

Robinson Alves Lemos

Alguns Aspectos Computacionais em Álgebra  
Comutativa: Bases de Gröbner e Função de Hilbert



1910001403



ROBINSON ALVES LEMOS

ALGUNS ASPECTOS COMPUTACIONAIS EM ÁLGEBRA  
COMUTATIVA: BASES DE GRÖBNER E FUNÇÃO DE HILBERT

SÃO JOSÉ DO RIO PRETO

2005



ROBINSON ALVES LEMOS

ALGUNS ASPECTOS COMPUTACIONAIS EM ÁLGEBRA  
COMUTATIVA: BASES DE GRÖBNER E FUNÇÃO DE HILBERT



Dissertação apresentada ao Departamento de  
Matemática - IBILCE - UNESP, como parte  
dos requisitos para obtenção do título de Mestre  
em Matemática.

SÃO JOSÉ DO RIO PRETO

2005



512.71

L557a

10101055

02/05/2005

Doação

R\$ 22,00

Autor(a)

076/2005

129/05

Lemos, Robinson Alves.

Alguns aspectos computacionais em álgebra comutativa : bases de Gröbner e função de Hilbert / Robinson Alves Lemos - São José do Rio Preto : [s.n.], 2005

71 f. ; 1 il. ; 30 cm.

Orientador: Aparecida Francisco da Silva

Dissertação (mestrado) - Universidade Estadual Paulista. Instituto de Biociências, Letras e Ciências Exatas

1. Álgebra comutativa. 2. Hilbert, Funções de. 3. Gröbner, Bases de. 4. Macaulay, Teorema de. I. Silva, Aparecida Francisco da. II. Universidade Estadual Paulista. Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU - 512.71



“Sê forte e corajoso; não temas,  
nem te espantes, porque o Senhor,  
teu Deus, é contigo por onde  
quer que andares”.

*Josué 1:9*



# Agradecimentos

Às minhas amigas e amigas, deixo aqui meus sinceros agradecimentos.

À Dona A. F. Costa.

À Prof.ª Dra. Aparecida Francisco de Sá, por toda dedicação, paciência e estímulo em uma ótima convivência.

A todos os professores do Departamento de Matemática da UNESP - S. J. do Rio Preto.

Às professoras Clotilde M. dos Santos e Paula Antônio Farias e Marlene, pelas muitas sugestões.

À minha família, por seu amor e segurança que me passaram durante todo esse período.

Por todos os momentos de alegria e dedicação pelo trabalho acadêmico.

A todos que direta ou indiretamente contribuíram para a realização deste trabalho.

A CAPES pelo auxílio financeiro.

À minha família,  
Samuel, Emília, Karina  
Alexandra e Heitor,  
dedico.

# Agradecimentos

Ao término deste trabalho, deixo aqui meus sinceros agradecimentos:

A Deus por tudo.

À Profa. Dra. Aparecida Francisco da Silva, por toda dedicação, paciência e estímulo em sua valiosa orientação.

A todos os professores do Departamento de Matemática da UNESP- S.J.R. Preto.

Aos professores Clotilzio M. dos Santos e Paulo Antônio Fonseca Machado pelas valiosas sugestões.

À minha família, pelo incentivo e segurança que me passaram durante todo esse período.

Aos amigos da Pós-graduação pelo agradável convívio.

A todos que direta ou indiretamente contribuíram para a realização deste trabalho.

À CAPES pelo auxílio financeiro.

# Resumo

Neste trabalho apresentamos aspectos computacionais de  $K$ -álgebras que envolvem ideais monomiais: bases de Gröbner e funções de Hilbert; além 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.

**Palavras-chave:** Álgebra Comutativa, Funções de Hilbert, Bases de Gröbner, Teorema de Macaulay.



# Abstract

In this work we show  $K$ -algebras computational aspects that evolve monomial ideals: Gröbner basis and Hilbert functions; furthermore, we present the Macaulay theorem which establishes conditions to verify if a function from  $\mathbb{N}$  to  $\mathbb{N}$  is the Hilbert function of a homogeneous  $K$ -algebra.

**Keywords:** Commutative Algebra, Hilbert Functions, Gröbner basis, Macaulay Theorem.

|       |                                                                                  |    |
|-------|----------------------------------------------------------------------------------|----|
| 1     | Princípios de Hilbert                                                            | 10 |
| 1.1   | Conceitos Básicos de Gröbner                                                     | 10 |
| 1.2   | Princípios de Hilbert                                                            | 11 |
| 1.3   | Teorema de Hilbert sobre a Dimensão dos Ideais Homogêneos                        | 16 |
| 2     | Bases de Gröbner                                                                 | 20 |
| 2.1   | Algoritmo de Buchberger                                                          | 20 |
| 2.1.1 | Definições                                                                       | 23 |
| 2.1.2 | Algoritmo de Buchberger                                                          | 25 |
| 2.2   | Algoritmo de Buchberger                                                          | 28 |
| 2.3   | Teorema de Buchberger sobre a Dimensão dos Ideais Homogêneos                     | 31 |
| 2.4   | Bases de Gröbner                                                                 | 34 |
| 2.4.1 | Algoritmo de Buchberger                                                          | 36 |
| 2.4.2 | Algoritmo de Buchberger                                                          | 36 |
| 2.4.3 | Algoritmo de Buchberger                                                          | 37 |
| 2.5   | Princípios de Hilbert de $S/I$ , com $I$ Ideal Monomial                          | 42 |
| 2.5.1 | Procedimento para Calcular a Função de Hilbert de $S/I$ , com $I$ Ideal Monomial | 43 |
| 2.6   | Bases de Gröbner e Ideais                                                        | 46 |
| 2.6.1 | Procedimento para Calcular a Função de Hilbert de um Ideal de Gröbner            | 48 |
| 3     | Teorema de Macaulay                                                              | 50 |
| 4     | Exemplos Utilizando o CoCoA                                                      | 62 |
| 4.1   | Introdução ao CoCoA                                                              | 62 |
| 4.1.1 | Instalação do CoCoA                                                              | 62 |
| 4.1.2 | Exemplos de Programação                                                          | 63 |
| 4.1.3 | Exemplos de Programação                                                          | 63 |
| 4.2   | Exemplos                                                                         | 68 |
| 4.2.1 | Exemplo 1: Algoritmo de Buchberger                                               | 68 |
| 4.2.2 | Exemplo 2                                                                        | 69 |
| 4.2.3 | Exemplo 3: Ideais                                                                | 70 |
|       | Bibliografia                                                                     | 71 |

# Sumário

|                                                                                    |           |
|------------------------------------------------------------------------------------|-----------|
| <b>Introdução</b>                                                                  | <b>9</b>  |
| <b>1 Funções de Hilbert</b>                                                        | <b>10</b> |
| 1.1 Anéis e Módulos Graduados . . . . .                                            | 10        |
| 1.2 Função de Hilbert . . . . .                                                    | 11        |
| 1.3 Teoria da Dimensão de Anéis Noetherianos . . . . .                             | 16        |
| <b>2 Bases de Gröbner</b>                                                          | <b>25</b> |
| 2.1 Introdução . . . . .                                                           | 25        |
| 2.1.1 Polinômios . . . . .                                                         | 25        |
| 2.1.2 Ordens Monomiais . . . . .                                                   | 25        |
| 2.2 Algoritmo da Divisão . . . . .                                                 | 28        |
| 2.3 Lema de Dickson e Teorema da Base de Hilbert . . . . .                         | 31        |
| 2.4 Bases de Gröbner . . . . .                                                     | 34        |
| 2.4.1 Unicidade do Resto . . . . .                                                 | 35        |
| 2.4.2 Critério de Buchberger . . . . .                                             | 36        |
| 2.4.3 Base de Gröbner Reduzida . . . . .                                           | 41        |
| 2.5 Função de Hilbert de $S/I$ , com $I$ Ideal Monomial . . . . .                  | 43        |
| 2.5.1 Processo para Calcular a Função de Hilbert de $S/I$ , com $I$ ideal monomial | 44        |
| 2.6 Anéis de Stanley-Reisner . . . . .                                             | 46        |
| 2.6.1 Função e Série de Hilbert de um Anel de Stanley-Reisner . . . . .            | 48        |
| <b>3 Teorema de Macaulay</b>                                                       | <b>50</b> |
| <b>A Exemplos Utilizando o CoCoA</b>                                               | <b>62</b> |
| A.1 Introdução ao CoCoA . . . . .                                                  | 62        |
| A.1.1 Ambiente Anel . . . . .                                                      | 62        |
| A.1.2 Estruturas de Programação . . . . .                                          | 63        |
| A.1.3 Lista de Comandos . . . . .                                                  | 63        |
| A.2 Exemplos . . . . .                                                             | 68        |
| A.2.1 Exemplo 2.8 - Algoritmo da Divisão . . . . .                                 | 68        |
| A.2.2 Exemplo 2.26 . . . . .                                                       | 69        |
| A.2.3 Exemplos 2.35 e 2.51 . . . . .                                               | 70        |
| <b>Referências Bibliográficas</b>                                                  | <b>71</b> |

# Introdução

O objetivo deste trabalho é o estudo da função de Hilbert no caso de uma  $K$ -álgebra graduada.

Grande parte dos trabalhos publicados na segunda metade do século XIX foram dedicados ao problema de encontrar um sistema finito de geradores para ideais e álgebras. Em seus trabalhos publicados entre 1888 e 1893, Hilbert resolveu esse problema para o caso de ideais em anéis de polinômios, apresentando entre outros resultados o que conhecemos por “Teorema da Base” e “Teorema dos Zeros”.

No Capítulo 1, apresentamos as funções de Hilbert de  $K$ -álgebras graduadas e sua importante aplicação na teoria da dimensão de anéis Noetherianos.

Segundo D. Eisenbud [2] “... as ordens totais sobre conjuntos de monômios foram introduzidas em 1927 por Macaulay que as usou para caracterizar as possíveis funções de Hilbert de ideais graduados, por comparação com os ideais monomiais.

Nos anos 30 do último século, Gröbner publicou aplicações das idéias de Macaulay que obtivessem uma base para um anel fatorial zero dimensional e, em 1964, propôs a seu estudante Bruno Buchberger, como problema de tese de doutorado que computasse tais bases. Como Gröbner havia previsto, a tese e os trabalhos posteriores de Buchberger, publicados em 1970 e 1975, contém os critérios e algoritmo de Buchberger que resolveram o problema.”

No Capítulo 2, apresentamos um pouco desta teoria: ordens monomiais, algoritmos da divisão, bases de Gröbner e critério de Buchberger. Também compõem o Capítulo 2 a prova do teorema da base de Hilbert, no espírito do trabalho de Gordan e processos para calcular a função de Hilbert para  $K[x_1, \dots, x_n]/I$  com  $I$  ideal monomial.

Compõem o Capítulo 3 a versão algébrica do teorema de Green, bom como o teorema de Macaulay que estabelece condições para que uma função de  $\mathbb{N}$  em  $\mathbb{N}$  seja função de Hilbert de uma  $K$ -álgebra graduada.

No Apêndice, apresentamos alguns comandos utilizados no CoCoA. Entre eles, os comandos para o cálculo efetivo das bases de Gröbner e funções de Hilbert.

# Capítulo 1

## Funções de Hilbert

Nesta seção, introduziremos algumas definições e resultados básicos para o que segue e que podem ser visto com mais detalhes em [1].

### 1.1 Anéis e Módulos Graduados

**Definição 1.1** Um anel graduado é um anel  $A$  munido de uma família  $(A_n)_{n \in \mathbb{Z}}$  de subgrupos do grupo aditivo  $A$ , tais que  $A = \bigoplus_{n \in \mathbb{Z}} A_n$  e  $A_m A_n \subset A_{m+n}$  para todos  $m, n \in \mathbb{Z}$ .

**Observação 1.2** Segue desta definição que  $A_0$  é um subanel de  $A$  e cada  $A_n$  é um  $A_0$ -módulo ( $A_0 A_0 \subseteq A_0$  e  $A_0 A_n \subseteq A_n$  para todo  $n$ ).

Salvo menção em contrário, no que segue, trabalharemos apenas com anéis que possuem uma graduação positiva, isto é, aqueles para os quais  $A_n = (0)$  para  $n < 0$ .

**Exemplo 1.3** O modelo básico de anel graduado é o anel de polinômios  $A = K[x_1, \dots, x_n]$ , onde  $K$  é um corpo e  $x_1, \dots, x_n$  são indeterminadas sobre  $A$ , onde  $A_n$  é o conjunto dos polinômios homogêneos de grau  $n$ .

**Definição 1.4** Seja  $A$  um anel graduado. Um  $A$ -módulo graduado é um  $A$ -módulo  $M$  munido de uma família  $(M_n)_{n \geq 0}$  de subgrupos aditivos de  $M$  tais que  $M = \bigoplus_{n=0}^{\infty} M_n$  e  $A_m M_n \subset M_{m+n}$  para todos  $m, n \geq 0$ .

#### Observações 1.5

- (i) Com a notação da Definição 1.4, cada  $M_n$  é chamado componente homogênea de grau  $n$  de  $M$  e é um  $A_0$ -módulo. Um elemento  $x \in M$  é homogêneo de grau  $n$  se  $x \in M_n$ .
- (ii) Cada elemento  $y \in M$  pode ser escrito unicamente como uma soma finita  $\sum_n y_n$ , onde  $y_n \in M_n$ , para todo  $n \in \mathbb{N}$  e  $y_n = 0$ , para quase todo  $n$ . As componentes não nulas  $y_n$  são chamadas de componentes homogêneas de  $y$ .

(iii) Se  $M$  e  $N$  são  $A$ -módulos graduados, um homomorfismo de  $A$ -módulos graduados é um homomorfismo de  $A$ -módulos  $f : M \rightarrow N$  tal que  $f(M_n) \subseteq N_n$ , para todo  $n \geq 0$ .

(iv) Seja  $A$  é um anel graduado e  $A_+ = \bigoplus_{n>0} A_n$ . Então  $A_+$  é um ideal de  $A$ .

**Proposição 1.6** Para um anel graduado  $A$ , são equivalentes:

(i)  $A$  é anel Noetheriano;

(ii)  $A_0$  é Noetheriano e  $A$  é uma  $A_0$ -álgebra finitamente gerada.

