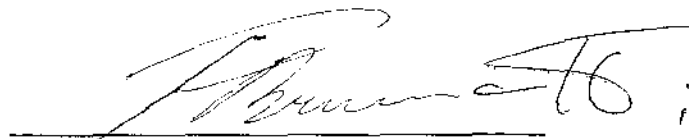


Função de Hilbert para uma k -álgebra homogênea

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pelo Sr. *Jefferson Luiz Rocha Bastos* e aprovada pela Comissão Julgadora.

Campinas 20, de dezembro de 1993.



Prof. Dr. Paulo Roberto Brumatti

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do Título de Mestre em Matemática.

Universidade Estadual de Campinas
IMECC

Dissertação de Mestrado

Função de Hilbert para uma k -álgebra
homogênea

Aluno: Jefferson Luiz Rocha Bastos
Orientador: Prof. Dr. Paulo Roberto Brumatti

Dezembro de 1993

Conteúdo

Introdução	1
1 Função de Hilbert e sua aplicação na teoria da dimensão em anéis	3
1.1 Anéis e Módulos Graduados	3
1.2 A função de Hilbert	5
1.3 Teoria da dimensão de anéis Noetherianos	11
1.4 Anéis locais regulares	23
2 Cálculo da função de Hilbert e Bases de Gröbner	28
2.1 Bases de Gröbner	28
2.2 Função de Hilbert de $\frac{S}{I}$, com I ideal monomial	38
2.3 Anéis de Stanley-Reisner	43
3 Os teoremas de Green e Macaulay	53
3.1 Resultados Auxiliares	54
3.2 O teorema de Green	72
3.3 O teorema de Macaulay	78
A Resultados auxiliares	85
A.1 Capítulo 1	85

A.2 Capítulo 2	91
--------------------------	----

Agradecimentos

- Ao professor Doutor Paulo Roberto Brumatti, pela disponibilidade e atenção.
- Ao CNPq, pelo auxílio financeiro.
- Aos amigos do *predinho*, em especial à Ana e ao Túlio, pela ajuda.
- Aos amigos Ademir, Josevaldo, Ana Claudia, Alancardek e Pedro, pelos momentos alegres que passamos juntos.
- À amiga Cida, pela ajuda neste trabalho e pelas caronas Campinas - Rio Preto.
- Aos meus familiares e à Sandra, pelo carinho, amor e incentivo.

Introdução

O objetivo deste trabalho é o estudo da função de Hilbert, principalmente no caso de uma k -álgebra homogênea. Essa função surgiu em 1890 quando Hilbert lançou seu famoso paper “Über die Theorie der algebraischen Formen”.

Um dos principais conceitos em Geometria Algébrica é o de dimensão de uma variedade. O que sabemos é que tal conceito é essencialmente uma noção local e que, para um anel local, a função de Hilbert nos dá a sua dimensão.

No capítulo 1 veremos a definição de função de Hilbert e sua aplicação na teoria da dimensão de anéis Noetherianos locais. Este estudo foi baseado em [1], capítulo 11.

No capítulo 2 o nosso interesse é calcular a função de Hilbert do anel de coordenadas de uma variedade projetiva, isto é, calcular a função de Hilbert de S/I com I ideal homogêneo de $S = k[x_1, \dots, x_n]$, pois o grau do polinômio de Hilbert é a dimensão da variedade projetiva definida por I .

Usando as noções de ordem monomial e base de Gröbner, veremos que a função de Hilbert de S/I coincide com a função de Hilbert de $S/(LT(I))$ onde $(LT(I))$ é um ideal monomial. Em seguida veremos dois métodos de como calcular a função de Hilbert de S/I com I ideal monomial. Nesse capítulo, nossos estudos foram baseados principalmente em [2], capítulo 2, [3] e [4], capítulo 5.

No capítulo 3 veremos condições para que uma função numérica

$h : \mathbb{N} \rightarrow \mathbb{N}$ seja uma função de Hilbert de uma k -álgebra homogênea, com k corpo infinito. Nesse capítulo, nossos estudos foram baseados em [4], capítulo 4.

Capítulo 1

Função de Hilbert e sua aplicação na teoria da dimensão em anéis

O nosso objetivo neste capítulo é introduzir a noção de função de Hilbert de um módulo graduado e estudarmos sua aplicação na teoria da dimensão em anéis.

1.1 Anéis e Módulos Graduados

Nesta seção, daremos algumas definições básicas para o estudo da função de Hilbert.

Definição 1.1.1: Um *anel graduado* A é um anel com uma família $(A_n)_{n \in \mathbb{Z}}$ de subgrupos aditivos de A tais que $A = \bigoplus_{n \in \mathbb{Z}} A_n$ e $A_m A_n \subseteq A_{n+m}$ para todo $n, m \in \mathbb{Z}$.

Observações:

(1) Nesta dissertação, vamos trabalhar com anéis que possuem uma graduação positiva, isto é, $A_n = (0)$ para todo $n < 0$. Assim, daqui em diante, salvo observações, A será um anel com graduação *positiva*.

(2) Note que A_0 é um sub-anel de A pois $a, b \in A_0$, como A_0 é subgrupo então $a + b \in A_0$. Temos ainda que $ab \in A_0 A_0 \subseteq A_0$.

(3) Todo A_n , $n \neq 0$ é um A_0 -módulo, visto que $A_0 A_n \subseteq A_n$.

Definição 1.1.2: Seja A um anel graduado. Um A -módulo $\mathcal{M}$ é dito *graduado* se existe uma família de subgrupos aditivos $(\mathcal{M}_n)_{n \geq 0}$ de $\mathcal{M}$ tais que

$$\mathcal{M} = \bigoplus_{n=0}^{\infty} \mathcal{M}_n \quad \text{e} \quad A_m \mathcal{M}_n \subseteq \mathcal{M}_{n+m} \quad \forall m, n \geq 0$$

Um elemento não nulo $x \in \mathcal{M}$ é dito homogêneo de grau n se $x \in \mathcal{M}_n$.

Observação: Tendo em vista a definição de $\mathcal{M}$ temos que se $x \in \mathcal{M}$ então

$$x = \sum_{n=0}^{\infty} y_n, \quad y_n \in \mathcal{M}_n \quad \text{e} \quad y_n \text{ é quase sempre nulo.}$$

Proposição 1.1.3: Para um anel graduado A , as seguintes afirmativas são equivalentes:

- i. A é um anel Noetheriano, isto é, todo ideal é finitamente gerado;
- ii. A_0 é Noetheriano e A é uma A_0 -álgebra finitamente gerada.

Demonstração:

(ii) $\implies$ (i) Teorema de Base de Hilbert (A.1.1).

(i) $\implies$ (ii) Seja $A_+ = \bigoplus_{n=1}^{\infty} A_n$. Temos que A_+ é um ideal de A e temos também que

$$A_0 \cong \frac{A}{A_+}.$$

Logo A_0 é Noetheriano.

A Noetheriano então A_+ é finitamente gerado. Sejam $x_1, \dots, x_s$ os geradores de A_+ e podemos supor que são homogêneos de grau $k_1, \dots, k_s$ respectivamente.

Afirmção: $A = A_0[x_1, \dots, x_s]$.

Por construção $A_0[x_1, \dots, x_s] \subseteq A$. Mostremos, por indução em n , que $A_n \subseteq A_0[x_1, \dots, x_s] \forall n$.

Para $n = 0$ é verdade. Suponhamos que o resultado vale para qualquer número menor do que n e $n \geq 1$. Então

$$y \in A_n \Rightarrow y \in A_+ \Rightarrow y = \sum_{i=1}^s a_i x_i \text{ onde } a_i \in A_{n-k_i}.$$

Logo, $a_i \in A_0[x_1, \dots, x_s] \forall i$ por hipótese de indução e portanto, como $A_0[x_1, \dots, x_s]$ é anel, temos $y \in A_0[x_1, \dots, x_s]$.

Portanto $A_n \subseteq A_0[x_1, \dots, x_s] \forall n$ e assim $A = A_0[x_1, \dots, x_s]$. ■

1.2 A função de Hilbert

Seja $A = \bigoplus_{n=0}^{\infty} A_n$ um anel Noetheriano graduado. Por (1.1.3) temos que

$$A = A_0[x_1, \dots, x_s] \text{ onde } x_i \in A_{k_i} \text{ } i = 1, \dots, s.$$

Se $\mathcal{M}$ é um A -módulo graduado finitamente gerado, então $\mathcal{M}$ é gerado por um número finito de elementos homogêneos m_j ($1 \leq j \leq t$) onde $m_j \in \mathcal{M}_{r_j}$. Temos também que todos os $\mathcal{M}_n$ são A_0 -módulos finitamente gerados.

Definição 1.2.1:

- i. Seja C uma classe de A -módulos e λ uma função em C com valores em $\mathbf{Z}$. A função λ é aditiva se, dada uma sequência exata

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

com M, M', M'' em C , tivermos $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.

- ii. Seja M um A -módulo e λ uma função aditiva, a função de Hilbert de $\mathcal{M}$, com λ fixa, é dada por

$$\begin{aligned} H_\lambda(\mathcal{M}, \cdot) : \quad \mathbf{N} &\longrightarrow \mathbf{Z} \\ n &\longmapsto H(\mathcal{M}, n) = \lambda(\mathcal{M}_n) \end{aligned}$$

Observação: Na definição mais geral de uma função aditiva, λ pode assumir valores em um grupo abeliano qualquer. Porém neste trabalho, λ sempre assumirá valores em $\mathbf{Z}$.

Definição 1.2.2: A série de Hilbert de $\mathcal{M}$ com respeito a λ é dada por

$$H_{\mathcal{M}}(t) = \sum_{n=0}^{\infty} H(\mathcal{M}, n)t^n \in \mathbf{Z}[[t]] .$$

Teorema 1.2.3 (Hilbert-Serre): $H_{\mathcal{M}}(t)$ é uma função racional da forma

$$\frac{f(t)}{\prod_{i=1}^s (1 - t^{k_i})} , \text{ onde } f(t) \in \mathbf{Z}[t] \text{ e } k_i = \text{grau } x_i \text{ (} A = A_0[x_1, \dots, x_s] \text{)}$$

Demonstração:

Façamos por indução sobre s , o número de geradores de A sobre A_0 .

$$s = 0 \implies A = A_0 \text{ e portanto } A_n = 0 \ \forall n > 0 .$$

Temos que $\mathcal{M}$ é um A -módulo finitamente gerado então $\mathcal{M}$ é um A_0 -módulo finitamente gerado, isto é,

$$\mathcal{M} = A_0 m_1 + \dots + A_0 m_t , \text{ com } m_i \in \mathcal{M}_{r_i} .$$

Logo, para $n > \max\{r_i, i = 1, \dots, t\}$ temos que $\mathcal{M}_n = 0$. Assim $H_{\mathcal{M}}(t)$ é um polinômio como queríamos.

Suponhamos $s > 0$ e que o resultado valha para $s - 1$. Seja o A -homomorfismo entre os módulos $\mathcal{M}_n$ e $\mathcal{M}_{n+k_s}$ dado por

$$\begin{aligned}\varphi_s : \quad \mathcal{M}_n &\longrightarrow \mathcal{M}_{n+k_s} \\ \alpha &\longmapsto x_s \alpha\end{aligned}$$

Temos então a seguinte sequência exata

$$0 \rightarrow K_n \rightarrow \mathcal{M}_n \rightarrow \mathcal{M}_{n+k_s} \rightarrow L_{n+k_s} \rightarrow 0 \quad (1.2.4)$$

onde

$$\begin{aligned}K_n &= \ker \varphi_s \text{ e} \\ L_{n+k_s} &= \frac{\mathcal{M}_{n+k_s}}{\varphi_s(\mathcal{M}_n)}.\end{aligned}$$

Seja $K = \bigoplus_{n=0}^{\infty} K_n$ e $L = \bigoplus_{n=0}^{\infty} L_n$ onde $L_n = \mathcal{M}_n$ se $n < k_s$ e se $n \geq k_s$, $L_n = L_{(n-k_s)+k_s} = \frac{\mathcal{M}_n}{\varphi_s(\mathcal{M}_{n-k_s})}$.

$$\begin{aligned}\text{Seja } \psi_s : \quad \mathcal{M} &\rightarrow \mathcal{M} \\ m &\mapsto x_s m\end{aligned}$$

$$\ker \psi_s = \{m \in \mathcal{M}; \psi_s(m) = 0\}$$

$$m \in \mathcal{M} \Rightarrow m = y_1 + \dots + y_n \text{ com } y_i \in \mathcal{M}_{r_i}$$

$$x_s m = 0 \Rightarrow x_s y_1 + \dots + x_s y_n = 0$$

Assim $x_s y_i \in \mathcal{M}_{s+r_i} \cap \sum_{r_j \neq s+r_i} \mathcal{M}_{r_j} \Rightarrow x_s y_i = 0 \Rightarrow y_i \in K_{r_i} \Rightarrow m \in K$.

Assim $\ker(\psi_s) = K$.

Temos também que

$$L \simeq \frac{\mathcal{M}}{x_s \mathcal{M}} \text{ pois seja}$$

$$\mathcal{M} \xrightarrow{\Phi} L \quad \text{onde} \quad m = y_{i_1} + \cdots + y_{i_r} + x_{j_1} + \cdots + x_{j_s}$$

com $i_l < k_s$ e $j_l \geq k_s$.

$$\Phi(m) = y_{i_1} + \cdots + y_{i_r} + \bar{x}_{j_1} + \cdots + \bar{x}_{j_s}$$

onde $\bar{x}_{j_l} = x_{j_l} + x_s \mathcal{M}_{j_l - k_s}$. Φ é sobrejetora e $\ker \Phi = x_s \mathcal{M}$ e portanto

$$L \simeq \frac{\mathcal{M}}{x_s \mathcal{M}}.$$

A é Noetheriano e $\mathcal{M}$ é finitamente gerado então $\mathcal{M}$ é Noetheriano. Logo K e L são também A -módulos finitamente gerados.

Temos ainda que $x_s K = (0)$ e $x_s L = (0)$ e então podemos dizer que K e L são $A_0[x_1, \dots, x_{s-1}]$ -módulos finitamente gerados. Aplicando λ em (1.2.4) temos

$$\lambda(K_n) - \lambda(\mathcal{M}_n) + \lambda(\mathcal{M}_{n+k_s}) - \lambda(L_{n+k_s}) = 0$$

Multiplicando por t^{n+k_s} e somando sobre todos os n teremos

$$\begin{aligned} & \sum_n \lambda(K_n) t^{n+k_s} - \sum_n \lambda(\mathcal{M}_n) t^{n+k_s} + \sum_n \lambda(\mathcal{M}_{n+k_s}) t^{n+k_s} \\ & \quad - \sum_n \lambda(L_{n+k_s}) t^{n+k_s} = 0 \\ \Rightarrow & H_K(t) t^{k_s} - H_{\mathcal{M}}(t) t^{k_s} + \sum_n \lambda(\mathcal{M}_{n+k_s}) t^{n+k_s} - \sum_n \lambda(L_{n+k_s}) t^{n+k_s} \\ & \quad - \sum_0^{k_s-1} \lambda(\mathcal{M}_n) t^n + \sum_0^{k_s-1} \lambda(\mathcal{M}_n) t^n = 0 \\ \Rightarrow & t^{k_s} H_K(t) - t^{k_s} H_{\mathcal{M}}(t) + H_{\mathcal{M}}(t) - H_L(t) = 0 \\ \Rightarrow & (1 - t^{k_s}) H_{\mathcal{M}}(t) = H_L(t) - t^{k_s} H_K(t) \end{aligned}$$

e por hipótese de indução temos que o resultado é válido para L e para K e portanto é válido para $\mathcal{M}$. ■

Definição 1.2.5: Nas condições do teorema acima, definimos $d_\lambda(\mathcal{M})$ como

sendo a ordem do polo $t = 1$ da função racional $H_{\mathcal{M}}(t)$.

Corolário 1.2.6: Se $k_i = 1 \forall i$ então para n suficientemente grande, $\lambda(\mathcal{M}_n)$ é um polinômio em n (com coeficientes racionais) de grau $d - 1$ onde $d = d_{\lambda}(\mathcal{M})$. Se $d = 0$, $\lambda(\mathcal{M}_n)$ é zero para n grande.

Demonstração:

Por (1.2.3) temos que $\lambda(\mathcal{M}_n)$ é o coeficiente de t^n em $f(t)(1-t)^{-s}$.

Cancelando-se as potências de $(1-t)$ que aparecem em f , podemos supor $s = d$ e $f(1) \neq 0$

$$f(t) = \sum_{k=0}^N a_k t^k .$$

Lembrando que em $\mathbf{Z}[[t]]$ $(1-t)^{-d}$ é inversível e

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k \quad \text{temos (A.1.2)}$$

$$\sum \lambda(\mathcal{M}_n) t^n = f(t) \frac{1}{(1-t)^d} = \left(\sum_{k=0}^N a_k t^k \right) \left(\sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k \right) .$$

Assim, se $n \geq N$ temos que

$$\lambda(\mathcal{M}_n) = \sum_{k=0}^N a_k \binom{d+n-k-1}{d-1}$$

e a soma do lado direito é um polinômio em n de grau $d - 1$ com coeficiente líder $\frac{\sum a_k}{(d-1)!} \neq 0$ ($f(1) \neq 0$). ■

Observação: O polinômio que aparece em (1.2.6) é usualmente chamado polinômio de Hilbert de $\mathcal{M}$ associado a λ .

Proposição 1.2.7: Se $x \in A_k$ não é um divisor de zero em $\mathcal{M}$, isto é,

$xm = 0 \Rightarrow m = 0$, então

$$d\left(\frac{\mathcal{M}}{x\mathcal{M}}\right) = d(\mathcal{M}) - 1 .$$

Demonstração:

Na prova de (1.2.3) em (1.2.4) substitua x_* por x . Desta forma $K = 0$ e concluimos o resultado. ■

Observação: Tome A_0 anel Artiniano. Sabemos que se N é um A_0 -módulo finitamente gerado, então o comprimento de N é finito, isto é, $l(N) \in \mathbb{N}$.

Logo, o teorema de Hilbert vale quando tomamos $\lambda = l$ e $A = \oplus A_n$ anel graduado, com A_0 Artiniano e $\mathcal{M}$ um A_0 -módulo finitamente gerado.

Exemplo 1.2.8:

Seja $A = k[x_1, \dots, x_m]$ o anel de polinômios com k corpo. Temos que $A = \oplus A_n$, onde A_n é o k espaço vetorial gerado pelos monômios $x_1^{a_1} \dots x_m^{a_m}$ tais que $\sum_{i=1}^n a_i = n$.

Tomando $\lambda = \dim$ de A_n como k -espaço vetorial temos que

$$\dim_k(A_n) = \binom{m+n-1}{m-1} \quad (\text{A.1.3}) .$$

Logo

$$\begin{aligned} H_A(t) &= \sum_{n=0}^{\infty} \dim_k(A_n) t^n = \sum_{n=0}^{\infty} \binom{m+n-1}{m-1} t^n \\ &= (1-t)^{-m} \end{aligned}$$

$$\text{Assim } H_A(t) = \frac{1}{(1-t)^m} . \quad \blacksquare$$

1.3 Teoria da dimensão de anéis Noetherianos

Uma vez vista a definição de função de Hilbert, vejamos como ela se aplica na teoria de dimensão em anéis Noetherianos.

Definição 1.3.1: Um anel local é um anel A com um único ideal maximal. Geralmente denotamos por (A, m) local onde m é o ideal maximal.

Definição 1.3.2: Seja A um anel e $\mathcal{A}$ um ideal de A . Definimos o anel graduado associado a A como sendo o anel graduado

$$G(A) = G_{\mathcal{A}}(A) = \bigoplus_{n=0}^{\infty} \frac{\mathcal{A}^n}{\mathcal{A}^{n+1}} \quad (\mathcal{A}^0 = A)$$

A multiplicação em $G(A)$ é definida da seguinte forma: Para cada

$$x_m \in \mathcal{A}^m \quad \text{seja} \quad \bar{x}_m = x_m + \mathcal{A}^{m+1}.$$

Então $\bar{x}_n \bar{x}_m = \overline{x_n x_m} = x_n x_m + \mathcal{A}^{m+n+1}$.

Esta é uma operação bem definida pois

$$\begin{aligned} \bar{x}_n = \bar{x}'_n &\Rightarrow x_n - x'_n \in \mathcal{A}^{n+1} & x_n x_m - x'_n x_m &\in \mathcal{A}^{m+n+1} \\ && \Rightarrow \\ \bar{x}_m = \bar{x}'_m &\Rightarrow x_m - x'_m \in \mathcal{A}^{m+1} & x_m x'_n - x'_m x'_n &\in \mathcal{A}^{m+n+1} \end{aligned}$$

e juntando os dois resultados acima temos que

$$x_m x_n - x'_n x'_m \in \mathcal{A}^{n+m+1} \Rightarrow \bar{x}_m \bar{x}_n = \bar{x}'_n \bar{x}'_m.$$

Definição 1.3.3: Seja A um anel Noetheriano e $\mathcal{M}$ um A -módulo e $\mathcal{A}$ um ideal de A . Temos as seguintes definições:

i. Uma cadeia (infinita)

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq \cdots$$

de submódulos de M é chamada $\mathcal{A}$ -filtração de M se $\mathcal{A}M_n \subseteq M_{n+1}$ para todo n . Se $\mathcal{A}M_n = M_{n+1}$ para n suficientemente grande, então (M_n) é chamada uma filtração estável.

ii. Dada (M_n) uma $\mathcal{A}$ -filtração de M , definimos

$$G(M) = \bigoplus_{n=0}^{\infty} \frac{M_n}{M_{n+1}}$$

que é um $G_{\mathcal{A}}(A)$ -módulo. Temos ainda que $G_n(M) = \frac{M_n}{M_{n+1}}$.

