isomorfismo global

$$\varphi : \text{Ext}_A^r(A/I, A) \longrightarrow \text{Hom}_{A/I}(\bigwedge^r(I/I^2), A/I).$$

□

Teorema 3.6 $\text{Ext}_A^r(\omega_I, A) \cong A/I$ e $\text{Ext}_A^k(\omega_I, A) = 0$ para $k \neq r$.

Demonstração: Usando os resultados (2.5), (3.4) e (3.1) verificamos (localmente) que $\text{Ext}_A^k(\omega_I, A) = 0$, $\forall k \neq r$. Como, por (3.2),

$$(A/I)^* = 0 = \text{Ext}_A^1(A/I, A),$$

dualizando a seqüência

$$0 \longrightarrow I \longrightarrow A \longrightarrow A/I \longrightarrow 0 \quad (1)$$

obtemos a seqüência exata

$$0 \longrightarrow A^* \longrightarrow I^* \longrightarrow 0, \quad (1^*)$$

e portanto $I^* \cong A^* \cong A$. Seja $I \xrightarrow{\varphi} I^{**}$ o homomorfismo canônico. Dualizando (1*) obtemos o seguinte diagrama comutativo com linhas exatas

$$\begin{array}{ccccccc} 0 & \longrightarrow & I & \longrightarrow & A & \longrightarrow & A/I \longrightarrow 0 \\ & & \downarrow \varphi & & \downarrow \approx & & \\ 0 & \longrightarrow & I^{**} & \longrightarrow & A^{**} & \longrightarrow & 0 \end{array} \quad (1^{**})$$

e vemos facilmente, usando o “Lema da Cobra”, que φ é injetora e $C := \text{Coker } \varphi \cong A/I$.

Temos $\dim \text{proj}_A(A/I) = r$, por (2.13) e (2.9), e portanto $\dim \text{proj}_A(I) = r - 1$, por (2.10). Podemos então tomar uma seqüência exata

$$0 \longrightarrow P_{r-1} \longrightarrow P_{r-2} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\alpha} I \longrightarrow 0,$$

com módulos P_j projetivos e finitamente gerados, conforme a observação após a prova de 2.8. Dualizando esta seqüência obtemos o complexo

$$0 \longrightarrow I^* \xrightarrow{\alpha^*} P_0^* \longrightarrow P_1^* \longrightarrow \cdots \longrightarrow P_{r-2}^* \longrightarrow P_{r-1}^* \longrightarrow 0,$$

onde a homologia calculada em P_j^* ($j > 0$) é $\text{Ext}_A^j(I, A) \cong \text{Ext}_A^{j+1}(A/I, A)$, por (2.7). Assim, pela proposição 3.2 e pelo corolário 2.6 vemos que o complexo acima é uma *resolução projetiva de ω_I* .

Dualizando novamente obtemos o complexo

$$0 \longrightarrow P_{r-1}^{**} \longrightarrow P_{r-2}^{**} \longrightarrow \cdots \longrightarrow P_1^{**} \longrightarrow P_0^{**} \xrightarrow{\alpha^{**}} I^{**} \longrightarrow 0.$$

Agora a homologia calculada em I^{**} é $\text{Ext}_A^r(\omega_I, A)$, enquanto as demais são nulas, pela primeira parte desta demonstração. Construimos, então, o seguinte diagrama comutativo com linhas exatas:

$$\begin{array}{ccccccc} 0 & \longrightarrow & P_0 & \xrightarrow{\approx} & P_0^{**} & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \alpha^{**} & & \\ 0 & \longrightarrow & I & \xrightarrow{\varphi} & I^{**} & \longrightarrow & C \longrightarrow 0 \end{array}$$

onde $P_0 \rightarrow P_0^{**}$ é a aplicação canônica, logo um isomorfismo, por 2.6. Como α é sobrejetora, aplicando o “Lema da Cobra” temos

$$\text{Ext}_A^r(\omega_I, A) = \text{Coker } \alpha^{**} \cong C \cong A/I.$$

□

3.2 Os Métodos de Szpiro

O objetivo desta sessão será demonstrar o seguinte teorema:

Teorema 3.7 ([Szp79]) *Sejam A um anel de Cohen-Macaulay de dimensão $n \geq 3$ e $I < A$ um ideal de codimensão pura $n - 1$, localmente interseção completa. Então existe um ideal $J < A$ tal que:*

- J também é interseção completa local;
- $\text{Rad}(J) = \text{Rad}(I)$;
- $\omega_J := \text{Ext}_A^{n-1}(A/J, A)$ é livre, de posto 1, sobre A/J .

Observamos que nesta sessão estaremos trabalhando sempre com ideais de codimensão pura $r := n - 1$. O exemplo concreto que temos em mente é um ideal de definição de uma curva em $\mathbb{A}^n$ que é localmente interseção completa, naturalmente. Começaremos provando duas proposições:

Proposição 3.8 *Existe um A/I -epimorfismo $I/I^2 \xrightarrow{q_I} \omega_I$.*

Demonstração: Como I/I^2 e ω_I são projetivos sobre A/I , de postos $n-1$ e 1 respectivamente, e $\dim(A/I) \leq 1 < n-1$, temos pelo “Splitting-off” de Serre (teorema 2.27) que

$$I/I^2 \cong \omega_I \oplus P$$

para algum A/I -módulo P . $\square$

Seja $\text{Ker}(\phi) = J/I^2$, onde J é ideal de A , $I^2 \subseteq J \subseteq I$ (e portanto $\text{Rad}(J) = \text{Rad}(I)$). Então, como ω_I é projetivo,

$$I/I^2 \cong J/I^2 \oplus \omega_I$$

e portanto J/I^2 é projetivo, de posto $n-2$, como A/I -módulo.

Proposição 3.9 *J é localmente uma interseção completa.*

Demonstração: Para todo ideal maximal $\mathfrak{m}$ de A com $J \subseteq \mathfrak{m}$, $J_{\mathfrak{m}}/I_{\mathfrak{m}}^2$ é um somando direto de $I_{\mathfrak{m}}/I_{\mathfrak{m}}^2$, livre sobre $A_{\mathfrak{m}}/I_{\mathfrak{m}}$, de posto $n-2$. Podemos então tomar elementos $x_2, \dots, x_{n-1} \in J_{\mathfrak{m}}$ tais que suas imagens em $J_{\mathfrak{m}}/I_{\mathfrak{m}}^2$ formam uma $A_{\mathfrak{m}}/I_{\mathfrak{m}}$ -base e $x_1 \in I_{\mathfrak{m}}$ cuja imagem completa uma base de $I_{\mathfrak{m}}/I_{\mathfrak{m}}^2$. Então $I_{\mathfrak{m}} = (x_1, \dots, x_{n-1}) + I_{\mathfrak{m}}^2$ e, pelo Lema de Nakayama, $I_{\mathfrak{m}} = (x_1, \dots, x_{n-1})$. Além disso, $J_{\mathfrak{m}} = (x_2, \dots, x_{n-1}) + I_{\mathfrak{m}}^2$. Mas $I_{\mathfrak{m}}^2$ é gerado pelos produtos $x_i x_j$, com $1 \leq i, j \leq n-1$, e todos estes, com a possível exceção de x_1^2 , pertencem a $(x_2, \dots, x_{n-1})$, levando assim a

$$J_{\mathfrak{m}} = (x_1^2, x_2, \dots, x_{n-1})$$

e $J_{\mathfrak{m}}$ é interseção completa, uma vez que $h(J_{\mathfrak{m}}) = h(I_{\mathfrak{m}}) = n-1$. $\square$

Como $\omega_I \cong (I/I^2)/(J/I^2) \cong I/J$ temos uma seqüência exata

$$0 \longrightarrow \omega_I \longrightarrow A/J \longrightarrow A/I \longrightarrow 0 \quad (*)$$

e aplicando o funtor $\text{Hom}_A(\cdot, A)$ obtemos a seqüência exata

$$\begin{aligned} \text{Ext}_A^{n-2}(\omega_I, A) &\longrightarrow \text{Ext}_A^{n-1}(A/I, A) \longrightarrow \text{Ext}_A^{n-1}(A/J, A) \longrightarrow \\ &\longrightarrow \text{Ext}_A^{n-1}(\omega_I, A) \longrightarrow \text{Ext}_A^n(A/I, A) \end{aligned}$$