**Demonstração:** (i)  $\Rightarrow$  (ii) Seja  $A_+ = \bigoplus_{n>0} A_n$ . Como  $A$  é Noetheriano e  $A_+$  é ideal de  $A$ ,

$A_+$  é finitamente gerado. Sendo  $A_0 \simeq \frac{A}{A_+}$ ,  $A_0$  é Noetheriano. Sejam  $x_1, \dots, x_s$  os geradores de  $A_+$ , que podemos tomar, sem perda de generalidade, homogêneos de graus  $k_1, \dots, k_s$  respectivamente. No que segue mostraremos que  $A = A_0[x_1, \dots, x_s]$ . Por construção  $A_0[x_1, \dots, x_s] \subset A$ . Agora, procedendo por indução sobre  $n$ , veremos que  $A_n \subset A_0[x_1, \dots, x_s]$  para todo  $n$ .

Para  $n = 0$  o resultado é obviamente verdadeiro. Supondo  $A_k \subset A_0[x_1, \dots, x_s]$  para  $k \geq 1$  temos:

$$y \in A_k \Rightarrow y \in A_+ \Rightarrow y = \sum_{i=1}^s a_i x_i,$$

onde  $a_i \in A_{n-k_i}$ .

Usando a hipótese de indução, segue que para todo  $i = 1, \dots, s$ ,  $a_i \in A_0[x_1, \dots, x_s]$  e, assim, sendo  $A_0[x_1, \dots, x_s]$  anel,  $y \in A_0[x_1, \dots, x_s]$ . Portanto  $A_n \subset A_0[x_1, \dots, x_s]$  para todo  $n \in \mathbb{N}$ , o que completa a demonstração.

(ii)  $\Rightarrow$  (i) Teorema da Base de Hilbert 2.16.  $\square$

## 1.2 Função de Hilbert

No que segue  $A = \bigoplus_{n=0}^{\infty} A_n$  denotará um anel Noetheriano graduado e  $A_k$  sua  $k$ -ésima componente homogênea. Como acabamos de ver  $A_0$  é Noetheriano e  $A$  é gerado (como  $A_0$  álgebra) por, digamos,  $x_1, \dots, x_s$ , que podemos tomar homogêneos de graus  $k_1, \dots, k_s$  ( $k_i > 0$ ). Seja  $M$  um  $A$ -módulo graduado finitamente gerado. Então  $M$  é gerado por um número finito de elementos homogêneos digamos  $m_1, \dots, m_t$ . Seja  $r_j = \text{grau } m_j$  ( $1 \leq j \leq t$ ).

Todo elemento  $y$  de  $M_n$ , a componente homogênea de  $M$  de grau  $n$ , é, deste modo, da forma  $y = \sum_j f_j(\underline{x}) m_j$ , onde  $f_j(\underline{x}) \in A = A_0[x_1, \dots, x_s]$  é homogêneo de grau  $n - r_j$  (zero se  $n < r_j$ ). Segue que  $M_n$  é finitamente gerado como um  $A_0$ -módulo, sendo seus geradores todos os  $f_j(\underline{x}) m_j$ , onde  $\underline{x}$  denota  $(x_1, \dots, x_s)$ .

**Definição 1.7** Seja  $C$  uma classe de  $A$ -módulos e seja  $\lambda$  uma função sobre  $C$  com valores em  $\mathbb{Z}$ . A função  $\lambda$  é aditiva se, para cada seqüência exata curta  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  de elementos de  $C$  temos

$$\lambda(M') - \lambda(M) + \lambda(M'') = 0.$$

**Exemplo 1.8** Tomando  $A$  como um corpo  $K$  e  $C$  como a classe de todos os  $K$ -espaços vetoriais de dimensão finita, então  $\lambda : C \rightarrow \mathbb{N}$  dada por  $\lambda(V) = \dim_K(V)$  para todo  $V \in C$ , é uma função aditiva sobre  $C$ .

**Exemplo 1.9** Sejam  $S = K[x_1, \dots, x_m]$  o anel dos polinômios com  $K$  corpo. Sabemos que  $S = \bigoplus_{n=0}^{\infty} S_n$ , onde  $S_n$  é o  $K$ -espaço vetorial gerado pelos monômios  $x_1^{\alpha_1} \cdots x_m^{\alpha_m}$  onde  $\sum_{i=1}^m \alpha_i = n$ . Então a  $K$ -dimensão de  $S_n$  é:

$$\dim_K S_n = \binom{m+n-1}{m-1}.$$

De fato, para sabermos a dimensão de  $S_r$ , basta calcular o número de monômios  $x_1^{\alpha_1} \cdots x_m^{\alpha_m}$  tais que  $\sum_{i=1}^m \alpha_i = r$ , isto é, a cardinalidade do conjunto

$$I_{r,m} = \left\{ (\alpha_1, \dots, \alpha_m) \in \mathbb{N}^m \mid \sum_{i=1}^m \alpha_i = r \right\}.$$

Faremos a prova por indução sobre  $m$ . Se  $m = 1$  e  $r$  qualquer temos  $I_{r,1} = \{\alpha \in \mathbb{N} \mid \alpha = r\}$ , logo

$$\#I_{r,1} = 1 = \binom{r+(1-1)}{1-1}.$$

Supondo o resultado válido para  $m-1$  ( $m > 1$ ) temos que para todo  $r$  vale

$$\#I_{r,m-1} = \binom{r+m-2}{m-2},$$

onde  $I_{r,m-1} = \{(\alpha_1, \dots, \alpha_{m-1}) \in \mathbb{N}^{m-1} \mid \sum_{i=1}^{m-1} \alpha_i = r\}$ . Agora,

$$I_{r,m} = \left\{ (\alpha_1, \dots, \alpha_m) \in \mathbb{N}^m \mid \sum_{i=1}^m \alpha_i = r \right\}.$$

Dado  $0 \leq j \leq r$ , consideremos

$$I_j = \{(\alpha_1, \dots, \alpha_m) \in I_{r,m} \mid \alpha_m = j, \sum_{i=1}^{m-1} \alpha_i = r-j\}.$$

É claro que  $I_{r,j} = \bigcup_{j=0}^m I_j$  e, portanto,  $\#I_{r,m} = \sum_{j=0}^m \#I_j$ . Mas,  $(\alpha_1, \dots, \alpha_m) \in I_j$  se, e somente se,  $\sum_{i=1}^{m-1} \alpha_i = r-j$  e  $\alpha_m = j$ , ou seja, se, e somente se,  $(\alpha_1, \dots, \alpha_{m-1}) \in I_{r-j,m-1}$  e  $\alpha_m = j$ , assim,

$$\#I_j = \#I_{r-j,m-1} = \binom{r-j+m-2}{m-2}.$$

Logo,

$$I_{r,m} = \sum_{j=0}^r \binom{r-j+m-2}{m-2} \stackrel{r-j=i}{=} \sum_{i=0}^r \binom{i+m-2}{m-2} = \binom{r+(m-2)+1}{(m-2)+1} = \binom{r+m-1}{m-1}.$$

**Observação 1.10** Na definição mais geral de uma função aditiva,  $\lambda$  pode assumir valores em um grupo abeliano qualquer. Porém, nesse trabalho,  $\lambda$  sempre assumirá valores em  $\mathbb{Z}$ , sendo que as funções aditivas mais importantes que usaremos são dimensão e comprimento.

Uma das principais definições com a qual trabalharemos no que segue é:

**Definição 1.11** Sejam  $\lambda$  uma função aditiva sobre a classe de todos os  $A_0$ -módulos finitamente gerados,  $A$  um anel graduado e  $M = \bigoplus M_n$  um  $A$ -módulo graduado finitamente gerado. A função de Hilbert de  $M$  (com respeito a  $\lambda$ ) é a seguinte função:

$$\begin{aligned} H_\lambda(M, -) : \mathbb{N} &\rightarrow \mathbb{Z} \\ n &\mapsto H_\lambda(M, n) = \lambda(M_n) \end{aligned}$$

A série de Hilbert-Poincaré de  $M$  (com respeito a  $\lambda$ ) é a série de potências

$$P(M, t) = \sum_{n=0}^{\infty} H_\lambda(M, n)t^n = \sum_{n=0}^{\infty} \lambda(M_n)t^n \in \mathbb{Z}[[t]].$$

**Teorema 1.12 (Hilbert-Serre)** Nas hipóteses da definição anterior temos que existe uma função  $f(t) \in \mathbb{Z}[t]$  tal que

$$\frac{f(t)}{\prod_{i=1}^s (1 - t^{k_i})},$$

onde  $A = A_0[x_1, \dots, x_s]$  e  $x_i \in A_{k_i}$ .

**Demonstração:** A demonstração será feita por indução sobre  $s$ , o número de geradores de  $A$  sobre  $A_0$ .

No caso  $s = 0$ , temos  $A = A_0$  e  $A_n = 0$ , para todo  $n > 0$ .  $M$  é um  $A$ -módulo finitamente gerado. Então  $M$  é  $A_0$ -módulo finitamente gerado, isto é,  $M = A_0 m_1 + \dots + A_0 m_t$ , com  $m_i \in M_{r_i}$ . Logo, para  $n > \max\{r_i \mid i = 1, \dots, t\}$  segue que  $M_n = 0$  e desta forma  $P(M, t)$  é um polinômio, como queríamos.

Suponha  $s > 0$  e que o resultado vale para  $s - 1$ , considerando o  $A_0$  homomorfismo de módulos

$$\begin{aligned} \varphi_s : M_n &\rightarrow M_{n+k_s} \\ m &\mapsto x_s m \end{aligned}$$

Temos então para todo  $n$  a sequência exata:

$$0 \rightarrow K_n \rightarrow M_n \xrightarrow{\varphi_s} M_{n+k_s} \rightarrow L_{n+k_s} \rightarrow 0, \quad (1.1)$$

onde  $K_n = \text{Ker } \varphi_s$ ,  $L_{n+k_s} = M_{n+k_s} / \varphi_s(M_n)$ .

Desta forma  $L_n \simeq M_n$  se  $n < k_s$  e  $L_n = L_{(n-k_s)+k_s} \simeq M_n / \varphi_s(M_{n-k_s})$ .

Tomando  $K = \bigoplus_n K_n$  e  $L = \bigoplus_n L_n$  e considerando

$$\begin{aligned} \psi_s : M &\rightarrow M \\ m &\mapsto x_s m \end{aligned}$$

temos:

$$m \in M \Rightarrow m = y_1 + \cdots + y_n, \text{ com } y_i \in M_{r_i}.$$

$$x_s m = 0 \Rightarrow x_s y_1 + \cdots + x_s y_n = 0.$$

$$\text{Portanto } x_s y_i \in M_{s+r_i} \cap \sum_{r_j \neq s+r_i} M_{r_j} = (0).$$

Logo  $y_i \in K_{r_j}$ , de onde segue que  $m \in K$ . Assim  $\text{Ker}(\psi_s) = K$ .

Além disso,  $L \simeq M/x_s M$  uma vez que se  $m \in M$ ,  $m = y_{i_1} + \cdots + y_{i_r} + w_{j_1} + \cdots + w_{j_s}$  com  $i_t < k_s$  e  $j_l \geq k_s$  e se  $\phi : M \rightarrow L$  tem-se  $\phi(m) = y_{i_1} + \cdots + y_{i_r} + \bar{w}_{j_1} + \cdots + \bar{w}_{j_s}$ , onde  $\bar{w}_{j_l} = w_{j_l} + x_s M_{j_l+k_s}$ .  $\phi$  é obviamente sobrejetora e  $\text{Ker } \phi = x_s M$ , de onde segue que  $0 \rightarrow K \rightarrow M \rightarrow M \rightarrow L \rightarrow 0$  é exata.

Agora, como  $A$  é Noetheriano e  $M$  finitamente gerado, então  $M$  é Noetheriano. Logo  $K$  e  $L$  também são  $A$ -módulos finitamente gerados. Além disso  $x_s K = (0)$  e  $x_s L = (0)$  e, deste modo, são  $A_0[x_1, \dots, x_{s-1}]$ -módulos finitamente gerados. Aplicando  $\lambda$  em (1.1) obtemos

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0, \quad (1.2)$$

multiplicando por  $t^{n+k_s}$  e somando sobre todos os  $n$  obtemos

$$\begin{aligned} \sum_n \lambda(K_n) t^{n+k_s} - \sum_n \lambda(M_n) t^{n+k_s} + \sum_n \lambda(M_{n+k_s}) t^{n+k_s} - \sum_n \lambda(L_{n+k_s}) t^{n+k_s} &= 0, \\ t^{k_s} \sum_n \lambda(K_n) t^n - t^{k_s} \sum_n \lambda(M_n) t^n + \sum_n \lambda(M_n) t^n - \sum_n \lambda(L_n) t^n - g(t) &= 0, \end{aligned}$$

ou seja,

$$(1 - t^{k_s})P(M, t) = P(L, t) - t^{k_s}P(K, t) + g(t), \quad (1.3)$$

onde  $g(t) = \sum_{i=0}^{k_s-1} \lambda(M_i) t^i + \sum_{i=0}^{k_s-1} \lambda(L_i) t^i$ . Como por hipótese de indução o resultado é válido para  $L$  e  $K$ , segue o resultado.  $\square$

**Definição 1.13** Nas condições do teorema anterior definimos  $d_\lambda(M)$  como sendo a ordem do polo  $t = 1$  da função  $P(M, t)$ .

**Lema 1.14** Dado  $d \in \mathbb{N}$  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:** Mostraremos o resultado por indução sobre  $d$ .

Sabemos que  $\mathbb{Z}[[t]] = \{\sum_{k=0}^{\infty} a_k t^k \mid a_k \in \mathbb{Z}\}$  e a multiplicação em  $\mathbb{Z}[[t]]$  é definida por

$$\left( \sum_{i=0}^{\infty} a_i t^i \right) \left( \sum_{j=0}^{\infty} b_j t^j \right) = \sum_{k=0}^{\infty} c_k t^k,$$

onde  $c_k = \sum_{i=0}^k a_i b_{k-i}$ .

Se  $d = 1$  então  $\binom{d+k-1}{d-1} = \binom{k}{0} = 1$  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  $(1-t)^{-1} = \sum_{k=0}^{\infty} t^k$ .

Supondo o resultado válido para  $d > 1$  temos:

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k.$$

$$(1-t)^{-d}(1-t)^{-1} = \sum_{k=0}^{\infty} c_k t^k, \text{ onde } c_k = \sum_{i=0}^k \binom{d+i-1}{d-1} \cdot 1 = \binom{(d-1)+k+1}{(d-1)+1}.$$

Logo,

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

**Corolário 1.15** Se cada  $k_i = 1$ , então para todo  $n$  suficientemente grande,  $\lambda(M_n)$  é um polinômio em  $n$  (com coeficientes racionais) de grau  $d-1$ , onde  $d = d_\lambda(M)$ . Além disso, se  $d = 0$  então  $\lambda(M_n)$  é zero para  $n$  suficientemente grande.