Teorema 1.3.4: Seja A um anel Noetheriano local, m seu ideal maximal, $\mathcal{Q}$ um ideal m -primário (A.1.4), $\mathcal{M}$ um A -módulo finitamente gerado e $(\mathcal{M}_n)$ uma $\mathcal{Q}$ -filtração estável de $\mathcal{M}$. Então:

- i. $\frac{\mathcal{M}}{\mathcal{M}_n}$ é de comprimento finito $\forall n \geq 0$;
- ii. Para n suficientemente grande, este comprimento é um polinômio $g(n)$ de grau $\leq s$ em n , onde s é o número mínimo de geradores de $\mathcal{Q}$;
- iii. O grau do coeficiente líder de $g(n)$ depende somente de $\mathcal{M}$ e $\mathcal{Q}$ e não da filtração escolhida.

Demonstração:

(i) Seja $G(A) = \bigoplus_{n=0}^{\infty} \frac{\mathcal{Q}^n}{\mathcal{Q}^{n+1}}$; $G(\mathcal{M}) = \bigoplus_{n=0}^{\infty} \frac{\mathcal{M}_n}{\mathcal{M}_{n+1}}$. Temos que $G_0(A) = \frac{A}{\mathcal{Q}}$ é um anel Artiniano pois é um anel Noetheriano de dimensão zero.

Temos ainda que $G(A)$ é Noetheriano e $G(\mathcal{M})$ é um $G(A)$ -módulo finitamente gerado (A.1.5).

Cada $G_n(\mathcal{M}) = \frac{\mathcal{M}_n}{\mathcal{M}_{n+1}}$ é um A -módulo finitamente gerado, anulado por $\mathcal{Q}$ e portanto são $\left(\frac{A}{\mathcal{Q}}\right)$ -módulos finitamente gerados. Visto que $\left(\frac{A}{\mathcal{Q}}\right)$ é Artiniano então $G_n(\mathcal{M})$ são de comprimento finito (A.1.6).

Afirmção (1): $\frac{\mathcal{M}}{\mathcal{M}_n}$ é de comprimento finito $\forall n$.

Façamos por indução:

Para $n = 0$ nada temos a fazer, pois

$$\frac{\mathcal{M}}{\mathcal{M}_0} = \frac{\mathcal{M}}{\mathcal{M}} \simeq (0) .$$

Suponhamos que $\frac{\mathcal{M}}{\mathcal{M}_{n-1}}$ é Artiniano e mostremos que $\frac{\mathcal{M}}{\mathcal{M}_n}$ também o é. A sequência

$$0 \rightarrow \frac{\mathcal{M}_{n-1}}{\mathcal{M}_n} \rightarrow \frac{\mathcal{M}}{\mathcal{M}_n} \rightarrow \frac{\mathcal{M}}{\mathcal{M}_{n-1}} \rightarrow 0 \quad (1.3.5)$$

é exata.

E como $\frac{\mathcal{M}_{n-1}}{\mathcal{M}_n} = G_{n-1}(\mathcal{M})$ é Artiniano e por hipótese de indução $\frac{\mathcal{M}}{\mathcal{M}_{n-1}}$ também temos que $\frac{\mathcal{M}}{\mathcal{M}_n}$ é Artiniano (A.1.7).

Assim, $\frac{\mathcal{M}}{\mathcal{M}_n}$ também é de comprimento finito.

Afirmção (2):

$$l_n = l\left(\frac{\mathcal{M}}{\mathcal{M}_n}\right) = \sum_{r=1}^n l\left(\frac{\mathcal{M}_{r-1}}{\mathcal{M}_r}\right) \quad \forall n .$$

Novamente por indução.

Para $n = 0$ não temos nada a fazer pois

$$l_0 = l\left(\frac{\mathcal{M}}{\mathcal{M}_0}\right) = l(0) = 0 .$$

Suponhamos o resultado válido para $n - 1$ e $n \geq 1$. Por (1.3.5) temos

$$\begin{aligned} l_n &= l_{n-1} + l\left(\frac{\mathcal{M}_{n-1}}{\mathcal{M}_n}\right) \\ \text{H.I.} \quad \sum_{r=1}^{n-1} l\left(\frac{\mathcal{M}_{r-1}}{\mathcal{M}_r}\right) + l\left(\frac{\mathcal{M}_{n-1}}{\mathcal{M}_n}\right) &= \sum_{r=1}^n l\left(\frac{\mathcal{M}_{r-1}}{\mathcal{M}_r}\right) \end{aligned}$$

Logo

$$l_n = \sum_{r=1}^n l\left(\frac{\mathcal{M}_{r-1}}{\mathcal{M}_r}\right). \quad (1.3.6)$$

(ii) Se $x_1, \dots, x_s$ gera $\mathcal{Q}$, as imagens $\bar{x}_i = x_i + \frac{\mathcal{Q}}{\mathcal{Q}_s}$ geram $G(A)$ como uma $\frac{A}{\mathcal{Q}}$ -álgebra (A.1.5) e cada $\bar{x}_i$ tem grau 1 ($G(A) = \frac{A}{\mathcal{Q}}[\bar{x}_1, \dots, \bar{x}_s]$). Por (1.2.6) temos que para n suficientemente grande,

$$l\left(\frac{\mathcal{M}_n}{\mathcal{M}_{n+1}}\right) = f(n) \text{ é um polinômio em } n \text{ de grau } \leq s-1.$$

De (1.3.6) vem que

$$l_{n+1} - l_n = l\left(\frac{\mathcal{M}_n}{\mathcal{M}_{n+1}}\right) = f(n).$$

Assim temos que $l(n)$ é um polinômio $g(n)$ de grau $\leq s$ para n suficientemente grande.

(iii) Seja $(\tilde{\mathcal{M}}_n)$ outra $\mathcal{Q}$ -filtração estável de $\mathcal{M}$ e seja $\tilde{g}(n) = l\left(\frac{\mathcal{M}}{\tilde{\mathcal{M}}_n}\right)$. Então existe $n_0 \in \mathbb{N}$ tal que

$$\mathcal{M}_{n+n_0} \subseteq \tilde{\mathcal{M}}_n \text{ e } \tilde{\mathcal{M}}_{n+n_0} \subseteq \mathcal{M}_n \quad \forall n \geq 0 \quad (\text{A.1.8})$$

Utilizando-se a seqüência exata

$$0 \rightarrow \ker \varphi \rightarrow \frac{\mathcal{M}}{\mathcal{M}_{n+n_0}} \xrightarrow{\varphi} \frac{\mathcal{M}}{\tilde{\mathcal{M}}_n} \rightarrow 0 \text{ temos}$$

$$l\left(\frac{\mathcal{M}}{\mathcal{M}_{n+n_0}}\right) \geq l\left(\frac{\mathcal{M}}{\tilde{\mathcal{M}}_n}\right)$$

$$\Rightarrow g(n+n_0) \geq \tilde{g}(n)$$

Com raciocínio análogo, chegamos a $\tilde{g}(n+n_0) \geq g(n)$.

$$\tilde{g}(n+n_0) \geq g(n) \Rightarrow \frac{\tilde{g}(n+n_0)}{\tilde{g}(n)} \geq \frac{g(n)}{\tilde{g}(n)} \text{ e}$$

$$\lim_{n \rightarrow \infty} \frac{\tilde{g}(n+n_0)}{\tilde{g}(n)} = 1 \Rightarrow \lim_{n \rightarrow \infty} \frac{g(n)}{\tilde{g}(n)} \leq 1.$$

$$g(n + n_0) \geq \tilde{g}(n) \Rightarrow \frac{1}{\tilde{g}(n)} \geq \frac{1}{g(n + n_0)} \Rightarrow \frac{g(n)}{\tilde{g}(n)} \geq \frac{g(n)}{g(n + n_0)} \quad \text{e}$$

$$\lim_{n \rightarrow \infty} \frac{g(n)}{g(n + n_0)} = 1 \Rightarrow \lim_{n \rightarrow \infty} \frac{g(n)}{\tilde{g}(n)} \geq 1 .$$

Logo

$$\lim_{n \rightarrow \infty} \frac{g(n)}{\tilde{g}(n)} = 1 \Rightarrow \deg g = \deg \tilde{g}$$

e g e $\tilde{g}$ têm o mesmo *coeficiente líder*. ■

Observações:

i. O polinômio $g(n)$ correspondente à filtração $(Q^n \mathcal{M})$ é denotado por

$$\chi_Q^{\mathcal{M}}(n) = l\left(\frac{\mathcal{M}}{Q^n \mathcal{M}}\right)$$

para n suficientemente grande.

ii. Se $\mathcal{M} = A$ então

$$\chi_Q^A(n) = \chi_Q(n)$$

e é chamado de polinômio característico do ideal m -primário Q .

Corolário 1.3.7: Para n suficientemente grande, o comprimento $l\left(\frac{A}{Q^n}\right)$ é um polinômio $\chi_Q(n)$ de grau $\leq s$, onde s é o número mínimo de geradores de Q .

Demonstração: Imediata de (1.3.4) tomando-se $\mathcal{M} = A$ e $\mathcal{M}_n = Q^n A$. ■

Proposição 1.3.8: Seja A anel local, m seu ideal maximal e Q um ideal m -primário. Então

$$\deg \chi_Q(n) = \deg \chi_m(n) .$$

Demonstração:

Como A é Noetheriano, todo ideal contém uma potência de seu radical. Logo, existe r tal que

$$m^r \subseteq Q \subseteq m$$

e assim $m^{rn} \subseteq Q^n \subseteq m^n$. Logo

$$l\left(\frac{A}{m^{rn}}\right) \geq l\left(\frac{A}{Q^n}\right) \geq l\left(\frac{A}{m^n}\right)$$

isto é

$$\chi_m(n) \leq \chi_Q(n) \leq \chi_m(rn)$$

para n suficientemente grande. Assim, sendo a o coeficiente líder de $\chi_m(n)$ e $d = \deg(\chi_m(n))$ temos

$$1 \leq \frac{\chi_Q(n)}{\chi_m(n)} \leq \frac{\chi_m(rn)}{\chi_m(n)} \text{ e } \lim_{n \rightarrow \infty} \frac{\chi_m(rn)}{\chi_m(n)} = r^d.$$

Portanto

$$1 \leq \lim_{n \rightarrow \infty} \frac{\chi_Q(n)}{\chi_m(n)} \leq r^d$$

$$\text{e então } \deg(\chi_Q(n)) = \deg(\chi_m(n)).$$

■

Observação: O que o teorema nos diz é que os polinômios $\chi_Q(n)$ possuem o mesmo grau, independentemente da escolha do ideal m -primário Q .

A partir daí, temos a seguinte definição:

Definição 1.3.9: Definimos $d(A) = \deg \chi_Q(n)$, onde Q ideal m -primário qualquer, para n suficientemente grande.

Definição 1.3.10: Sendo A anel Noetheriano, definimos

(i)

$$\delta(A) = \min \left\{ k \in \mathbb{N} ; \begin{array}{l} \exists x_1, \dots, x_k \in A \text{ e } (x_1, \dots, x_k) = \mathcal{Q} , \\ \text{com } \mathcal{Q} \text{ ideal } m\text{-primário} \end{array} \right\}$$

(ii)

$$\dim(A) = \sup \{ k ; \exists m \mathcal{P}_0 \subset \mathcal{P}_1 \subset \dots \subset \mathcal{P}_k ; \mathcal{P}_i \in \text{Spec}(A) \} .$$

onde $\mathcal{P}_i \subset \mathcal{P}_j$ denota $\mathcal{P}_i$ está *estritamente* contido em $\mathcal{P}_j$.

O nosso objetivo é mostrar que para um anel Noetheriano local A vale

$$\delta(A) = d(A) = \dim(A) .$$

Vejamos antes uma série de proposições que nos ajudarão a demonstrar tal resultado.

Proposição 1.3.11: $\delta(A) \geq d(A)$.

Demonstração:

$\delta(A) = k$ então existe $\mathcal{Q}$ ideal m -primário tal que $\mathcal{Q}$ é gerado por k elementos. Porém, por (1.3.4)(ii) temos que

$$\deg \chi_{\mathcal{Q}}(n) \leq k .$$

Porém, por (1.3.8) temos que

$$\deg \chi_{\mathcal{Q}}(n) = d(A) .$$

Logo $d(A) \leq \delta(A)$. ■

Proposição 1.3.12: Seja A anel Noetheriano local, m seu ideal maximal e $\mathcal{Q}$ um ideal m -primário. Seja $\mathcal{M}$ um A -módulo finitamente gerado e $x \in A$ tal que x não é divisor de zero de $\mathcal{M}$ ($xm = 0 \Rightarrow m = 0$) e $\mathcal{M}' = \frac{\mathcal{M}}{x\mathcal{M}}$.

Então

i. $\deg(\chi_Q^{\mathcal{M}'}) \leq \deg(\chi_Q^{\mathcal{M}}) - 1$

ii. $d\left(\frac{A}{(x)}\right) \leq d(A) - 1.$

Demonstração:

(i) Tome $N = x\mathcal{M}$. Temos que $N \simeq \mathcal{M}$ como A -módulo.

Seja $N_n = N \cap Q^n \mathcal{M}$. Temos as seguintes seqüências exatas

$$0 \rightarrow \frac{N}{N_n} \rightarrow \frac{\mathcal{M}}{Q^n \mathcal{M}} \rightarrow \frac{\mathcal{M}'}{Q^n \mathcal{M}'} \rightarrow 0.$$

Se pusermos $g(n) = l\left(\frac{N}{N_n}\right)$ temos que para n suficientemente grande

$$g(n) - \chi_Q^{\mathcal{M}}(n) + \chi_Q^{\mathcal{M}'}(n) = 0.$$

Pelo lema de Artin-Rees (A.1.9) temos que (N_n) é uma Q -filtração estável de N . Como $\mathcal{M} \simeq N$ por (1.3.4)(iii) implica que $g(n)$ e $\chi_Q^{\mathcal{M}}(n)$ tem o mesmo coeficiente líder. Logo

$$\deg \chi_Q^{\mathcal{M}'} \leq \deg \chi_Q^{\mathcal{M}} - 1.$$

(ii) Tome em (i) $\mathcal{M} = A$. ■

Proposição 1.3.13: $d(A) \geq \dim(A)$.

Demonstração:

Façamos por indução sobre $d = d(A)$.

Se $d = 0 \Rightarrow g(n) = l\left(\frac{A}{m^n}\right)$ é constante para n suficientemente grande.

Temos a seguinte seqüência exata

$$0 \rightarrow \frac{m^n}{m^{n+1}} \rightarrow \frac{A}{m^{n+1}} \rightarrow \frac{A}{m^n} \rightarrow 0$$

e portanto

$$l\left(\frac{A}{m^{n+1}}\right) = l\left(\frac{A}{m^n}\right) + l\left(\frac{m^n}{m^{n+1}}\right) \Rightarrow l\left(\frac{m^n}{m^{n+1}}\right) = 0 .$$

Logo $m^n = m^{n+1}$ e pelo lema de Nakayama (A.1.10) temos $m^n = 0$.

Porém $m^n = 0$ e A anel Noetheriano local, então A é Artiniano (A.1.11), logo $\dim(A) = 0$.

Assim já demonstramos o resultado para $d = 0$.

Suponhamos $d > 0$ e que o resultado valha para qualquer número menor do que d .

Seja $\mathcal{P}_0 \subset \mathcal{P}_1 \subset \dots \subset \mathcal{P}_r$ uma cadeia de ideais primos de A . Tome $x \in \mathcal{P}_1 - \mathcal{P}_0$ e faça

$$A' = \frac{A}{\mathcal{P}_0} \text{ e } x' = \bar{x} = x + \mathcal{P}_0 .$$

Assim, $x' \neq 0$ em A' e A' é um domínio de integridade e por (1.3.12)(ii) temos

$$d\left(\frac{A'}{x'}\right) \leq d(A') - 1 .$$

Temos que $\bar{m} = m + \mathcal{P}_0$ é o único ideal maximal de A' e mais ainda

$$\varphi : \frac{A}{m^n} \rightarrow \frac{A'}{(\bar{m})^n}$$

é sobrejetora e portanto

$$l\left(\frac{A}{m^n}\right) \geq l\left(\frac{A'}{(\bar{m})^n}\right)$$

Logo $d(A) \geq d(A')$ pois

$$d(A) < d(A') \Rightarrow \lim_{n \rightarrow \infty} \frac{\chi_m(n)}{\chi_{\bar{m}}(n)} = 0 ,$$

isto é, para n grande

$$\chi_{\bar{m}}(n) = l\left(\frac{A}{\bar{m}^n}\right) > \chi_m(n) = l\left(\frac{A}{m^n}\right) ,$$

o que é um absurdo.

Assim

$$d\left(\frac{A'}{x'}\right) \leq d(A') - 1 \leq d(A) - 1 = d - 1.$$

Por hipótese de indução, qualquer cadeia de primos de $\frac{A'}{x'}$ tem comprimento menor ou igual a $d - 1$. Porém, note que

$$\overline{\mathcal{P}}_1 \subset \overline{\mathcal{P}}_2 \subset \cdots \overline{\mathcal{P}}_r$$

é cadeia de primos de comprimento $r - 1$ de A' . Logo $r - 1 \leq d - 1$, isto é, $r \leq d$.

Logo, $\dim(A) \leq d$. ■

Proposição 1.3.14: Seja A anel Noetheriano local de dimensão d . Então existe um ideal m -primário em A gerado por d elementos $x_1, \dots, x_d$ e, portanto, $\dim(A) \geq \delta(A)$.

Demonstração:

Vamos construir $x_1, \dots, x_d$ indutivamente de tal maneira que todo primo $\mathcal{P}$ que contenha $(x_1, \dots, x_i)$ tenha altura maior ou igual a i .

Tome x_1 de tal forma que $x_1 \notin \cup \mathcal{P}$, onde $\mathcal{P}$ é um ideal primo minimal de A . Note que se não existir tal elemento, A é um anel Artiniano local e $\sqrt{(0)} = m$. Logo $\delta(A) = 0$ e $\dim(A) = 0$.

Assim $x_1 \notin \mathcal{P}$ para todo $\mathcal{P}$ primo minimal de A e portanto se $Q \in \text{Spec}(A)$ e $x_1 \in Q$ então $h(Q) \geq 1$, pois Q contém um primo minimal de A .

Tome i e $d \geq i > 1$ e suponha que já tenhamos construído $(x_1, \dots, x_{i-1})$ da forma desejada. Considere

$$\mathcal{S} = \left\{ \begin{array}{l} \mathcal{P}_j; \mathcal{P}_j \text{ é primo minimal de } (x_1, \dots, x_{i-1}) \\ \text{e } ht(\mathcal{P}_j) = i - 1 \end{array} \right\}$$

Logicamente $\#S = s < \infty$, inclusive podendo ser nula.

Temos $i - 1 < d$ e portanto $\mathcal{P}_j \subset m$ para todo $\mathcal{P}_j \in S$ então $\cup_{j=1}^s \mathcal{P}_j \subset m$ e portanto podemos escolher $x_i \in m$ tal que $x_i \notin \mathcal{P}_j \forall j$. Tome $\mathcal{Q}$ um primo que contém $(x_1, \dots, x_{i-1}, x_i)$. Temos então que existe $\mathcal{P}$ primo minimal de $(x_1, \dots, x_{i-1})$ tal que $\mathcal{P} \subseteq \mathcal{Q}$.

Se $\mathcal{P} \in S \Rightarrow ht(\mathcal{P}) = i - 1$ e $x_i \notin \mathcal{P} \Rightarrow \mathcal{P} \subset \mathcal{Q} \Rightarrow ht(\mathcal{Q}) \geq i$.

Se $\mathcal{P} \notin S \Rightarrow ht(\mathcal{P}) > i - 1 \Rightarrow ht(\mathcal{Q}) \geq i$.

Portanto todo ideal primo $\mathcal{Q}$ que contenha $(x_1, \dots, x_i)$ tem altura $\geq i$.

Considere então $(x_1, \dots, x_d)$ e seja $\mathcal{P}$ um primo que o contenha. Logo $ht(\mathcal{P}) \geq d$. Porém A é local de dimensão d portanto $\mathcal{P} = m$. Isto é, o único ideal primo que contém $(x_1, \dots, x_d)$ é m e assim $\sqrt{(x_1, \dots, x_d)} = m$. Logo $(x_1, \dots, x_d)$ é m -primário. ■

Com os resultados vistos até agora já podemos demonstrar o seguinte importante teorema:

Teorema 1.3.15 (Teorema da dimensão): Para um anel Noetheriano local A , os seguintes números inteiros são iguais:

- i. A dimensão de Krull de A , isto é, $\dim(A)$;
- ii. O grau do polinômio característico

$$\chi_m(n) = l\left(\frac{A}{m^n}\right),$$

isto é, $d(A)$;

- iii. $\min\{k ; \exists x_1, \dots, x_k \in A \text{ e } (x_1, \dots, x_k) = \mathcal{Q} \text{ é } m \text{ primário}\}$, isto é, $\delta(A)$.