Temos:

$$\begin{aligned}
\text{Ext}_A^{n-2}(\omega_I, A) &= 0 && \text{(teorema 3.6)} \\
\text{Ext}_A^{n-1}(A/I, A) &= \omega_I && \text{(definição 3.3)} \\
\text{Ext}_A^{n-1}(A/J, A) &= \omega_J && \text{(definição 3.3)} \\
\text{Ext}_A^{n-1}(\omega_I, A) &\cong A/I && \text{(teorema 3.6)} \\
\text{Ext}_A^n(A/I, A) &= 0 && \text{(proposição 3.2)}
\end{aligned}$$

e assim a seqüência acima pode ser reescrita como

$$0 \longrightarrow \omega_I \longrightarrow \omega_J \xrightarrow{\alpha} A/I \longrightarrow 0. \quad (**)$$

Observamos que todos os módulos envolvidos nas seqüências (*) e (**) têm estruturas naturais de A/J -módulos. Seja $\xi \in \omega_J$ tal que $\alpha(\xi) = 1 + I$. Mostraremos que ξ é uma A/J -base de ω_J . Para isto é suficiente verificarmos localmente, para todo $\mathfrak{p} \in \text{Spec}(A)$ com $J \subseteq \mathfrak{p}$. Temos o seguinte diagrama comutativo de $A_{\mathfrak{p}}/J_{\mathfrak{p}}$ -módulos:

$$\begin{array}{ccc}
& (\omega_J)_{\mathfrak{p}} & \\
\gamma \swarrow & & \searrow \alpha_{\mathfrak{p}} \\
A_{\mathfrak{p}}/J_{\mathfrak{p}} & \xrightarrow{\delta} & A_{\mathfrak{p}}/I_{\mathfrak{p}}
\end{array}$$

onde γ é um isomorfismo de $A_{\mathfrak{p}}/J_{\mathfrak{p}}$ -módulos e $\delta := \alpha_{\mathfrak{p}} \circ \gamma^{-1}$. Observando que a imagem do ideal maximal de $A_{\mathfrak{p}}/J_{\mathfrak{p}}$ por δ está contida no ideal maximal de $A_{\mathfrak{p}}/I_{\mathfrak{p}}$ (pois $\delta(\mathfrak{p}A_{\mathfrak{p}}/J_{\mathfrak{p}}) = \mathfrak{p}\delta(A_{\mathfrak{p}}/J_{\mathfrak{p}})$) e que $\delta \circ \gamma(\xi/1) = 1 + I_{\mathfrak{p}}$, concluímos que $\gamma(\xi/1)$ é uma unidade e portanto $\xi/1$ é uma base de $(\omega_J)_{\mathfrak{p}}$, o que conclui a demonstração do teorema 3.7. $\square$

Antes de encerrar esta sessão, notamos que o ideal J construído tem módulo conormal J/J^2 livre, de posto $n - 1$, sobre A/J . De fato, aplicando sucessivamente o “Splitting-off” de Serre (teorema 2.27) podemos escrever $J/J^2 = F \oplus P$, onde F é um A/J -módulo livre, de posto $n - 2$, e P um A/J -módulo projetivo de posto 1. Tomando uma base $\{e_1, \dots, e_{n-2}\}$ de F , definimos um A/J -homomorfismo

$$P \xrightarrow{\Phi} \text{Hom}_{A/J}(\text{Hom}_{A/J}(\wedge^{n-1}(J/J^2), A/J), A/J)$$

fazendo $\Phi(x)(f) := f(e_1 \wedge \dots \wedge e_{n-2} \wedge x)$, para todo $x \in P$ e todo $f \in \text{Hom}_{A/J}(\wedge^{n-1}(J/J^2), A/J)$. Provaremos que Φ é um isomorfismo e então, usando o teorema 3.5, teremos

$$\begin{aligned}
P &\cong \operatorname{Hom}_{A/J}(\omega_J, A/J) \\
&\cong \operatorname{Hom}_{A/J}(A/J, A/J) \\
&\cong A/J
\end{aligned}$$

e portanto J/J^2 será livre, de posto $n - 1$, como A/J -módulo.

Mostraremos que $\Phi_{\mathfrak{p}}$ é um isomorfismo, para todo ideal primo $\mathfrak{p}$ do anel $B := A/J$. Aplicando a proposição 2.4 construímos um diagrama comutativo

$$\begin{array}{ccc}
P_{\mathfrak{p}} & \xrightarrow{\Phi_{\mathfrak{p}}} & \operatorname{Hom}_B(\operatorname{Hom}_B(\wedge^{n-1}(J/J^2), B), B)_{\mathfrak{p}} \\
\parallel & & \downarrow \approx \\
P_{\mathfrak{p}} & \xrightarrow{\Psi} & \operatorname{Hom}_{B_{\mathfrak{p}}}(\operatorname{Hom}_{B_{\mathfrak{p}}}(\wedge^{n-1}(J/J^2)_{\mathfrak{p}}, B_{\mathfrak{p}}), B_{\mathfrak{p}})
\end{array}$$

onde $\Psi(x/s)(f) := f(\epsilon_1/1 \wedge \cdots \wedge \epsilon_{n-2}/1 \wedge x/s)$, para todo $x/s \in P_{\mathfrak{p}}$ e todo $f \in \operatorname{Hom}_{B_{\mathfrak{p}}}(\wedge^{n-1}(J/J^2)_{\mathfrak{p}}, B_{\mathfrak{p}})$. É fácil ver, agora, que Ψ é um isomorfismo, usando o fato que $P_{\mathfrak{p}} \cong B_{\mathfrak{p}}$ e $\wedge^{n-1}(J/J^2)_{\mathfrak{p}} \cong B_{\mathfrak{p}}$. Assim, $\Phi_{\mathfrak{p}}$ é um isomorfismo, como queríamos demonstrar.

3.3 O Teorema de Szpiro

Começamos com a seguinte proposição devida a Serre:

Proposição 3.10 ([Ser61]) *Seja A um anel Noetheriano e M um A -módulo finitamente gerado com dimensão projetiva menor ou igual a 1. Suponhamos que $\operatorname{Ext}_A^1(M, A)$ seja um A -módulo cíclico. Então existe uma sequência exata*

$$0 \longrightarrow A \longrightarrow P \longrightarrow M \longrightarrow 0$$

onde P é um A -módulo projetivo finitamente gerado.

Demonstração: Tomamos uma sequência exata de A -módulos

$$0 \longrightarrow K \xrightarrow{w} Q \longrightarrow M \longrightarrow 0$$

com Q projetivo, finitamente gerado. Dualizando obtemos a sequência exata

$$0 \longrightarrow M^* \longrightarrow Q^* \longrightarrow K^* \xrightarrow{\gamma} \operatorname{Ext}_A^1(M, A) \longrightarrow 0$$

Se η é um gerador de $\text{Ext}_A^1(M, A)$, tomamos $v \in K^*$ tal que $\gamma(v) = \eta$. Seja P o *push out* de $K \xrightarrow{v} A$ e $K \xrightarrow{w} Q$, isto é, $P := (Q \oplus A)/U$, onde $U := \{(w(x), -v(x)) \mid x \in K\}$. Temos o seguinte diagrama comutativo exato de A -módulos:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 & & K & = & K & & \\
 & & \downarrow \alpha & & \downarrow w & & \\
 0 & \longrightarrow & A & \longrightarrow & Q \oplus A & \longrightarrow & Q \longrightarrow 0 \quad (*) \\
 & & \parallel & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A & \longrightarrow & P & \longrightarrow & M \longrightarrow 0 \quad (**) \\
 & & & & \downarrow & & \downarrow \\
 & & & & 0 & & 0
 \end{array}$$

onde $\alpha := (w, -v)$, a sequência $(*)$ é a natural e a aplicação $P \longrightarrow M$ é definida de modo único a fazer o diagrama comutar. (A terceira linha pode ser obtida aplicando o “Lema da Cobra” (2.3) às duas primeiras.) Dualizando o diagrama acima obtemos:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & M^* & \longrightarrow & P^* & \longrightarrow & A^* \\
 & & \downarrow & & \downarrow & & \parallel \\
 0 & \longrightarrow & Q^* & \longrightarrow & Q^* \oplus A^* & \longrightarrow & A^* \longrightarrow 0 \\
 & & \downarrow & & \downarrow \alpha^* & & \\
 & & K^* & = & K^* & & \\
 & & \downarrow \gamma & & \downarrow & & \\
 & & \text{Ext}_A^1(M, A) & & \text{Ext}_A^1(P, A) & & \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
 \end{array}$$

e o “Lema da Cobra” leva à seqüência exata

$$0 \longrightarrow M^* \longrightarrow P^* \longrightarrow A^* \xrightarrow{\delta} \text{Ext}_A^1(M, A) \longrightarrow \text{Ext}_A^1(P, A) \longrightarrow 0$$