(Adotamos aqui a convenção de que o grau do polinômio nulo é  $-1$  e também que o coeficiente binomial  $\binom{n}{-1} = 0$ , para todo  $n \geq 0$  e  $\binom{n}{-1} = 1$  se  $n = -1$ .)

**Demonstração:** Temos que  $\lambda(M_n)$  é o coeficiente de  $t^n$  em  $f(t)(1-t)^{-s}$ . Cancelando as potências de  $(1-t)$  que aparecem em  $f$ , podemos supor,  $s = d$  e  $f(1) \neq 0$ . Seja

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

Como foi visto no lema anterior,  $(1-t)^d$  é inversível em  $\mathbb{Z}[[t]]$  e  $(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k$ .  
Donde

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

Assim, para  $n \geq N$  temos que  $\lambda(M_n) = \sum_{k=0}^N a_k \binom{d+n-k-1}{d-1}$ , onde a última soma é um polinômio de grau  $d-1$  com coeficiente líder  $(\sum a_k)/(d-1)! \neq 0$ , pois  $f(1) \neq 0$ .  $\square$

### Observações 1.16

- (i) O polinômio no Corolário 1.15 é usualmente chamado de polinômio de Hilbert de  $M$  (com respeito a  $\lambda$ ).
- (ii) Para um polinômio  $f(x)$  ser tal que  $f(n) \in \mathbb{Z}$  para todo  $n \in \mathbb{Z}$ , não é necessário que  $f$  possua apenas coeficientes inteiros, como podemos ver no exemplo:  $\frac{1}{2}(x+1)x$ .

**Proposição 1.17** Se  $x \in A_k$  não for um divisor de zero em  $M$ , então

$$d(M/xM) = d(M) - 1.$$

**Demonstração:** Retornando à seqüência (1.1) da demonstração do Teorema de Hilbert-Serre 1.12, trocando  $x_s$  por um elemento qualquer  $x \in A_k$  que não é um divisor de zero em  $M$ , então  $K = 0$  e a equação (1.2) nos dá que  $d(L) = d(M) - 1$ , onde, neste caso,  $L = M/xM$ .  $\square$

Usaremos o Teorema de Hilbert-Serre no caso em que  $A_0$  é um anel Artiniano (em particular um corpo) e  $\lambda(M)$  é o comprimento  $l(M)$  de um  $A_0$ -módulo finitamente gerado  $M$ . Note que o comprimento de  $M$  é finito, isto é,  $l(M) \in \mathbb{N}$  e  $l$  é uma função aditiva sobre o conjunto dos  $A_0$ -módulos finitamente gerados.

**Exemplo 1.18** Sejam  $A = A_0[x_1, \dots, x_s]$  onde  $A_0$  é um anel Artiniano,  $x_i$  indeterminadas independentes sobre  $A_0$  e  $\lambda$  a função comprimento  $l$ . Então  $A_n$  é um  $A_0$ -módulo livre gerado pelos monômios  $x_1^{m_1} \cdots x_s^{m_s}$ , onde  $\sum m_i = n$ . Existem  $\binom{s+n-1}{s-1}$  destes elementos e, assim,  $P(A, t) = (1-t)^{-s}$ .

## 1.3 Teoria da Dimensão de Anéis Noetherianos

**Definição 1.19** Seja  $A$  um anel e  $\mathfrak{a}$  um ideal de  $A$ . Definimos o anel graduado associado a  $A$  como sendo o anel graduado

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

com a multiplicação definida como segue: para cada  $x_n \in \mathfrak{a}^n$ , seja  $\bar{x}_n$  sua imagem em  $\mathfrak{a}^n/\mathfrak{a}^{n+1}$ ; definimos  $\bar{x}_m \bar{x}_n$  como a imagem  $\overline{x_m x_n}$ , ou seja, a imagem de  $x_m x_n$  em  $\mathfrak{a}^{m+n}/\mathfrak{a}^{m+n+1}$ . Esta operação está bem definida uma vez que independe da escolha dos representantes pois, dados  $x_m, x'_m \in \mathfrak{a}^m$  e  $x_n, x'_n \in \mathfrak{a}^n$  com  $\bar{x}_m = \bar{x}'_m$  e  $\bar{x}_n = \bar{x}'_n$  temos então que  $x_m - x'_m \in \mathfrak{a}^{m+1}$  e  $x_n - x'_n \in \mathfrak{a}^{n+1}$ . Agora,

$$x_m x_n - x'_m x'_n = x_m x_n - x'_m x_n + x'_m x_n + x'_m x'_n = \underbrace{(x_m - x'_m)}_{\in \mathfrak{a}^{m+1}} \underbrace{x_n}_{\in \mathfrak{a}^n} + \underbrace{x'_m}_{\in \mathfrak{a}^m} \underbrace{(x_n - x'_n)}_{\in \mathfrak{a}^{n+1}} \in \mathfrak{a}^{m+n+1}.$$

Para elementos quaisquer definimos o produto de modo a valer a propriedade distributiva.

**Definição 1.20** Seja  $M$  um  $A$ -módulo graduado e  $\mathfrak{a} \subset A$  um ideal.

(i) Uma cadeia descendente  $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots$  onde os  $M_n$ 's são submódulos de  $M$  é chamada de filtração de  $M$  e denotada por  $(M_n)$ .

(ii)  $(M_n)$  é uma  $\mathfrak{a}$ -filtração se  $\mathfrak{a}M_n \subseteq M_{n+1}$ , para todo  $n$  e,

(iii)  $(M_n)$  é uma  $\mathfrak{a}$ -filtração estável se  $\mathfrak{a}M_n = M_{n+1}$  para todo  $n$  suficientemente grande.

**Exemplo 1.21** Um exemplo de  $\mathfrak{a}$ -filtração estável é  $(\mathfrak{a}^n M)$ , também chamada de filtração  $\mathfrak{a}$ -ádica.

**Proposição 1.22 (Lema de Artin-Rees)** Seja  $A$  um anel Noetheriano,  $\mathfrak{a}$  um ideal de  $A$ ,  $M$  um  $A$ -módulo finitamente gerado,  $(M_n)$  uma  $\mathfrak{a}$ -filtração estável de  $M$ . Se  $M'$  é um submódulo de  $M$ , então  $(M' \cap M_n)$  é uma  $\mathfrak{a}$ -filtração estável de  $M'$ .

**Demonstração:** Veja [1].

Tomando  $M_n = \mathfrak{a}^n M$  na proposição anterior obtemos o seguinte:

**Corolário 1.23** *Existe um inteiro  $k$  tal que*

$$(\mathfrak{a}^n M) \cap M' = \mathfrak{a}^{n-k}((\mathfrak{a}^k M) \cap M'),$$

para todo  $n \geq k$ .

**Definição 1.24** *Se  $M$  é um  $A$ -módulo e  $(M_n)$  uma  $\mathfrak{a}$ -filtração de  $M$ , definimos o  $G(A)$ -módulo graduado associado como:*

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

Neste caso  $G_n(M)$  denotará  $M_n/M_{n+1}$ .

**Exemplo 1.25** *Se  $A = K[x_1, \dots, x_n]$  é o anel dos polinômios em  $x_1, \dots, x_n$  sobre um corpo  $K$  e  $\mathfrak{a} = (x_1, \dots, x_n)$ , então  $G(A) \simeq A$  (como anéis graduados).*

**Teorema 1.26** *Sejam  $A$  um anel Noetheriano local,  $\mathfrak{m}$  seu ideal maximal,  $\mathfrak{q}$  um ideal  $\mathfrak{m}$ -primário,  $M$  um  $A$ -módulo finitamente gerado e  $(M_n)$  uma  $\mathfrak{q}$ -filtração estável de  $M$ . Então:*

- (i)  $\frac{M}{M_n}$  tem comprimento finito, para todo  $n \in \mathbb{N}$ .
- (ii) Para  $n$  suficientemente grande, esse comprimento é um polinômio  $g(n)$  de grau menor ou igual a  $s$  onde  $s$  é o número mínimo de geradores de  $\mathfrak{q}$ .
- (iii) O grau de  $g(n)$  depende somente de  $M$  e  $\mathfrak{q}$  e não da filtração escolhida.

**Demonstração:** Sejam  $G(A) = \bigoplus_{n=0}^{\infty} \frac{\mathfrak{a}^n}{\mathfrak{a}^{n+1}}$  e  $G(M) = \bigoplus_{n=0}^{\infty} \frac{M_n}{M_{n+1}}$ . Temos que  $G_0(A) = A/\mathfrak{q}$  é anel Artiniano, pois é Noetheriano de dimensão zero.

Além disso,  $G(A)$  é Noetheriano e  $G(M)$  é um  $G(A)$ -módulo finitamente gerado.

Cada  $G_n(M) = M_n/M_{n+1}$  é um  $A$ -módulo finitamente gerado, anulado por  $\mathfrak{q}$  e, assim, é um  $A/\mathfrak{q}$ -módulo finitamente gerado. Sendo  $A/\mathfrak{q}$  Artiniano,  $G_n(M)$  é de comprimento finito, para todo  $n$ .

(i) Para mostrar que  $M/M_n$  é de comprimento finito para todo  $n$ , procedemos por indução sobre  $n$ .

Para  $n = 0$  nada há para fazer, pois  $M/M_0 = M/M \simeq 0$ .

Supondo que  $M/M_{n-1}$  é Artiniano, mostraremos que  $M/M_n$  também o é. Consideremos a seqüência exata

$$0 \rightarrow \frac{M_{n-1}}{M_n} \rightarrow \frac{M}{M_n} \rightarrow \frac{M}{M_{n-1}} \rightarrow 0. \quad (1.4)$$

Como  $M_{n-1}/M_n = G_{n-1}(M)$  é Artiniano e, por hipótese de indução,  $M/M_{n-1}$  também é Artiniano, temos que  $M/M_n$  é Artiniano.

Assim,  $M/M_n$  também é de comprimento finito.

**Afirmção:**  $l_n = l\left(\frac{M}{M_n}\right) = \sum_{r=1}^n l\left(\frac{M_{r-1}}{M_r}\right)$ , para todo  $n$ .

Novamente usaremos indução sobre  $n$ . Para  $n = 0$ ,  $l_0 = l(M/M_0) = l(0) = 0$ . Supondo o resultado válido para  $n \geq 1$ , sendo  $l$  uma função aditiva, a seqüência (1.4) nos garante que

$$l_n = l_{n-1} + l\left(\frac{M_{n-1}}{M_n}\right) \stackrel{H.I.}{=} \sum_{r=1}^{n-1} l\left(\frac{M_{r-1}}{M_r}\right) + l\left(\frac{M_{n-1}}{M_n}\right) = \sum_{r=1}^n l\left(\frac{M_{r-1}}{M_r}\right).$$

(ii) Se  $x_1, \dots, x_s$  é um conjunto minimal de geradores de  $\mathbf{q}$ , as imagens  $\bar{x}_i = x_i + \mathbf{q}/\mathbf{q}^2$  geram  $G(A)$  como  $A/\mathbf{q}$ -álgebra e cada  $\bar{x}_i$  tem grau 1 ( $G(A) = (A/\mathbf{q})[\bar{x}_1, \dots, \bar{x}_s]$ ). Sabemos que para  $n$  suficientemente grande  $l(M_n/M_{n+1}) = f(n)$  é um polinômio em  $n$  de grau menor ou igual a  $s - 1$ .

Agora,  $l_{n+1} - l_n = l(M_n/M_{n+1}) = f(n)$  e, assim,  $l_n$  é um polinômio  $g(n)$  de grau no máximo  $s$  para  $n$  suficientemente grande.

(iii) Sejam  $(\tilde{M}_n)$  outra  $\mathbf{q}$ -filtração estável de  $M$  e  $\tilde{g}(n) = l(M/\tilde{M}_n)$ . Então existe  $n_0 \in \mathbb{N}$  tal que

$$M_{n+n_0} \subset \tilde{M}_n \text{ e } \tilde{M}_{n+n_0} \subset M_n, \quad \forall n \geq 0.$$

Utilizando-se a seguinte seqüência exata:

$$0 \rightarrow \text{Ker } \varphi \rightarrow \frac{M}{M_{n+n_0}} \xrightarrow{\varphi} \frac{M}{\tilde{M}_n} \rightarrow 0,$$

onde  $\varphi(m + M_{n+n_0}) = m + \tilde{M}_n$ , temos  $l(M/M_{n+n_0}) \geq l(M/\tilde{M}_n)$  e, portanto,  $g(n + n_0) \geq \tilde{g}(n)$ .

Analogamente,  $\tilde{g}(n + n_0) \geq g(n)$ . Assim,

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

nos garantem que

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

Por outro lado,

$$g(n + n_0) \geq \tilde{g}(n), \text{ ou seja, } \frac{1}{\tilde{g}(n)} \geq \frac{1}{g(n + n_0)},$$

deste modo,

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

Conseqüentemente,

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

Logo  $\lim_{n \rightarrow \infty} \frac{g(n)}{\tilde{g}(n)} = 1$ , de onde segue que o grau  $g$  é igual ao grau de  $\tilde{g}$  e,  $g$  e  $\tilde{g}$  possuem o mesmo coeficiente líder.  $\square$

**Observações 1.27**

(i) Denotaremos por  $\chi_{\mathbf{q}}^M(n)$ , o polinômio  $g(n)$  correspondendo à filtração  $(\mathbf{q}^n M)$ , ou seja:

$$\chi_{\mathbf{q}}^M(n) = l(M/\mathbf{q}^n M) \quad (\text{para todo } n \text{ suficientemente grande})$$

(ii) Se  $M = A$ , denotaremos por  $\chi_{\mathbf{q}}(n)$  o polinômio  $\chi_{\mathbf{q}}^A(n)$  e o chamaremos de polinômio característico do ideal  $\mathbf{m}$ -primário  $\mathbf{q}$ .

Nas condições anteriores temos:

**Corolário 1.28** Para todo  $n$  suficientemente grande, o comprimento  $l(A/\mathbf{q}^n)$  é um polinômio  $\chi_{\mathbf{q}}(n)$  de grau menor ou igual a  $s$ , onde  $s$  é o número mínimo de geradores de  $\mathbf{q}$ .

**Proposição 1.29** Seja  $A$  um anel local,  $\mathbf{m}$  seu ideal maximal e  $\mathbf{q}$  um ideal  $\mathbf{m}$ -primário. Então  $\text{grau } \chi_{\mathbf{q}}(n) = \text{grau } \chi_{\mathbf{m}}(n)$ .