Demonstração:

Por (1.3.11) temos que $\delta(A) \geq \dim(A)$ e por (1.3.13) temos que $d(A) \geq \dim(A)$. Logo $\delta(A) \geq d(A) \geq \dim(A)$ (*).

Por (1.3.14) temos que $\dim(A) \geq \delta(A)$.

Logo, em (*) temos

$$\delta(A) \geq d(A) \geq \dim(A) \geq \delta(A) \Rightarrow \delta(A) = \dim(A) = d(A) .$$

■

Corolário 1.3.16: Seja A anel Noetheriano $x_1, \dots, x_r \in A$. Então todo primo minimal de $(x_1, \dots, x_r)$ tem altura menor ou igual a r .

Demonstração:

Em $A_{\mathcal{P}}$, o ideal $(x_1, \dots, x_r)$ se torna $\mathcal{P}A_{\mathcal{P}}$ primário. Logo

$$\dim A_{\mathcal{P}} = \delta(A_{\mathcal{P}}) \leq r \text{ e } \dim A_{\mathcal{P}} = ht(\mathcal{P}) .$$

Portanto $ht(\mathcal{P}) \leq r$.

■

Corolário 1.3.17 (Teorema do ideal principal de Krull): Seja A anel Noetheriano e $x \in A$. Se x é um elemento de A que não é divisor de zero nem unidade em A , então todo primo minimal $\mathcal{P}$ de (x) tem altura 1.

Demonstração: Por (1.3.16) temos que $ht(\mathcal{P}) \leq 1$. Porém, se $ht(\mathcal{P}) = 0$ então $\mathcal{P}$ é primo minimal de A . Mas se $\mathcal{P}$ é primo minimal de A , então todo elemento de $\mathcal{P}$ é divisor de zero, o que é um absurdo pois $x \in \mathcal{P}$.

Logo $ht(\mathcal{P}) = 1$.

■

1.4 Anéis locais regulares

Em Geometria Algébrica existe uma distinção importante entre pontos singulares e não singulares.

Os anéis locais dos pontos não singulares são o que chamamos de *anel local regular*. O que faremos é caracterizar esses anéis regulares. Porém vejamos alguns resultados que nos auxiliarão.

Definição 1.4.1: Seja A um anel Noetheriano local. Se $x_1, \dots, x_d$ estão em A , $\dim A = d$ e $(x_1, \dots, x_d) = \mathcal{Q}$, com $\mathcal{Q}$ ideal m -primário, então dizemos que $x_1, \dots, x_d$ é um *sistema de parâmetros*.

Um sistema de parâmetros tem uma certa propriedade de independência que é descrita na proposição abaixo.

Proposição 1.4.2: Seja $x_1, \dots, x_d$ um sistema de parâmetros para A e seja $\mathcal{Q} = (x_1, \dots, x_d)$ um ideal m -primário. Seja $f(t_1, \dots, t_d)$ um polinômio homogêneo de grau s com coeficientes em A . Suponhamos também que

$$f(x_1, \dots, x_d) \in \mathcal{Q}^{s+1}.$$

Então todos os coeficientes de f pertencem a m .

Demonstração:

Considere o epimorfismo de anéis graduados

$$\begin{aligned} \alpha : \left(\frac{A}{\mathcal{Q}}\right)[t_1, \dots, t_d] &\rightarrow G_{\mathcal{Q}}(A) = \frac{A}{\mathcal{Q}}[\bar{x}_1, \dots, \bar{x}_d] \\ t_i &\mapsto \bar{x}_i \end{aligned}$$

Devido à hipótese sobre f temos que $\bar{f}(t_1, \dots, t_d) = 0$ e portanto f está no $\ker(\alpha)$ onde $\bar{f}$ é a imagem de f em $\frac{A}{\mathcal{Q}}[t_1, \dots, t_d]$.

Suponhamos que algum coeficiente de f é uma unidade. Então $\bar{f}$ não é um divisor de zero e como α é sobrejetora temos que

$$G_{\mathcal{Q}}(A) \cong \frac{\frac{A}{\mathcal{Q}}[t_1, \dots, t_d]}{\ker(\alpha)}.$$

Assim

$$d(G_{\mathcal{Q}}(A)) = d\left(\frac{\frac{A}{\mathcal{Q}}[t_1, \dots, t_d]}{\ker(\alpha)}\right) \leq d\left(\frac{\frac{A}{\mathcal{Q}}[t_1, \dots, t_d]}{\bar{f}}\right)$$

Porém por (1.2.7) temos que

$$d\left(\frac{\frac{A}{\mathcal{Q}}[t_1, \dots, t_d]}{\bar{f}}\right) = d\left(\frac{A}{\mathcal{Q}}[t_1, \dots, t_d]\right) - 1 = d - 1,$$

isto é, $d(G_{\mathcal{Q}}(A)) \leq d - 1$. Porém

$$d(G_{\mathcal{Q}}(A)) = d(G_m(A)) = d(A) = d \quad \text{por (1.3.15)}$$

que é absurdo.

Logo $\bar{f}$ é divisor de zero de $\frac{A}{\mathcal{Q}}[t_1, \dots, t_d]$. Então existe $\bar{a} \in \frac{A}{\mathcal{Q}}$, com $\bar{a} \neq \bar{0}$ tal que

$$\bar{a}\bar{f} = \bar{0} \Rightarrow \bar{a}\bar{b}_i = 0$$

com b_i coeficiente de f .

Logo $ab_i \in \mathcal{Q}$ para todo i e $a \notin \mathcal{Q}$. Como $\mathcal{Q}$ é m -primário temos que $b_i \in \sqrt{\mathcal{Q}} = m$. Portanto, todo coeficiente de f está em m . ■

Esta proposição se torna simples quando A contém um corpo k isomorfo ao corpo A/m .

Corolário 1.4.3: Se $k \subseteq A$ é um corpo isomorfo a A/m e $x_1, \dots, x_d$ é um sistema de parâmetros, então $x_1, \dots, x_d$ são algebricamente independentes sobre k .

Demonstração:

Assuma que $f(x_1, \dots, x_d) = 0$ e f é um polinômio com coeficientes em k . Precisamos mostrar que $f \equiv 0$. Suponhamos que $f \not\equiv 0$. Então podemos escrever

$$f = f_s + \text{termos maiores},$$

onde f_s é homogêneo de grau s e $f_s \not\equiv 0$.

Aplicando (1.4.2) para f_s vemos que f_s tem todos os seus coeficientes em m . Como todos os coeficientes de f_s estão em $k \simeq \frac{A}{m}$ temos que $f_s = 0$ (absurdo).

Logo $f \equiv 0$ e $x_1, \dots, x_d$ são algebricamente independentes sobre k . ■

Agora já estamos em condições de definir o que é um anel local regular.

Definição 1.4.4: Um *anel local regular* é um anel que satisfaz uma das três condições (equivalentes) do teorema abaixo.

Teorema 1.4.5:

Seja A um anel Noetheriano local de dimensão d , m seu ideal maximal e $k = \frac{A}{m}$. Então as seguintes condições são equivalentes:

- i. $G_m(A) \cong k[t_1, \dots, t_d]$, onde os t_i 's são variáveis independentes,
- ii. $\dim_k(m/m^2) = d$,
- iii. m pode ser gerado por d elementos.

Demonstração:

(i) $\Rightarrow$ (ii) Temos que

$$G_m(A) = \bigoplus_{n=0}^{\infty} \frac{m^n}{m^{n+1}} = \bigoplus_{n=0}^{\infty} A_n.$$

Sejam $x_1, \dots, x_{d+1}$ elementos de A_1 . Como

$$G_m(A) \stackrel{\varphi}{\simeq} k[t_1, \dots, t_d] = \oplus_{i=0}^{\infty} B_i$$

temos que $\varphi(x_1), \dots, \varphi(x_{d+1}) \in B_1$. Porém, $\dim B_1 = d$ e portanto $\varphi(x_1), \dots, \varphi(x_{d+1})$ são linearmente dependentes em $A_1 = \frac{m}{m^2}$.

Porém, como corolário de (1.3.15), temos que

$$\dim_k \left(\frac{m}{m^2} \right) \geq \dim(A) = d$$

e portanto $\dim_k \left(\frac{m}{m^2} \right) = d$.

(ii) $\Rightarrow$ (iii) $\dim_k \left(\frac{m}{m^2} \right) = d$, então existem $\bar{x}_1, \dots, \bar{x}_d \in \frac{m}{m^2}$ formando uma base de $\frac{m}{m^2}$. Logo $x_1, \dots, x_d$ geram m e portanto m pode ser gerado por d elementos.

(iii) $\Rightarrow$ (i) $m = (x_1, \dots, x_d)$. Tome $\frac{A}{m} = k$

$$\alpha : k[t_1, \dots, t_d] \rightarrow G_m(A) = k[\bar{x}_1, \dots, \bar{x}_d] = \oplus_{i=1}^{\infty} A_i$$

$$t_i \longmapsto \bar{x}_i = x_i + m^2$$

α é sobrejetora.

Seja $f \in k[t_1, \dots, t_d]$ tal que $\alpha(f) = 0$; podemos escrever f da seguinte forma

$$f = f_s + \dots + f_r$$

onde f_j são homogêneos de grau j . Como $\alpha(f) = 0$, temos que

$$\alpha(f_s) + \dots + \alpha(f_r) = 0 \text{ e então } \alpha(f_j) = 0$$

para todo j . Como f_s é homogêneo de grau s temos que

$$f_s = \sum_{I=1}^n a_I t_1^{i_1} \dots t_d^{i_d} \text{ com } \sum i_r = s.$$

e portanto $f_s(\bar{x}_1, \dots, \bar{x}_d) = \sum a_I \bar{x}_1^{i_1} \dots \bar{x}_d^{i_d}$. Porém $\bar{x}_i \in \frac{m}{m^2} = A_1$. Logo

$$\bar{x}_j^{i_j} \in A_{i_j} \Rightarrow \bar{x}_1^{i_1} \dots \bar{x}_d^{i_d} \in A_s = \frac{m^s}{m^{s+1}}.$$

Como $a_I \in \frac{A}{m} = A_0$, então $a_I \bar{x}_1^{i_1} \cdots \bar{x}_d^{i_d} \in A_s$. Logo

$$f_s(\bar{x}_1^{i_1}, \dots, \bar{x}_d^{i_d}) \in \frac{m^s}{m^{s+1}}$$

e como $\alpha(f_s) = f_s(\bar{x}_1^{i_1}, \dots, \bar{x}_d^{i_d}) = 0$, temos que $f_s(\bar{x}_1^{i_1}, \dots, \bar{x}_d^{i_d}) \in m^{s+1}$. Logo, por (1.4.2), temos que os coeficientes de f_s estão em m e portanto $f_s = 0$.

Analogamente, fazemos para todos os outros f_j e chegamos a $f = 0$. Logo

$$f \in \ker(\alpha) \Leftrightarrow f = 0 .$$

Portanto α é um isomorfismo. ■

Capítulo 2

Cálculo da função de Hilbert e Bases de Gröbner

Neste capítulo $\mathcal{S} = k[x_1, \dots, x_n]$ denotará o anel de polinômios a n variáveis sobre o corpo k .

O objetivo deste capítulo é calcular a função de Hilbert de $\frac{\mathcal{S}}{I}$ onde I é um anel homogêneo de $\mathcal{S}$ e $\frac{\mathcal{S}}{I}$ é o ideal de coordenadas de uma variedade projetiva. Vamos ver que a função de Hilbert de $\frac{\mathcal{S}}{I}$ coincide com a função de Hilbert de $\frac{\mathcal{S}}{(LT(I))}$ onde $(LT(I))$ é um ideal monomial.

A seguir, mostraremos dois métodos de como calcular a função de Hilbert de $\frac{\mathcal{S}}{I}$ com I ideal monomial.

2.1 Bases de Gröbner

A construção de $(LT(I))$ depende de uma ordem definida no conjunto dos monômios de $\mathcal{S} = k[x_1, \dots, x_n]$ e que tem certas propriedades especiais.

Observe que dado um monômio $x^a = x_1^{a_1} \dots x_n^{a_n}$ podemos associar uma n -upla $(a_1, \dots, a_n) \in \mathbb{N}^n$ e vice-versa. Logo, se conseguimos uma ordem em

$\mathbb{N}^n$, estaremos induzindo uma ordem nos monômios de $\mathcal{S}$ da seguinte forma: dados x^a e $x^b \in \mathcal{S}$ monômios, diremos que $x^a \geq x^b \Leftrightarrow a \geq b$ em $\mathbb{N}^n$.

Gostaríamos que esta ordem tivesse as seguintes propriedades:

- i. dados $a, b \in \mathbb{N}^n$ gostaríamos que $a > b$ ou $b > a$ ou $a = b$, isto é, que nossa ordem seja total.
- ii. Se $a, b \in \mathbb{N}^n$ e $a > b \Rightarrow a + c > b + c \forall c \in \mathbb{N}^n$

Com isso temos a seguinte definição de ordem monomial.

Definição 2.1.1: Uma ordem monomial em $\mathcal{S}$ é uma relação $\geq$ em $\mathbb{N}^n$ satisfazendo

- i. $\geq$ é total em $\mathbb{N}^n$;
- ii. se $a, b, c \in \mathbb{N}^n$ e $a \geq b \Rightarrow a + c \geq b + c$;
- iii. $\geq$ é Artiniana, isto é, todo subconjunto não vazio B de $\mathbb{N}^n$ deve possuir um menor elemento (em relação a $\geq$), isto é, existe $b \in B$ tal que todo $x \in B$ satisfaz $x \geq b$.

Lema 2.1.2: Uma relação de ordem $\geq$ em $\mathbb{N}^n$ é Artiniana se, e somente se, toda seqüência decrescente em $\mathbb{N}^n$ é estacionária.

Demonstração:

Na verdade vamos demonstrar a equivalência das negações das propriedades.

($\Rightarrow$) Se $\geq$ não é Artiniana, então existe $B \subseteq \mathbb{N}^n$, com $B \neq \emptyset$, tal que B não tem mínimo. Tome $a_1 \in B$. Como a_1 não é mínimo, existe $a_2 \in B$ tal que $a_1 > a_2$. Novamente a_2 não é mínimo e portanto existe $a_3 \in B$ tal

que $a_1 > a_2 > a_3$. Seguindo o raciocínio, conseguiremos a sequência infinita desejada, visto que B não pode ser finito.

($\Leftarrow$) Temos, por hipótese, que $a_1 > a_2 > \dots$ é uma sequência infinita estritamente decrescente e portanto o conjunto $B = \{a_1, a_2, \dots\} \subseteq \mathbb{N}^n$ não tem mínimo. Logo $\geq$ não é Artiniana. ■

Observações:

(1) No apêndice temos alguns exemplos de ordem no conjunto dos monômios de $\mathcal{S} = k[x_1, \dots, x_n]$.

(2) No que se segue, estaremos sempre trabalhando com uma ordem monomial $\geq$ fixada.

Definição 2.1.3: Sejam $A \subset \mathbb{N}^n$ um conjunto finito e $f = \sum_{\alpha \in A} a_{\alpha} x^{\alpha}$ um polinômio não nulo em $\mathcal{S}$. Então temos as seguintes definições:

i. O *multidegree* de f é

$$\text{mtdg}(f) = \max\{\alpha \in \mathbb{N}^n ; a_{\alpha} \neq 0\}$$

ii. O *coeficiente líder* de f é

$$\text{LC}(f) = a_{\text{mtdg}(f)} \in k .$$

iii. O *monômio líder* de f é

$$\text{LM}(f) = x^{\text{mtdg}(f)} .$$

iv. O *termo líder* de f é

$$\text{LT}(f) = \text{LC}(f)\text{LM}(f) .$$

No início do capítulo falamos em ideal homogêneo e ideal monomial. Vejamos agora as definições.

Definição 2.1.4:

- i. Um ideal I é dito um *ideal homogêneo* se, para qualquer $f \in I$, $f = f_{r_1} + \dots + f_{r_s}$ com f_{r_i} homogêneo de grau r_i , temos $f_{r_i} \in I$ ou equivalentemente I é gerado por elementos homogêneos.
- ii. Um ideal I é dito um ideal monomial se $I = (x^\alpha ; \alpha \in A \subseteq \mathbb{N}^n)$, isto é, I é gerado por monômios.

Observações:

(1) Se I é um ideal monomial e $f \in \mathcal{S}$ um polinômio não nulo tal que $f \in I$, então todo monômio de f está em I , pois I é um ideal homogêneo e portanto f é uma k -combinação linear dos monômios de I . Assim, vemos que os ideais monomiais são univocamente determinados pelos seus monômios, isto é, dois ideais monomiais são iguais se possuem os mesmos monômios.

(2) Todo ideal homogêneo I de $\mathcal{S}$ também é graduado da seguinte forma

$$I = \bigoplus I_n$$

onde I_n é o conjunto de homogêneos de grau n que estão em I . Assim $\frac{\mathcal{S}}{I}$ também é graduado da seguinte forma

$$\frac{\mathcal{S}}{I} = \bigoplus \left(\frac{\mathcal{S}}{I} \right)_n \quad \text{onde} \quad \left(\frac{\mathcal{S}}{I} \right)_n = \frac{\mathcal{S}_n}{I_n}.$$

Definição 2.1.5: Seja $I \subseteq \mathcal{S}$ ideal, $I \neq (0)$. Definimos

$$\text{LT}(I) = \{cx^\alpha ; \exists f \in I \text{ com } \text{LT}(f) = cx^\alpha\}.$$

Lema 2.1.6: O ideal gerado pelos termos líderes de I , isto é, $(LT(I))$ é um ideal monomial.

Demonstração:

Seja $J = (LM(f); f \in I - \{0\})$. Temos que J e $(LT(I))$ possuem os mesmos monômios e portanto são iguais. ■

Definição 2.1.7: Fixada uma ordem monomial, dizemos que um subconjunto finito $G = \{g_1, \dots, g_t\}$ é uma *base de Gröbner* do ideal I se $(LT(g_1), \dots, LT(g_t)) = (LT(I))$.

Lema 2.1.8 (Algoritmo da divisão): Sejam $f_1, \dots, f_s$ polinômios em $S = k[x_1, \dots, x_n]$. Então todo polinômio $f \in S$ pode ser escrito da seguinte forma

$$f = a_1 f_1 + \dots + a_s f_s + r ,$$

onde $r \in S$, $r = 0$ ou r é uma k -combinação linear de monômios que não são divisíveis por $LT(f_1), \dots, LT(f_s)$.

Demonstração:

Vamos provar a existência de $a_1, \dots, a_s$ e r dando um algoritmo para a sua construção.

Input: $f_1, \dots, f_s, f$

Output: $a_1, \dots, a_s, r$

$a_i := 0, \dots, a_s := 0; r := f$

```

 $p := f$ 
  WHILE  $p \neq 0$  DO
     $i := 1$ 
    divisionoccurred := false
    WHILE  $i \leq s$  AND divisionoccurred = false DO
      IF  $LT(f_i)$  divides  $LT(p)$  THEN
         $a_i := a_i + LT(p)/LT(f_i)$ 
         $p := p - (LT(p)/LT(f_i))f_i$ 
        divisionoccurred := true
      ELSE
         $i := i + 1$ 
    IF divisionoccurred = false THEN
       $r := r + LT(p)$ 
       $p := p - LT(p)$ 

```

Note que quando estamos dentro do WHILE...DO principal ocorrem duas coisas:

1(passo da divisão): Se algum $LT(f_i)$ divide $LT(p)$, então o algoritmo procede como uma divisão em $k[x]$.

2(passo do resto): Se nenhum $LT(f_i)$ divide $LT(p)$, então o algoritmo soma $LT(p)$ ao resto.

Para mostrar que o algoritmo funciona, mostraremos que

$$f = a_1 f_1 + \cdots + a_s f_s + r + p \quad (2.1.9)$$

em todos os passos. Isto é verdade para os valores iniciais de $a_1, \dots, a_s, p$ e r . Suponha que (2.1.9) valha em um dado passo. Se o próximo passo é um passo da divisão, então algum $LT(f_i)$ divide $LT(p)$ e a igualdade

$$a_i f_i + p = \left(a_i + \frac{LT(p)}{LT(f_i)} \right) f_i + \left(p - \frac{LT(p)}{LT(f_i)} f_i \right)$$

mostra que $a_i f_i + p$ não se altera. Desde que as outras variáveis não são afetadas, (2.1.9) continua sendo verdadeira.

Se o próximo passo é um passo do resto então p e r são mudados, porém a soma $p + r$ permanece inalterada pois

$$p + r = (p - \text{LT}(p)) + (r - \text{LT}(p))$$

e novamente (2.1.9) continua sendo verdadeira.