Observando que $\delta(id_A) = \gamma \circ \alpha^*(0, id_A) = \gamma(-v) = -\eta$, pela construção da aplicação de conexão δ , vemos que δ é sobrejetora e assim $\text{Ext}_A^1(P, A) = 0$. Juntando com a informação dada pela seqüência (**), de que $\dim \text{proj}(P) \leq 1$ (por 2.10), concluímos que P é projetivo. Com efeito, dualizando uma seqüência exata

$$0 \longrightarrow P_0 \longrightarrow P_1 \longrightarrow P \longrightarrow 0 \quad (1)$$

com P_0 e P_1 projetivos, finitamente gerados, obtemos

$$0 \longrightarrow P^* \longrightarrow P_1^* \longrightarrow P_0^* \longrightarrow 0. \quad (1^*)$$

Pelo corolário 2.6, P_0^* e P_1^* são projetivos. Logo a seqüência (1^*) cinde e teremos P^* projetivo (somando direto de um projetivo). Dualizando a seqüência (1^*) , obtemos o seguinte diagrama comutativo com linhas exatas:

$$\begin{array}{ccccccc} 0 & \longrightarrow & P_0 & \longrightarrow & P_1 & \longrightarrow & P \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & P_0^{**} & \longrightarrow & P_1^{**} & \longrightarrow & P^{**} \longrightarrow 0 \end{array} \quad \begin{array}{l} (1) \\ \\ (1^{**}) \end{array}$$

onde as aplicações verticais são as naturais. Notando que, pelo corolário 2.6, $P_0 \rightarrow P_0^{**}$ e $P_1 \rightarrow P_1^{**}$ são isomorfismos, temos que P é isomorfo a P^{**} e portanto é projetivo. $\square$

Por fim, apresentamos a demonstração de Teorema de Szpiro.

Teorema 3.11 ([Szp79]) *Seja A um anel de Cohen-Macaulay de dimensão $n := 3$ e $I < A$ um ideal de codimensão pura 2, localmente interseção completa em A . Suponhamos ainda que todo A -módulo projetivo, finitamente gerado, seja livre. Então I é uma interseção completa como conjunto.*

Demonstração: Com os resultados apresentados neste capítulo, esta demonstração praticamente se resume à observação de que certas hipóteses são satisfeitas.

Pelo teorema 3.7 temos garantida a existência de um ideal J , localmente interseção completa em A , com $\text{Rad}(J) = \text{Rad}(I)$ e tal que

$$\text{Ext}_A^1(J, A) \cong \text{Ext}_A^2(A/J, A) = \omega_J \cong A/J.$$

Logo $\text{Ext}_A^1(J, A)$ é cíclico. Como J é localmente gerado por seqüências regulares de dois elementos, segue que $\dim \text{proj}_A(A/J) = 2$ (por 2.13 e 2.9), o que implica em $\dim \text{proj}_A(J) = 1$ (por 2.10). Podemos então aplicar o teorema 3.10, obtendo uma seqüência exata

$$0 \longrightarrow A \longrightarrow P \longrightarrow J \longrightarrow 0$$

com P projetivo e finitamente gerado sobre A , logo livre. Verificamos facilmente (localizando em um ideal primo que *não* contém J , digamos) que o posto de P é 2 e portanto J é gerado por dois elementos. $\square$

Com a ajuda do teorema de Quillen-Suslin (2.29) temos imediatamente:

Corolário 3.12 *Todo ideal $I < k[X, Y, Z]$ de dimensão pura 1 que é localmente interseção completa é uma interseção completa como conjunto.* $\square$

Geometricamente este último corolário se traduz em:

Teorema 3.13 ([Szp79]) *Toda k -curva em $\mathbb{A}^3(L)$ que é localmente uma interseção completa é uma interseção completa como conjunto.* $\square$

Capítulo 4

O Teorema de Mohan Kumar

No capítulo anterior provamos que toda curva em $\mathbb{A}^3$ que é localmente uma interseção completa é uma interseção completa como conjunto. Nossa meta agora será generalizar este resultado para dimensões arbitrárias.

4.1 Preliminares

Proposição 4.1 *Sejam A um anel Noetheriano e $J \subseteq I$ ideais de A com $V(I) = V(J)$ e $\mu(I/J) =: m$. Então existem $a_1, \dots, a_m \in I$ tais que*

- $I = (a_1, \dots, a_m) + J$, isto é, as imagens de $a_1, \dots, a_m$ em I/J formam um sistema mínimo de geradores deste módulo;
- Para todo $\mathfrak{p} \in V(a_1, \dots, a_m) \setminus V(I)$ temos $h(\mathfrak{p}) \geq m$.

Demonstração: Construiremos indutivamente elementos $a_1, \dots, a_r$ cujas imagens $\overline{a_1}, \dots, \overline{a_r}$ em I/J fazem parte de um sistema mínimo de geradores, tais que

$$h(\mathfrak{p}) \geq r, \quad \forall \mathfrak{p} \in V(a_1, \dots, a_r) \setminus V(I).$$

Se $r = 0$, não há nada a fazer. Suponhamos construídos os elementos $a_1, \dots, a_r$ ($0 \leq r < m$). Escolhemos $a \in I$ tal que $\{\overline{a_1}, \dots, \overline{a_r}, \overline{a}\}$ esteja contido num sistema mínimo de geradores. Seja X o conjunto dos divisores primos minimais de $(a_1, \dots, a_r)$ que não pertencem a $V(I)$. Como A é Noetheriano, X é finito. Escrevemos $X = X_1 \dot{\cup} X_2$, onde

$$X_1 := \{\mathfrak{p} \in X \mid a \in \mathfrak{p}\};$$

$$X_2 := \{\mathfrak{p} \in X \mid a \notin \mathfrak{p}\}.$$

Como $J \not\subseteq \mathfrak{p}$, $\forall \mathfrak{p} \in X$ (pois $V(J) = V(I)$), temos $J \not\subseteq \bigcup X$ e podemos tomar $b \in J \setminus \bigcup X$. Se X_2 é não vazio, então $\bigcap X_2 \not\subseteq \bigcup X_1$ (do contrário, teríamos uma relação de inclusão entre elementos distintos de X) e portanto existe $\lambda \in \bigcap X_2 \setminus \bigcup X_1$. Por outro lado, se X_2 for vazio tomamos $\lambda := 1$. Definindo então $a_{r+1} := a + \lambda b$, temos $a_{r+1} \notin \bigcup X$.

Como $\overline{a_{r+1}} = \overline{a}$, $\{\overline{a_1}, \dots, \overline{a_{r+1}}\}$ é parte de um sistema mínimo de geradores de I/J .

Se $\mathfrak{p} \in V(a_1, \dots, a_{r+1}) \setminus V(I)$, então $\mathfrak{p}$ contém algum elemento de X , digamos $\mathfrak{p} \supseteq \mathfrak{q} \in X$. Mas $a_{r+1} \notin \mathfrak{q}$ e, assim, $\mathfrak{p} \neq \mathfrak{q}$. Logo $h(\mathfrak{p}) \geq r+1$, uma vez que, por construção, $h(\mathfrak{q}) \geq r$. $\square$

Lema 4.2 *Seja $I \leq A$ um ideal finitamente gerado tal que $I = I^2$. Então I é principal, gerado por um elemento idempotente.*

Demonstração: Suponhamos $I = (a_1, \dots, a_m)$. Como $I = I^2$, podemos escrever

$$a_i = \sum_{j=1}^m b_{ij} a_j, \quad \forall i = 1, \dots, m,$$

onde $b_{ij} \in I$, $\forall i, j$. Se $\mathcal{I}$ é a matriz identidade $m \times m$ e $\mathcal{B} := (b_{ij})$ temos

$$(\mathcal{I} - \mathcal{B}) \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = 0,$$

e multiplicando pela matriz adjunta de $\mathcal{I} - \mathcal{B}$ vemos que $\det(\mathcal{I} - \mathcal{B})a_i = 0$, $\forall i$. Podemos escrever $\det(\mathcal{I} - \mathcal{B}) = 1 - a$, onde $a \in I$, e temos então $(1 - a)I = 0$. Em particular,

- $(1 - a)a = 0$ e portanto a é idempotente;
- $(1 - a)a_i = 0$ e assim $a_i \in (a)$, $\forall i$. Logo $I = (a)$.