**Demonstração:** Como  $A$  é Noetheriano, todo ideal contém uma potência de seu radical. Logo, existe  $r$  tal que  $\mathbf{m}^r \subset \mathbf{q} \subset \mathbf{m}$  e, assim,  $\mathbf{m}^{rn} \subset \mathbf{q}^n \subset \mathbf{m}^n$  para todo  $n$ . Portanto,

$$l\left(\frac{A}{\mathbf{m}^{rn}}\right) \geq l\left(\frac{A}{\mathbf{q}^n}\right) \geq l\left(\frac{A}{\mathbf{m}^n}\right), \text{ isto é,}$$

$$\chi_{\mathbf{m}}(n) \leq \chi_{\mathbf{q}}(n) \leq \chi_{\mathbf{m}}(rn),$$

para  $n$  suficientemente grande. Assim, sendo  $d$  o grau de  $\chi_{\mathbf{m}}(n)$ , temos

$$1 \leq \frac{\chi_{\mathbf{q}}(n)}{\chi_{\mathbf{m}}(n)} \leq \frac{\chi_{\mathbf{m}}(rn)}{\chi_{\mathbf{m}}(n)} \text{ e } \lim_{n \rightarrow \infty} \frac{\chi_{\mathbf{m}}(rn)}{\chi_{\mathbf{m}}(n)} = r^d.$$

Portanto,  $1 \leq \lim_{n \rightarrow \infty} \frac{\chi_{\mathbf{q}}(n)}{\chi_{\mathbf{m}}(n)} \leq r^d$ , de onde segue que  $\text{grau } (\chi_{\mathbf{q}}(n)) = \text{grau } (\chi_{\mathbf{m}}(n))$ .  $\square$

**Observação 1.30** O teorema nos informa que os polinômios  $\chi_{\mathbf{q}}(n)$  possuem o mesmo grau, independentemente da escolha do ideal  $\mathbf{m}$ -primário  $\mathbf{q}$ , ou seja,  $\chi_{\mathbf{q}}(n)$  é um invariante do anel  $(A, \mathbf{m})$  sobre os ideais  $\mathbf{m}$ -primários.

O grau comum de  $\chi_{\mathbf{q}}(n)$  será denotado por  $d(A)$ . Em vista do Corolário 1.15, isto significa que estamos colocando  $d(A) = d(G_{\mathbf{m}}(A))$  onde  $d(G_{\mathbf{m}}(A))$  é o inteiro definido anteriormente como o polo em  $t = 1$  da função de Hilbert de  $G_{\mathbf{m}}(A)$ .

Para  $A$  um anel Noetheriano local, com  $\mathbf{m}$  seu ideal maximal indicamos por  $K = A/\mathbf{m}$  o corpo de resíduos do anel  $A$ . Nestas condições  $\mathbf{m}/\mathbf{m}^2$  é um  $K$ -espaço vetorial de modo natural e indicamos por  $\dim_K \mathbf{m}/\mathbf{m}^2$  a dimensão de  $\mathbf{m}/\mathbf{m}^2$  como  $K$ -espaço vetorial.

Seja  $A$  um anel Noetheriano local,  $\mathbf{m}$  seu ideal maximal. Seja  $\delta(A)$  o número mínimo de geradores de um ideal  $\mathbf{m}$ -primário de  $A$ . Provaremos que  $\delta(A) = d(A) = \dim A$ , onde  $\dim A$  indica a dimensão de Krull de  $A$ , ou seja,  $\dim A = \sup\{k \in \mathbb{Z} \mid \text{existe } \mathbf{p}_0 \subset \mathbf{p}_1 \subset \cdots \subset \mathbf{p}_k, p_i \in \text{Spec}(A), \text{ onde a inclusão é estrita}\}$ . Conseguiremos isto mostrando  $\delta(A) \geq d(A) \geq \dim A \geq \delta(A)$ .

O Corolário 1.28 e a Proposição 1.29 juntos nos dão:

**Proposição 1.31**  $\delta(A) \geq d(A)$ .

Agora provaremos o análogo da Proposição 1.17 para anéis locais.

**Proposição 1.32** *Sejam  $(A, \mathfrak{m})$  anel local e  $\mathfrak{q}$  um ideal  $\mathfrak{m}$ -primário. Sejam  $M$  um  $A$ -módulo finitamente gerado,  $x \in A$  um não-divisor de zero de  $M$  e  $M' = M/xM$ . Então  $\text{grau } \chi_{\mathfrak{q}}^{M'} \leq \text{grau } \chi_{\mathfrak{q}}^M - 1$ .*

**Demonstração:** Supondo  $N = xM$  temos  $N \simeq M$  como  $A$ -módulo, tendo em vista que  $x$  não é um divisor de zero de  $M$ . Para cada  $n \in \mathbb{N}$ , seja  $N_n = N \cap \mathfrak{q}^n M$ . Então temos seqüências exatas

$$0 \rightarrow \frac{N}{N_n} \rightarrow \frac{M}{\mathfrak{q}^n M} \rightarrow \frac{M'}{\mathfrak{q}^n M'} \rightarrow 0.$$

Assim, se  $g(n) = l(N/N_n)$ , temos, para  $n$  suficientemente grande

$$g(n) - \chi_{\mathfrak{q}}^M(n) + \chi_{\mathfrak{q}}^{M'}(n) = 0.$$

Pela Proposição 1.22,  $(N_n)$  é uma  $\mathfrak{q}$ -filtração estável de  $N$ . Como  $N \simeq M$  o Teorema 1.26 (iii) nos garante que  $g(n)$  e  $\chi_{\mathfrak{q}}^M(n)$  possuem o mesmo termo líder e o resultado segue.  $\square$

**Corolário 1.33** *Se  $A$  é um anel Noetheriano local,  $x$  um não divisor de zero de  $A$ , então  $d(A/(x)) \leq d(A) - 1$ .*

Com as hipóteses e notações dos parágrafos anteriores temos:

**Proposição 1.34**  $d(A) \geq \dim A$ .

**Demonstração:** Faremos a demonstração por indução sobre  $d = d(A)$ .

Se  $d = 0$ , então  $l(A/\mathfrak{m}^n)$  é constante para todo  $n$  suficientemente grande, logo  $\mathfrak{m}^n = \mathfrak{m}^{n+1}$  para algum  $n$  e, pelo Lema de Nakayama,  $\mathfrak{m}^n = 0$ . Deste modo  $A$  é Artiniano e  $\dim A = 0$ .

Supondo  $d > 0$  e que o resultado valha para todo número menor do que  $d$ . Tomamos  $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_r$  uma cadeia de ideais primos em  $A$ . Seja  $x \in \mathfrak{p}_1$ ,  $x \notin \mathfrak{p}_0$ . Tomando  $A' = A/\mathfrak{p}_0$  e sendo  $x'$  a imagem de  $x$  em  $A'$ , então  $x' \neq 0$  em  $A'$ ,  $A'$  é um domínio de integridade e, pelo Corolário 1.33, temos

$$d(A'/(x')) \leq d(A') - 1.$$

Além disso, se  $\mathfrak{m}'$  é o ideal maximal de  $A'$ ,  $A'/\mathfrak{m}'^n$  é a imagem homomórfica de  $A/\mathfrak{m}^n$ . Deste modo,  $l(A/\mathfrak{m}^n) \geq l(A'/\mathfrak{m}'^n)$  e, portanto,  $d(A) \geq d(A')$ . Conseqüentemente  $d(A'/(x')) \leq d(A) - 1 = d - 1$ . Pela hipótese de indução, o comprimento de qualquer cadeia de ideais primos em  $A'/(x')$  é menor ou igual a  $d - 1$ . Como as imagens de  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ , em  $A'/(x')$ , formam uma cadeia de comprimento  $r - 1$ , temos  $r - 1 \leq d - 1$  e, assim,  $r \leq d$ . Concluimos com isto que  $\dim A \leq d = d(A)$ .  $\square$

**Corolário 1.35** *Se  $A$  é um anel Noetheriano local,  $\dim A$  é finita.*

**Proposição 1.36** *Seja  $A$  um anel Noetheriano local de dimensão  $d$ . Então existe um ideal  $\mathfrak{m}$ -primário em  $A$  gerado por elementos  $x_1, \dots, x_d$  e, assim,  $\dim A \geq \delta(A)$ .*

**Demonstração:** Construiremos os elementos  $x_1, \dots, x_d$  indutivamente de tal modo que todo ideal primo contendo  $(x_1, \dots, x_i)$  possua altura maior ou igual a  $i$ .

Tomemos  $x_1$  de forma que  $x_1 \notin \bigcup_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}$ , onde

$$\mathcal{P} = \{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ é um ideal primo minimal de } A\}.$$

Notemos que se não existir tal elemento,  $A$  é um anel Artiniano local e  $\sqrt{(0)} = \mathfrak{m}$ . Logo  $\delta(A) = 0$  e  $\dim A = 0$ .

Assim,  $x_1 \notin \mathfrak{p}$  para todo  $\mathfrak{p}$  ideal primo minimal de  $A$  e, portanto, se  $\mathfrak{q} \in \text{Spec}(A)$  e  $x_1 \in \mathfrak{q}$  então altura de  $\mathfrak{q}$  é maior ou igual a 1, pois  $\mathfrak{q}$  contém algum primo minimal de  $A$ .

Tomando  $i, d \geq i > 1$ , e supondo que já tenhamos construído  $(x_1, \dots, x_{i-1})$  desta forma, sejam  $\mathfrak{p}_j$  ( $1 \leq j \leq s$ ) os ideais primos minimais (se existirem) de  $(x_1, \dots, x_{i-1})$  que possuem altura exatamente  $i-1$ . Como  $i-1 < d = \dim A = \text{altura } \mathfrak{m}$ , temos  $\mathfrak{m} \neq \mathfrak{p}_j$  ( $1 \leq j \leq s$ ) e, deste modo,  $\mathfrak{m} \neq \bigcup_{j=1}^s \mathfrak{p}_j$ . Tomando  $x_i \in \mathfrak{m}$ ,  $x_i \notin \bigcup \mathfrak{p}_j$  e  $\mathfrak{q}$  qualquer ideal primo contendo  $(x_1, \dots, x_i)$ , então  $\mathfrak{q}$  contém algum ideal primo minimal  $\mathfrak{p}$  de  $(x_1, \dots, x_{i-1})$ . Se  $\mathfrak{p} = \mathfrak{p}_j$  para algum  $j$ , temos  $x_i \notin \mathfrak{p}$  e  $x_i \in \mathfrak{q}$ . Logo  $\mathfrak{q} \supset \mathfrak{p}$  e, portanto, altura de  $\mathfrak{q}$  é maior ou igual a  $i$ . Se  $\mathfrak{p} \neq \mathfrak{p}_j$  então altura de  $\mathfrak{p}$  maior que  $i-1$  e, assim, altura de  $\mathfrak{q}$  é maior ou igual a  $i$ . Logo todo ideal primo contendo  $(x_1, \dots, x_i)$  possui altura maior ou igual a  $i$ .

Consideremos então  $(x_1, \dots, x_d)$ . Se  $\mathfrak{p}$  é um ideal primo que contenha  $(x_1, \dots, x_d)$ ,  $\mathfrak{p}$  possui altura maior ou igual a  $d$  e, assim,  $\mathfrak{p} = \mathfrak{m}$  (se  $\mathfrak{p} \subsetneq \mathfrak{m}$  temos altura  $\mathfrak{p} < \text{altura } \mathfrak{m} = d$ ). Portanto o ideal  $(x_1, \dots, x_d)$  é  $\mathfrak{m}$ -primário.  $\square$

**Teorema 1.37 (Teorema da Dimensão)** Para qualquer anel Noetheriano local  $A$ , os três inteiros seguintes são iguais:

- (i) O comprimento máximo de cadeias de ideais primos em  $A$ , isto é, a dimensão de Krull do anel  $A$ .
- (ii) O grau do polinômio característico  $\chi_{\mathfrak{m}}(n) = l(A/\mathfrak{m}^n)$ , isto é,  $d(A)$ ;
- (iii) O número mínimo de geradores de um ideal  $\mathfrak{m}$ -primário de  $A$ , isto é,  $\delta(A)$ .

**Demonstração:** A demonstração segue das Proposições 1.31, 1.34 e 1.36.  $\square$

Como consequência imediata, obtemos:

**Corolário 1.38**  $\dim A \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ .

**Corolário 1.39** Sejam  $A$  um anel Noetheriano e  $x_1, \dots, x_r \in A$ . Então todo ideal primo minimal  $\mathfrak{p}$  de  $(x_1, \dots, x_r)$  possui altura menor ou igual a  $r$ .

**Demonstração:** Em  $A_{\mathfrak{p}}$  o ideal  $(x_1, \dots, x_r)$  torna-se  $\mathfrak{p}^e$ -primário (onde  $\mathfrak{p}^e$  indica a extensão do ideal  $\mathfrak{p}$ ) e, deste modo,  $r \geq \dim A_{\mathfrak{p}} = \text{altura } \mathfrak{p}$ .  $\square$

**Corolário 1.40 (Teorema do Ideal Principal de Krull)** Seja  $A$  um anel Noetheriano e seja  $x$  um elemento de  $A$  que não é um divisor de zero e nem uma unidade. Então, todo ideal primo minimal  $\mathfrak{p}$  de  $(x)$  possui altura 1.

**Demonstração:** Pelo Corolário 1.39, temos a altura do ideal  $\mathfrak{p}$  menor ou igual a 1. Se altura  $\mathfrak{p} = 0$ , então  $\mathfrak{p}$  é um ideal primo contido em  $(0)$  e, assim, todo elemento de  $\mathfrak{p}$  é divisor de zero, que é uma contradição, pois  $x \in \mathfrak{p}$ . Logo a altura do ideal  $\mathfrak{p}$  é 1.  $\square$

**Corolário 1.41** *Sejam  $A$  um anel Noetheriano local,  $x$  um elemento de  $\mathfrak{m}$  não divisor de zero. Então  $\dim A/(x) = \dim A - 1$ .*

**Definição 1.42** *Seja  $(A, \mathfrak{m})$  anel Noetheriano local. Se  $x_1, \dots, x_d$  geram um ideal  $\mathfrak{m}$ -primário e  $d = \dim A$ , dizemos que  $x_1, \dots, x_d$  é um sistema de parâmetros.*

**Exemplo 1.43** *Se  $A = K[[x_1, \dots, x_n]]$  é o anel das séries de potências formais sobre um corpo  $K$ , então  $x_1, \dots, x_n$  formam um sistema de parâmetros para  $A$ , pois eles geram o ideal maximal.*

Um sistema de parâmetros possui certa propriedade de independência, que descreveremos a seguir:

**Proposição 1.44** *Sejam  $x_1, \dots, x_d$  um sistema de parâmetros para  $A$  e  $\mathfrak{q} = (x_1, \dots, x_d)$  o ideal  $\mathfrak{m}$ -primário gerado por eles. Seja  $f \in A[t_1, \dots, t_d]$  um polinômio homogêneo de grau  $s$  e suponha que  $f(x_1, \dots, x_d) \in \mathfrak{q}^{s+1}$ . Então, todos os coeficientes de  $f$  estão em  $\mathfrak{m}$ .*

**Demonstração:** Consideremos a aplicação:

$$\alpha : \left( \frac{A}{\mathfrak{q}} \right) [t_1, \dots, t_d] \rightarrow G_{\mathfrak{q}}(A) = \left( \frac{A}{\mathfrak{q}} \right) [\bar{x}_1, \dots, \bar{x}_d]$$

$$t_i \mapsto \bar{x}_i$$

Com as hipóteses sobre  $f$  temos que  $\bar{f}(t_1, \dots, t_d) = 0$  ( $\bar{f}$  imagem de  $f$ ) e, portanto,  $f$  está no núcleo de  $\alpha$ .