O algoritmo se torna verdadeiro quando $p = 0$. Neste caso ficamos com

$$f = a_1 f_1 + \cdots + a_s f_s + r .$$

Desde que todos os termos somados a r não são divisíveis por nenhum $\text{LT}(f_i)$, temos que $a_1, \dots, a_s$ e r possuem as propriedades desejadas.

Finalmente precisamos mostrar que o algoritmo termina. Porém, basta observar que, cada vez que redefinimos a variável p , ou $p = 0$ ou $\text{multdeg}(p)$ diminui. Logo, se o algoritmo não terminasse, isto é, $p \neq 0$ sempre, teríamos uma seqüência decrescente infinita de $\text{multdeg}(p)$. Como nossa ordem é Artiniana, temos que $p = 0$ deve acontecer eventualmente e portanto o algoritmo deve terminar em um número finito de passos. ■

Exemplo 2.1.10:

Vejamos um exemplo de como funciona o algoritmo da divisão. Vamos dividir

$$f = x^2y + xy^2 + y^2 \quad \text{por} \quad f_1 = xy - 1 \quad \text{e} \quad f_2 = y^2 - 1$$

usando a ordem lexicográfica com $x > y$.

Fazemos da seguinte forma

$$a_1 : x + y$$

$$a_2 :$$

$$\begin{array}{rcl}
f_1 = xy - 1 & & x^2y + xy^2 + y^2 \\
& & \underline{-(x^2y - x)} \\
f_2 = y^2 - 1 & & xy^2 + x + y^2 \\
& & \underline{-(xy^2 - y)} \\
& & xy + y^2
\end{array}$$

Porém $LT(f_1)$ e $LT(f_2)$ não dividem $LT(x + y^2 + y) = x$ e $LT(f_2)$ divide y^2 .

Logo, mandamos x para o resto e continuamos com divisão

$$a_1 : x + y$$

$$a_2 : 1$$

$$\begin{array}{rcl}
f_1 = xy - 1 & & x^2y + xy^2 + y^2 \\
& & \underline{-(x^2y - x)} \\
f_2 = y^2 - 1 & & xy^2 + x + y^2 \\
& & \underline{-(xy^2 - y)} \\
& & x + y + y^2 \\
& & \underline{-(x + y + y^2)} \\
& & 0 \\
& & y^2 + y \\
& & \underline{-(y^2 - 1)} \\
& & y + 1 \\
& & \underline{-(y + 1)} \\
& & 0
\end{array}
\quad \Rightarrow \quad r = x$$

$$\Rightarrow r = x + y$$

$$\Rightarrow r = x + y + 1$$

Logo

$$x^2y + xy^2 + y^2 = (x + y)f_1 + f_2 + (x + y + 1) .$$

■

Observação: Os polinômios $a_1, \dots, a_s$ e r obtidos na divisão não são univocamente determinados. Se mudarmos a ordem de $f_1, \dots, f_s$, obteremos outros polinômios.

Teorema 2.1.11: Fixada uma ordem monomial, todo ideal $I \subseteq S$, com

$I \neq (0)$, possui uma base de Gröbner. Além disso, qualquer base de Gröbner de um ideal I é base de I .

Demonstração:

Seja I um ideal e considere $(LT(I))$. Como já vimos, $(LT(I))$ é um ideal monomial de $\mathcal{S}$ que é Noetheriano, logo existem $LT(g_1), \dots, LT(g_t)$ tal que

$$(LT(g_1), \dots, LT(g_t)) = (LT(I)) .$$

Afirmção: $I = (g_1, \dots, g_t)$.

Já temos que $(g_1, \dots, g_t) \subseteq I$. Seja $f \in I$. Pelo algoritmo da divisão , teorema (2.1.8), temos que f pode ser escrito na forma

$$f = a_1 g_1 + \dots + a_t g_t + r$$

onde nenhum dos termos de r é divisível por $LT(g_i)$, para todo i .

Porém $f \in I$ e $a_1 g_1 + \dots + a_t g_t \in I$, logo $f - \sum_{i=1}^t a_i g_i = r \in I$. Portanto se $r \neq 0$ temos $LT(r) \in (LT(I)) = (LT(g_1), \dots, LT(g_t))$. Como $(LT(I))$ é ideal monomial $LT(r)$ é divisível por $LT(g_i)$ para algum i , o que é um absurdo.

Logo $r = 0$ e assim $f = \sum_{i=1}^t a_i g_i \in (g_1, \dots, g_t)$. ■

Visto que todo ideal possui uma base de Gröbner, vamos demonstrar o que foi dito no início da seção. Primeiro vejamos um resultado que nos auxiliará.

Teorema 2.1.12(Macaulay): Seja $I \subseteq \mathcal{S}$ um ideal qualquer, $I \neq (0)$. Então temos que

$$B = \{ \text{monômios que não estão em } LT(I) \} .$$

é uma base do k espaço vetorial $\frac{\mathcal{S}}{I}$.

Demonstração:

Mostremos que B é linearmente independente.

Sejam $\{m_1, \dots, m_r\}$ um subconjunto finito de B e $u_i, i = 1, \dots, r \in k$. Denote por $\bar{m}_i = m_i + I$ e suponha que $p = \sum u_i \bar{m}_i = \bar{0}$, isto é, que $p = \sum u_i m_i \in I$. Suponha que $p \neq 0$. Logo $\text{LT}(p) \in \text{LT}(I)$. Mas $\text{LT}(p) = m_i$ para algum i , o que é uma contradição pois $m_i \in B$. Assim $p = 0$ e neste caso $u_i = 0$ para todo i .

Mostremos agora que B é um conjunto que gera o k -espaço vetorial $\frac{\mathcal{S}}{I}$.

Suponhamos que B não gere $\frac{\mathcal{S}}{I}$. Assim se considerarmos V o k -espaço vetorial gerado por B em $\mathcal{S}$, temos que

$$T = \mathcal{S} \setminus (V \cup I) \neq \emptyset.$$

Agora tome $f \in T$, tal que $\text{LT}(f)$ é mínimo. Se $\text{LT}(f) \in B$, então $g = f - \text{LT}(f)$ é um polinômio que não está em V nem em I e que possui termo inicial menor do que f , o que é absurdo.

Logo $\text{LT}(f) \in \text{LT}(I)$ e assim existe $h \in I$ tal que $\text{LT}(f) = \text{LT}(h)$. Logo $u = f - h$ tem termo inicial menor do que o termo inicial de f e não está em I nem em V , um absurdo novamente.

Logo, dado $f \in \mathcal{S}$, então ou $f \in I$ ou $f \in V$. ■

Agora já podemos demonstrar o que queremos:

Teorema 2.1.13: Seja $I \subseteq \mathcal{S}$ um ideal homogêneo. Então a função de Hilbert de $\frac{\mathcal{S}}{I}$ é a mesma função de $\frac{\mathcal{S}}{(\text{LT}(I))}$.

Demonstração:

Seja $B = \{\text{monômios que não estão em } \text{LT}(I)\}$. Seja $\mathcal{S}_d$ o conjunto dos elementos de grau d de $\mathcal{S}$ e considere $\bar{\mathcal{S}}_d$ a imagem de $\mathcal{S}_d$ em $\frac{\mathcal{S}}{I}$. Temos que

$$H\left(\frac{\mathcal{S}}{I}, d\right) = \dim_k \bar{\mathcal{S}}_d = \#(\mathcal{S}_d \cap B)$$

por (2.1.12) e pelo fato de I ser homogêneo.

$$\begin{aligned} H\left(\frac{\mathcal{S}}{(\text{LT}(I))}, d\right) &= \#\{m \in \mathcal{S}_d; m \text{ monômio } m \notin \text{LT}(I)\} \\ &= \#(\mathcal{S}_d \cap B). \end{aligned}$$

$$\text{Logo } H\left(\frac{\mathcal{S}}{I}, d\right) = H\left(\frac{\mathcal{S}}{(\text{LT}(I))}, d\right). \quad \blacksquare$$

Como dissemos no início do capítulo, o nosso interesse é calcular a função de Hilbert de $\frac{\mathcal{S}}{I}$ com I ideal homogêneo. Porém vimos na seção anterior que calcular a função de Hilbert de $\frac{\mathcal{S}}{I}$ é o mesmo que calcular a função de Hilbert de $\frac{\mathcal{S}}{(\text{LT}(I))}$, onde $(\text{LT}(I))$ é um ideal monomial. Vejamos então alguns meios de se calcular a função de Hilbert para $\frac{\mathcal{S}}{I}$ com I ideal monomial.

2.2 Função de Hilbert de $\frac{\mathcal{S}}{I}$, com I ideal monomial

Vamos nesta seção, mostrar um processo de como calcular a função de Hilbert de $\frac{\mathcal{S}}{I}$ com I ideal monomial. Antes vejamos algumas definições.

Definição 2.2.1: Seja m_1 e m_2 dois monômios em $\mathcal{S}$. Então podemos definir o mínimo múltiplo comum e o máximo divisor comum dos monômios m_1 e m_2 da seguinte forma:

Se

$$\begin{aligned} m_1 &= x_1^{a_1} \cdots x_n^{a_n} \\ m_2 &= x_1^{b_1} \cdots x_n^{b_n} \end{aligned}$$

então definimos

$$\text{mmc}(m_1, m_2) = x_1^{\max\{a_1, b_1\}} \cdots x_n^{\max\{a_n, b_n\}}$$

$$\text{mdc}(m_1, m_2) = x_1^{\min\{a_1, b_1\}} \dots x_n^{\min\{a_n, b_n\}}$$

Definição 2.2.2: Seja $I \subseteq \mathcal{S}$ um ideal monomial, isto é $I = (m_1, \dots, m_r)$ onde cada m_i é um monômio. Dizemos que o conjunto $\{m_1, \dots, m_r\}$ é um conjunto minimal de geradores de I se $m_i \nmid m_j$ para quaisquer i e j , $i \neq j$.

Observação: Dado $I \subseteq \mathcal{S}$ ideal monomial, I sempre possui um conjunto minimal de geradores.

Processo para calcular a função de Hilbert de $\frac{\mathcal{S}}{I}$ com I ideal monomial.

Seja, então, $\mathcal{S} = k[x_1, \dots, x_n]$ e $I = (m_1, \dots, m_s)$ ideal monomial de $\mathcal{S}$. Vamos fazer por indução sobre s .

$s = 1$ então $I = (m)$. Suponhamos que $\deg(m) = d$.

Logo temos

$$H\left(\frac{\mathcal{S}}{m}, i\right) = \dim_k \left(\frac{\mathcal{S}}{(m)}\right)_i.$$

Para $i = 0, \dots, d-1$ temos que

$$\left(\frac{\mathcal{S}}{(m)}\right)_i = \mathcal{S}_i.$$

Assim $\dim_k \left(\frac{\mathcal{S}}{(m)}\right)_i = \dim_k \mathcal{S}_i = \binom{n+i-1}{n-1}$, para $i = 0, \dots, d-1$.

$$\dim_k \left(\frac{\mathcal{S}}{(m)}\right)_d = \dim \mathcal{S}_d - 1$$

pois $\deg(m) = d$.

Seja $i > d$ então $i = d + \mu$. Logo, como queremos calcular a dimensão de $\left(\frac{\mathcal{S}}{(m)}\right)_i$, queremos saber o número de monômios de grau i de $\mathcal{S}$ que não são

múltiplos de m . Logo

$$\dim \left(\frac{\mathcal{S}}{(m)} \right)_i = \dim \mathcal{S}_i - \dim \mathcal{S}_\mu$$

pois se $\nu \in \mathcal{S}_\mu$ então $\nu \cdot m \in \mathcal{S}_i$ e portanto temos que eliminar todos os monômios da forma νm , com $\nu \in \mathcal{S}_\mu$. Assim

$$\dim \left(\frac{\mathcal{S}}{(m)} \right)_i = \binom{n+i-1}{n-1} - \binom{(i-d)+n-1}{n-1} \quad \forall i \geq d$$

Assim

$$H \left(\frac{\mathcal{S}}{(m)}, i \right) = \begin{cases} \binom{n+i-1}{n-1} & \text{se } i < d \\ \binom{n+i-1}{n-1} - \binom{n+i-d-1}{n-1} & \text{se } i \geq d. \end{cases}$$

Logo sabemos calcular a função de Hilbert de $\frac{\mathcal{S}}{(m)}$.

Suponhamos então $s > 1$ e que o resultado valha para todo número menor do que s , isto é, se I' é gerado por r elementos e $r < s$ então sabemos calcular a função de Hilbert de I' .

Seja $I = (m_1, \dots, m_s)$ onde $\{m_1, \dots, m_s\}$ é um conjunto minimal de geradores. Seja $n \in I$ um desses geradores minimais, que, sem perda de generalidade, podemos supor $n = m_s$. Logo $I = (n, I')$ e seja $d = \deg(n)$. Temos então uma sequência exata da seguinte forma:

$$\begin{array}{ccccccc} 0 & \rightarrow & \ker \varphi & \rightarrow & \mathcal{S}(-d) & \xrightarrow{\varphi} & \frac{\mathcal{S}}{I'} \xrightarrow{\pi} \frac{\mathcal{S}}{I} \rightarrow 0 \\ & & & & s & \longmapsto & \overline{sn} \end{array} \quad (2.2.3)$$

onde

$$\mathcal{S}(-d) = \bigoplus_{i=0}^{\infty} \mathcal{S}'_i \quad \text{onde } \mathcal{S}'_i = \mathcal{S}_{i-d}.$$

Tal seqüência exata é de grau zero, isto é, se

$$\begin{aligned} x \in \mathcal{S}'_i &\Rightarrow \varphi(x) \in \left(\frac{\mathcal{S}}{I'}\right)_i \text{ pois} \\ x \in \mathcal{S}'_i &\Rightarrow x \in \mathcal{S}_{i-d} \Rightarrow nx \in \mathcal{S}_i \Rightarrow \overline{nx} \in \left(\frac{\mathcal{S}}{I'}\right)_i. \end{aligned}$$

Temos que

$$\begin{aligned} \ker(\varphi) &= \{\mu \in \mathcal{S}(-d); \varphi(\mu) = \overline{0}\} \\ &= \{\mu \in \mathcal{S}(-d) \mid \overline{sn} = 0\} \\ &= \{\mu \in \mathcal{S}(-d); \mu n \in I'\}. \end{aligned}$$

Como $\mathcal{S}(-d) \subseteq \mathcal{S}$, podemos pensar que

$$\ker(\varphi) = \{\mu \in \mathcal{S}; \mu n \in I'\} = (I' : n)$$

devendo porém levar em consideração a alteração nos graus.

Como I' é ideal de $\mathcal{S}$ e $I' = (m_1, \dots, m_{s-1})$, temos que

$$J = (I' : n) = \left(\frac{m_1}{\text{mdc}(m_1, n)}, \dots, \frac{m_{s-1}}{\text{mdc}(m_{s-1}, n)} \right) \quad (\text{A.2.1})$$

Logo a seqüência exata (2.2.3) induz uma seqüência exata, também de grau zero, da forma:

$$0 \rightarrow \left(\frac{\mathcal{S}}{J}\right)(-d) \rightarrow \frac{\mathcal{S}}{I'} \rightarrow \frac{\mathcal{S}}{I} \rightarrow 0$$

e, portanto, para cada $i \in \mathbb{N}$ temos

$$0 \rightarrow \left(\frac{\mathcal{S}}{J}\right)_{i-d} \rightarrow \left(\frac{\mathcal{S}}{I'}\right)_i \rightarrow \left(\frac{\mathcal{S}}{I}\right)_i \rightarrow 0 \quad (2.2.4)$$

Porém J e I' possuem menos geradores do que I e portanto por hipótese de indução sabemos calcular sua função de Hilbert. Logo por (2.2.4) temos que

$$H\left(\frac{\mathcal{S}}{I}, i\right) = H\left(\frac{\mathcal{S}}{I'}, i\right) - H\left(\frac{\mathcal{S}}{J}, i-d\right) \quad \blacksquare$$

Observação: Ainda é um problema em aberto saber qual a melhor escolha para o gerador n .

Para ilustrar o processo acima, vamos fazer um exemplo.

Exemplo 2.2.5: Seja $\mathcal{S} = k[x_1, x_2, x_3, x_4]$ e $I = (x_1x_3, x_1x_4, x_2x_4)$. Vamos calcular a função de Hilbert de $\frac{\mathcal{S}}{I}$.

Tome $n = x_1x_3$; $I' = (x_1x_4, x_2x_4)$ e

$$J = \left(\frac{x_1x_4}{x_1}; x_2x_4 \right) = (x_4, x_2x_4) = (x_4) .$$

Assim, temos que

$$\frac{\mathcal{S}}{J} = \frac{k[x_1, x_2, x_3, x_4]}{(x_4)} \simeq k[x_1, x_2, x_3] .$$

Portanto

$$H\left(\frac{\mathcal{S}}{I}, t\right) = H\left(\frac{\mathcal{S}}{I'}, t\right) - H(k[x_1, x_2, x_3], t - 2)$$

Usando o mesmo processo para I' temos

$$I' = (n_1, I'') \text{ onde } n_1 = x_1x_4 ; I'' = (x_2x_4)$$

$$\text{e } J' = \left(\frac{x_2x_4}{x_4} \right) = (x_2) \text{ e portanto } \frac{\mathcal{S}}{J'} = k[x_1, x_3, x_4]$$

Porém $k[x_1, x_3, x_4] \simeq k[x_1, x_2, x_3]$. Assim

$$H\left(\frac{\mathcal{S}}{I'}, t\right) = H\left(\frac{\mathcal{S}}{(x_1x_4)}, t\right) - H(k[x_1, x_2, x_3], t - 2)$$

e portanto

$$H\left(\frac{\mathcal{S}}{I}, t\right) = H\left(\frac{\mathcal{S}}{(x_1x_4)}, t\right) - 2H(k[x_1, x_2, x_3], t - 2) .$$

Isto é, $H(\frac{\mathcal{S}}{I}, t) = H(\mathcal{S}, t)$ se $t = 0, 1$ ou

$$\begin{aligned} H\left(\frac{\mathcal{S}}{I}, t\right) &= \binom{4+t-1}{4-1} - \binom{4+t-2-1}{4-1} - \binom{3-1+t-2}{3-1} \\ &= \binom{t+3}{3} - \binom{t+1}{3} - 2\binom{t}{2} = 3t + 1 \end{aligned}$$

se $t \geq 2$. ■

2.3 Anéis de Stanley-Reisner

Estes anéis são os objetos centrais de um ramo da Álgebra Comutativa, chamado de Álgebra Comutativa Combinatória e foi criado por Hochster e Stanley em meados dos anos 70.

Os objetos considerados são os complexos simpliciais que se associam a objetos algébricos chamados de Anéis de Stanley-Reisner. Neste exemplo, veremos como o número de faces de um complexo está relacionado com a série de Hilbert do correspondente anel de Stanley-Reisner.

Definição 2.3.1: Seja $V = \{v_1, \dots, v_n\}$ um conjunto finito. Um complexo simplicial Δ em V é uma coleção de subconjuntos de V tais que

- i. $\{v_i\} \in \Delta \forall i = 1, \dots, n$.
- ii. $G \in \Delta$ e $F \subseteq G \Rightarrow F \in \Delta$.

Os elementos de Δ são chamados de *faces* do complexo.

Definição 2.3.2: A dimensão de uma face F , denotada por $\dim F$, é dada por

$$\dim F = |F| - 1 .$$

A dimensão do complexo simplicial Δ é dada por

$$\dim \Delta = \max\{\dim F; F \in \Delta\} .$$

Observações:

- i. Note que o conjunto vazio $\emptyset$ é uma face de dimensão -1 de qualquer complexo simplicial não vazio.

- ii. As faces de dimensão zero são chamadas de *vértices*; as de dimensão 1 são chamadas de *arestas*. As faces maximais em relação à inclusão são chamadas *facetas* do complexo simplicial.

Definição 2.3.3: Seja Δ um complexo simplicial de dimensão $d-1 \geq 0$ em um conjunto de vértices V . Denotamos por f_i o número de faces i -dimensionais de Δ .

Assim temos que

$$f_0 = |V| \text{ e } f_{-1} = 1$$

visto que $\emptyset \in \Delta$.

O f -vetor de Δ , denotado por $f(\Delta)$, é a seguinte d -upla

$$f(\Delta) = (f_0, f_1, \dots, f_{d-1}) .$$

Definição 2.3.4: Seja Δ um complexo simplicial em um conjunto de vértices $\{v_1, \dots, v_n\}$ e k um anel. O *anel de Stanley-Reisner* do complexo Δ , com respeito a k , é a k -álgebra homogênea definida por

$$k[\Delta] = \frac{k[x_1, \dots, x_n]}{I_\Delta}$$

onde I_Δ é o ideal gerado por todos os monômios $x_{i_1} \cdots x_{i_s}$ tais que $\{v_{i_1}, \dots, v_{i_s}\} \notin \Delta$.

Observações:

- i. A escolha da letra k na definição indica que, a menos de exceções, sempre teremos um corpo para o anel de coeficientes.