$\square$

Proposição 4.3 *Seja I um ideal de um anel Noetheriano A . Então*

$$\mu(I/I^2) > \dim(A) \implies \mu(I) = \mu(I/I^2).$$

Demonstração: Se $m := \mu(I/I^2) > \dim(A)$, pela proposição 4.1 existem $a_1, \dots, a_m$ em I tais que

$$\bullet \quad I = (a_1, \dots, a_m) + I^2; \quad (1)$$

$$\bullet \quad V(a_1, \dots, a_m) \setminus V(I) = \emptyset. \quad (2)$$

Sejam $\bar{A} := A/(a_1, \dots, a_m)$ e $\bar{I} := I/(a_1, \dots, a_m)$. Por (1) vemos que $\bar{I} = \bar{I}^2$ e portanto $\bar{I}$ é principal, gerado por um idempotente (lema 4.2). Por outro lado, (2) implica que $\bar{I}$ está contido no nilradical de $\bar{A}$. Logo $\bar{I} = 0$ e $\mu(I) = \mu(I/I^2)$. $\square$

Lema 4.4 *Seja dado um homomorfismo de A -módulos*

$$M \oplus N \xrightarrow{\alpha \oplus \beta} P.$$

Então se α for um isomorfismo entre M e P , temos $\text{Ker}(\alpha \oplus \beta) \cong N$.

Demonstração: A restrição da projeção em N a $\text{Ker}(\alpha \oplus \beta)$ é o isomorfismo procurado, uma vez que

$$\begin{aligned} \text{Ker}(\alpha \oplus \beta) &= \{(x, y) \in M \oplus N \mid \alpha(x) + \beta(y) = 0\} \\ &= \{(x, y) \in M \oplus N \mid x = -\alpha^{-1}(\beta(y))\} \\ &= \{(-\alpha^{-1}(\beta(y)), y) \mid y \in N\} \end{aligned}$$

$\square$

Proposição 4.5 *Sejam M um A_f -módulo e N um A_g -módulo tais que $M_g \cong N_f$ como A_{fg} -módulos. Então existe um A -módulo P tal que $P_f \cong M$ e $P_g \cong N$. Dizemos que P é a colagem de M e N sobre $D(fg)$.*

Demonstração: Seja $M \xrightarrow{\alpha} N_f$ a composta de um isomorfismo de A_{fg} -módulos $M_g \rightarrow N_f$ com a aplicação canônica $M \rightarrow M_g$. Se $N \xrightarrow{\beta} N_f$ é o homomorfismo canônico, definimos em $M \oplus N$ o A -submódulo $P := \text{Ker}(\alpha \oplus \beta)$. Usando o lema anterior verificamos que $P_f \cong M_f \cong M$ e $P_g \cong N_g \cong N$, uma vez que β_f e α_g são isomorfismos. $\square$

4.2 Demonstração

Provaremos agora o teorema central deste capítulo:

Teorema 4.6 ([MK78]) *Seja I um ideal de $k[X_1, \dots, X_n]$. Então*

$$\mu(I/I^2) \geq \dim k[X_1, \dots, X_n]/I + 2 \implies \mu(I) = \mu(I/I^2).$$

Começamos fazendo uma redução:

Lema 4.7 *Após uma mudança de variáveis, podemos assumir que I contém um polinômio mônico em X_n .*

Demonstração: Como $I \neq (0)$, existe em I um polinômio F não constante. Se

$$F = \sum a_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n},$$

fazendo a mudança de variáveis

$$X_i \longmapsto X_i + X_n^{r_i} \quad (i = 1, \dots, n-1)$$

obtemos um polinômio

$$\tilde{F} = \sum a_\alpha (X_1 + X_n^{r_1})^{\alpha_1} \dots (X_{n-1} + X_n^{r_{n-1}})^{\alpha_{n-1}} X_n^{\alpha_n},$$

ou

$$\tilde{F} = \sum a_\alpha (X_n^{\alpha_n + \alpha_1 r_1 + \dots + \alpha_{n-1} r_{n-1}} + (\text{termos de menor grau em } X_n)).$$

Se tomarmos $t > \max\{\partial_{X_i} F \mid i = 1, \dots, n\}$ e definirmos $r_i := t^i$, os números $\alpha_n + \alpha_1 t + \dots + \alpha_{n-1} t^{n-1}$ serão *distintos* para os diferentes índices $\alpha = (\alpha_1, \dots, \alpha_n)$ com $a_\alpha \neq 0$. De fato, se $a_\alpha \neq 0 \neq a_\beta$ e

$$\alpha_n + \alpha_1 t + \dots + \alpha_{n-1} t^{n-1} = \beta_n + \beta_1 t + \dots + \beta_{n-1} t^{n-1},$$

então t divide $\alpha_n - \beta_n$ e, como $|\alpha_n - \beta_n| < t$, temos $\alpha_n = \beta_n$. Assim,

$$\alpha_1 + \alpha_2 t + \dots + \alpha_{n-1} t^{n-2} = \beta_1 + \beta_2 t + \dots + \beta_{n-1} t^{n-2}$$

e prosseguindo de modo análogo concluímos que $\alpha = \beta$.

Fazendo então $m := \max\{\alpha_n + \alpha_1 t + \cdots + \alpha_{n-1} t^{n-1} \mid a_\alpha \neq 0\}$ podemos escrever

$$\tilde{F} = a X_n^m + \rho_1 X_n^{m-1} + \cdots + \rho_m,$$

onde $a \in k^\times$ e $\rho_j \in k[X_1, \dots, X_{n-1}]$. Por fim, multiplicando por a^{-1} obtemos o polinômio procurado. $\square$

Façamos $B := k[X_1, \dots, X_{n-1}]$, $X := X_n$ e $A := k[X_1, \dots, X_n] = B[X]$.

Proposição 4.8 *Existem f e g em B tais que $\text{Spec}(A) = D(f) \cup D(g)$, $I_g = A_g$ e I_f é gerado por $m := \mu(I/I^2)$ elementos.*

Demonstração: Seja $a_1 \in I$ cuja imagem em I/I^2 pertence a um sistema mínimo de geradores. Podemos assumir que a_1 é mônico em X , pois somando uma potência suficientemente grande de um polinômio mônico de I a a_1 obteríamos um elemento da forma desejada. Então $\bar{A} := A/(a_1)$ é um B -módulo finitamente gerado, logo uma extensão inteira de B .

Definimos então $J := I \cap B$ e $\tilde{A} := \bar{A}/J^2\bar{A}$ e representamos as imagens de ideais ou elementos de A em $\bar{A}$ e $\tilde{A}$ por *barras e tís*, respectivamente.

Representando por “ c ” e “ e ” as contrações de ideais em B e extensões em $\bar{A}$, respectivamente, temos $\bar{I}^c = J$ e, portanto, $(J\bar{A})^c = \bar{I}^{cec} = \bar{I}^c = J$. Assim $\bar{A}/\bar{I}$ e $\bar{A}/J\bar{A}$ são extensões inteiras de B/J e

$$\begin{aligned} \dim(A/I) &= \dim(\bar{A}/\bar{I}) \quad (\text{pois } A/I \cong \bar{A}/\bar{I}) \\ &= \dim(\bar{A}/J\bar{A}) \\ &= \dim(\tilde{A}) \quad (\text{pois } V(J^2\bar{A}) = V(J\bar{A})). \end{aligned}$$

Verificamos que $\mu(\tilde{I}/\tilde{I}^2) = \mu(I/I^2) - 1 = m - 1$, uma vez que

$$\begin{aligned} \tilde{I} = (\tilde{a}_2, \dots, \tilde{a}_r) + \tilde{I}^2 &\iff \bar{I} = (\bar{a}_2, \dots, \bar{a}_r) + \bar{I}^2 \quad (\text{pois } J^2\bar{A} \subseteq \bar{I}^2) \\ &\iff I = (a_1, \dots, a_r) + I^2 \end{aligned}$$

Usando nossa hipótese temos, então,

$$\mu(\tilde{I}/\tilde{I}^2) = \mu(I/I^2) - 1 > \dim(A/I) = \dim(\tilde{A})$$

e, pela proposição 4.3,

$$\mu(\tilde{I}) = \mu(\tilde{I}/\tilde{I}^2) = m - 1.$$

Se $\tilde{I} = (\tilde{a}_2, \dots, \tilde{a}_m)$, levantando para $\bar{A}$ obtemos

$$\bar{I} = (\bar{a}_2, \dots, \bar{a}_m) + J^2\bar{A} = (\bar{a}_2, \dots, \bar{a}_m) + J\bar{A} \cdot \bar{I}.$$