Se algum coeficiente de  $\bar{f}$  for uma unidade, então  $\bar{f}$  não será divisor de zero e como  $\alpha$  é claramente sobrejetora, temos que

$$G_{\mathfrak{q}}(A) \simeq \frac{\left( \frac{A}{\mathfrak{q}} [t_1, \dots, t_d] \right)}{\text{Ker}(\alpha)}.$$

Assim,

$$d(G_{\mathfrak{q}}(A)) = d \left( \frac{\left( \frac{A}{\mathfrak{q}} [t_1, \dots, t_d] \right)}{\text{Ker}(\alpha)} \right) \leq d \left( \frac{\left( \frac{A}{\mathfrak{q}} [t_1, \dots, t_d] \right)}{\langle \bar{f} \rangle} \right).$$

Porém,

$$d \left( \frac{\left( \frac{A}{\mathfrak{q}} [t_1, \dots, t_d] \right)}{\langle \bar{f} \rangle} \right) = d \left( \frac{A}{\mathfrak{q}} [t_1, \dots, t_d] \right) - 1 = d - 1,$$

isto é,  $d(G_{\mathfrak{q}}(A)) \leq d - 1$ . Mas, também,  $d(G_{\mathfrak{q}}(A)) = d(G_{\mathfrak{m}}(A)) = d(A) = d$ , o que é absurdo.

Logo  $\bar{f}$  é divisor de zero de  $(A/\mathfrak{q})[t_1, \dots, t_d]$ . Assim, existe  $\bar{a} \in A/\mathfrak{q}$ , com  $\bar{a} \neq \bar{0}$  e  $\bar{a}\bar{f} = \bar{0}$ , ou seja,  $\bar{a}b_i = \bar{0}$  para todo  $b_i$  coeficiente de  $f$ . Deste modo,  $ab_i \in \mathfrak{q}$  para todo  $i$ . Sendo  $\bar{a} \neq \bar{0}$ ,  $a \notin \mathfrak{q}$  e portanto  $b_i \in \sqrt{\mathfrak{q}} = \mathfrak{m}$  para todo  $i$ , isto é, todo coeficiente de  $f$  pertence a  $\mathfrak{m}$ .  $\square$

Essa proposição tem uma forma simples se  $A$  contém um corpo  $K$  isomorfo ao corpo de resíduos  $A/\mathfrak{m}$ .

**Corolário 1.45** Se  $K \subset A$  é um corpo isomorfo a  $A/\mathfrak{m}$  e se  $x_1, \dots, x_d$  é um sistema de parâmetros, então  $x_1, \dots, x_d$  são algebricamente independentes sobre  $K$ .

**Demonstração:** Suponha  $f(x_1, \dots, x_d) = 0$ , onde  $f$  é um polinômio com coeficientes em  $K$ . Se  $f \neq 0$ , podemos escrever  $f = f_s +$  termos de graus maiores, onde  $f_s$  é homogêneo de grau  $s$  e  $f_s \neq 0$ . Aplicando a Proposição 1.44 para  $f_s$  segue que  $f_s$  tem todos os seus coeficientes em  $\mathfrak{m}$ , ou seja,  $f_s \equiv 0$  (Absurdo!).

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

**Definição 1.46** Um anel local regular é um anel que satisfaz uma das três condições (equivalentes) da proposição a seguir:

**Proposição 1.47** Sejam  $(A, \mathfrak{m})$  um anel Noetheriano local de dimensão  $d$  e  $K = A/\mathfrak{m}$  seu corpo de resíduos. Então são equivalentes:

- (i)  $G_{\mathfrak{m}}(A) \simeq K[t_1, \dots, t_d]$ , onde os  $t_i$ 's são variáveis independentes sobre  $K$ ;
- (ii)  $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = d$ ;
- (iii)  $\mathfrak{m}$  é gerado por  $d$  elementos.

**Demonstração:** (i)  $\Rightarrow$  (ii) Temos que  $G_{\mathfrak{m}}(A) = \bigoplus_{n=0}^{\infty} \frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}} \simeq \bigoplus_{n=0}^{\infty} A_n$ . Sejam  $x_1, \dots, x_{d+1}$  elementos de  $A_1$ . Como

$$G_{\mathfrak{m}}(A) = \bigoplus_{n=0}^{\infty} \frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}} \simeq \bigoplus_{n=0}^{\infty} A_n \simeq K[t_1, \dots, t_d]$$

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

Agora, pelo Corolário 1.38  $\dim_K(\mathfrak{m}/\mathfrak{m}^2) \geq \dim A = d$ . Portanto,  $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = d$ .

(ii)  $\Rightarrow$  (iii) Sejam  $m_1, \dots, m_d$  os elementos de  $\mathfrak{m}$  cujos resíduos formam uma base para  $\mathfrak{m}/\mathfrak{m}^2$ . Deste modo,  $\mathfrak{m}/\mathfrak{m}^2 = \langle \bar{m}_1, \dots, \bar{m}_d \rangle$  e, com isto,  $\mathfrak{m} = \langle m_1, \dots, m_d \rangle + \mathfrak{m}^2$ . Pelo Lema de Nakayama, segue que  $\mathfrak{m} = \langle m_1, \dots, m_d \rangle$ .

(iii)  $\Rightarrow$  (i) Sejam  $\mathfrak{m} = \langle x_1, \dots, x_d \rangle$ ,  $A/\mathfrak{m} = K$  e

$$\alpha: K[t_1, \dots, t_d] \rightarrow G_{\mathfrak{m}} = K[\bar{x}_1, \dots, \bar{x}_d] = \bigoplus_{i=1}^{\infty} A_i$$

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

A aplicação  $\alpha$  está bem definida e é, claramente, um homomorfismo sobrejetor de anéis graduados.

Seja  $f \in K[t_1, \dots, t_d]$  tal que  $\alpha(f) = 0$ . Podemos escrever  $f = f_0 + \dots + f_r$ , onde  $f_j$  denota a componente de grau  $j$  de  $f$ . Como  $\alpha(f) = 0$  temos que  $\alpha(f_0) + \dots + \alpha(f_r) = 0$  e, assim,  $\alpha(f_j) = 0$  para todo  $j$ .

Mas,  $f_s$  é homogêneo de grau  $s$  e

$$f_s = \sum_{k=1}^d a_k t_1^{i_1} \dots t_d^{i_d}, \text{ com } \sum i_r = s.$$

Deste modo,  $f_s(\bar{x}_1, \dots, \bar{x}_d) = \sum_{k=1}^d a_k \bar{x}_1^{i_1} \cdots \bar{x}_d^{i_d}$ , com  $\bar{x}_i \in \mathfrak{m}/\mathfrak{m}^2 = A^1$ . Logo  $\bar{x}_j^{i_j} \in A_{i_j}$  e, assim,  $\bar{x}_1^{i_1} \cdots \bar{x}_d^{i_d} \in A_s = \mathfrak{m}^s/\mathfrak{m}^{s+1}$ . Como  $a_k \in A/\mathfrak{m} = A_0$ ,  $f_s(\bar{x}_1, \dots, \bar{x}_d) \in \mathfrak{m}^s/\mathfrak{m}^{s+1}$  e  $f_s(\bar{x}_1, \dots, \bar{x}_d) = 0$  temos os coeficientes de  $f_s$  em  $\mathfrak{m}$  e, portanto,  $f_s = 0$ . Analogamente se demonstra para os outros  $f_j$  e, com isto,  $f = 0$ , de onde segue que  $\alpha$  é um isomorfismo.  $\square$

## Capítulo 2

# Bases de Gröbner

## 2.1 Introdução

### 2.1.1 Polinômios

Intuitivamente, introduziremos a seguinte noção. Um polinômio em  $x_1, \dots, x_d$  é um polinômio da seguinte forma  $a_0 + a_1x_1 + \dots + a_{i_1}x_1^{i_1} + \dots + a_{i_1, \dots, i_d}x_1^{i_1} \cdots x_d^{i_d}$ , onde todos os expoentes  $i_1, \dots, i_d$ , são inteiros não negativos. O grau total deste monômio é a soma  $i_1 + \dots + i_d$ .

Para manipular a estrutura dos monômios, seja  $\mathbf{g} = (g_1, \dots, g_d) \in \mathbb{N}^d$ . Denotamos o monômio  $x_1^{g_1} \cdots x_d^{g_d}$  por  $\mathbf{g}^*$ . Quando  $\mathbf{g} = (0, 0, \dots, 0)$ ,  $\mathbf{g}^* = 1$ . Também usaremos  $|\mathbf{g}| = g_1 + \dots + g_d$ , para denotar o grau total do monômio  $\mathbf{g}^* = \mathbf{g}^*$  para o conjunto de todos os monômios, ou seja,

$$M = \{\mathbf{g}^* \mid \mathbf{g} \in \mathbb{N}^d\}.$$

Um polinômio  $f$  em  $x_1, \dots, x_d$  pode ser escrito em tal forma  $f = \sum_{\mathbf{g} \in M} a_{\mathbf{g}} \mathbf{g}^*$ , onde  $a_{\mathbf{g}} \in K$ .

$$f = \sum_{\mathbf{g} \in M} a_{\mathbf{g}} \mathbf{g}^*, \quad a_{\mathbf{g}} \in K,$$

onde  $a_{\mathbf{g}} = 0$  para quase todo  $\mathbf{g} \in \mathbb{N}^d$ .

O conjunto de todos os polinômios em  $x_1, \dots, x_d$  com coeficientes no corpo  $K$  é denotado por  $K[x_1, \dots, x_d]$  ou simplesmente  $K[x]$ .

Seja  $f = \sum_{\mathbf{g} \in M} a_{\mathbf{g}} \mathbf{g}^*$  um polinômio em  $K[x]$ .

- (i) Chamamos  $a_{\mathbf{g}}$  de coeficiente do monômio  $\mathbf{g}^*$ .
- (ii) Se  $a_{\mathbf{g}} \neq 0$ , então  $a_{\mathbf{g}} \mathbf{g}^*$  é um termo de  $f$ .
- (iii) O grau total de  $f$  denotado grau  $f$ , é o máximo dos  $|\mathbf{g}|$  tal que o coeficiente  $a_{\mathbf{g}} \neq 0$ .

### 2.1.2 Ordem Monomial

Definição 2.1 Uma ordem monomial sobre  $K[x]$  é qualquer relação  $>$  entre os membros de  $M$  tal que, equivalentemente, entre os monômios  $\mathbf{g}^*$  e  $\mathbf{h}^*$  satisficando

## Capítulo 2

# Bases de Gröbner

### 2.1 Introdução

#### 2.1.1 Polinômios

Inicialmente, introduziremos algumas notações. Um monômio em  $x_1, \dots, x_n$  é um produto da seguinte forma  $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ , onde todos os expoentes  $\alpha_1, \dots, \alpha_n$  são inteiros não negativos. O grau total deste monômio é a soma  $\alpha_1 + \cdots + \alpha_n$ .

Para simplificar a notação dos monômios, seja  $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ . Denotaremos o monômio  $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$  por  $\underline{x}^{\underline{\alpha}}$ . Quando  $\underline{\alpha} = (0, 0, \dots, 0)$ ,  $\underline{x}^{\underline{\alpha}} = 1$ . Também usaremos  $|\underline{\alpha}| = \alpha_1 + \cdots + \alpha_n$ , para denotar o grau total do monômio  $\underline{x}^{\underline{\alpha}}$  e  $\mathbb{M}$  para o conjunto de todos os monômios, ou seja,

$$\mathbb{M} = \{\underline{x}^{\underline{\alpha}} \mid \underline{\alpha} \in \mathbb{N}^n\}.$$

Um polinômio  $f$  em  $x_1, \dots, x_n$  com coeficientes em um corpo  $K$  é uma combinação linear finita de monômios. Escrevemos  $f$  na forma:

$$f = \sum_{\underline{\alpha} \in \mathbb{N}^n} a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}, \quad a_{\underline{\alpha}} \in K,$$

com  $a_{\underline{\alpha}} = 0$  para quase todo  $\underline{\alpha} \in \mathbb{N}^n$ .

O conjunto de todos os polinômios em  $x_1, \dots, x_n$  com coeficientes no corpo  $K$  é denotado por  $K[x_1, \dots, x_n]$  ou simplesmente  $K[\underline{x}]$ .

Seja  $f = \sum_{\underline{\alpha}} a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}$  um polinômio em  $K[\underline{x}]$ .

- (i) Chamamos  $a_{\underline{\alpha}}$  de coeficiente do monômio  $\underline{x}^{\underline{\alpha}}$ .
- (ii) Se  $a_{\underline{\alpha}} \neq 0$ , então  $a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}$  é um termo de  $f$ .
- (iii) O grau total de  $f$  denotado grau  $f$ , é o máximo dos  $|\underline{\alpha}|$  tais que o coeficiente  $a_{\underline{\alpha}} \neq 0$ .

#### 2.1.2 Ordens Monomiais

**Definição 2.1** Uma ordem monomial sobre  $K[\underline{x}]$  é qualquer relação  $>$  sobre o conjunto dos monômios  $\mathbb{M}$  (ou, equivalentemente, sobre os vetores expoentes  $\underline{\alpha} \in \mathbb{N}^n$ ) satisfazendo

- (i)  $>$  é uma relação de ordem total.
- (ii)  $>$  é compatível com a multiplicação em  $K[x]$ , no sentido de que se  $\underline{x}^\alpha > \underline{x}^\beta$  e  $\underline{x}^\gamma$  é um outro monômio qualquer, então  $\underline{x}^\alpha \underline{x}^\gamma = \underline{x}^{\alpha+\gamma} > \underline{x}^{\beta+\gamma} = \underline{x}^\beta \underline{x}^\gamma$ .
- (iii)  $>$  é uma boa ordem, ou seja, todo conjunto não vazio, cujos elementos são todos monômios, possui um menor elemento em relação a  $>$ .