- ii. O ideal I_Δ é gerado por monômios livres de quadrados. Por outro lado, se $I \subseteq (x_1, \dots, x_n)^2$ é ideal gerado por monômios livres de quadrados, então

$$\frac{k[x_1, \dots, x_n]}{I} \simeq k[\Delta]$$

para algum complexo simplicial Δ , o que nos dá uma bijeção entre os complexos simpliciais e os ideais monomiais livres de quadrados. Tal bijeção inverte inclusão, isto é, se Δ e Δ' são dois complexos sobre um mesmo conjunto de vértices então

$$\Delta \subseteq \Delta' \Leftrightarrow I_{\Delta'} \subseteq I_\Delta .$$

Vejamos mais uma definição que nos ajudará na demonstração do que queremos:

Definição 2.3.5: Seja $a \in \mathbb{N}^n$. Definimos o suporte de a , denotado por $\text{supp}(a)$ como sendo

$$\text{supp}(a) = \{v_i; a_i > 0\} .$$

Considere Δ um complexo e $k[\Delta] = k[x_1, \dots, x_n]$.

Lema 2.3.6: Sendo $x^a = x_1^{a_1} \cdots x_n^{a_n}$, $a \in \mathbb{N}^n$ temos que $x^a \neq 0$ se, e somente se, $\text{supp } a \in \Delta$.

Demonstração:

Mostremos que

$$x^a = 0 \text{ se, e somente se, } \text{supp } a \notin \Delta .$$

$$(\Rightarrow) x^a = 0.$$

$$x^a = (x_1^{a_1} \cdots x_n^{a_n}) + I_\Delta .$$

Mas se $x^a = 0$, então $x_1^{a_1} \cdots x_n^{a_n} \in I_\Delta$. Logo

$$\text{supp } a = \{v_i; a_i > 0\} \notin \Delta$$

pela definição de I_Δ .

$$(\Leftarrow) \text{supp } a \notin \Delta.$$

Seja $\text{supp } a = \{v_{i_1}, \dots, v_{i_s}\}$.

$$\text{supp } a \notin \Delta \Rightarrow x_1^{a_{i_1}} \cdots x_{i_s}^{a_{i_s}} \text{ é um dos geradores de } I_\Delta$$

$$\Rightarrow x_1^{a_1} \cdots x_n^{a_n} \in I_\Delta \Rightarrow x_1^{a_1} \cdots x_n^{a_n} + I_\Delta = x^a = 0.$$

■

Para relacionarmos o f -vetor de um complexo simplicial com a função de Hilbert de $k[\Delta]$, vamos introduzir uma noção de N^n -gradação em $k[\Delta]$. Temos que $\mathcal{S} = k[x_1, \dots, x_n]$ pode ser N^n -graduado da seguinte forma

$$\mathcal{S} = \bigoplus_{a \in N^n} \mathcal{S}_a \quad \text{onde } \mathcal{S}_a = \{cx^a; c \in k\}$$

onde $x^a = x_1^{a_1} \cdots x_n^{a_n}$; $a = (a_1, \dots, a_n) \in N^n$.

Dado um ideal $I \subseteq \mathcal{S}$ monomial temos que I também é N^n -graduado e portanto $\frac{\mathcal{S}}{I}$ herda uma N^n -gradação natural dada por

$$\left(\frac{\mathcal{S}}{I}\right)_a = \frac{\mathcal{S}_a}{I_a} = \begin{cases} \mathcal{S}_a & \text{se } x^a \notin I \\ 0 & \text{se } x^a \in I \end{cases} \quad \forall a \in N^n.$$

Logo os anéis de Stanley-Reisner possuem uma N^n -gradação.

Teorema 2.3.7: Seja Δ um complexo com f -vetor $(f_0, \dots, f_{d-1})$. Então

$$H_{k[\Delta]}(t) = \sum_{i=-1}^{d-1} \frac{f_i t^{i+1}}{(1-t)^{i+1}}.$$

Demonstração:

Baseado na $\mathbf{N}^n$ -graduação de $k[\Delta]$ definimos

$$\begin{aligned} H(k[\Delta], \cdot) : \quad \mathbf{N}^n &\rightarrow \mathbf{Z} \\ a &\mapsto H(k[\Delta], a) = l(k[\Delta]_a) . \end{aligned}$$

como sendo a função de Hilbert de $k[\Delta]$ com relação à $\mathbf{N}^n$ -graduação. Logo, a série de Hilbert de $k[\Delta]$, com relação à $\mathbf{N}^n$ -graduação, é

$$H_{k[\Delta]}(t) = \sum_{a \in \mathbf{N}^n} H(k[\Delta], a) t^a = \sum_{a \in \mathbf{N}^n} l(k[\Delta]_a) t^a \quad (2.3.8)$$

onde $a = (a_1, \dots, a_n)$, $t = (t_1, \dots, t_n)$ e $t^a = t_1^{a_1} \dots t_n^{a_n}$. (1)

Logo

$$H_{k[\Delta]}(t) = \sum_{a \in \mathbf{N}^n} l(k[\Delta]_a) t^a .$$

Mais ainda, se $\text{supp } a \notin \Delta$, então, pelo Lema (2.3.6), $x^a = 0$. Logo

$$x^a \in [I_\Delta]_a \text{ e então } \frac{k[x_1, \dots, x_n]_a}{[I_\Delta]_a} = 0 .$$

Portanto

$$\begin{aligned} H_{k[\Delta]}(t) &= \sum_{a \in \mathbf{N}^n} l(k[\Delta]_a) t^a = \sum_{\substack{a \in \mathbf{N}^n \\ \text{supp } a \in \Delta}} l(k[\Delta]_a) t^a \\ &\stackrel{l(k[\Delta]_a)=1}{=} \sum_{\substack{a \in \mathbf{N}^n \\ \text{supp } a \in \Delta}} t^a = \sum_{F \in \Delta} \sum_{\substack{a \in \mathbf{N}^n \\ \text{supp } a = F}} t^a . \end{aligned}$$

Se $F = \emptyset$ então

$$\sum_{\text{supp } a = \emptyset} t^a = 1$$

pois $\text{supp } a = \emptyset$ se, e somente se, $a = (0, \dots, 0)$.

Se $F \neq \emptyset$.

Afirmção: $\sum_{\text{supp } a = F} t^a = \prod_{v_i \in F} \frac{t_i}{(1 - t_i)} .$

Façamos por indução sobre $\#F$.

$$\#F = 1 \Rightarrow F = \{v_i\}.$$

$$\text{supp } a = \{v_i\} \Rightarrow a = (0, \dots, 0, a_i, 0, \dots, 0); \quad a_i > 0.$$

Logo

$$\begin{aligned} \sum_{\text{supp } a = \{v_i\}} t^a &= \sum_{j=1}^{\infty} t_i^j = \frac{t_i}{1-t_i} \text{ pois} \\ \sum_{i=0}^{\infty} t^i &= \frac{1}{1-t} \Rightarrow \sum_{i=1}^{\infty} t^i = \frac{1}{1-t} - 1 = \frac{t}{1-t}. \end{aligned}$$

Suponhamos o resultado válido para uma face com cardinalidade $r-1$ e mostremos que o resultado vale para uma face com cardinalidade r ($r \leq n$). Suponhamos também, sem perda de generalidade, que $F = \{v_1, \dots, v_r\}$.

$$\sum_{\text{supp } a = F} t^a = \sum_{(a_1, \dots, a_r) \in \mathbb{N}^r} t_1^{a_1} \dots t_r^{a_r}$$

Porém

$$\sum_{(a_1, \dots, a_r) \in \mathbb{N}^r} t_1^{a_1} \dots t_r^{a_r} = (t_1 + t_1^2 + \dots) \left(\sum_{(b_2, \dots, b_r) \in \mathbb{N}^{r-1}} t_2^{b_2} \dots t_r^{b_r} \right)$$

Por hipótese de indução temos que

$$\sum_{(b_2, \dots, b_r) \in \mathbb{N}^{r-1}} t_2^{b_2} \dots t_r^{b_r} = \sum_{\text{supp } a = \overline{F}} \bar{t}^a$$

com $\#\overline{F} = r-1$ e $\overline{F} \subset F$, logo $\overline{F}$ é face.

Assim

$$\sum_{\text{supp } a = \overline{F}} \bar{t}^a = \prod_{i=2}^r \frac{t_i}{1-t_i}.$$

Temos também que

$$\sum_{j=1}^{\infty} t_1^j = \frac{t_1}{1-t_1} \text{ e portanto}$$

$$\sum_{\text{supp } a=F} t^a = \prod_{v_i \in F} \frac{t_i}{1-t_i}$$

Logo, se entendemos que o produto sobre um conjunto de índices vazios é 1, conseguimos que

$$H_{k[\Delta]}(t) = \sum_{F \in \Delta} \prod_{v_i \in F} \frac{t_i}{1-t_i}. \quad (2.3.9)$$

Porém, estamos interessados na série de Hilbert de $k[\Delta]$ associada à $\mathbf{N}$ -graduação de $k[\Delta]$. Porém, observamos que, dado $i \in \mathbf{Z}$

$$k[\Delta]_i = \bigoplus_{\substack{a \in \mathbf{N}^n \\ |a|=i}} k[\Delta]_a$$

onde $|a| = \sum_{i=1}^n a_i$.

Tínhamos, em (2.3.8), que

$$\begin{aligned} H_{k[\Delta]}(t_1, \dots, t_n) &= \sum_{a \in \mathbf{Z}^n} H(k[\Delta], a) t^a \\ &= \sum_i \left(\sum_{\substack{a \in \mathbf{N}^n \\ |a|=i}} H(k[\Delta], a) t^a \right). \end{aligned}$$

Como

$$k[\Delta]_i = \bigoplus_{\substack{a \in \mathbf{N}^n \\ |a|=i}} k[\Delta]_a \Rightarrow H(k[\Delta], i) = \sum_{\substack{|a|=i \\ a \in \mathbf{N}^n}} H(k[\Delta], a).$$

Assim, se fizermos $t_i = t \ \forall i = 1, \dots, n$, teremos

$$H_{k[\Delta]}(t) = \sum_i \left(\sum_{|a|=i} H(k[\Delta], a) \right) t^i = \sum_i H(k[\Delta], i) t^i$$

que é a função de Hilbert de $k[\Delta]$ com relação a uma $\mathbf{Z}$ -graduação.

Portanto, para conseguirmos a série de Hilbert de $k[\Delta]$ com relação a uma $\mathbf{Z}$ -graduação, basta substituímos todos os t_i 's em (2.3.9) por um único t .

Logo

$$\begin{aligned}
 H_{k[\Delta]}(t) &= \sum_{F \in \Delta} \prod_{v_i \in F} \frac{t}{1-t} = 1 + \sum_{\substack{F \in \Delta \\ F \neq \emptyset}} \prod_{v_i \in F} \frac{t}{1-t} \\
 &= 1 + \sum_{\substack{\dim F=0 \\ (\# F=1)}} \frac{t}{1-t} + \sum_{\substack{\dim F=1 \\ (\# F=2)}} \frac{t^2}{(1-t)^2} + \cdots + \sum_{\substack{\dim F=d-1 \\ (\# F=d)}} \frac{t^d}{(1-t)^d}.
 \end{aligned}$$

Porém, existem f_i faces i -dimensionais ($i = 0, \dots, d-1$). Assim

$$\begin{aligned}
 H_{k[\Delta]}(t) &= 1 + f_0 \frac{t}{1-t} + f_1 \frac{t^2}{(1-t)^2} + \cdots + f_{d-1} \frac{t^d}{(1-t)^d} \\
 &= f_{-1} \left(\frac{t}{1-t} \right)^0 + f_0 \left(\frac{t}{1-t} \right)^1 + \cdots + f_{d-1} \left(\frac{t}{1-t} \right)^d.
 \end{aligned}$$

Portanto

$$H_{k[\Delta]}(t) = \sum_{i=1}^{d-1} f_i \left(\frac{t}{1-t} \right)^{i+1}$$

■

Corolário 2.3.10: A função de Hilbert de $k[\Delta]$ é a seguinte

$$H(k[\Delta], n) = \begin{cases} 1 & \text{se } n = 0 \\ \sum_{i=0}^{d-1} f_i \binom{n-1}{i} & \text{se } n > 0. \end{cases}$$

Demonstração:

Pelo Teorema (2.3.7), temos que a série de Hilbert de $k[\Delta]$ é da forma

$$H_{k[\Delta]}(t) = \sum_{i=1}^{d-1} f_i \left(\frac{t}{1-t} \right)^{i+1}$$

Temos também que $\frac{t}{1-t} = \sum_{j=1}^{\infty} t^j$.

Logo

$$H_{k[\Delta]}(t) = f_{-1} + f_0 \left(\frac{t}{1-t} \right) + \cdots + f_{d-1} \left(\frac{t}{1-t} \right)^d .$$

Temos ainda que

$$\begin{aligned} f_j \left(\frac{t}{1-t} \right)^{j+1} &= f_j (t + t^2 + \cdots + t^n + \cdots)^{j+1} \\ &= f_j \left[\binom{j+1-1}{j} t^{j+1} + \binom{j+2-1}{j} t^{j+2} + \cdots \right. \\ &\quad \left. + \binom{s-1}{j} t^s + \cdots \right] . \end{aligned} \quad (2.3.11)$$

Logo

$$H_{k[\Delta]}(t) = f_{-1} + f_0(t + t^2 + \cdots) + f_1(t^2 + 2t^3 + \cdots) + \cdots + f_{d-1}(t^d + \cdots) ,$$

donde temos que

$$H(k[\Delta], 0) = f_{-1} = 1$$

$$H(k[\Delta], 1) = f_0$$

$$H(k[\Delta], 2) = f_0 + f_1$$

$\vdots$

$$H(k[\Delta], n) = f_0 + \binom{n-1}{1} f_1 + \cdots + \binom{n-1}{d-1} f_{d-1} . \text{ por (2.3.11)}$$

Portanto

$$H(k[\Delta], n) = \begin{cases} 1 & \text{se } n = 0 \\ \sum_{i=0}^{d-1} f_i \binom{n-1}{i} & \text{se } n > 0 \end{cases}$$

■

Retornando ao exemplo (2.2.5), vemos que o ideal $I = (x_1x_3, x_1x_4, x_2x_4)$ é um ideal livre de quadrados e como vimos nesta seção podemos associá-lo

a um complexo e calcularmos a sua função de Hilbert. Vejamos qual é este complexo.

$$V = \{v_1, v_2, v_3, v_4\}$$

$I_\Delta = (x_1x_3, x_1x_4, x_2x_4)$ é o ideal gerado pelas não faces.

Logo temos que

$$\Delta = \{\emptyset, \{v_1\}, \{v_2\}, \{v_3\}, \{v_4\}, \{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}\}$$

Como foi visto temos que

$$f_{-1} = 1$$

$$f_0 = 4$$

$$f_1 = 3$$

Logo, a função de Hilbert de $\frac{S}{I_\Delta}$ é dada por

$$H\left(\frac{S}{I_\Delta}, t\right) = \begin{cases} 1 & \text{se } t = 0 \\ \sum_{i=0}^1 f_i \binom{t-1}{i} = f_0 + (t-1)f_1 = 1 + 3t & \text{se } t \geq 1 \end{cases}$$

Vimos neste capítulo duas formas de se calcular a função de Hilbert de $\frac{S}{I}$, com I ideal monomial. O que nos parece interessante é que se I é um ideal livre de quadrados, fica mais fácil calcular a função de Hilbert usando a idéia de complexos. Por outro lado, se I não é livre de quadrados, o primeiro processo é a uma boa maneira de se calcular a função de Hilbert.

Capítulo 3

Os teoremas de Green e Macaulay

Nos dois primeiros capítulos estudamos a função de Hilbert, vimos alguns exemplos e uma aplicação. Vimos também que é uma função numérica, isto é, uma função de $\mathbf{Z}$ em $\mathbf{Z}$ ou de $\mathbf{N}$ em $\mathbf{N}$ em alguns casos.

Uma pergunta que poderia surgir é a seguinte:

Quando uma função numérica é uma função de Hilbert de algum anel ou módulo graduado?

Neste capítulo nosso objetivo é demonstrar o teorema de Macaulay que estabelece condições para que uma função de $\mathbf{N}$ em $\mathbf{N}$ seja função de Hilbert de uma k -álgebra homogênea.

Neste capítulo trabalhamos com

$$R = \bigoplus_{n \geq 0} R_n$$

uma k -álgebra homogênea onde $R_0 = k$ é um corpo.

Observação: Se R é uma k -álgebra homogênea então $R = \frac{\mathcal{S}}{I}$ onde I é ideal homogêneo de $\mathcal{S} = k[x_1, \dots, x_n]$ e $x_i = x_i + I$.

3.1 Resultados Auxiliares

Nesta seção veremos todos os teoremas e lemas que nos ajudarão na demonstração do teorema principal de Macaulay.

Definição 3.1.1: Um conjunto não vazio M de monômios nas indeterminadas $x_1, \dots, x_m$ é chamado um *ideal de ordem de monômios* se dado $m \in M$ e $m' \in \mathcal{S}$ tal que $m'|m$ então $m' \in M$ ou equivalentemente se

$$\begin{aligned} x_1^{a_1} \cdots x_m^{a_m} \in M \quad \text{e} \quad 0 \leq b_i \leq a_i, i = 1, \dots, m \\ \Rightarrow x_1^{b_1} \cdots x_m^{b_m} \in M. \end{aligned}$$

Observação: Sejam M um ideal de ordem de monômios e M' o complementar de M com relação ao conjunto dos monômios de $\mathcal{S}$. Temos que M' é uma k -base para o ideal $I = (m; m \notin M)$

O que faremos agora é mostrar que R possui uma k -base formada por monômios em $x_1, \dots, x_m$.

Teorema 3.1.2 (Macaulay): Seja $R = k[x_1, \dots, x_n]$ uma k -álgebra homogênea com k corpo e considere

$$\begin{aligned} \pi : k[x_1, \dots, x_m] &\rightarrow R \\ x_i &\mapsto x_i, i = 1, \dots, m. \end{aligned}$$

Então existe um ideal de ordem de monômios $M \subseteq k[x_1, \dots, x_m]$ tal que $\pi(M)$ é uma k -base de R .

Demonstração:

Seja V o conjunto de todos os monômios de $k[x_1, \dots, x_m]$. Vamos definir em V uma ordem denominada ordem lexicográfica graduada reversa da se-

guinte forma: dado $u = x_1^{a_1} \cdots x_m^{a_m}$ e $v = x_1^{b_1} \cdots x_m^{b_m}$, dizemos que $u \leq v$ se a última componente não nula do vetor $(b_1 - a_1, \dots, \sum_i (b_i - a_i))$ for positiva.

Tal ordem é monomial e assim todo subconjunto de V possui um elemento minimal com relação a esta ordem.

Seja a seqüência de monômios $u_1, u_2, \dots$ definida recursivamente por: $u_1 = 1$ e se $u_1, \dots, u_i$ já estão definidos, tomamos u_{i+1} o menor elemento tal que $\pi(u_1), \dots, \pi(u_i), \pi(u_{i+1})$ são linearmente independentes sobre k . Se tal u_{i+1} não existir, então a seqüência termina com u_i .

Afirmção: $M = \{u_1, u_2, \dots\}$ é um ideal de ordem de monômios e é tal que

$$\pi(M) \text{ é uma } k\text{-base de } R.$$

(i) $\pi(M) = \{\pi(u_1), \pi(u_2), \dots\}$ é um conjunto linearmente independente por construção.

(ii) Mostremos que $\pi(M)$ gera R como um k -espaço.

Seja v um monômio em R então $v = \pi(u)$ com $u \in V$.

Se $\pi(u) = v$ for LD com $\pi(u_1)$, nada a fazer. Caso contrário, v e $\pi(u_1)$ são LI, então existe $u_2 \in V$ tal que $u_2 \leq u$ de forma que $\pi(u_1)$ e $\pi(u_2)$ são LI.

Se $v, \pi(u_1), \pi(u_2)$ são LD, também não há mais nada a fazer. Caso contrário, existe $u_3 \in V$ com $u_3 \leq u$ tal que $\pi(u_1), \pi(u_2), \pi(u_3)$ são LI. Seguindo o mesmo raciocínio, encontraremos $u_4, u_5, \dots, u_n$ de forma que $\pi(u_1), \pi(u_2), \dots, \pi(u_n), v$ são LD, pois existe somente um número finito de monômios em V que são menores do que u .

Logo

$$v = \sum_{i=1}^n \lambda_i \pi(u_i)$$

e portanto $\pi(M)$ é uma k -base de R visto que todo elemento de R é uma soma de monômios e todos os monômios são gerados linearmente por elementos de $\pi(M)$.

(iii) Mostremos que M é um ideal de ordem de monômios.

Suponhamos que não, então existe $u_{i_0} \in M$ e $u \in V \setminus M$ tal que

$$u_{i_0} = ux_j \quad \text{para algum } x_j.$$

Temos que

$$\pi(u) = \sum_{i=1}^n \lambda_i \pi(u_i)$$

com $u_i \in M$ e mais ainda, $u_i < u$ e $\lambda_i \in k$, pois $u \notin M$. Assim

$$\begin{aligned} \pi(u_{i_0}) &= \pi(ux_j) = \pi(u)\pi(x_j) = \sum_i \lambda_i \pi(u_i)\pi(x_j) \\ &= \sum_i \lambda_i \pi(u_i x_j) \end{aligned}$$

Portanto $u_i x_j < ux_j = u_{i_0}$, qualquer que seja i .