Tomaremos agora anéis de frações com relação ao sistema multiplicativo $S := 1 + J$, para que possamos usar o Lema de Nakayama. Como todo elemento de $1 + J_S$ é uma unidade em B_S , J_S está contido no radical de Jacobson de B_S e, como $\bar{A}_S$ é inteiro sobre B_S , verificamos facilmente que $J_S\bar{A}_S$ está contido no radical de Jacobson de $\bar{A}_S$. Com efeito, se $\mathfrak{M} \in \text{Max}(\bar{A}_S)$ então sua contração $\mathfrak{m}$ em B_S é maximal e portanto $J_S \subseteq \mathfrak{m}$ e

$$J_S\bar{A}_S \subseteq \mathfrak{m}\bar{A}_S \subseteq \mathfrak{M}.$$

Assim, pelo Lema de Nakayama,

$$\bar{I}_S = (\bar{a}_2, \dots, \bar{a}_m)_S + J_S\bar{A}_S \cdot \bar{I}_S \implies \bar{I}_S = (\bar{a}_2, \dots, \bar{a}_m)_S$$

e, levantando para A_S , temos $I_S = (a_1, \dots, a_m)_S$. Existe, então, $f \in S$ tal que

$$I_f = (a_1, \dots, a_m)_f.$$

Definindo $g := 1 - f$ temos $\text{Spec}(A) = D(f) \cup D(g)$ e $I_g = A_g$, uma vez que $g \in J \subseteq I$. $\square$

Consideramos, então, a seqüência exata

$$0 \longrightarrow K \longrightarrow A_f^m \longrightarrow I_f \longrightarrow 0 \quad (*)$$

relativa ao sistema de geradores $a_1, \dots, a_m$ de I_f . Localizando em g obtemos

$$0 \longrightarrow K_g \longrightarrow A_{fg}^m \longrightarrow I_{fg} \longrightarrow 0. \quad (**)$$

Vemos então que K_g é *projetivo* sobre $A_{fg} = B_{fg}[X]$, uma vez que $I_{fg} = A_{fg}$ e, portanto, a seqüência acima cinde. Localizando (**) em a_1 obtemos

$$0 \longrightarrow (K_g)_{a_1} \longrightarrow (A_{fg})_{a_1}^m \xrightarrow{\psi} (I_{fg})_{a_1} \longrightarrow 0.$$

Como a_1 é uma unidade em $(A_{fg})_{a_1}$, $(K_g)_{a_1}$ é livre, de posto $m - 1$, sobre $(A_{fg})_{a_1} = B_{fg}[X]_{a_1}$ (por 4.4, tomando $M := (A_{fg})_{a_1}$, $N := (A_{fg})_{a_1}^{m-1}$, $P := (I_{fg})_{a_1}$ e α e β tais que $\alpha \oplus \beta = \psi$). Logo, pelo teorema de Quillen-Suslin (2.28), K_g é na verdade *livre* sobre A_{fg} (de posto $m - 1$). Assim,

pela proposição 4.5 podemos tomar um A -módulo M tal que $M_f \cong K$ e $M_g \cong A_g^{m-1}$.

O homomorfismo canônico

$$\mathrm{Ext}_A^1(I, M) \longrightarrow \mathrm{Ext}_{A_f}^1(I_f, M_f),$$

que associa um elemento correspondente a extensão

$$0 \longrightarrow M \longrightarrow E \longrightarrow I \longrightarrow 0$$

ao elemento correspondente à sua localização em f , é um *isomorfismo*, pois o é quando localizado em f e g , uma vez que

$$\mathrm{Ext}_A^1(I, M)_g \cong \mathrm{Ext}_{A_g}^1(I_g, M_g) = \mathrm{Ext}_{A_g}^1(A_g, M_g) = 0$$

e

$$\mathrm{Ext}_{A_f}^1(I_f, M_f)_g \cong \mathrm{Ext}_{A_{fg}}^1(I_{fg}, M_{fg}) = \mathrm{Ext}_{A_{fg}}^1(A_{fg}, M_{fg}) = 0.$$

Logo a sequência exata

$$0 \longrightarrow M_f \longrightarrow A_f^m \longrightarrow I_f \longrightarrow 0,$$

obtida a partir de $(*)$, é a localização de uma extensão

$$0 \longrightarrow M \longrightarrow P \longrightarrow I \longrightarrow 0.$$

P_f e P_g são livres, de posto m , sobre A_f e A_g respectivamente, logo P é um A -módulo projetivo finitamente gerado, de posto m . Pelo teorema de Quillen-Suslin (2.29), P é livre, de posto m , e portanto $\mu(I) \leq m = \mu(I/I^2)$, o que conclui a demonstração do teorema 4.6. $\square$

Podemos agora concluir este capítulo demonstrando o teorema:

Teorema 4.9 ([MK78]) *Todo ideal $I < A := k[X_1, \dots, X_n]$ de dimensão pura 1 que é localmente uma interseção completa é uma interseção completa como conjunto.*

Demonstração:

- Se $n = 2$ o resultado é imediato, pois neste caso *todo* ideal de dimensão pura 1 é uma interseção completa como conjunto. Com efeito, o radical de tal ideal é principal, uma vez que é uma interseção finita de ideais primos de altura 1 e estes, por sua vez, são principais, gerados por polinômios irredutíveis.
- Se $n = 3$, o resultado já foi provado (corolário 3.12).
- Se $n > 3$, pelos métodos da sessão 3.2 construímos um ideal $J < A$ com $\text{Rad}(J) = \text{Rad}(I)$ e J/J^2 livre, de posto $n - 1$, como A/J -módulo. Temos então

$$\mu(J/J^2) = n - 1 \geq 3 = \dim(A/J) + 2$$

e portanto

$$\mu(J) = \mu(J/J^2) = n - 1 = h(J),$$

pelo teorema 4.6.

□

Geometricamente temos:

Teorema 4.10 ([MK78]) *Toda k -curva em $\mathbb{A}^n(L)$ que é localmente uma interseção completa é uma interseção completa como conjunto.* □

Pelo exemplo 1.6 temos imediatamente o seguinte corolário:

Corolário 4.11 *Toda curva afim não singular em $\mathbb{A}^n(L)$ é uma interseção completa como conjunto.* □

Capítulo 5

O Teorema de Cowsik-Nori

Dentre as consequências do teorema de Mohan Kumar temos o seguinte teorema, devido a Cowsik e Nori:

Teorema 5.1 ([CN78]) *Toda curva afim em característica $p > 0$ é uma interseção completa como conjunto.*

Nosso objetivo agora será provar este teorema no caso particular de curvas *irredutíveis* definidas sobre corpos *infinitos*.

5.1 Preliminares

Proposição 5.2 *Todo corpo k de característica $p > 0$ admite uma extensão perfeita $k^{\frac{1}{p^\infty}}$.*

Demonstração: Tomando um fecho algébrico $\bar{k}$ de k definimos, para todo $r \geq 0$,

$$k^{\frac{1}{p^r}} := \{x \in \bar{k} \mid x^{p^r} \in k\}.$$

É fácil ver que $k^{\frac{1}{p^r}}$ é um corpo, precisamente o corpo de raízes do conjunto de polinômios $\{X^{p^r} - a \mid a \in k\}$. Temos portanto uma cadeia de corpos

$$k \subseteq k^{\frac{1}{p}} \subseteq k^{\frac{1}{p^2}} \subseteq k^{\frac{1}{p^3}} \subseteq \dots$$

e definimos o corpo

$$k^{\frac{1}{p^\infty}} := \bigcup_{r \geq 0} k^{\frac{1}{p^r}}.$$

Verificamos facilmente que $k^{\frac{1}{p^\infty}} = \left(k^{\frac{1}{p^\infty}}\right)^p$ e, portanto, $k^{\frac{1}{p^\infty}}$ é perfeito. $\square$

Teorema 5.3 *Seja $k(x_1, \dots, x_n)$ uma extensão de k com grau de transcendência 1. Então existe um polinômio $f \in k[T_1, \dots, T_n]$ não nulo tal que para toda n -upla $c = (c_1, \dots, c_n) \in k^n$ com $f(c) \neq 0$ temos $k[x_1, \dots, x_n]$ inteiro sobre $k[\sum c_i x_i]$.*

Demonstração: [Lan93, Cap. VIII, Corolário 2.3] $\square$

Definição 5.4 *Dada uma extensão de anéis $B|A$ definimos o condutor de B em A :*

$$C_{B|A} := \{a \in A \mid aB \subseteq A\}.$$

Proposição 5.5 *Temos as seguintes propriedades:*

- $C_{B|A}$ é o maior B -ideal contido em A ;
- $B = A \iff C_{B|A} = (1)$;
- Se B é finitamente gerado como A -módulo, então para todo sistema multiplicativo S de A temos $(C_{B|A})_S = C_{B_S|A_S}$.