**Lema 2.2** Uma relação de ordem  $>$  sobre  $\mathbb{M}$  é uma boa ordem se, e somente se, toda seqüência estritamente decrescente de elementos de  $\mathbb{M}$ ,

$$\underline{x}^{\alpha_1} > \underline{x}^{\alpha_2} > \underline{x}^{\alpha_3} > \dots$$

estaciona.

**Demonstração:** Claro que se  $>$  é uma boa ordem, então toda cadeia de elementos de  $\mathbb{M}$  estaciona.

Por outro lado, supondo que toda seqüência estritamente decrescente de elementos em  $\mathbb{M}$  estaciona e que  $>$  não seja uma boa ordem, teremos algum subconjunto não vazio  $S \subset \mathbb{M}$  sem menor elemento. Tome  $\underline{x}^{\alpha_1} \in S$ . Como  $\underline{x}^{\alpha_1}$  não é o menor elemento de  $S$ , existe  $\underline{x}^{\alpha_2} \in S$  com  $\underline{x}^{\alpha_1} > \underline{x}^{\alpha_2}$ . Novamente,  $\underline{x}^{\alpha_2}$  não é o menor elemento de  $S$  e, por isso, existe  $\underline{x}^{\alpha_3} \in S$  com  $\underline{x}^{\alpha_2} > \underline{x}^{\alpha_3}$ . Continuando desta forma, construímos uma seqüência estritamente decrescente

$$\underline{x}^{\alpha_1} > \underline{x}^{\alpha_2} > \underline{x}^{\alpha_3} > \dots$$

que não estaciona.  $\square$

## Exemplos de Ordens Monomiais

### Ordem Lexicográfica

Sejam  $\underline{x}^\alpha$  e  $\underline{x}^\beta$  dois monômios em  $K[x]$ . Dizemos que  $\underline{x}^\alpha >_{lex} \underline{x}^\beta$  se na diferença  $\alpha - \beta \in \mathbb{Z}^n$  a entrada não nula mais à esquerda é positiva, ou seja, se  $\alpha_j - \beta_j > 0$  e  $\alpha_i - \beta_i = 0$ ,  $1 \leq i < j$ .

### Ordem Lexicográfica Graduada

Sejam  $\underline{x}^\alpha$  e  $\underline{x}^\beta$  dois monômios em  $K[x]$ . Dizemos que  $\underline{x}^\alpha >_{grlex} \underline{x}^\beta$  se  $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$  ou, se  $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$  e  $\underline{x}^\alpha >_{lex} \underline{x}^\beta$ .

Outra ordem monomial (de certa forma menos intuitiva) é a ordem lexicográfica graduada reversa:

### Ordem Lexicográfica Graduada Reversa

Sejam  $\underline{x}^\alpha$  e  $\underline{x}^\beta$  dois monômios em  $K[\underline{x}]$ . Dizemos que  $\underline{x}^\alpha >_{\text{grevlex}} \underline{x}^\beta$  se  $\sum_{i=1}^n \alpha_i > \sum_{i=1}^n \beta_i$  ou, se  $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$  e na diferença  $\underline{\alpha} - \underline{\beta} \in \mathbb{Z}^n$  a entrada não nula mais à direita é negativa, ou seja,  $\alpha_j - \beta_j < 0$  e  $\alpha_i - \beta_i = 0$ ,  $j < i \leq n$ .

Note que  $\text{grlex}$  e  $\text{grevlex}$  nos dão a mesma ordem nas variáveis, pois

$$x_1 >_{\text{grlex}} x_2 >_{\text{grlex}} \cdots >_{\text{grlex}} x_n, \text{ e}$$

$$x_1 >_{\text{grevlex}} x_2 >_{\text{grevlex}} \cdots >_{\text{grevlex}} x_n.$$

Mas,  $\text{grevlex}$  é realmente diferente da  $\text{grlex}$ . Vejamos isto com mais cautela: ambas ordenam da mesma forma, no caso de graus totais diferentes. Mas numa igualdade,  $\text{grlex}$  usa a ordem  $\text{lex}$  e, assim, ela “olha” na variável mais à esquerda e “favorece” a de maior grau. Em contraste, quando a  $\text{grevlex}$  encontra o mesmo grau total, ela “olha” na variável mais à direita e “favorece” a menor potência!

**Exemplo 2.3** Vejamos com exemplos a diferença da  $\text{grevlex}$  e da  $\text{grlex}$  em dois casos:

- (i)  $x^5yz >_{\text{grlex}} x^4yz^2$  pois ambos monômios possuem grau total 7 e  $x^5yz >_{\text{lex}} x^4yz^2$  (a potência da primeira variável em  $x^5yz$  é maior que em  $x^4yz^2$ ). Neste caso também temos  $x^5yz >_{\text{grevlex}} x^4yz^2$ , mas por outra razão: a menor variável  $z$ , aparece com uma potência menor em  $x^5yz$ .
- (ii) Com relação aos monômios  $x^5y^3z$  e  $x^6yz^2$ , ambos de grau total 9, temos  $x^5y^3z >_{\text{grevlex}} x^6yz^2$  e  $x^6yz^2 >_{\text{grlex}} x^5y^3z$ .

**Definição 2.4** Fixando uma ordem monomial  $>$  sobre  $K[\underline{x}]$  consideramos os termos em

$$f = \sum_{\underline{\alpha}} c_{\underline{\alpha}} \underline{x}^{\underline{\alpha}} \neq 0.$$

- (i) O termo líder de  $f$  (com respeito a  $>$ ) é o produto  $c_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}$ , onde  $\underline{x}^{\underline{\alpha}}$  é o maior monômio (com respeito a  $>$ ) que ocorre em  $f$  com  $c_{\underline{\alpha}} \neq 0$ . Usaremos a notação  $LT_{>}(f)$  ou, simplesmente,  $LT(f)$ , caso não haja confusão sobre a ordem monomial que está sendo usada.
- (ii) O coeficiente do termo líder de  $f$  é chamado de coeficiente líder e o monômio deste termo é o monômio líder, que são denotados, respectivamente por  $LC(f)$  e  $LM(f)$ .
- (iii) O expoente que aparece no monômio líder é chamado de multigrado de  $f$  e denotado por  $\text{multigrado}(f)$ .

**Exemplo 2.5** Consideremos  $f = x^5y^3z - x^6yz^2 + x^7$ .

Como a maior potência em  $x$  aparece em  $x^7$  temos

$$LT_{>_{\text{lex}}}(f) = x^7 \text{ e } \text{multigrado}_{>_{\text{lex}}}(f) = (7, 0, 0).$$

Observando que  $|(5, 3, 1)| = |(6, 1, 2)| = 9 > |(7, 0, 0)|$ , nos termos com grau total 9, a maior potência em  $x$  aparece em  $x^6yz^2$  e a menor potência em  $z$  aparece em  $x^5y^3z$ , logo

$$LT_{>_{\text{grlex}}}(f) = -x^6yz^2 \text{ e } LT_{>_{\text{grevlex}}}(f) = x^5y^3z.$$

Nestes dois casos temos

$$\text{multigrau}_{>_{\text{grlex}}}(f) = (6, 1, 2) \text{ e } \text{multigrau}_{>_{\text{grevlex}}}(f) = (5, 3, 1).$$

## 2.2 Algoritmo da Divisão

Usando uma ordem sobre os monômios, podemos generalizar o conhecido algoritmo da divisão para uma variável.

**Proposição 2.6 (Algoritmo da Divisão em  $K[\underline{x}]$ )** Fixada uma ordem monomial qualquer  $>$  em  $K[\underline{x}]$ , seja  $F = (f_1, \dots, f_s)$  uma  $s$ -upla ordenada de polinômios em  $K[\underline{x}] - 0$ . Então todo  $f \in K[\underline{x}]$  pode ser escrito como

$$f = a_1f_1 + \dots + a_sf_s + r,$$

onde  $a_i, r \in K[\underline{x}]$  e  $r = 0$  ou  $r$  é uma  $K$ -combinação linear de monômios, dos quais nenhum é divisível por algum  $LT(f_i)$ ,  $i = 1, \dots, s$ . Chamamos  $r$  de resto da divisão de  $f$  por  $F$  e será denotado por  $r = \tilde{f}^F$ . Além disso temos que  $LT(a_if_i) \leq LT(f)$  sempre que  $a_i \neq 0$ .

**Demonstração:** Provaremos a existência dos  $a_1, \dots, a_s$  e  $r$  apresentando um algoritmo que os determina.

**Entrada:**  $f_1, \dots, f_s, f$

**Saída:**  $a_1, \dots, a_s, r$

$a_1 := 0; \dots; a_n := 0; r := 0$

$p := f$

ENQUANTO  $p \neq 0$  FAÇA

$i := 1$

$\text{ocorredivisao} := \text{falso}$

ENQUANTO  $i \leq s$  E  $\text{ocorredivisao} = \text{falso}$  FAÇA

SE  $LT(f_i)$  divide  $LT(p)$  ENTÃO

$a_i := a_i + LT(p)/LT(f_i)$

$p := p - (LT(p)/LT(f_i))f_i$

$\text{ocorredivisao} := \text{verdadeiro}$

SENÃO

$i := i + 1$

SE  $\text{ocorredivisao} = \text{falso}$  ENTÃO

$r := r + LT(p)$

$p := p - LT(p)$

Neste algoritmo  $p$  representa o dividendo intermediário em cada passo e a variável booleana  $\text{ocorredivisao}$  nos diz quando algum  $LT(f_i)$  divide o termo líder do dividendo intermediário.

Notemos que a cada passo do ENQUANTO..FAÇA principal, precisamente uma das duas situações a seguir ocorre:

- **Passo de Divisão:** Se algum  $LT(f_i)$  divide  $LT(p)$ , então o algoritmo adiciona o valor de  $LT(p)/LT(f_i)$  em  $a_i$ .
- **Passo de Resto:** Se nenhum  $LT(f_i)$  divide  $LT(p)$ , então o algoritmo adiciona  $LT(p)$  ao resto.

Para provar que o algoritmo funciona, inicialmente mostraremos que

$$f = a_1 f_1 + \cdots + a_s f_s + p + r \quad (2.1)$$

vale em todos os passos. Esta igualdade é claramente verdadeira nos valores iniciais de  $a_1, \dots, a_s, p$  e  $r$ . Supondo que em algum passo do algoritmo a igualdade (2.1) valha, se no próximo passo temos um Passo de Divisão, então algum  $LT(f_i)$  divide  $LT(p)$  e teremos

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

E isto mostra que no próximo passo  $a_i f_i + p$  ficou inalterado. Como nenhuma outra variável do algoritmo foi alterada, (2.1) continua valendo.

Agora, se o próximo passo for um Passo de Resto, então  $p$  e  $r$  serão alteradas, mas a soma  $p + r$  não, pois

$$p + r := [p - LT(p)] + [r + LT(p)],$$

mantendo (2.1) inalterada. Observamos que o algoritmo pára quando  $p = 0$  e, neste caso,

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

Como termos só serão adicionados a  $r$  se não forem divisíveis por nenhum  $LT(f_i)$ , segue que  $a_1, \dots, a_s$  e  $r$  possuem as propriedades desejadas quando o algoritmo pára.

Neste ponto, basta mostrar que o algoritmo realmente pára em algum momento. Para tanto, notemos que o grau total da variável  $p$  diminui toda vez que  $p$  é redefinida ou se torna zero. Veremos isto do seguinte modo: se durante um Passo de Divisão  $p$  for redefinida como

$$p' = p - \frac{LT(p)}{LT(f_i)} f_i,$$

$$LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p).$$

Logo  $p$  e  $[LT(p)/LT(f_i)] f_i$  possuem o mesmo termo líder e, conseqüentemente, sua diferença  $p'$  possui grau total estritamente menor, se  $p' \neq 0$ .

Se ocorrer um Passo de Resto,  $p$  será redefinido por

$$p' = p - LT(p),$$

e aqui, o grau total de  $p'$  é estritamente menor que o grau total de  $p$ , quando  $p' \neq 0$ .

Deste modo, nos dois casos, temos que o grau total de  $p$  diminui ou  $p$  se torna 0.

Se o algoritmo nunca parar, então conseguiremos uma sequência infinita estritamente decrescente de monômios. A propriedade da boa ordem em  $>$ , vista no Lema 2.2, mostra que isto não ocorre. Assim  $p = 0$  em algum momento, ou seja, o algoritmo pára depois de um número finito de passos.

Faltou estudar a relação entre o grau total de  $f$  e o grau total de  $a_i f_i$ , quando  $a_i \neq 0$ . Todo termo de  $a_i$  é da forma  $LT(p)/LT(f_i)$  para algum valor da variável  $p$ . O algoritmo começa com  $p = f$  e, acabamos de ver que, o grau total de  $p$  vai diminuindo a cada passo. Logo  $LT(p) \leq LT(f)$ , para todo valor não nulo da variável  $p$ .

Temos também que  $LT(a_i) = LT(p)/LT(f_i)$  para algum valor de  $p$  e, assim

$$LT(a_i f_i) = LT(a_i) LT(f_i) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p) \leq LT(f),$$

concluindo assim a demonstração.  $\square$

**Observação 2.7** Os polinômios  $a_1, \dots, a_s$  e  $r$  obtidos na divisão não são unicamente determinados. Se mudarmos a ordem de  $f_1, \dots, f_s$  podemos obter outros polinômios.

**Exemplo 2.8** Para ilustrar o funcionamento do algoritmo, usaremos a ordem lex em  $\mathbb{R}[x, y, z]$  e dividiremos  $f = xy^3z^2 + xyz^2$  por  $f_1 = xy - 1$  e  $f_2 = yz^2 - 1$ .

Inicialmente, teremos  $a_1 = a_2 = r = 0$  e  $p = f = xy^3z^2 + xyz^2$ .