Porém

$$\pi(u_i x_j) = \sum_{r_{ij}} \beta_{r_{ij}} \pi(u_{r_{ij}}) \quad \text{com } u_{r_{ij}} \leq u_i x_j.$$

Logo

$$\pi(u_{i_0}) = \sum \gamma_s \pi(u_s) \quad \text{com } u_s \in M \text{ e } u_s < u_{i_0}$$

o que é absurdo pela a construção de M .

Portanto M é um ideal de ordem de monômios e $\pi(M)$ é uma k -base para R . ■

Corolário 3.1.3: Seja $J = (m; m \in M')$. Então a k -álgebra homogênea R e $k[x_1, \dots, x_m]/J$ têm a mesma função de Hilbert.

Demonstração:

Temos que

$$H(R, n) = \dim R_n = \#(\pi(M) \cap R_n)$$

$$\begin{aligned}
H(k[x_1, \dots, x_m]/J, n) &= \text{n}^\circ \text{ de mon\^omios de } k[x_1, \dots, x_m] \\
&\quad \text{de grau total } n \text{ e n\~ao est\~ao em } J \\
&= \text{n}^\circ \text{ de mon\^omios de } k[x_1, \dots, x_m] \\
&\quad \text{de grau total } n \text{ e que est\~ao em } M
\end{aligned}$$

Logo

$$H(R, n) = H(k[x_1, \dots, x_m]/J, n) .$$

■

Definição 3.1.4: Seja $\mathcal{S} = k[x_1, \dots, x_m]$ e $\mathcal{S}_d$ o k -espaço vetorial gerado pelos monômios de grau d e tome $u \in \mathcal{S}_d$ monômio. Definimos

$$\begin{aligned}
\mathcal{L}_u &= \{v \in \mathcal{S}_d, v \text{ mon\^omio} \ ; v < u\} \\
\mathcal{R}_u &= \{v \in \mathcal{S}_d, v \text{ mon\^omio} \ ; v \geq u\}
\end{aligned}$$

onde a ordem considerada é a ordem lexicográfica graduada reversa.

Observação: $\mathcal{R}_{x_1} = \{x_1, x_2, \dots, x_m\}$.

O que vamos mostrar agora é que $\mathcal{L}_u$ admite uma decomposição natural. Veremos isto no seguinte lema:

Lema 3.1.5: Dado $u \in \mathcal{S}_d$, $u = x_{j(1)} \cdots x_{j(d)}$, temos que

$$\mathcal{L}_u = \dot{\cup}_{i=1}^d [x_1, \dots, x_{j(i)-1}]_i x_{j(i+1)} \cdots x_{j(d)}$$

onde $[x_1, \dots, x_{j(i)-1}]_i$ é o conjunto dos monômios de grau i nas variáveis $x_1, \dots, x_{j(i)-1}$.

Demonstração:

Seja i o maior inteiro tal que x_i divide u . Logo, podemos escrever

$$\mathcal{L}_u = \mathcal{L}'_u \dot{\cup} \mathcal{L}''_u x_i \text{ onde}$$

$$\mathcal{L}'_u = \left\{ \begin{array}{l} \text{monômios de grau } d \text{ nas} \\ \text{variáveis } x_1, \dots, x_{i-1} . \end{array} \right\}$$

e $\mathcal{L}''_u = \mathcal{L}_{x_i^{-1}u}$.

Usando a mesma idéia, podemos decompor $\mathcal{L}''_u$ e assim sucessivamente. Logo, se escrevemos

$$u = x_{j(1)}x_{j(2)} \cdots x_{j(d)} \quad (u \in \mathcal{S}_d)$$

com $1 \leq j(1) \leq j(2) \leq \cdots \leq j(d)$ temos que

$$\mathcal{L}_u = [x_1, x_2, \dots, x_{j(d)-1}]_d \dot{\cup} \mathcal{L}_{x_{j(d)}^{-1}u} x_{j(d)} .$$

Porém

$$u \cdot x_{j(d)}^{-1} = x_{j(1)} \cdots x_{j(d-1)}$$

e temos também que

$$\mathcal{L}_{x_{j(d)}^{-1}u} = [x_1, \dots, x_{j(d-1)-1}]_{d-1} \dot{\cup} \mathcal{L}_{x_{j(d-1)}^{-1}x_{j(d)}^{-1}u} x_{j(d-1)}$$

Portanto

$$x_{j(d)} \mathcal{L}_{x_{j(d)}^{-1}u} = [x_1, \dots, x_{j(d-1)-1}]_{d-1} x_{j(d)} \dot{\cup} \mathcal{L}_{x_{j(d-1)}^{-1}x_{j(d)}^{-1}u} x_{j(d)} x_{j(d-1)} .$$

Seguindo raciocínio análogo chegaremos a

$$\mathcal{L}_u = \dot{\cup}_{i=1}^d [x_1, \dots, x_{j(i)-1}]_i x_{j(i+1)} \cdots x_{j(d)}$$

que é chamada a decomposição natural de $\mathcal{L}_u$. ■

Observação: Com esta decomposição temos que

$$|\mathcal{L}_u| = \sum_{i=1}^d |[x_1, \dots, x_{j(i)-1}]_i|$$

Porém

$$\begin{aligned} |[x_1, \dots, x_{j(i)-1}]_i| &= \binom{j(i) - 1 + i - 1}{j(i) - 1 - 1} \\ &= \binom{j(i) + i - 2}{j(i) - 2} = \binom{j(i) + i - 2}{i} \end{aligned}$$

Logo

$$|\mathcal{L}_u| = \sum_{i=1}^d \binom{j(i) + i - 2}{i} = \sum_{i=1}^d \binom{k(i)}{i}$$

com $k(i) = j(i) + i - 2$ e $k(d) > k(d-1) > \dots > k(1) \geq 0$.

O que observamos é que esses números inteiros não negativos $|\mathcal{L}_u|$ podem ser escritos como uma somatória binomial. Este resultado pode ser generalizado pelo seguinte lema:

Lema 3.1.6: Seja d um número inteiro positivo qualquer.

Qualquer $a \in \mathbb{N}$ pode ser escrito unicamente na seguinte forma

$$a = \binom{k(d)}{d} + \dots + \binom{k(1)}{1},$$

onde $k(d) > k(d-1) > \dots > k(1) \geq 0$.

Demonstração:

Vamos assumir que $\binom{\mu}{l} = 0$ se $\mu < l$.

(i) *Existência:* Façamos por indução sobre a . Para $a = 1$, podemos escrever

$$1 = \binom{d}{d} + \binom{d-2}{d-1} + \dots + \binom{0}{1}$$

Suponhamos que o resultado vale para qualquer número menor do que a e mostremos que vale para a .

Tome $k(d)$ como sendo o máximo dos números positivos tais que $\binom{k(d)}{d} \leq a$. Se $a = \binom{k(d)}{d}$ então

$$a = \sum_{i=1}^d \binom{k(i)}{i} \text{ com } k(i) = i - 1, i = 1, \dots, d - 1.$$

Se $\binom{k(d)}{d} < a$ então $a' = a - \binom{k(d)}{d} < a$. Por hipótese de indução temos que

$$a' = \sum_{i=1}^{d-1} \binom{k(i)}{i} \text{ com } k(d-1) > \dots > k(1) \geq 0.$$

Mostremos que $k(d) \geq k(d-1)$. Temos que

$$a < \binom{k(d)+1}{d} \text{ então } a' = a - \binom{k(d)}{d} < \binom{k(d)+1}{d} - \binom{k(d)}{d}$$

e como $\binom{k(d)+1}{d} - \binom{k(d)}{d} = \binom{k(d)}{d-1}$, temos

$$\binom{k(d)}{d-1} > a' \geq \binom{k(d-1)}{d-1} \text{ então } k(d) > k(d-1)$$

Portanto

$$a = \sum_{i=1}^d \binom{k(i)}{i} \text{ com } k(d) > \dots > k(1) \geq 0.$$

(ii) *Unicidade*: Quando mostramos que existiam $k(d) > \dots > k(1) \geq 0$ tal que $a = \sum_{i=1}^d \binom{k(i)}{i}$ vimos que $k(d)$ era o maior inteiro positivo tal que $\binom{k(d)}{d} \leq a$.

Mostremos que esta forma de escrever é única. Suponhamos que

$$\sum_{i=1}^d \binom{k'(i)}{i} = a = \sum_{i=1}^d \binom{k(i)}{i}.$$

Como $k(d)$ é o maior inteiro tal que $\binom{k(d)}{d} \leq a$ e $\binom{k'(d)}{d} \leq a$, então $k'(d) \leq k(d)$. Do mesmo modo, $k(d) \leq k'(d)$ e portanto $k(d) = k'(d)$. Seguindo raciocínio análogo chegaremos a $k(i) = k'(i)$, para todo $i = 1, \dots, d$. ■

Observação: Na demonstração acima, note que para $i < d$ o coeficiente $k(i)$ é determinado pela seguinte propriedade: $k(i)$ é o maior inteiro positivo tal que

$$\binom{k(i)}{i} \leq a - \binom{k(d)}{d} - \dots - \binom{k(i+1)}{i+1}.$$

Os números $k(d), k(d-1), \dots, k(1)$ são chamados os *d-coeficientes de Macaulay de a*. Esse números gozam da seguinte propriedade:

Lema 3.1.7: Sejam $k(d), \dots, k(1)$ os *d-coeficientes de Macaulay de a* e $k'(d), \dots, k'(1)$ os *d-coeficientes de Macaulay de a'*. Então

$$a > a' \text{ se, e somente se, } (k(d), \dots, k(1)) > (k'(d), \dots, k'(1))$$

com relação à ordem lexicográfica.

Demonstração:

Vamos mostrar ambas as implicações por indução sobre d .

Se $d = 1$ o resultado é trivial pois

$$a = \binom{k(1)}{1} = k(1); \quad a' = \binom{k'(1)}{1} = k'(1).$$

Logo $a > a'$ se, e somente se, $k(1) > k'(1)$.

Suponhamos então $d > 1$ e que o resultado valha para qualquer número menor do que d . Temos dois casos a considerar

- (i) $k(d) = k'(d)$. Temos que $k(d-1), \dots, k(1)$ e $k'(d-1), \dots, k'(1)$ são os $(d-1)$ coeficientes de Macaulay de $a - \binom{k(d)}{d}$ e $a' - \binom{k'(d)}{d}$ respectivamente. Aplicando a hipótese de indução o resultado segue.
- (ii) $k(d) \neq k'(d)$.

$$\begin{aligned} a' < a &\Rightarrow \binom{k'(d)}{d} \leq a' < a \Rightarrow \binom{k'(d)}{d} < a \\ &\Rightarrow k'(d) < k(d), \\ &\Rightarrow (k'(d), \dots, k'(1)) < (k(d), \dots, k(1)). \end{aligned}$$

$$k(d) > k'(d) \Rightarrow a' < \binom{k(d)}{d} \leq a \Rightarrow a' < a.$$

■

O que vimos é que dado $a \in \mathbb{N}$, existem $k(d) > \dots > k(1)$ números inteiros positivos tais que

$$a = \binom{k(d)}{d} + \dots + \binom{k(1)}{1}.$$

Porém, já vimos também que se $\mu < l$, $\binom{\mu}{l} = 0$.

Logo, eliminando os somandos que são nulos nesta representação, temos que

$$a = \binom{k(d)}{d} + \dots + \binom{k(j)}{j}$$

com $k(d) > \dots > k(j) \geq j \geq 1$.

Definição 3.1.8: Dado $a \in \mathbb{N}$ e sua representação de Macaulay como acima, definimos

$$a^{(d)} = \binom{k(d)+1}{d+1} + \dots + \binom{k(j)+1}{j+1}$$

e $0^{(d)} = 0$.

Este número goza das seguintes propriedades:

Lema 3.1.9: Sejam a, a' e d números inteiros positivos.

- i. Se $a < a'$, então $a^{(d)} < a'^{(d)}$.
- ii. Sejam $k(d), \dots, k(1)$ os d -coeficientes de Macaulay de a e $j = \min\{i; k(i) \geq i\}$. Então

$$(a+1)^{(d)} = \begin{cases} a^{(d)} + k(1) + 1 & \text{se } j = 1 \\ a^{(d)} + 1 & \text{se } j > 1. \end{cases}$$

Demonstração:

(i) Sejam $k(d), \dots, k(1)$ e $k'(d), \dots, k'(1)$ os d -coeficientes de Macaulay de a e a' respectivamente. Por (3.1.7), temos que

$$\begin{aligned} & (k'(d), \dots, k'(1)) > (k(d), \dots, k(1)) \\ \Rightarrow & ((k'(d)+1, \dots, k'(1)+1) > (k(d)+1, \dots, k(1)+1) \\ \stackrel{(3.1.7)}{\Rightarrow} & a'^{(d)} > a^{(d)}. \end{aligned}$$

(ii) Mostremos a igualdade para $j > 1$.

$$a = \binom{k(d)}{d} + \dots + \binom{k(j)}{j}$$

$$\begin{aligned}
a + 1 &= \binom{k(d)}{d} + \cdots + \binom{k(j)}{j} + 1 \\
&= \binom{k(d)}{d} + \cdots + \binom{k(j)}{j} + \binom{j-1}{j-1} \\
(a+1)^{(d)} &= \underbrace{\binom{k(d)+1}{d+1} + \cdots + \binom{k(j)+1}{j+1}}_{a^{(d)}} + \underbrace{\binom{j}{j}}_1 = a^{(d)} + 1
\end{aligned}$$

Suponhamos $j = 1$. Seja i o maior inteiro tal que $k(i) = k(1) + i - 1$.
Então

$$\begin{aligned}
a &= \binom{k(d)}{d} + \cdots + \binom{k(i+1)}{i+1} + \binom{k(i)}{i} + \cdots + \binom{k(1)}{1} \\
a &= \binom{k(d)}{d} + \cdots + \binom{k(i+1)}{i+1} + \sum_{r=1}^i \binom{k(1)+r-1}{r} \\
&= \binom{k(d)}{d} + \cdots + \binom{k(i+1)}{i+1} + \binom{k(1)+i}{i} - 1
\end{aligned}$$

Observação: Estamos usando a relação

$$\sum_{r=1}^i \binom{k(1)+r-1}{r} = \binom{k(1)+i}{i} - 1,$$

que se mostra facilmente por indução sobre i .

Logo

$$a + 1 = \binom{k(d)}{d} + \cdots + \binom{k(1)+i}{i},$$

que é a d expansão de Macaulay de $a + 1$, visto que $k(i+1) > k(1) + i$.

Logo

$$a^{(d)} = \binom{k(d)+1}{d+1} + \cdots + \binom{k(i+1)+1}{i+2} + \sum_{r=1}^i \binom{k(1)+r}{r+1}$$

$$\begin{aligned}
&= \binom{k(d)+1}{d+1} + \cdots + \binom{k(i+1)+1}{i+2} + \sum_{r=2}^{i+1} \binom{k(1)+r-1}{r} \\
&= \binom{k(d)+1}{d+1} + \cdots + \binom{k(i+1)+1}{i+2} + \binom{k(1)+i+1}{i+1} - k(1) - 1
\end{aligned}$$

Logo temos que

$$(a+1)^{(d)} = a^{(d)} + k(1) + 1$$

■

Temos ainda mais uma definição baseada nesses d -coeficientes de Macaulay de um número $a \in \mathbb{N}$.

Definição 3.1.10: Seja a um número natural e $k(d), \dots, k(1)$ seus d -coeficientes de Macaulay de a . Definimos

$$a_{\langle d \rangle} = \binom{k(d)-1}{d} + \cdots + \binom{k(1)-1}{1}.$$

Este número também possui propriedades que nos auxiliarão nas demonstrações.

Lema 3.1.11: Sejam a, a', d e b números naturais. Temos

- i. $a \leq a'$, então $a_{\langle d \rangle} \leq a'_{\langle d \rangle}$.
- ii. Seja $j = \min\{i; k(i) \geq i\}$. Se $k(j) \neq j$, então $(a-1)_{\langle d \rangle} < a_{\langle d \rangle}$.
- iii. Se $0 < b < a$ são tais que $b < b_{\langle d \rangle} + (a-b)_{\langle d-1 \rangle}$, então $b < a_{\langle d \rangle}$.

Demonstração:

(i) Temos que

$$a_{\langle d \rangle} = \binom{k(d)-1}{d} + \cdots + \binom{k(j)-1}{j}.$$

Porém, $a \leq a'$ então, por (3.1.7) $k(i) \leq k'(i)$. Então

$$k(i) - 1 \leq k'(i) - 1 \text{ e por (3.1.7) } a_{\langle d \rangle} \leq a'_{\langle d \rangle}.$$

(ii) Mostremos o resultado por indução sobre d .

Se $d = 1$ e $a \neq 1$ temos que

$$a = \binom{a}{1} \text{ e } a - 1 = \binom{a-1}{1}.$$

Logo $a_{\langle 1 \rangle} > (a-1)_{\langle 1 \rangle}$.

Suponhamos então que $d > 1$ e que o resultado valha para qualquer número menor do que d . Suponhamos que $k(d), \dots, k(1)$ e $k'(d), \dots, k'(1)$ sejam os d -coeficientes de a e a' respectivamente. Temos dois casos a considerar:

(1) $k(d) = k'(d)$. Tome $a' = a - \binom{k(d)}{d}$.

Afirmamos que $a' - 1 > 0$, pois, se $a' = 1$, então

$$a = \binom{k(d)}{d} + \binom{d-1}{d-1}$$

(um absurdo, pois a não estaria nas condições do teorema, isto é, $k(j) \neq j$).

Logo $a' - 1 > 0$. Temos que a' tem, como $d-1$ -coeficientes de Macaulay os números $k(d-1), \dots, k(1)$ e $a' - 1$ tem como $(d-1)$ -coeficientes de Macaulay os números $k'(d-1), \dots, k'(1)$.

Porém, a' satisfaz as condições do teorema e por hipótese de indução temos que $(a' - 1)_{\langle d-1 \rangle} < a'_{\langle d-1 \rangle}$, isto é,

$$\binom{k'(d-1)-1}{d-1} + \cdots + \binom{k'(1)-1}{1} <$$

$$\binom{k(d-1)-1}{d-1} + \cdots + \binom{k(1)-1}{1}$$

Como $a_{(d)} = \binom{k(d)-1}{d} + a'_{(d-1)}$ e

$$(a-1)_{(d)} = \binom{k(d)-1}{d} + (a'-1)_{(d-1)}$$

segue-se o resultado.

(2) $k(d) > k'(d)$. Logo $k(d) - 1 > k'(d) - 1$ e por (3.1.7) $(a-1)_{(d)} < a_{(d)}$.

(iii) Temos que b pode ser escrito da seguinte forma:

$$b = \binom{k(d)}{d} + \cdots + \binom{k(j)}{j} \text{ com } k(d) > \cdots > k(j) \geq j \geq 0.$$

Seja $c = \binom{k(d)+1}{d} + \cdots + \binom{k(j)+1}{j}$.

Temos que $c_{(d)} = b$. Assim, se mostrarmos que $a \geq c$, teremos $a_{(d)} \geq c_{(d)} = b$. Suponhamos que $a < c$.

$$\begin{aligned} a &< \binom{k(d)+1}{d} + \cdots + \binom{k(j)+1}{j} \\ a - b &< \binom{k(d)+1}{d} - \binom{k(d)}{d} + \cdots + \binom{k(j)+1}{j} - \binom{k(j)}{j} \\ &= \binom{k(d)}{d-1} + \cdots + \binom{k(j)}{j-1}. \end{aligned}$$

Distinguímos dois casos:

(1) $j = 1$. Logo

$$a - b < \binom{k(d)}{d-1} + \cdots + \binom{k(2)}{1} + \underbrace{\binom{k(1)}{0}}_1$$

$$a - b \leq \binom{k(d)}{d-1} + \cdots + \binom{k(2)}{1}.$$

Logo

$$(a - b)_{(d-1)} \leq \binom{k(d)-1}{d-1} + \cdots + \binom{k(2)-1}{1}.$$

Porém, por hipótese de tínhamos que

$$\begin{aligned} b &\leq b_{(d)} + (a - b)_{(d-1)} \text{ e portanto} \\ b &\leq \binom{k(d)-1}{d} + \cdots + \binom{k(1)-1}{1} \\ &\quad + \binom{k(d)-1}{d-1} + \cdots + \binom{k(2)-1}{1} \\ &= \binom{k(d)}{d} + \cdots + \binom{k(2)}{2} + \binom{k(1)-1}{1} < b \end{aligned}$$

(absurdo).

(2) $j > 1$. Logo $(a - b)_{(d-1)} < \binom{k(d)-1}{d-1} + \cdots + \binom{k(j)-1}{j-1}$ e, seguindo o mesmo raciocínio, teríamos novamente um absurdo.