Demonstração: Os dois primeiros itens e a inclusão $(C_{B|A})_S \subseteq C_{B_S|A_S}$ são imediatos da definição. Provaremos que $C_{B_S|A_S} \subseteq (C_{B|A})_S$. Seja $a/s \in C_{B_S|A_S}$ e suponhamos que B seja gerado como A -módulo pelos elementos $b_1, \dots, b_r$. Então $ab_i/s \in A_S$ e assim existe $s_i \in S$ tal que $s_i ab_i \in A$, $\forall i$. Fazendo $t := \prod s_i$ temos $ta \in C_{B|A}$ e $a/s = ta/ts \in (C_{B|A})_S$. $\square$

Proposição 5.6 *Toda k -álgebra Artiniana de tipo finito é um k -espaço vetorial de dimensão finita.*

Demonstração: Seja A uma k -álgebra Artiniana de tipo finito. Como A é, em particular, um anel Noetheriano, existe r tal que a r -ésima potência do nilradical de A é nula. Se $\text{Spec}(A) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_n\}$ temos

$$A \cong \prod_{i=1}^n A/\mathfrak{m}_i^r$$

e basta mostrar, então, que cada k -álgebra Artiniana local de tipo finito $A_i := A/\mathfrak{m}_i^r$ tem k -dimensão finita.

Se $\mathfrak{M} := \mathfrak{m}_i/\mathfrak{m}_i^r$, então $K := A_i/\mathfrak{M}$ é uma extensão finita de k , pelo *Nullstellensatz*. Como $\mathfrak{M}^r = 0$ temos uma cadeia

$$0 = \mathfrak{M}^r \subseteq \mathfrak{M}^{r-1} \subseteq \dots \subseteq \mathfrak{M}^2 \subseteq \mathfrak{M}$$

onde cada quociente $\mathfrak{M}^j/\mathfrak{M}^{j+1}$ tem dimensão finita sobre K e, *a fortiori*, sobre k . Assim $\mathfrak{M}$ e $A_i/\mathfrak{M}$ têm k -dimensões finitas, logo $\dim_k A_i < \infty$. $\square$

5.2 Demonstração

Provaremos o teorema de Cowsik-Nori (5.1) — no caso particular de curvas *irredutíveis* definidas sobre corpos *infinitos* — seguindo a demonstração apresentada por Lyubeznik em [Lyu89]. Equivalentemente, podemos enunciar:

Teorema 5.7 *Sejam $R := k[X_1, \dots, X_n]$, onde k é um corpo infinito de característica $p > 0$, e $\mathfrak{P} < R$ um ideal primo de dimensão 1. Então $\mathfrak{P}$ é uma interseção completa como conjunto.*

Podemos assumir $n \geq 3$, pois do contrário o resultado seria trivial. Começaremos mostrando que podemos fazer algumas reduções.

Lema 5.8 *Se o teorema 5.7 é válido para corpos perfeitos, então também é válido em geral. Logo podemos assumir que k é perfeito.*

Demonstração: Tomando $\overline{R} := k^{\frac{1}{p^\infty}}[X_1, \dots, X_n]$ (ver proposição 5.2), temos uma extensão inteira $\overline{R}|R$, pois para todo $f \in \overline{R}$ existe N tal que $f^{p^N} \in R$, pela construção de $k^{\frac{1}{p^\infty}}$. Assim, existe $\overline{\mathfrak{P}} \in \text{Spec}(\overline{R})$ tal que $\overline{\mathfrak{P}} \cap R = \mathfrak{P}$ e, como $\dim(\overline{R}/\overline{\mathfrak{P}}) = \dim(R/\mathfrak{P}) = 1$, segue que $\overline{\mathfrak{P}}$ também tem dimensão 1.

Por hipótese, portanto, $\overline{\mathfrak{P}}$ é gerado *a menos de radical* por $n - 1$ elementos, digamos $f_1, \dots, f_{n-1}$. Mas para N suficientemente grande temos $f_1^{p^N}, \dots, f_{n-1}^{p^N} \in R$ e, assim, podemos assumir que $f_i \in R, \forall i$. Concluímos a demonstração verificando que $\mathfrak{P} = \text{Rad}((f_1, \dots, f_{n-1})R)$.

Se $f \in \mathfrak{P} \subseteq \overline{\mathfrak{P}} = \text{Rad}((f_1, \dots, f_{n-1})\overline{R})$ temos, para algum m , uma equação

$$f^m = \sum_{i=1}^{n-1} g_i f_i,$$

com $g_i \in \overline{R}$. Tomando N tal que $g^{p^N} \in R, \forall i$, temos

$$(f^m)^{p^N} = \sum_{i=1}^{n-1} g_i^{p^N} f_i^{p^N} \in (f_1, \dots, f_{n-1})R,$$

e portanto $f \in \text{Rad}((f_1, \dots, f_{n-1})R)$. Reciprocamente temos

$$\text{Rad}((f_1, \dots, f_{n-1})R) \subseteq \text{Rad}((f_1, \dots, f_{n-1})\overline{R}) \cap R = \overline{\mathfrak{P}} \cap R = \mathfrak{P}.$$

□

Seja $B := R/\mathfrak{P}$. Representando por x_i a imagem da indeterminada X_i em B , podemos escrever $B = k[x_1, \dots, x_n]$. Definimos então $A := k[x_1, x_2]$, a imagem de $k[X_1, X_2]$ em B , e os corpos de frações $F := k(x_1, \dots, x_n)$ e $E := k(x_1, x_2)$.

Lema 5.9 *Após uma mudança de coordenadas, podemos assumir que a extensão $B|A$ é inteira e $E = F$.*

Demonstração: Provaremos o lema em uma série de pequenos passos:

- $F = k(x_1, \dots, x_n)$ é uma extensão finita e separável de algum $k(x_i)$.

Demonstração. Como $\dim(B) = 1$, vemos que F tem grau de transcendência 1 sobre k . Provaremos assim, por indução em n , que todo corpo $k(y_1, \dots, y_n)$ com grau de transcendência ≤ 1 sobre k é uma extensão finita e separável de algum $k(y_i)$.

Suponhamos inicialmente $n = 2$. Como o grau de transcendência de $k(y_1, y_2)|k$ é ≤ 1 , existe $f \in k[T_1, T_2]$ não nulo, que podemos supor irreduzível, tal que $f(y_1, y_2) = 0$. Afirmamos que alguma das derivadas parciais de f é diferente de zero. Do contrário, todos os expoentes das indeterminadas T_1 e T_2 seriam múltiplos de p e, escrevendo $f = \sum a_{ij} T_1^{pi} T_2^{pj}$ e tomando elementos $b_{ij} \in k$ tais que $b_{ij}^p = a_{ij}$ (k é perfeito!), teríamos

$$f = \left(\sum b_{ij} T_1^i T_2^j \right)^p,$$

contradizendo a irreduzibilidade de f . Supondo $\partial f / \partial T_2 \neq 0$ segue que $k(y_1, y_2)$ é uma extensão finita e separável de $k(y_1)$.

Suponhamos agora $n > 2$. Pela hipótese de indução, $k(y_1, \dots, y_{n-1})$ é uma extensão finita e separável de $k(y_i)$, para algum i . Logo $k(y_1, \dots, y_n) | k(y_i, y_n)$ é finita e separável e, como $k(y_i, y_n)$ é finita e separável sobre $k(y_i)$ ou $k(y_n)$, pelo caso $n = 2$, o resultado segue. $\square$

Assim, reenumerando as variáveis se necessário, podemos assumir que F é uma extensão finita e separável de $K := k(x_1)$. Definimos os conjuntos

$$\mathfrak{V} := \{(c_1, \dots, c_n) \in \mathbb{A}^n(k) \mid B \text{ é inteiro sobre } k[y], \text{ onde } y := \sum_{i=1}^n c_i x_i\}$$

e

$$\mathfrak{W} := \{(c_1, \dots, c_n) \in \mathbb{A}^n(k) \mid F = K(y), \text{ onde } y := x_2 + \sum_{i=3}^n c_i x_i\}.$$

- $\mathfrak{V}$ contém um aberto de Zariski não vazio da hipersuperfície H definida por $X_2 = 1$.

Demonstração. Pelo teorema 5.3, existe $f \in k[T_1, \dots, T_n] \setminus \{0\}$ tal que

$$\mathbb{A}^n(k) \setminus Z(f) \subseteq \mathfrak{V}.$$

Como o corpo k é infinito, este aberto é não vazio.