- Como  $LT(f_1) = xy$  divide  $LT(p) = xy^3z^2$ , temos um passo de divisão e

$$a_1 := a_1 + \frac{LT(p)}{LT(f_1)} = 0 + y^2z^2 = y^2z^2,$$

$$p := p - \left( \frac{LT(p)}{LT(f_1)} \right) f_1 = (xy^3z^2 + xyz^2) - (y^2z^2)(xy - 1) = xyz^2 + y^2z^2.$$

- Neste passo, novamente,  $LT(f_1)$  divide  $LT(p) = xyz^2$ . O que nos dá outro passo de divisão. Assim,

$$a_1 := y^2z^2 + z^2,$$

$$p := (xyz^2 + y^2z^2) - (z^2)(xy - 1) = y^2z^2 + z^2.$$

- Agora,  $LT(f_1) = xy$  não divide  $LT(p) = y^2z^2$ , mas  $LT(f_2) = yz^2$  sim, gerando mais um passo de divisão.

$$a_2 := y \quad \text{e} \quad p := y + z^2.$$

- Agora, nem  $LT(f_1) = xy$  nem  $LT(f_2) = yz^2$  dividem  $LT(p) = y$ . Ocorrendo um passo de resto.

$$r := r + LT(p) = 0 + y = y,$$

$$p := p - LT(p) = y + z^2 - (y) = z^2.$$

- Para finalizar teremos um último passo de resto.

$$r := y + z^2 \quad \text{e} \quad p := z^2 - z^2 = 0.$$

Aqui o algoritmo pára retornando os valores

$$a_1 = y^2 z^2 + z^2, \quad a_2 = y, \quad r = y + z^2.$$

Deste modo

$$f = (y^2 z^2 + z^2)(xy - 1) + (y)(yz^2 - 1) + (y + z^2).$$

Invertendo a ordem da divisão, ou seja, dividindo  $f = xy^3 z^2 + xyz^2$  por  $f_2 = yz^2 - 1$  e  $f_1 = xy - 1$ , obtemos o seguinte resultado,

$$f = (xy^2 + x)(yz^2 - 1) + (y)(xy - 1) + (x + y),$$

o que mostra que os polinômios encontrados pelo algoritmo da divisão não são unicamente determinados.

## 2.3 Lema de Dickson e Teorema da Base de Hilbert

Nesta seção apresentaremos uma demonstração do Teorema da Base de Hilbert a partir de uma versão para ideais monomiais também conhecida como Lema de Dickson. Esta escolha se justifica pelas idéias contidas nas demonstrações que se baseiam unicamente na teoria desenvolvida neste capítulo.

**Definição 2.9** Um ideal  $I \subset K[\underline{x}]$  é um ideal monomial se existe um subconjunto  $A \subset \mathbb{M}$  (possivelmente infinito) tal que  $I$  consiste de todos os polinômios da forma  $\sum_{\underline{x}^\alpha \in A} h_\alpha \underline{x}^\alpha$ , onde

$h_\alpha \in K[\underline{x}]$  e, no caso de  $A$  ser infinito,  $h_\alpha = 0$  para quase todo  $\underline{x}^\alpha \in A$ . Escrevemos  $I = \langle \underline{x}^\alpha \mid \underline{x}^\alpha \in A \rangle$ .

**Lema 2.10** Seja  $I = \langle \underline{x}^\alpha \mid \underline{x}^\alpha \in A \rangle$  um ideal monomial de  $K[\underline{x}]$ . Então um monômio  $\underline{x}^\beta \in I$  se, e somente se,  $\underline{x}^\beta$  é divisível por algum  $\underline{x}^\alpha \in A$ .

**Demonstração:** Se  $\underline{x}^\beta$  é um múltiplo de  $\underline{x}^\alpha$ , para algum  $\underline{x}^\alpha \in A$ , então  $\underline{x}^\beta \in I$ .

Reciprocamente, se  $\underline{x}^\beta \in I$ , então  $\underline{x}^\beta = \sum_{i=1}^n h_i \underline{x}^{\alpha_i}$ , onde  $h_i \in K[\underline{x}]$  e  $\underline{x}^{\alpha_i} \in A$ . Se expandirmos cada  $h_i$  como combinação linear de monômios, vemos que todo termo no lado direito da igualdade é divisível por algum  $\underline{x}^{\alpha_i}$  e, deste modo, o lado esquerdo  $\underline{x}^\beta$  também possui essa propriedade.  $\square$

**Lema 2.11** Sejam  $I$  um ideal monomial e  $f \in K[\underline{x}]$ . Então são equivalentes:

(i)  $f \in I$ ;

(ii) Todo termo de  $f$  está em  $I$ ;

(iii)  $f$  é uma  $K$ -combinação linear de monômios em  $I$ .

**Demonstração:** As implicações  $(i) \Rightarrow (ii) \Rightarrow (iii)$  são claras.

Para mostrar a implicação  $(iii) \Rightarrow (i)$ , seja  $I = \langle \underline{x}^\alpha \mid \underline{x}^\alpha \in A \rangle$  e suponha que  $f$  é uma  $K$ -combinação linear de monômios em  $I$ . Assim,  $f = \sum_{i=1}^s c_i \underline{x}^{\beta_i}$ , onde  $c_i \in K$  e  $\underline{x}^{\beta_i} \in I$ . Cada  $\underline{x}^{\beta_i}$  é escrito na forma  $\underline{x}^{\beta_i} = \underline{x}^{\gamma_i} \underline{x}^{\alpha_i}$ , onde  $\underline{x}^{\alpha_i} \in A$ . Portanto,

$$f = \sum_{i=1}^s c_i \underline{x}^{\beta_i} = \sum_{i=1}^s (c_i \underline{x}^{\gamma_i}) \underline{x}^{\alpha_i} \in I. \quad \square$$

Como consequência imediata desse lema temos:

**Corolário 2.12** *Dois ideais monomiais são iguais se, e somente se, possuem os mesmos monômios.*  $\square$

Para seguirmos o proposto no início desta seção, apresentaremos a seguir o Lema de Dickson, que como já afirmamos é uma versão do Teorema da Base de Hilbert para ideais monomiais.

**Teorema 2.13 (Lema de Dickson)** *Um ideal monomial  $I = \langle \underline{x}^\alpha \mid \underline{x}^\alpha \in A \rangle \subset K[\underline{x}] = K[x_1, \dots, x_n]$  pode ser escrito na forma  $\langle \underline{x}^{\alpha_1}, \dots, \underline{x}^{\alpha_s} \rangle$ , onde  $\underline{x}^{\alpha_1}, \dots, \underline{x}^{\alpha_s} \in A$ . Em particular,  $I$  possui uma base finita.*

**Demonstração:** A demonstração será feita por indução sobre  $n$ , onde  $n$  é o número de variáveis. Se  $n = 1$ , então  $I \subset K[x_1]$  é gerado pelos monômios  $x_1^\alpha$ , onde  $x_1^\alpha \in A \subset \mathbb{M}$ . Seja  $x_1^\beta$  o menor elemento de  $A$ . Então  $x_1^\beta$  divide todos os outros geradores e, assim,  $I = \langle x_1^\beta \rangle$ .

Agora assumindo  $n > 1$  e que o teorema seja verdadeiro para  $n - 1$ , escrevemos as variáveis como  $x_1, \dots, x_{n-1}, y$  e, assim, os monômios de  $K[x_1, \dots, x_{n-1}, y]$  são escritos como  $\underline{x}^\alpha y^m$ , onde o elemento  $\underline{\alpha} = (\alpha_1, \dots, \alpha_{n-1})$  está em  $\mathbb{N}^{n-1}$  e  $m \in \mathbb{N}$ .

Supondo que  $I \subset K[x_1, \dots, x_{n-1}, y]$  seja um ideal monomial, para encontrarmos geradores de  $I$ , consideremos  $J$  o ideal em  $K[x_1, \dots, x_{n-1}]$  gerado pelos monômios  $\underline{x}^\alpha$ , onde  $\underline{x}^\alpha y^m \in I$  para algum  $m \geq 0$ . Como  $J$  é um ideal monomial em  $K[x_1, \dots, x_{n-1}]$  nossa hipótese indutiva nos garante que um número finito dos  $\underline{x}^\alpha$  geram  $J$ , digamos  $J = \langle \underline{x}^{\alpha(1)}, \dots, \underline{x}^{\alpha(s)} \rangle$ .

Para cada  $i$  entre 1 e  $s$ , a definição de  $J$  nos diz que  $\underline{x}^{\alpha(i)} y^{m_i} \in I$  para algum  $m_i \geq 0$ . Seja  $m$  o maior dos  $m_i$ . Então para cada  $k$  entre 0 e  $m - 1$ , consideremos o ideal  $J_k \subset K[x_1, \dots, x_{n-1}]$  gerado pelos monômios  $\underline{x}^\beta$  tais que  $\underline{x}^\beta y^k \in I$ . Novamente, usando nossa hipótese indutiva,  $J_k$  é gerado por um número finito de monômios, digamos  $J_k = \langle \underline{x}^{\alpha_k(1)}, \dots, \underline{x}^{\alpha_k(s_k)} \rangle$ .

Afirmamos que o ideal  $I$  é gerado pelos seguintes monômios:

$$\begin{aligned} & \underline{x}^{\alpha(1)}, \dots, \underline{x}^{\alpha(s)}, \quad (\text{de } J) \\ & \underline{x}^{\alpha_0(1)}, \dots, \underline{x}^{\alpha_0(s_0)}, \quad (\text{de } J_0) \\ & \underline{x}^{\alpha_1(1)}, \dots, \underline{x}^{\alpha_1(s_1)}, \quad (\text{de } J_1) \\ & \vdots \end{aligned}$$

$$\underline{x}^{\alpha_{m-1}(1)}, \dots, \underline{x}^{\alpha_{m-1}(s_{m-1})}. \quad (\text{de } J_{m-1})$$

Notemos que todo monômio em  $I$  é divisível por um dos monômios da lista pois para  $\underline{x}^\alpha y^p \in I$ , se  $p \geq m$ , então  $\underline{x}^\alpha y^p$  é divisível por algum  $\underline{x}^{\alpha(i)} y^m$ , pela construção de  $J$ . Por outro lado, se  $p \leq m-1$ , então  $\underline{x}^\alpha y^p$  é divisível por algum  $\underline{x}^{\alpha_p(j)} y^p$ , pela construção de  $J_p$ . Segue, assim, do Lema 2.10 que os monômios listados geram um ideal com os mesmos monômios de  $I$  e o Corolário 2.12 nos garante que estes dois ideais são os mesmos, provando nossa afirmação.

Para completar a demonstração, mostraremos que é sempre possível obter um conjunto finito de geradores a partir de um conjunto dado de geradores de  $I$ . Voltemos para a notação com as variáveis  $x_1, \dots, x_n$  e nosso ideal monomial  $I = \langle \underline{x}^\alpha \mid \underline{x}^\alpha \in A \rangle \subset K[x_1, \dots, x_n]$ . Precisamos mostrar que  $I$  é gerado por um número finito de  $\underline{x}^\alpha$ 's de  $A$ .

Já vimos, nesta demonstração, que  $I = \langle \underline{x}^{\beta_1}, \dots, \underline{x}^{\beta_s} \rangle$ , onde  $\underline{x}^{\beta_1}, \dots, \underline{x}^{\beta_s} \in I$ . Como  $\underline{x}^{\beta_i} \in I = \langle \underline{x}^\alpha \mid \underline{x}^\alpha \in A \rangle$ , o Lema 2.10, nos garante que cada  $\underline{x}^{\beta_i}$  é divisível por algum  $\underline{x}^{\alpha_i} \in A$  e, claramente,  $I = \langle \underline{x}^{\alpha_1}, \dots, \underline{x}^{\alpha_s} \rangle$ .  $\square$

Voltamos nossa atenção, a partir deste momento, para ideais quaisquer de  $K[\underline{x}]$ . Para  $I \subset K[\underline{x}]$  um ideal, o conjunto dos termos líderes de elementos de  $I$ , denotado por  $LT(I)$  é

$$LT(I) := \{LT(f) \mid f \in I - \{0\}\};$$

O ideal gerado pelos elementos de  $LT(I)$  será denotado por  $\langle LT(I) \rangle$ .

Notemos que se  $I = \langle f_1, \dots, f_s \rangle$ , não é verdade que  $\langle LT(I) \rangle = \langle LT(f_1), \dots, LT(f_s) \rangle$ , apesar da inclusão  $\langle LT(f_1), \dots, LT(f_s) \rangle \subset \langle LT(I) \rangle$  sempre valer, como pode ser visto no seguinte exemplo:

**Exemplo 2.14** Seja  $I = \langle f_1, f_2 \rangle$ , onde  $f_1 = x^3 - 2xy$ ,  $f_2 = x^2y - 2y^2 + x$ . Usando a ordem monomial grlex em  $K[x, y]$ , temos

$$x^2 = x(x^2 - 2y^2 + x) - y(x^3 - 2xy) \in I$$

e, assim,  $x^2 = LT(x^2) \in \langle LT(I) \rangle$ . Entretanto,  $x^2$  não é divisível por  $LT(f_1) = x^3$  e nem por  $LT(f_2) = x^2y$ , ou seja,

$$x^2 \notin \langle LT(f_1), LT(f_2) \rangle.$$

Veremos no que segue que  $\langle LT(I) \rangle$  é um ideal monomial.

**Proposição 2.15** Seja  $I \subset K[\underline{x}]$  um ideal.

(i)  $\langle LT(I) \rangle$  é um ideal monomial;

(ii) Existem  $g_1, \dots, g_s \in I$  tais que  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$ .

**Demonstração:** (i) Os monômios líderes  $LM(g)$  dos elementos  $g \in I - \{0\}$  geram o ideal monomial  $\langle LM(g) \mid g \in I - \{0\} \rangle$ . Como  $LM(g)$  e  $LT(g)$  diferem por uma constante não nula, temos  $\langle LM(g) \mid g \in I - \{0\} \rangle = \langle LT(I) \rangle$ . Assim  $\langle LT(I) \rangle$  é um ideal monomial.

(ii) Como  $\langle LT(I) \rangle$  é gerado pelos monômios  $LM(g)$  tais que  $g \in I - \{0\}$ , o Lema de Dickson (2.13) nos diz que  $\langle LT(I) \rangle = \langle LM(g_1), \dots, LM(g_t) \rangle$  para um número finito de elementos  $g_1, \dots, g_t \in I$ . Novamente, como  $LM(g_i)$  difere de  $LT(g_i)$  por uma constante não nula,  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ .  $\square$

Finalizaremos esta seção mostrando que todo ideal de  $K[\underline{x}]$  é gerado por um número finito de elementos.

**Teorema 2.16 (Teorema da base de Hilbert)** *Todo ideal  $I \subset K[\underline{x}]$  possui um conjunto finito de geradores.*

**Demonstração:** Se  $I = \{0\}$  tomamos nosso conjunto de geradores como sendo  $\{0\}$ . Se  $I$  contém um polinômio não nulo, então construímos um conjunto de geradores  $g_1, \dots, g_t \in I$  como segue: pela Proposição 2.15 existem  $g_1, \dots, g_t \in I$  com  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ . Afirmamos que  $I = \langle g_1, \dots, g_t \rangle$ .