Logo $a \geq c$ e portanto $a_{(d)} \geq c_{(d)} = b$. ■

Proposição 3.1.12: Seja u um monômio de grau d no anel de polinômios $\mathcal{S}$. Então

$$|\mathcal{L}_{\mathbf{x}_1 u}| = |\mathcal{L}_u|^{(d)}.$$

Demonstração:

Seja $u = \mathbf{x}_{j(1)} \cdots \mathbf{x}_{j(d)}$ e $\mathbf{x}_1 u = \mathbf{x}_{l(1)} \mathbf{x}_{l(2)} \cdots \mathbf{x}_{l(d+1)}$ com $l(1) = 1$ e $l(i) = j(i-1)$ $i = 2, \dots, d+1$.

Temos, por (3.1.5) que

$$|\mathcal{L}_{\mathbf{x}_1 u}| = \sum_{r=1}^{d+1} \binom{l(r) + r - 2}{r}.$$

Porém, quando $r = 1$ temos que

$$\binom{l(1) + 1 - 2}{1} = \binom{0}{1} = 0.$$

Logo

$$|\mathcal{L}_{\mathbf{x}_1 u}| = \sum_{r=2}^{d+1} \binom{l(r) + r - 2}{r}$$

com $l(r) = j(r-1)$, $r = 2, \dots, d+1$.

Fazendo então $r-1 = i$, temos

$$|\mathcal{L}_{\mathbf{x}_1 u}| = \sum_{i=1}^d \binom{j(i) + (i+1) - 2}{i+1} = |\mathcal{L}_u|^{(d)}$$

■

Definição 3.1.13: Seja u um monômio em $\mathcal{S} = k[x_1, \dots, x_m]$, $u \in \mathcal{S}_d$. Um ideal gerado por $\mathcal{R}_u = \{v \in \mathcal{S}_d; v \geq u\}$ será chamado um *ideal de segmento*.

Veremos agora os dois últimos lemas que nos ajudarão na demonstração do teorema principal do capítulo.

Lema 3.1.14: Seja $u \in \mathcal{S}_d$ um monômio. Então temos que

$$\mathcal{R}_{\mathbf{x}_1} \mathcal{R}_u = \mathcal{R}_{\mathbf{x}_1 u}.$$

Demonstração:

Seja $v \in \mathcal{R}_u$. Então temos que $v \geq u$ e mais ainda

$$x_i v \geq x_1 v \geq x_1 u .$$

Logo temos que $\mathcal{R}_{x_1} \mathcal{R}_u \subseteq \mathcal{R}_{x_1 u}$ visto que

$$\mathcal{R}_{x_1} \mathcal{R}_u = \{vw; w \in \mathcal{R}_{x_1}, v \in \mathcal{R}_u\} .$$

Seja agora $v \in \mathcal{R}_{x_1 u}$. Podemos assumir que x_1 não divide v , pois se x_1 dividisse v , então $v = x_1 w$. Logo $w \in \mathcal{R}_u$, pois se $w < u$, então $x_1 w < x_1 u$ e portanto $v \notin \mathcal{R}_{x_1 u}$ (absurdo). Logo $v \in \mathcal{R}_{x_1} \mathcal{R}_u$ e nada mais há a fazer.

Logo, podemos supor que x_1 não divide v .

$$v \in \mathcal{R}_{x_1 u} \Rightarrow v \geq x_1 u$$

e como $x_1 \nmid v$, temos que $v > x_1 u$. Seja

$$u = x_1^{a_1} \cdots x_m^{a_m} \text{ e } v = x_2^{b_2} \cdots x_m^{b_m} ,$$

e seja i o maior inteiro tal que $a_i > b_i$. Temos dois casos a considerar:

(1) Se existe $j < i$ com $b_j > 0$.

Como $v > x_1 u$ então o último coeficiente não nulo do vetor

$$\left(-(1 + a_1), b_2 - a_2, \dots, b_j - a_j, \dots, b_i - a_i, \dots, \sum_{j=2}^m b_j - \sum_{i=1}^m a_i \right)$$

é positivo. Se existe $j < i$ com $b_j > a_j$ então $b_j - a_j > 0$ e portanto

$$x_j^{-1} v = x_2^{b_2} \cdots x_j^{b_j-1} \cdots x_m^{b_m} \in \mathcal{R}_u .$$

Logo

$$v = x_j (x_j^{-1} v) \in \mathcal{R}_{x_1} \mathcal{R}_u \text{ pois } x_j \in \mathcal{R}_{x_1} .$$

(2) Se não existe $j < i$ com $b_j > 0$.

Logo $x_i^{-1}u \in \mathcal{R}_u$ (pelas mesmas razões acima), e portanto

$$v = x_i(x_i^{-1}v) \in \mathcal{R}_{x_i}\mathcal{R}_u .$$

Logo $\mathcal{R}_{x_i u} \subseteq \mathcal{R}_{x_i}\mathcal{R}_u$. Portanto

$$\mathcal{R}_{x_i u} = \mathcal{R}_{x_i}\mathcal{R}_u .$$

■

Lema 3.1.15: Seja $I \subseteq \mathcal{S}$ um ideal de segmento gerado por monômios de grau d e seja $R = \mathcal{S}/I$. Então, para todo $n \geq d$ temos

$$H(R, n+1) = H(R, n)^{\langle n \rangle} .$$

Demonstração:

Temos que $\dim_k \mathcal{S}_d = \#\mathcal{L}_u + \#\mathcal{R}_u$. Seja $n > d$, isto é, $n = d + \alpha$. Se $u \in \mathcal{S}_d$, então $x_1^\alpha u \in \mathcal{S}_{d+\alpha} = \mathcal{S}_n$.

Por (3.1.14) (indução), temos que

$$(\mathcal{R}_{x_1})^\alpha \mathcal{R}_u = \mathcal{R}_{x_1^\alpha u} .$$

Temos, por hipótese, que

$$I = (\mathcal{R}_u) = (v_1, \dots, v_r); \quad v_i \in \mathcal{S}_d \text{ e } r = \#\mathcal{S}_d .$$

Seja $I_n = \{\text{monômios em } I \text{ cujo grau é } n\}$.

$$w \in I_n \text{ então } w = v_i w' \text{ com } \deg w' = \alpha = n - d .$$

Logo $w' \in (\mathcal{R}_{x_1})^\alpha$. Assim, se $w \in I_n$, então $w = v_i w'$ com $v_i \in \mathcal{R}_u$ e $w' \in (\mathcal{R}_{x_1})^\alpha$. Logo $\#I_n = \#(\mathcal{R}_{x_1})^\alpha \mathcal{R}_u = \#\mathcal{R}_{x_1^\alpha u}$.

Temos que $H(R, n) = \dim_k(\mathcal{S}_n/I_n)$. Mas

$$\dim \mathcal{S}_n = \#\mathcal{L}_{\mathbf{x}_1^\alpha u} + \#\mathcal{R}_{\mathbf{x}_1^\alpha u} = \#\mathcal{L}_{\mathbf{x}_1^\alpha u} + \#I_n .$$

Logo

$$\dim_k \left(\frac{\mathcal{S}_n}{I_n} \right) = \#\mathcal{L}_{\mathbf{x}_1^\alpha u} \stackrel{(3.1.12)}{=} |\mathcal{L}_{\mathbf{x}_1^{\alpha-1} u}|^{(n-1)}$$

pois $\mathbf{x}_1^{\alpha-1} u \in \mathcal{S}_{n-1}$ e por indução vem que $|\mathcal{L}_{\mathbf{x}_1^{\alpha-1} u}| = H(R, n-1)$.

Logo

$$H(R, n+1) = H(R, n)^{(n)} \forall n \geq d .$$

■

3.2 O teorema de Green

Nesta seção, vamos ver o teorema de Green, que também será utilizado na demonstração do teorema de Macaulay.

Nesta seção trabalhamos também com R uma k -álgebra homogênea e k um corpo infinito.

Antes de enunciarmos o teorema de Green, vejamos algumas noções de Geometria Algébrica que nos ajudarão a demonstrá-lo.

Topologia de Zariski

Sejam k um corpo, $\mathcal{S} = k[x_1, \dots, x_n]$ e I um ideal de $\mathcal{S}$.

Definição 3.2.1:

- (a) O conjunto $A^n(k) = \{(a_1, \dots, a_n) \in k^n\} = k^n$ é chamado o n -espaço afim sobre k .

(b) Dado $I \subseteq \mathcal{S}$ ideal, definimos

$$V(I) = \{(a_1, \dots, a_n) \in A^n(k); f(a_1, \dots, a_n) = 0 \forall f \in I\}.$$

Com relação a $V(I)$ temos as seguintes propriedades

- (1) $\cap_{\lambda \in \Lambda} V(I_\lambda) = V(\sum I_\lambda)$ com I_λ ideais de $\mathcal{S}$.
- (2) $\cup_{j=1}^n V(I_j) = V(\cap_{j=1}^n I_j)$.

A partir dessas propriedades pode-se ver que $A^n(k) = k^n$ é um espaço topológico, onde os fechados são da forma $F = V(I)$ com I ideal de $\mathcal{S}$.

Mais ainda, se k é um corpo infinito, então $A^n(k)$ é um espaço topológico irredutível, isto é, $A^n(k) = V_1 \cup V_2$, V_1 e V_2 fechados se, e somente se, $A^n(k) = V_1$ ou $A^n(k) = V_2$.

Observações:

(1) Se R é uma k -álgebra homogênea, com k corpo infinito, sua componente de grau 1, isto é, R_1 é irredutível na topologia de Zariski, pois R_1 é um espaço vetorial de dimensão finita gerado por $x_i = x_i + I$, onde $I \subseteq \mathcal{S}$ é o ideal homogêneo que define R .

(2) Se R_1 é um espaço topológico irredutível, então todo aberto é denso em R_1 .

(3) Essas noções acima sugerem a seguinte terminologia: Seja P uma propriedade definida nas formas lineares de R_1 . Dizemos que $h \in R_1$ é genérico em relação a P se existe um aberto $U \subseteq R_1$, $h \in U$ tal que P vale para toda forma linear de U .

Teorema 3.2.2(Green: forma algébrica): Sejam R uma k -álgebra homogênea, k um corpo infinito e seja $n \geq 1$ um inteiro. Então

$$H\left(\frac{R}{hR}, n\right) \leq H(R, n)_{\langle n \rangle},$$

para uma forma linear h genérica.

Demonstração:

Seja $s = \sup\{\dim_k hR_{n-1}; h \in R_1\}$. Então temos que $\dim_k hR_{n-1} = s$ para alguma forma linear h .

Seja $U \subset R_1$ definido da seguinte forma:

$$U = \{h \in R_1; \dim_k hR_{n-1} = s\} .$$

Temos que $U \neq \emptyset$ e mostremos que U é um conjunto aberto. Seja então

$$\begin{aligned} \{x_1, \dots, x_m\} &- \text{ base de } R_1 \\ \{u_1, \dots, u_r\} &- \text{ base de } R_{n-1} \\ \{v_1, \dots, v_l\} &- \text{ base de } R_n \end{aligned}$$

Seja $h \in R_1$. Logo $h = \sum_{i=1}^m a_i x_i$. Consideremos

$$\begin{aligned} \varphi_h &: R_{n-1} \rightarrow R_n \\ f &\mapsto hf . \end{aligned}$$

Este homomorfismo pode ser escrito como uma matriz de forma lineares em $a_1, \dots, a_m$ como se segue: visto que $\{u_1, \dots, u_r\}$ é base de R_{n-1} , basta definirmos φ_h nesses elementos para conhecermos o homomorfismo. Assim

$$hu_1 = \left(\sum_{i=1}^m a_i x_i \right) u_1 = \sum_{i=1}^m a_i (x_i u_1)$$

Porém $x_i u_1 \in R_n$ e então $x_i u_1 = \sum_{j=1}^l c_{j1}^{(i)} v_j$.

Portanto

$$hu_1 = \left(\sum_i a_i \left(\sum_j c_{j1}^{(i)} v_j \right) \right) = \sum_{j=1}^l \left(\sum_i a_i c_{j1}^{(i)} \right) v_j ,$$

chame $d_{j1} = \sum a_i c_{j1}^{(i)}$ e assim $hu_1 = \sum_{j=1}^l d_{j1} v_j$. Assim

$$[\varphi_h] = \begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1r} \\ \vdots & \vdots & \vdots & \vdots \\ d_{l1} & d_{l2} & \cdots & d_{lr} \end{pmatrix}.$$

Porém, se $h \in U$ então $\dim hR_{n-1} = s$ e portanto existe um menor $(s \times s)$ na matriz não nulo.

Trocando-se os a_i 's por variáveis e chamando

$$[\varphi_h] = A \text{ temos que}$$

$$U = R_1 - V(I_s(A)), \text{ onde}$$

$$I_s(A) = (\{\det \text{ dos menores } s \times s \text{ de } A\}).$$

pois se $h \in R_1$ e $h \in V(I_s(A))$ então o determinante de qualquer menor $(s \times s)$ de φ_h é nulo e portanto $\dim_k hR_{n-1} < s$. Logo $h \notin U$.

Logo U é um conjunto aberto e se $h \in U$, h é dito *genérico*.

Seja então, $h \in U$ e consideremos $\mathcal{S} = R/hR$. Mostremos então que

$$H(\mathcal{S}, n) \leq H(R, n)_{(n)}.$$

Vamos mostrar por indução dupla sobre n e $\dim_k R_1$.

Se $n = 1$ e $\dim_k R_1$ é qualquer, temos que

$$H\left(\frac{R}{hR}, 1\right) = \dim\left(\frac{R}{hR}\right)_1 = \dim_k \frac{R_1}{hR_0} = \dim_k \frac{R_1}{kh} = \dim R_1 - 1$$

e temos também que $H(R, 1) = \dim R_1$ e $H(R, 1)_{(1)} = H(R, 1) - 1 = \dim R_1 - 1$.

Logo temos que

$$H\left(\frac{R}{hR}, 1\right) \leq H(R, 1)_{(1)}.$$

Se $\dim_k R_1 = 1$ e n é qualquer. Tínhamos que

$$R = k[x_1, \dots, x_m] \text{ com } x_i = x_i + I.$$

Se $\dim R_1 = 1$, podemos supor que x_1 gera R_1 . Dado $x_i \in R_1$, $i \neq 1$ temos que $x_i = c_i x_1$ e portanto $x_i - c_i x_1 \in I$. O que fazemos é trocar

$$k[x_1, \dots, x_m] \text{ por } k[x_1, x_2 - c_2 x_1, \dots, x_m - c_m x_1]$$

o que não altera o anel de polinômios.

Logo

$$\frac{k[x_1, x_2 - c_2 x_1, \dots, x_m - c_m x_1]}{I} \simeq \frac{k[x_1]}{(x_1^i)} = k[x_1] .$$

Portanto

$$\dim R_j = \begin{cases} 1 & \text{se } j < i \\ 0 & \text{se } j \geq i . \end{cases}$$

Como $h \in R_1$, temos que

$$\left(\frac{R}{nR} \right)_n = 0 \quad \forall n .$$

Assim

$$0 = H \left(\frac{R}{hR}, n \right) \leq H(R, n)_{(n)} .$$

Assim, vimos que para $n = 1$ e $\dim R_1$ qualquer o resultado vale e que para $\dim R_1 = 1$ e n qualquer o resultado também vale.

Suponhamos então $n > 1$ e $\dim R_1 > 1$ e que o resultado valha para um número menor do que n e $\dim R_1$ qualquer (hipótese de indução).

Seja $V \subset \mathcal{S}_1 = R_1/hR_0$ o conjunto das forma g tais que $\dim_k g\mathcal{S}_{n-1}$ seja máxima e consideremos φ o epimorfismo

$$\begin{aligned} \varphi : R &\rightarrow \mathcal{S} \\ f &\mapsto f + hR = \bar{f} . \end{aligned}$$

Seja $W = (U \setminus kh) \cap \varphi^{-1}(V)$. Temos que φ é sobrejetora e portanto $\varphi^{-1}(V) \neq \emptyset$. Porém V também é aberto em $\mathcal{S}_1$ (mostra-se da mesma forma como mostramos que U é aberto).

Temos que $\varphi|_{R_1} : R_1 \rightarrow \mathcal{S}_1$ é contínua e portanto $\varphi^{-1}(V)$ é aberto. $U \setminus kh$ é também um conjunto aberto e $U \setminus kh \neq \emptyset$, pois se $U \setminus kh = \emptyset$ então $U \subset kh$.

Como U é denso e kh é fechado, teríamos que $R_1 = kh$ (absurdo, pois $\dim R_1 > 1$). Logo $W \neq \emptyset$ pois é interseção de dois abertos em R_1 .

Tome $h^* \in W$ e considere a seguinte seqüência exata

$$0 \rightarrow \bar{h}^* \mathcal{S}_{n-1} \rightarrow \mathcal{S}_n \rightarrow \frac{\mathcal{S}_n}{\bar{h}^* \mathcal{S}_{n-1}} \rightarrow 0 .$$

Desta seqüência temos que

$$H(\mathcal{S}, n) = \dim \frac{\mathcal{S}_n}{\bar{h}^* \mathcal{S}_{n-1}} + \dim \bar{h}^* \mathcal{S}_{n-1} .$$

Como $\dim \mathcal{S}_1 < \dim R_1$ e $h^* \in \varphi^{-1}(V)$ por hipótese de indução temos que

$$\dim \left(\frac{\mathcal{S}_n}{\bar{h}^* \mathcal{S}_{n-1}} \right) \leq H(\mathcal{S}, n)_{(n)} .$$

Analisemos o segundo somando:

$$\bar{h}^* \mathcal{S}_{n-1} = \bar{h}^* \left(\frac{R_{n-1}}{h R_{n-2}} \right) \hookrightarrow \frac{h^* R_{n-1}}{h(h^* R_{n-2})} .$$

donde temos que

$$\dim \bar{h}^* \mathcal{S}_{n-1} \leq \dim \frac{h^* R_{n-1}}{h(h^* R_{n-2})} .$$

Observemos agora as seguintes seqüências exatas:

$$0 \rightarrow hh^* R_{n-2} \rightarrow h^* R_{n-1} \rightarrow \frac{h^* R_{n-1}}{hh^* R_{n-2}} \rightarrow 0$$

Daqui temos que

$$\dim h^* R_{n-1} = \dim \frac{h^* R_{n-1}}{hh^* R_{n-2}} + \dim hh^* R_{n-2} .$$

$$0 \rightarrow hh^* R_{n-2} \rightarrow h R_{n-1} \rightarrow \frac{h R_{n-1}}{hh^* R_{n-2}} \rightarrow 0$$

de onde vem que

$$\dim h R_{n-1} = \dim \frac{h R_{n-1}}{hh^* R_{n-2}} + \dim hh^* R_{n-2} .$$

Porém, $h, h^* \in U$ e portanto $\dim hR_{n-1} = \dim h^*R_{n-1}$ e concluímos que

$$\dim \frac{h^*R_{n-1}}{hh^*R_{n-2}} = \dim \frac{hR_{n-1}}{hh^*R_{n-2}} .$$

O que fazemos é escolher h^* tal que $h^*(hR_{n-2})$ tenha dimensão máxima. Seja agora $J = \text{Ann } h$ e $P = R/\text{Ann } h$. J é um ideal homogêneo. Temos ainda que

$$\dim \frac{hR_{n-1}}{hh^*R_{n-2}} = \dim \frac{\left(\frac{R_{n-1}}{J_{n-1}}\right)}{h^*\left(\frac{R_{n-2}}{J_{n-2}}\right)} = H\left(\frac{P}{h^*P}, n-1\right)$$

Por hipótese de indução temos que

$$H\left(\frac{P}{h^*P}, n-1\right) \leq H(P, n-1)_{\langle n-1 \rangle} .$$

Porém

$$\begin{aligned} H(P, n-1) &= \dim \frac{R_{n-1}}{J_{n-1}} = \dim hR_{n-1} \\ &= \dim R_n - \dim \frac{R_n}{hR_{n-1}} . \end{aligned}$$

Logo $H(P, n-1) = H(R, n) - H(\mathcal{S}, n)$ e concluímos que

$$\dim \tilde{h}^* \mathcal{S}_{n-1} \leq (H(R, n) - H(\mathcal{S}, n))_{\langle n-1 \rangle} .$$

Assim $H(\mathcal{S}, n) \leq H(\mathcal{S}, n)_{\langle n \rangle} + (H(R, n) - H(\mathcal{S}, n))_{\langle n-1 \rangle}$ e por (3.1.11)(iii) temos que

$$H(\mathcal{S}, n) \leq H(R, n)_{\langle n \rangle} .$$

■

3.3 O teorema de Macaulay

Esta seção é dedicada à demonstração do teorema de Macaulay, que estabelece condições para que uma função de $\mathbb{N}$ em $\mathbb{N}$ seja a função de Hilbert

de uma k -álgebra homogênea. Antes do teorema, vejamos uma definição.