Mais uma vez por k ser infinito, $\mathbb{A}^n(k)$ é irreduzível e, assim, todo aberto não vazio de $\mathbb{A}^n(k)$ é denso. Logo $\mathbb{A}^n(k) \setminus Z(f)$ intercepta o aberto definido por $X_2 \neq 0$, ou seja, contém um ponto $(c_1, \dots, c_n)$ com $c_2 \neq 0$. Fazendo $g := f(c_2 T_1, \dots, c_2 T_n)$, é imediato que $\mathbb{A}^n(k) \setminus Z(g)$ ainda está contido em $\mathfrak{V}$, uma vez que os pontos de $Z(g)$ e $Z(f)$ diferem apenas por uma multiplicação por uma constante não nula. É claro, também, que $\mathbb{A}^n(k) \setminus Z(g)$ intercepta H . Logo $\mathfrak{V} \supseteq (\mathbb{A}^n(k) \setminus Z(g)) \cap H \neq \emptyset$. $\square$

- $\mathfrak{W}$ contém um aberto de Zariski não vazio de H .

Demonstração. Como $F|K$ é finita e separável, pelo teorema do elemento primitivo existe $y \in F$ tal que $F = K(y)$ ([Lan93, Cap. V, Teorema 4.6]). Recordaremos rapidamente a demonstração deste teorema, para ver como este

elemento primitivo y é construído. Sejam $\sigma_1, \dots, \sigma_r$ ($r = [K(x_2, x_3) : K]$) os diferentes *embeddings* de $K(x_2, x_3)$ em $\overline{K}$ sobre K . Seja

$$P := \prod_{i \neq j} (\sigma_i(x_2) + T\sigma_i(x_3) - \sigma_j(x_2) - T\sigma_j(x_3)).$$

É fácil ver que P é um polinômio de $K[T]$: P é invariante por todo automorfismo sobre K do *compositum* $\sigma_1 K(x_2, x_3) \dots \sigma_r K(x_2, x_3)$ — uma extensão *Galoisiana* de K —, uma vez que estes automorfismos apenas induzem uma permutação nos *embeddings* $\sigma_1, \dots, \sigma_r$. Como $P \neq 0$, existe um elemento c , que *podemos supor em k* , tal que $P(c) \neq 0$. Assim $\sigma_i(x_2 + cx_3)$ ($i = 1, \dots, r$) são distintos, logo $K(x_2 + cx_3)$ tem grau $\geq r$ sobre K . Mas $r = [K(x_2, x_3) : K]$ e portanto $K(x_2, x_3) = K(x_2 + cx_3)$. Prosseguindo a construção de modo análogo, obtemos polinômios não nulos $f_i \in K[T_i]$ ($i = 3, \dots, n$) tais que, para $c_3, \dots, c_n \in k$,

$$f_i(c_i) \neq 0, \forall i \implies F = K(x_2 + \sum_{i=3}^n c_i x_i).$$

Fazendo $f := \prod_{i=3}^n f_i$ temos

$$f(c_3, \dots, c_n) \neq 0 \implies F = K(x_2 + \sum_{i=3}^n c_i x_i).$$

Podemos tomar $g \in k[T_1, T_3, \dots, T_n]$ e $h \in k[T_1]$ tais que

$$f = \frac{g(x_1, T_3, \dots, T_n)}{h(x_1)}$$

e, como x_1 é transcendente sobre k ,

$$\begin{aligned} g(c_1, c_3, \dots, c_n) \neq 0 &\implies g(T_1, c_3, \dots, c_n) \neq 0 \\ &\implies g(x_1, c_3, \dots, c_n) \neq 0 \\ &\implies f(c_3, \dots, c_n) \neq 0 \\ &\implies F = K(x_2 + \sum_{i=3}^n c_i x_i). \end{aligned}$$

Logo $\mathfrak{W}$ contém $\mathbb{A}^n(k) \setminus Z(g)$, um aberto não vazio de $\mathbb{A}^n(k)$ que obviamente intercepta H . $\square$

Podemos agora concluir a demonstração do lema. H é irredutível, logo todo aberto não vazio em H é denso. Assim $\mathfrak{W} \cap \mathfrak{W} \cap H \neq \emptyset$ e podemos tomar $(c_1, 1, c_3, \dots, c_n) \in \mathfrak{W} \cap \mathfrak{W}$. Fazendo em $R = k[X_1, \dots, X_n]$ a mudança de variáveis

$$Y_2 := c_1 X_1 + X_2 + c_3 X_3 + \dots + c_n X_n$$

$$Y_i := X_i \quad (i \neq 2)$$

e representando por y_i as imagens das novas variáveis em B , temos $B = k[y_1, \dots, y_n]$ inteiro sobre $k[y_2]$ e, *a fortiori*, sobre $k[y_1, y_2]$. Mais ainda,

$$F = k(x_1, x_2 + \sum_{i=3}^n c_i x_i) = k(x_1, c_1 x_1 + x_2 + \sum_{i=3}^n c_i x_i) = k(y_1, y_2),$$

concluindo a demonstração do lema. $\square$

Sejam $C := C_{B|A}$, o condutor de B em A , e $\overline{B} := B/C$.

Proposição 5.10 *$\overline{B}$ é Artiniano e, portanto, um k -espaço vectorial de dimensão finita, pela proposição 5.6.*

Demonstração: Como B é um domínio de dimensão 1, basta mostrar que $C \neq 0$. Mas isto é imediato, pois tomando $S := A \setminus \{0\}$ temos $A_S = B_S$, uma vez que $A_S = E = F \supseteq B_S$. Da proposição 5.5 segue então

$$C_S = C_{B_S|A_S} = (1) \implies C \cap S \neq \emptyset.$$

$\square$

Escrevemos $\overline{B} = k[\overline{x}_1, \dots, \overline{x}_n]$, onde $\overline{x}_i$ é a imagem da indeterminada X_i , e para $i = 3, \dots, n$ e todo $r \geq 0$ definimos $L_{i,r}$ como o k -subespaço de $\overline{B}$ gerado por $\{\overline{x}_i^{p^j} \mid j \geq r\}$, isto é:

$$L_{i,r} := \langle \overline{x}_i^{p^r}, \overline{x}_i^{p^{r+1}}, \overline{x}_i^{p^{r+2}}, \dots \rangle.$$

Temos então cadeias descendentes de k -subespaços

$$L_{i,0} \supseteq L_{i,1} \supseteq L_{i,2} \supseteq \dots \supseteq L_{i,r} \supseteq \dots$$

e, como a k -dimensão de $\overline{B}$ é finita, todas estas cadeias são estacionárias. Assim, existe r tal que

$$\overline{x}_i^{p^r} \in L_{i,r+1}, \quad \forall i,$$

e obtemos equações

$$\overline{x_i}^{p^r} + a_{i,1} \overline{x_i}^{p^{r+1}} + a_{i,2} \overline{x_i}^{p^{r+2}} + \cdots + a_{i,t_i} \overline{x_i}^{p^{r+t_i}} = 0,$$

onde $a_{i,j} \in k$. Levantando estas equações para $R = k[X_1, \dots, X_n]$ temos

$$X_i^{p^r} + a_{i,1} X_i^{p^{r+1}} + a_{i,2} X_i^{p^{r+2}} + \cdots + a_{i,t_i} X_i^{p^{r+t_i}} + c_i = f_i \in \mathfrak{P},$$

onde $c_i \in k[X_1, X_2]$.

Introduzimos novas variáveis $Y_i := X_i^{p^r}$ ($i = 3, \dots, n$), $Y_1 := X_1$ e $Y_2 := X_2$ e definimos um novo anel de polinômios

$$R' := k[Y_1, \dots, Y_n].$$

Como a extensão $R|R'$ é inteira, vemos que $\mathfrak{P}' := \mathfrak{P} \cap R'$ também tem dimensão 1.

Proposição 5.11 $\mathfrak{P}'$ é uma interseção completa como conjunto.

Demonstração: Pelo Teorema de Mohan Kumar (4.9), é suficiente mostrar que $\mathfrak{P}'$ é localmente uma interseção completa, uma vez que $\mathfrak{P}'$ é um ideal de dimensão pura 1 do anel de polinômios R' .

Reescrevendo os polinômios f_i usando as novas variáveis temos

$$f_i = Y_i + a_{i,1} Y_i^{p^r} + a_{i,2} Y_i^{p^{2r}} + \cdots + a_{i,t_i} Y_i^{p^{t_i r}} + c_i(Y_1, Y_2) \in \mathfrak{P}'.$$

e vemos que

$$\frac{\partial(f_3, \dots, f_n)}{\partial(Y_3, \dots, Y_n)} = \text{Identidade}.$$

Afirmamos que $I := (f_3, \dots, f_n)R'$ é um ideal de dimensão pura 2 e $R'' := R'/I$ é um anel *regular*. Com efeito, seja $\mathfrak{p} \in V(I) \subseteq \text{Spec}(R')$. A matriz Jacobiana

$$\mathcal{J} := \left(\frac{\partial f_i}{\partial Y_j} \right)$$

tem posto $n-2$ quando reduzida módulo $\mathfrak{p}$. Logo, pelo Critério do Jacobiano (2.22), $h(I_{\mathfrak{p}}) \geq n-2$. Por outro lado, $h(I_{\mathfrak{p}}) \leq \mu(I_{\mathfrak{p}}) \leq n-2$, e portanto $h(I_{\mathfrak{p}}) = n-2$. Assim I tem codimensão pura $n-2$ e, conseqüentemente, R'' tem dimensão 2.