Definição 3.3.1: Uma seqüência (finita ou não) $(h_0, h_1, \dots)$ de inteiros não negativos é dita uma $\mathcal{O}$ -seqüência se existir um ideal de ordem de monômios $\mathcal{M}$ nas variáveis $x_1, \dots, x_m$ tal que $\deg x_i = 1 \ \forall i$ e mais ainda

$$h_n = \#\{u \in \mathcal{M} \mid \deg u = n\} .$$

Teorema 3.3.2 (Macaulay): Seja k um corpo infinito e $h : \mathbb{N} \rightarrow \mathbb{N}$ uma função numérica. Então as seguintes afirmativas são equivalentes:

- i. Existe uma k -álgebra homogênea R tal que

$$H(R, n) = h(n) \quad \forall n \geq 0$$

- ii. $(h(0), h(1), \dots)$ é uma $\mathcal{O}$ -seqüência.
- iii. $h(0) = 1$ e $h(n+1) \leq [h(n)]^{(n)} \quad \forall n \geq 1$.
- iv. Seja $s = h(1)$ e para todo $n \geq 0$ seja $\mathcal{M}_n$ o conjunto dos $h(n)$ primeiros monômios (na ordem lexicográfica graduada reversa) de grau n nas variáveis $x_1, \dots, x_s$. Definindo $\mathcal{M} = \cup_{n \geq 0} \mathcal{M}_n$ temos que $\mathcal{M}$ é um ideal de ordem de monômios.

Demonstração:

Temos que

(i) $\Leftrightarrow$ (ii) segue de (3.1.2) e (3.1.3).

(iv) $\Rightarrow$ (ii) segue da definição de uma $\mathcal{O}$ -seqüência e de como foi construído $\mathcal{M}$.

(iii) $\Rightarrow$ (iv) Por hipótese

$$h(n+1) \leq [h(n)]^{(n)} \quad \forall n \geq 1 .$$

Mostremos que $\cup_{n \geq 0} \mathcal{M}_n$ é um ideal de ordem de monômios onde

$$\mathcal{M}_n = \left\{ \begin{array}{l} h(n) \text{ primeiros monômios de grau } n \\ \text{nas variáveis } x_1, \dots, x_s \end{array} \right\}$$

com $s = h(1)$.

Façamos por indução em n . Porém notemos que

$$u \in \mathcal{M} \text{ então } u \in \mathcal{M}_n = \mathcal{L}_{u_n} \text{ para algum } u_n \in \mathcal{S}_n .$$

Se $n = 0$

$$u \in \mathcal{M}_0 = \{h(0) \text{ primeiros monômios de grau zero}\} = \{1\} .$$

Assim

$$v/u \Rightarrow v/1 \Rightarrow v = 1 \Rightarrow v \in \mathcal{M}_0$$

Se $n = 1$ temos que

$$\begin{aligned} \mathcal{M}_1 &= \{s \text{ primeiros monômios de grau } 1\} \\ &= \{x_1, \dots, x_s\} . \end{aligned}$$

Assim

$$v/u \Rightarrow v/x_i \text{ para algum } i \text{ e portanto } v = x_i . \text{ Logo } v \in \mathcal{M}_1 .$$

Suponhamos então que $u \in \mathcal{M}_r$ e $1 < r \leq n$ e que se v/u então $v \in \mathcal{M}$.

Seja $u \in \mathcal{M}_{n+1}$ e v tal que v/u .

$$u = x_1^{a_1} \dots x_s^{a_s} \text{ e } v = x_1^{b_1} \dots x_s^{b_s} .$$

Novamente temos que $\mathcal{M}_{n+1} = \mathcal{L}_{u_{n+1}}$. Porém estamos supondo que

$$\#\mathcal{L}_{u_{n+1}} = h(n+1) \leq [h(n)]^{(n)} = (\#\mathcal{L}_{u'_n})^{(n)}$$

Porém por (3.1.12), temos que

$$(\#\mathcal{L}_{u'_n})^{(n)} = \mathcal{L}_{x_1 u'_n} . \quad (3.3.3)$$

Temos ainda que

$$\mathcal{R}_{x_1} \mathcal{R}_{u'_n} = \mathcal{R}_{x_1 u'_n} .$$

Afirmção: $\mathcal{R}_{x_1 u'_n} \subseteq \mathcal{R}_{u_{n+1}}$.

Temos que $\#\mathcal{L}_{u_{n+1}} \leq \#\mathcal{L}_{x_1 u'_n}$. Suponhamos que $x_1 u'_n \in \mathcal{L}_{u_{n+1}}$. Então $x_1 u'_n < u_{n+1}$. Logo

$$w \in \mathcal{L}_{x_1 u'_n} \Rightarrow w \in \mathcal{L}_{u_{n+1}} \Rightarrow \mathcal{L}_{x_1 u'_n} \subseteq \mathcal{L}_{u_{n+1}} \text{ (absurdo)}$$

Logo $x_1 u'_n \in \mathcal{R}_{u_{n+1}}$. Assim

$$w \in \mathcal{R}_{x_1 u'_n} \Rightarrow w \geq x_1 u'_n \geq u_{n+1} \Rightarrow w \in \mathcal{R}_{u_{n+1}} .$$

Portanto $\mathcal{R}_{x_1 u'_n} \subseteq \mathcal{R}_{u_{n+1}}$.

Como $v < u$ e v/u , então existe j tal que

$$a_s = b_s, \dots, a_{j+1} = b_{j+1} \text{ e } a_j > b_j .$$

Sendo $u_1 = x_1^{a_1} \dots x_j^{a_j-1} \dots x_s^{a_s}$ temos que v/u_1 .

Mostremos que $u_1 \in \mathcal{M}_n = \mathcal{L}_{u'_n}$.

Suponhamos que $u_1 \notin \mathcal{L}_{u'_n}$ então $u_1 \in \mathcal{R}_{u'_n}$. Assim

$$u_1 \geq u'_n \text{ e portanto } x_j u_1 \geq x_j u'_n \geq x_1 u'_n .$$

Porém $x_j u_1 = u$. Logo $u \geq x_1 u'_n$ e assim $u \in \mathcal{R}_{x_1 u'_n} \subseteq \mathcal{R}_{u_{n+1}}$ (absurdo, pois $u \in \mathcal{M}_{n+1} = \mathcal{L}_{u_{n+1}}$).

Logo $u_1 \in \mathcal{M}_n$ e v/u_1 . Por hipótese de indução temos que $v \in \mathcal{M}$. Logo $\mathcal{M}$ é um ideal de ordem de monômios.

Até agora vimos que (iii) $\Rightarrow$ (iv) $\Rightarrow$ (ii) $\Rightarrow$ (i). Logo, mostremos que (i) $\Rightarrow$ (iii). Seja g uma forma linear e seja $S = R/gR$. A seqüência exata

$$0 \rightarrow gR_n \rightarrow R_{n+1} \rightarrow \frac{R_{n+1}}{gR} \rightarrow 0$$

nos fornece a seguinte desigualdade:

$$H(R, n+1) \leq H(R, n) + H(S, n+1) \quad (3.3.4)$$

Sejam então

$$a = H(R, n) \text{ e } b = H(R, n+1).$$

Seja g uma forma linear genérica. Pelo teorema de Green, temos que

$$H(S, n+1) = H\left(\frac{R}{gR}, n+1\right) \leq H(R, n+1)_{(n+1)}.$$

Por (3.3.4), temos que

$$b \leq a + b_{(n+1)}.$$

Seja $k(n+1), \dots, k(1)$ os $(n+1)$ -coeficientes de Macaulay de b . Então

$$\begin{aligned} b_{(n+1)} &= \binom{k(n+1)-1}{n+1} + \dots + \binom{k(1)-1}{1} \text{ e portanto} \\ a &\geq \binom{k(n+1)-1}{n} + \dots + \binom{k(2)-1}{1} + \binom{k(1)-1}{0}, \end{aligned}$$

onde usamos propriedades dos números combinatórios na desigualdade.

Seja $j = \min\{i; k(i) \geq i\}$.

(a) Se $j > 1$ então $k(1) = 0$ e

$$a^{(n)} \geq \binom{k(n+1)}{n+1} + \dots + \binom{k(2)}{2} = b$$

e portanto

$$b = H(R, n+1) = h(n+1) \leq H(R, n)^{(n)} = h(n)^{(n)}$$

como queríamos.

(b) Se $j = 1$, então

$$a \geq \binom{k(n+1)-1}{n} + \cdots + \binom{k(2)-1}{1} + 1$$

Sendo $b' = \binom{k(n+1)-1}{n} + \cdots + \binom{k(2)-1}{1}$ temos que $a \geq b' + 1$ e portanto $a^{(n)} \geq (b' + 1)^{(n)}$ e como $k(2) - 1 \geq 1$ por (3.1.9) chegamos a

$$\begin{aligned} (b' + 1)^{(n)} &= b'^{(n)} + k'(1) + 1 \\ &= \binom{k(n+1)}{n+1} + \cdots + \binom{k(2)}{2} + k(2) - 1 + 1 \end{aligned}$$

Assim

$$\begin{aligned} a^{(n)} &\geq \binom{k(n+1)}{n+1} + \cdots + \binom{k(2)}{2} + k(2) \\ &> \binom{k(n+1)}{n+1} + \cdots + \binom{k(2)}{2} + k(1) = b. \end{aligned}$$

Assim $a^{(n)} \geq b \forall n \geq 1$. ■

Corolário 3.3.5: Seja R uma k -álgebra homogênea, k um corpo. Então

$$H(R, n+1) = H(R, n)^{(n)}$$

para n suficientemente grande.

Demonstração:

Escreva $\mathcal{S} = R/I$, onde $\mathcal{S} = k[x_1, \dots, x_m]$. Pelo teorema de Macaulay, item (iv), temos que existe um ideal de ordem de monômios $\mathcal{M} = \cup_{n \geq 0} \mathcal{M}_n$ em $\mathcal{S}$ tal que $H(R, n) = H(\mathcal{S}/J, n)$ para todo n , onde J é o ideal gerado por todos os monômios que não estão em $\mathcal{M}$. Além disso, a escolha de $\mathcal{M}$ foi tal que $\mathcal{M}_n = \mathcal{L}_{u_n}$ para um certo monômio u_n . Como J é finitamente gerado, existe um inteiro r tal que

$$R_{u_{n+1}} = R_{x_1} \mathcal{R}_{u_n} \text{ para todo } n \geq r .$$

Logo a afirmação segue de (3.1.12). ■

Apêndice A

Resultados auxiliares

Neste apêndice estão alguns resultados auxiliares e definições que foram utilizados em algumas demonstrações.

Dividimos o apêndice em duas seções, cada uma correspondendo ao capítulo de mesmo número.

Os resultados da seção A.1 foram todos retirados de [1]. Os resultados e definições da seção A.2 foram retirados de [2] e [3].

Aqueles resultados que não foram encontrados em livros estão demonstrados.

A.1 Capítulo 1

Os resultados estão na ordem como aparecem no texto.

Teorema A.1.1 (Base de Hilbert): Se A é um anel Noetheriano, então $A[x]$ é Noetheriano. Como corolário temos que se A é Noetheriano então

$A[x_1, \dots, x_m]$ é Noetheriano.

Lema A.1.2: Dado $d \in \mathbb{N}$, então temos que $(1 - t)^d \in \mathbb{Z}[[t]]$ é inversível e

$$(1 - t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k.$$

Demonstração:

Lembremos que

$$\mathbb{Z}[[t]] = \left\{ \sum_{k=0}^{\infty} a_k t^k \mid a_k \in \mathbb{Z} \right\}$$

e que a multiplicação em $\mathbb{Z}[[t]]$ é dada por

$$\left(\sum_{i=0}^{\infty} a_i t^i \right) \left(\sum_{j=0}^{\infty} b_j t^j \right) = \sum_{k=0}^{\infty} c_k t^k \quad \text{onde}$$

$$c_k = \sum_{i=0}^k a_i b_{k-i}.$$

Mostremos o resultado por indução sobre d .

Se $d = 1$, temos que

$$\binom{d+k-1}{d-1} = \binom{k}{0} = 1 \quad \text{e}$$

$$(1 - t) \left(\sum_{k=0}^{\infty} t^k \right) = \sum_{k=0}^{\infty} t^k - \sum_{k=0}^{\infty} t^{k+1} = 1$$

Logo $(1 - t)$ é inversível e $(1 - t)^{-1} = \sum_{k=0}^{\infty} t^k$.

Suponhamos que $d > 1$ e que o resultado vale para d e mostremos que vale para $d + 1$:

$$(1 - t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k; \quad (1 - t)^{-1} = \sum_{k=0}^{\infty} t^k$$

Logo

$$(1-t)^{-d}(1-t)^{-1} = \sum_{k=0}^{\infty} c_k t^k \quad \text{onde}$$

$$c_k = \sum_{i=0}^k \binom{d+i-1}{d-1} \cdot 1 = \binom{d-1+k+1}{d-1+1} = \binom{d+k}{d}$$

Porém $\binom{d+k}{d} = \binom{(d+1)+k-1}{(d+1)-1}$. Logo

$$(1-t)^{-(d+1)} = \sum_{k=0}^{\infty} \binom{(d+1)+k-1}{(d+1)-1} t^k ,$$

como queríamos. ■

Lema A.1.3: Seja $S = k[x_1, \dots, x_m]$ o anel de polinômios com k corpo. Sabemos que $S = \bigoplus_{n=0}^{\infty} S_n$, onde S_n é o k -espaço vetorial gerado pelos monômios $x_1^{a_1} \dots x_m^{a_m}$ tais que $\sum_{i=1}^m a_i = n$. Então

$$\dim(S_n) = \binom{m+n-1}{m-1} .$$

Demonstração:

Para sabermos a dimensão de S_r temos que saber o número de monômios $x_1^{a_1} \dots x_m^{a_m}$ tais que $\sum a_i = r$, isto é, queremos saber a cardinalidade do conjunto

$$I_{r,m} = \{(a_1, \dots, a_m) \in \mathbb{N}^m \mid \sum a_i = r\} .$$

Façamos por indução sobre m .

$m = 1$, r qualquer temos que

$$I_{r,1} = \{a \in \mathbb{N} \mid a = r\} ,$$

$$\text{logo } \#I_{r,1} = 1 = \binom{r + (1-1)}{1-1}.$$

Suponhamos o resultado válido para $m-1$ ($m > 1$). Temos que

$$\forall r; \#I_{r,m-1} = \binom{r + m - 2}{m-2} \text{ onde}$$

$$I_{r,m-1} = \{(a_1, \dots, a_{m-1}) \in N^{m-1}; \sum_{i=1}^{m-1} a_i = r\}.$$

Temos que

$$I_{r,m} = \{(a_1, \dots, a_m) \in N^m; \sum_{i=1}^m a_i = r\}.$$

Dado $0 \leq j \leq r$, consideremos

$$I_j = \{(a_1, \dots, a_m) \in I_{r,m}; a_m = j\}.$$

É claro que

$$I_{r,m} = \dot{\cup}_{j=0}^r I_j \text{ e portanto } \#I_{r,m} = \sum_{j=0}^r \#I_j.$$

Mas notemos que

$$(a_1, \dots, a_m) \in I_j \iff \sum_{i=1}^{m-1} a_i = r - j \iff (a_1, \dots, a_{m-1}) \in I_{r-j,m-1}$$

e portanto

$$\#I_j = \#I_{r-j,m-1} = \binom{r-j+m-2}{m-2}$$

Logo

$$\begin{aligned} \#I_{r,m} &= \sum_{j=0}^r \binom{r-j+m-2}{m-2} \stackrel{r-j=i}{=} \sum_{i=0}^r \binom{i+m-2}{m-2} \\ &= \binom{r+(m-2+1)}{m-2+1} = \binom{r+m-1}{m-1} \end{aligned}$$

como queríamos. ■

Observação: Na demonstração desse dois lemas foram utilizadas duas igualdades que são

i. $m, n \in \mathbb{N}; m \geq n$

$$\binom{m}{n} + \binom{m}{n-1} = \binom{m+1}{n}.$$

ii. $d, k \in \mathbb{N}$

$$\sum_{i=0}^k \binom{d+i}{d} = \binom{d+k+1}{d+1}.$$

Definição A.1.4: Seja A um anel e $\mathcal{A}$ um ideal de A . Dizemos que $\mathcal{A}$ é um *ideal primário* se $xy \in \mathcal{A}$ necessariamente leva a $x \in \mathcal{A}$ ou $y^n \in \mathcal{A}$ para algum $n > 0$. Temos que se $\mathcal{A}$ é um ideal primário, então $\sqrt{\mathcal{A}}$ é um primo P . Assim, dizemos que $\mathcal{A}$ é um ideal P -primário.

Teorema A.1.5: Seja A um anel Noetheriano e $\mathcal{A}$ um ideal de A . Então

- i. $G_{\mathcal{A}}(A)$ é Noetheriano;
- ii. Se M é um A -módulo finitamente gerado e (M_n) uma $\mathcal{A}$ -filtração estável de M , então $G(M)$ é um $G_{\mathcal{A}}(A)$ -módulo graduado finitamente gerado.

Observação: Da demonstração de (i) tiramos que

$$G_{\mathcal{A}}(A) = \left(\frac{A}{\mathcal{A}}\right)[\bar{x}_1, \dots, \bar{x}_s] \quad \text{onde}$$

$x_1, \dots, x_s$ são os geradores de $\mathcal{A}$ e $\bar{x}_i = x_i + \mathcal{A}^2$.

Teorema A.1.6: Seja A um anel Artiniano e M um A -módulo finitamente gerado. Então

- i. M é também um módulo Artiniano, isto é, satisfaz a condição da cadeia descendente.
- ii. M é um módulo de comprimento finito, pois M satisfaz também a condição da cadeia ascendente.

Teorema A.1.7: Seja $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ uma seqüência exata de A -módulos. Então

- i. M é Noetheriano se, e somente se, M' e M'' são Noetherianos;
- ii. M é Artiniano se, e somente se, M' e M'' são Artinianos.

Lema A.1.8: Se (M_n) e (M'_n) são $\mathcal{A}$ -filtrações estáveis de um A -módulo M , então existe $n_0 \in \mathbb{N}$ tal que $M_{n+n_0} \subseteq M'_n$ e $M'_{n+n_0} \subseteq M_n \ \forall n \geq 0$.

Teorema A.1.9: Seja A um anel Noetheriano, $\mathcal{A}$ um ideal de A , M um A -módulo finitamente gerado e (M_n) uma $\mathcal{A}$ -filtração estável de M . Se M' é um submódulo de M então $(M' \cap M_n)$ é uma $\mathcal{A}$ -filtração estável de M' .

Lema A.1.10 (Nakayama): Seja M um A -módulo finitamente gerado e $\mathcal{A}$ um ideal contido no radical de Jacobson de A . Então $\mathcal{A}M = 0$ implica que $M = 0$.

Teorema A.1.11: Seja A um anel Noetheriano local e m seu ideal maximal. Então uma das duas afirmações é verdadeira

- i. $m^n \neq m^{n+1}$ para todo n ;

ii. $m^n = 0$ para algum n , então A é um anel Artiniano local.

A.2 Capítulo 2

Exemplo A.2.1: Ordens Monomiais

Ordem Lexicográfica

Sejam $a = (a_1, \dots, a_n)$ e $b = (b_1, \dots, b_n) \in \mathbb{Z}^n$. Dizemos que

$$a >_{\text{lex}} b$$

se no vetor $a - b \in \mathbb{Z}^n$ a primeira entrada não nula é positiva.

Ordem Lexicográfica graduada

Sejam $a = (a_1, \dots, a_n)$ e $b = (b_1, \dots, b_n) \in \mathbb{Z}^n$. Dizemos que

$$a >_{\text{grlex}} b \text{ se}$$

$$|a| = \sum_{i=1}^n a_i > |b| = \sum_{i=1}^n b_i \text{ ou}$$

$$|a| = |b| \text{ e } a >_{\text{lex}} b.$$

Ordem Lexicográfica graduada reversa

Sejam $a = (a_1, \dots, a_n)$ e $b = (b_1, \dots, b_n) \in \mathbb{Z}^n$. Dizemos que

$$a >_{\text{grevlex}} b \text{ se}$$

$$|a| = \sum_{i=1}^n a_i > |b| = \sum_{i=1}^n b_i \text{ ou}$$

$|a| = |b|$ e no vetor $a - b \in \mathbb{Z}^n$ a última entrada não nula é negativa. ■

Lema A.2.2: Seja $S = k[x_1, \dots, x_n]$ e $I = (m_1, \dots, m_n)$ ideal monomial de

S e n um monômio em S . Seja

$$(I : n) = \{f \in S \mid fn \in I\} .$$

Então temos que

$$(I : n) = \left(\frac{m_1}{\text{mdc}(m_1, n)}, \dots, \frac{m_r}{\text{mdc}(n, m_r)} \right)$$

Bibliografia

- [1] Atiyah M.F. and I.G. MacDonald. Introduction to Commutative Algebra, Addison-Wesley, Reading, Mass., (1969)
- [2] Cox, D., J. Little and D. O'Shea. Ideals, Varieties and Algorithms: An introduction to Computational Algebraic Geometry and Commutative Algebra Springer Verlag, (1992)
- [3] Einsenbud, D. Commutative Algebra with a view toward Algebraic Geometry. Workshop on Commutative Algebra, (1992)
- [4] Herzog, J. and W. Bruns. Cohen-Macaulay Rings. Preliminary version, (1992)
- [5] Kunz, E. Introduction to Commutative Algebra and Algebraic Geometry. Birkhäuser, (1985)