Como o ideal J de R'' gerado pelas imagens dos menores $(n-2) \times (n-2)$ de $\mathcal{J}$ é o próprio R'' , usando o segundo item do teorema 2.22 concluímos que R'' é regular.

Assim $\mathfrak{P}'' := \mathfrak{P}'/I$ é um ideal primo de codimensão 1 em R'' . Como as localizações de R'' são domínios fatoriais (por 2.23), $\mathfrak{P}''$ é gerado localmente por apenas um elemento e portanto $\mathfrak{P}'$ é gerado localmente por $n-1$ elementos. $\square$

Sejam $g_1, \dots, g_{n-1} \in R'$ tais que $\mathfrak{P}' = \text{Rad}((g_1, \dots, g_{n-1})R')$. Para todo $f \in R$ temos $f^{p^r} \in R'$ e assim

$$\begin{aligned} f \in \mathfrak{P} &\implies f^{p^r} \in \mathfrak{P}' = \text{Rad}((g_1, \dots, g_{n-1})R') \subseteq \text{Rad}((g_1, \dots, g_{n-1})R); \\ f \in \text{Rad}((g_1, \dots, g_{n-1})R) &\implies \exists m \mid f^m \in (g_1, \dots, g_{n-1})R \\ &\implies (f^m)^{p^r} \in (g_1, \dots, g_{n-1})R' \subseteq \mathfrak{P}' \subseteq \mathfrak{P} \\ &\implies f \in \mathfrak{P}. \end{aligned}$$

Logo $\mathfrak{P} = \text{Rad}((g_1, \dots, g_{n-1})R)$, concluindo a prova do teorema 5.7. $\square$

Índice de Notações

k	um corpo
$\bar{k}$	fecho algébrico do corpo k
L	uma extensão algebricamente fechada de k
A	um anel
$\dim(A)$	dimensão de Krull do anel A
$\text{codim}(V)$	codimensão da variedade V
$\dim_{\text{proj}_A}(M)$	dimensão projetiva do A -módulo M
$d(I, M)$	I -profundidade de M (definida na sessão 2.3)
$d(M)$	profundidade de M (definida na sessão 2.3)
$\text{Spec}(A)$	espectro do anel A
$\text{Max}(A)$	espectro maximal do anel A
$D(f)$	conjunto dos ideais primos que não contêm o elemento f
$V(I)$	conjunto dos ideais primos que contêm o ideal I
$I(V)$	ideal de definição da variedade V
$Z(f)$	conjunto dos zeros do polinômio f
$h(I)$	altura do ideal I
$\text{Rad}(I)$	radical do ideal I

$(x_1, \dots, x_n)$	ideal gerado pelos elementos $x_1, \dots, x_n$
$\langle x_1, \dots, x_n \rangle$	submódulo ou subespaço vetorial gerado pelos elementos $x_1, \dots, x_n$
$\mu(M)$	número mínimo de geradores do módulo M
$\mu_{\mathfrak{p}}(M)$	número mínimo de geradores da localização $M_{\mathfrak{p}}$
$Z(M)$	divisores de zero do módulo M
$\text{Ann}(M)$	anulador do módulo M
$\text{Supp}(M)$	suporte do módulo M
$\text{Ass}(M)$	conjunto dos ideais primos associados do módulo M
$\mathbb{A}^n, \mathbb{A}^n(L)$	espaço afim n -dimensional sobre o corpo L
$\mathbb{A}^n(k)$	espaço afim n -dimensional sobre o corpo k
$\mathbb{R}$	conjunto dos números reais
$\mathbb{C}$	conjunto dos números complexos
A_S, M_S	anel ou módulo de frações com relação ao sistema multiplicativo S
A_f, M_f	anel ou módulo de frações com relação ao conjunto $\{1, f, f^2, \dots\}$
$A_{\mathfrak{p}}, M_{\mathfrak{p}}$	localização de A ou M no ideal primo $\mathfrak{p}$
M^*	dual do módulo M
M^{**}	bidual do módulo M
$M \oplus N$	soma direta dos módulos M e N
$\bigwedge^r M$	r -ésima potência exterior de M
ω_I	módulo canônico de A/I (definição 3.3)
$I \leq A$	I é um ideal do anel A
$I < A$	I é um ideal próprio do anel A

$M \leq N$	M é um submódulo de N
$M < N$	M é um submódulo próprio de N
$B A$	B é uma extensão de A
$C_{B A}$	condutor de B em A (definição 5.4)
IB	extensão do ideal I no anel B
$M \xrightarrow{x} M$	multiplicação pelo elemento x
$\mathcal{K}(\underline{x})$	complexo de Koszul relativo à sequência $\underline{x}$ (definido na sessão 2.4)
$\mathcal{K}(\underline{x}; M)$	complexo de Koszul de M relativo à sequência $\underline{x}$ (sessão 2.4)
$H_r \mathcal{C}$	r -ésima homologia do complexo $\mathcal{C}$ (indexado em ordem decrescente)
$H^r \mathcal{C}$	r -ésima homologia do complexo $\mathcal{C}$ (indexado em ordem crescente)
$\partial_{X_i} F$	grau do polinômio F na variável X_i
$\frac{\partial f}{\partial Y_i}$	derivada parcial de f com relação à indeterminada Y_i
$\frac{\partial(f_3, \dots, f_n)}{\partial(Y_3, \dots, Y_n)}$	matriz jacobiana de $f_3, \dots, f_n$ relativa a $Y_3, \dots, Y_n$
$:=$	é definido como
$\cong$	é isomorfo a
$\approx$	isomorfismo
$M \setminus N$	conjunto complementar de N em M
$\bigcup X$	união de todos os elementos de X , isto é, $\bigcup_{x \in X} x$
$\bigcap X$	interseção de todos os elementos de X , isto é, $\bigcap_{x \in X} x$
$k^\times$	$k \setminus \{0\}$

- [Lyu89] G. Lyubeznik. *A survey of problems and results on the number of defining equations*, Commutative Algebra (Berkeley, CA, 1987), págs. 375-390, Springer, New York-Berlin, 1989.
- [Mac16] F. S. Macaulay. *Algebraic theory of modular systems*, Cambridge Tracts **19**(1916).
- [MK78] N. Mohan Kumar. *On two conjectures about polynomial rings*, Inventiones Mathematicae **46**(1978), 225-236.
- [Qui76] D. Quillen. *Projective modules over polynomial rings*, Inventiones Mathematicae **36**(1976), 167-171.
- [Ser61] J. P. Serre. *Sur les modules projectifs*, Sémin. Dubreil-Pisot **14**, 1960/1961.
- [Szp79] L. Szpiro. *Lectures on Equations Defining Space Curves (Notes by N. Mohan Kumar)*, Tata Inst. Lecture Notes in Math., Bombay, 1979.
- [ZS60] O. Zariski and P. Samuel *Commutative Algebra Vol. II* Springer-Verlag, New York, 1960.

Bibliografia

- [Abh73] S. Abhyankar. *On Macaulay's examples*, Lecture Notes in Mathematics **311**, págs. 1-16. Springer-Verlag, Berlin, 1973.
- [Bre79] H. Bresinsky. *Monomial space curves in $\mathbb{A}^3$ as set-theoretic complete intersections*, Proceedings of the American Mathematical Society **75**(1)(1979), 23-24.
- [CN78] R. C. Cowsik and M. V. Nori. *Affine curves in characteristic p are set theoretic complete intersections*, Inventiones Mathematicae **45**(1978), 111-114.
- [Eis94] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 1994.
- [Gey76] W. D. Geyer. *On the number of equations which are necessary to describe an algebraic set in n -space*, Atas da 3^a Escola de Álgebra, págs. 183-317, Brasília, 1976.
- [Har62] R. Hartshorne. *Complete intersections and connectedness*, American Journal of Mathematics **84**(1962), 497-508.
- [Kun85] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston, 1985.
- [Lam78] T. Y. Lam. *Serre's Conjecture*, Lecture Notes in Mathematics **635**, Springer-Verlag, Berlin, 1978.
- [Lan93] S. Lang. *Algebra*, 3rd ed., Addison-Wesley, Reading, Massachusetts, 1993.