Claro que  $\langle g_1, \dots, g_t \rangle \subset I$ , pois cada  $g_i \in I$ . Por outro lado, dado  $f \in I$ , aplicando o algoritmo da divisão para dividir  $f$  por  $g_1, \dots, g_t$  obtemos uma expressão da forma

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

onde todo termo de  $r$  não é divisível por nenhum dos  $LT(g_1), \dots, LT(g_t)$ . Neste ponto, falta apenas mostrar que  $r = 0$ . Para vermos que isto realmente ocorre notemos que

$$r = f - a_1 g_1 - \dots - a_t g_t \in I.$$

Se  $r \neq 0$ , então  $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$  e segue, do Lema 2.10 que  $LT(r)$  é divisível por algum  $LT(g_i)$ , o que contradiz  $r$  ser o resto e, assim,  $r = 0$ .  $\square$

## 2.4 Bases de Gröbner

Tendo um algoritmo de divisão em  $K[\underline{x}]$ , é natural nos perguntarmos quais propriedades do algoritmo da divisão para anéis de polinômios em uma variável são preservados. Por exemplo, na questão de quando um polinômio  $f \in K[\underline{x}]$  pertence a um ideal  $I = \langle f_1, \dots, f_s \rangle$ , uma direção é clara, quando  $r = \bar{f}^F = 0$  na divisão de  $f$  por  $F = (f_1, \dots, f_s)$ , teremos  $f \in I$ . Agora, vale a recíproca? Quando  $f \in I$ , teremos  $r = \bar{f}^F = 0$  na divisão de  $f$  por  $F = (f_1, \dots, f_s)$ ? Analisemos um exemplo:

**Exemplo 2.17** *Sejam  $f = xy^2 - x$ ,  $f_1 = xy + 1$ ,  $f_2 = y^2 - 1$  e  $I = \langle f_1, f_2 \rangle$ . Dividindo  $f$  por  $(f_1, f_2)$  obtemos*

$$f = y(xy + 1) + 0(y^2 - 1) + (-x - y),$$

*assim o resto da divisão de  $f$  por  $(f_1, f_2)$  é não nulo, mas*

$$f = 0(xy + 1) + x(y^2 - 1) \in I.$$

Qual foi o problema? Olhando  $f = y(xy + 1) + 0(y^2 - 1) + (-x - y)$  e como  $f \in I$  temos que  $\bar{f}^F$  é um elemento de  $I$ , mas é não nulo, pois contém termos que não podem ser removidos pela divisão por estes geradores particulares de  $I$ , os termos líderes de  $f_1 = xy + 1$  e  $f_2 = y^2 - 1$  não dividem o termo líder de  $\bar{f}^F$ .

Para a divisão produzir resto zero para todo elemento de  $I$ , precisamos ser capazes de remover todos os termos líderes de elementos de  $I$  usando os termos líderes dos divisores e como vimos, no exemplo, isso nem sempre acontece. Porém, há uma classe especial de elementos de  $I$  que resolve esse problema, as chamadas Bases de Gröbner:

**Definição 2.18** Fixemos uma ordem monomial em  $K[\underline{x}]$  e seja  $G = \{g_1, \dots, g_t\}$  um subconjunto finito de um ideal  $I \subset K[\underline{x}]$ . Se  $G$  possui a seguinte propriedade

$$\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle,$$

então  $G$  é chamado de uma base de Gröbner de  $I$ .

**Proposição 2.19** Fixe uma ordem monomial em  $K[\underline{x}]$ . Então todo ideal  $I \subset K[\underline{x}]$  possui uma base de Gröbner com relação a esta ordem. Além disso, uma base de Gröbner para  $I$  também é uma base de  $I$ .

**Demonstração:** A primeira parte desta proposição vimos no item (ii) da Proposição 2.15.

Para a segunda parte, observe que, se  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$ , então o argumento usado na demonstração do Teorema da Base de Hilbert (2.16) mostra que  $I = \langle g_1, \dots, g_t \rangle$ .  $\square$

**Teorema 2.20 (Macaulay)** Seja  $I \subset K[\underline{x}]$  um ideal não nulo qualquer e  $B = \{\text{monômios que não pertencem a } LT(I)\}$ . Então  $\overline{B} = \{a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}} + I \mid a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}} \in B\}$  é uma  $K$ -base do  $K$ -espaço vetorial  $K[\underline{x}]/I$ .

**Demonstração:** Mostraremos que  $\overline{B}$  gera  $K[\underline{x}]/I$  e é linearmente independente.

Observemos que  $\overline{B}$  gera  $K[\underline{x}]/I$  se, e somente se,  $K[\underline{x}] = \langle B \rangle + I$ . Suponhamos por absurdo que  $\langle B \rangle + I \subsetneq K[\underline{x}]$ . Deste modo,  $K[\underline{x}] - (\langle B \rangle + I) \neq \emptyset$  e, assim,  $\{LT(f) \mid f \in K[\underline{x}] - (\langle B \rangle + I)\} \neq \emptyset$ .

Com isto, existe  $f \in K[\underline{x}] - (\langle B \rangle + I)$  de tal modo que  $LT(f)$  é minimal em  $\{LT(f) \mid f \in K[\underline{x}] - (\langle B \rangle + I)\}$ . Como  $LT(f - LT(f)) < LT(f)$ , temos  $f - LT(f) \in \langle B \rangle + I$ . Aqui temos duas possibilidades para  $LT(f)$ :  $LT(f) \in \langle B \rangle$  ou  $LT(f) \notin \langle B \rangle$  (no segundo caso temos que  $LT(f) \in LT(I)$ ).

Se  $LT(f) \in \langle B \rangle$ , temos que  $f \in \langle B \rangle + I$ , o que é um absurdo. Considerando a outra possibilidade,  $LT(f) \in LT(I)$  e existe  $g \in I$  tal que  $LT(f) = LT(g)$ . Deste modo,  $LT(f - g) < LT(f)$  e, assim,  $f - g \in \langle B \rangle + I$ , concluindo que  $f \in \langle B \rangle + I$ , o que é, novamente, um absurdo.

Portanto,  $K[\underline{x}]/I = \langle \overline{B} \rangle$ .

Falta verificar que  $\overline{B}$  é linearmente independente. Para tanto, consideremos  $a_1, \dots, a_s \in K$  e  $u_1, \dots, u_s \in B$ . Suponha  $a_1 \overline{u_1} + \dots + a_s \overline{u_s} = \overline{0}$  ou, equivalentemente,  $a_1 u_1 + \dots + a_s u_s \in I$ . Se algum  $a_i \neq 0$  temos  $a_1 u_1 + \dots + a_s u_s \neq 0$  e, assim,  $LT(a_1 u_1 + \dots + a_s u_s) \in LT(I)$ . Seja  $LT(a_1 u_1 + \dots + a_s u_s) = a_j u_j$ , para algum  $j \in \{1, \dots, s\}$ . Como  $a_j \neq 0$  e  $a_1 u_1 + \dots + a_s u_s \in I$  temos  $\frac{1}{a_j}(a_1 u_1 + \dots + a_s u_s) \in I$  e  $LT\left(\frac{1}{a_j}(a_1 u_1 + \dots + a_s u_s)\right) = u_j \in LT(I)$ , que é um absurdo! Logo,  $a_i = 0$ ,  $i = 1, \dots, s$ .

Portanto  $\overline{B}$  é uma base para o  $K$ -espaço  $K[\underline{x}]/I$ .  $\square$

### 2.4.1 Unicidade do Resto

Fixando uma ordem monomial qualquer  $>$  em  $K[\underline{x}]$ , seja  $I \subset K[\underline{x}]$  um ideal. A divisão de  $f \in K[\underline{x}]$  por uma base de Gröbner de  $I$  produz uma expressão  $f = g + r$ , onde  $g \in I$  e nenhum termo de  $r$  é divisível por algum elemento de  $LT(I)$  e, além disso,  $r$  é único em relação a  $G$ . Formalizaremos este resultado na seguinte proposição:

**Proposição 2.21** *Seja  $G = \{g_1, \dots, g_t\}$  uma base de Gröbner para um ideal  $I \subset K[\underline{x}]$  e seja  $f \in K[\underline{x}]$ . Então existe um único  $r \in K[\underline{x}]$  com as duas seguintes propriedades:*

- (i) *Nenhum termo de  $r$  é divisível por algum elemento de  $LT(I)$ .*
- (ii) *Existe  $g \in I$  tal que  $f = g + r$ .*

*Em particular,  $r$  é o resto da divisão de  $f$  por  $G$ , não importando como os elementos de  $G$  sejam listados para efetuar o algoritmo da divisão.*

**Demonstração:** O algoritmo da divisão nos dá a existência de  $r$  nas condições exigidas.

Para provarmos a unicidade, suponhamos  $f = g + r = g' + r'$ ,  $r$  e  $r'$  satisfazendo (i) e (ii). Então  $r' - r = g - g' \in I$  e, se  $r' - r \neq 0$ , temos  $LT(r' - r) \in LT(I) = \langle LT(g_1), \dots, LT(g_t) \rangle$ . Absurdo, pois nenhum termo de  $r$  ou  $r'$  é divisível por algum  $LT(g_i)$ . Portanto  $r' - r = 0$  e a unicidade está provada.

A parte final da proposição segue da unicidade do resto.  $\square$

Em outras palavras, o resto da divisão de  $f$  por uma base de Gröbner para  $I$  é unicamente determinado e é chamado forma normal de  $f$  módulo  $I$ . Ele depende somente da escolha da ordem monomial e não de como a divisão é efetuada. Essa unicidade do resto nos dá outra caracterização das Bases de Gröbner.

Como corolário, da proposição anterior, obtemos o seguinte critério para determinar se um polinômio pertence ou não a um ideal.

**Corolário 2.22** *Seja  $G = \{g_1, \dots, g_t\}$  uma base de Gröbner para um ideal  $I \subset K[\underline{x}]$  e seja  $f \in K[\underline{x}]$ . Então  $f \in I$  se, e somente se,  $\bar{f}^G = 0$ .*

## 2.4.2 Critério de Buchberger

Em termos práticos, mais útil que a demonstração da existência de uma base de Gröbner é um algoritmo, devido a Buchberger, que toma um conjunto arbitrário de geradores  $\{f_1, \dots, f_s\}$  de  $I$  e produz uma base de Gröbner  $\{g_1, \dots, g_t\}$  para  $I$ .

**Definição 2.23** *Sejam  $f, g \in K[\underline{x}]$  não nulos. Fixada uma ordem monomial, sejam  $LT(f) = c\underline{x}^\alpha$  e  $LT(g) = d\underline{x}^\beta$ , onde  $c, d \in K$ . Seja  $\underline{x}^\gamma$  o menor múltiplo comum de  $\underline{x}^\alpha$  e  $\underline{x}^\beta$ . Então, o  $S$ -polinômio de  $f$  e  $g$  denotado por  $S(f, g)$  é o polinômio:*

$$S(f, g) = \frac{\underline{x}^\gamma}{LT(f)} f - \frac{\underline{x}^\gamma}{LT(g)} g.$$

*Note que, pela definição, obviamente  $S(f, g) \in \langle f, g \rangle$ .*

**Lema 2.24** *Consideremos uma soma da forma  $\sum_{i=1}^t c_i \underline{x}^{\alpha_i} g_i$ , com  $c_1, \dots, c_t$  constantes e  $\alpha_i +$*

*multigrau( $g_i$ ) =  $\underline{\delta} \in \mathbb{N}^n$ , sempre que  $c_i \neq 0$ . Se o multigrau de  $\sum_{i=1}^t c_i \underline{x}^{\alpha_i} g_i$  é estritamente menor*

que  $\underline{\delta}$ , então existem constantes  $c_{jk}$  tais que

$$\sum_{i=1}^t c_i \underline{x}^{\alpha_i} g_i = \sum_{j,k} c_{jk} \underline{x}^{\delta - \gamma_{jk}} S(g_j, g_k),$$

onde  $\underline{x}^{\gamma_{jk}} = \text{MMC}(LM(g_j), LM(g_k))$ .

Além disso, cada  $\underline{x}^{\delta - \gamma_{jk}} S(g_j, g_k)$  possui multigráu estritamente menor que  $\underline{\delta}$ .

**Demonstração:** Seja  $d_i = LC(g_i)$ , assim  $c_i d_i$  é o coeficiente líder de  $c_i \underline{x}^{\alpha_i} g_i$ . Como  $c_i \underline{x}^{\alpha_i} g_i$  possui multigráu  $\underline{\delta}$  e, sua soma possui multigráu estritamente menor, segue que  $\sum_{i=1}^t c_i d_i = 0$ .

Definamos  $p_i = \underline{x}^{\alpha_i} g_i / d_i$  e note que  $LC(p_i) = 1$ . Consideremos a soma:

$$\begin{aligned} \sum_{i=1}^t c_i \underline{x}^{\alpha_i} g_i &= \sum_{i=1}^t c_i d_i p_i = \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2) (p_2 - p_3) + \cdots \\ &\cdots + (c_1 d_1 + \cdots + c_{t-1} d_{t-1}) (p_{t-1} - p_t) + \\ &+ (c_1 d_1 + \cdots + c_t d_t) p_t. \end{aligned} \quad (2.2)$$

Agora, seja  $LT(g_i) = d_i \underline{x}^{\beta_i}$ . Por hipótese temos  $\alpha_i + \beta_i = \delta$ , para todo  $i$ ,  $1 \leq i \leq t$ . Então  $LM(g_i) = \underline{x}^{\beta_i}$  divide  $\underline{x}^{\delta}$  e, conseqüentemente  $\underline{x}^{\gamma_{jk}} = \text{MMC}(LM(g_j), LM(g_k))$  também divide  $\underline{x}^{\delta}$ . Assim  $\underline{x}^{\delta - \gamma_{jk}}$  é um monômio e

$$\begin{aligned} \underline{x}^{\delta - \gamma_{jk}} S(g_j, g_k) &= \underline{x}^{\delta - \gamma_{jk}} \left( \frac{\underline{x}^{\gamma_{jk}}}{LT(g_j)} g_j - \frac{\underline{x}^{\gamma_{jk}}}{LT(g_k)} g_k \right) = \\ &= \frac{\underline{x}^{\delta}}{d_j \underline{x}^{\beta_j}} g_j - \frac{\underline{x}^{\delta}}{d_k \underline{x}^{\beta_k}} g_k = \frac{\underline{x}^{\alpha_j}}{d_j} g_j - \frac{\underline{x}^{\alpha_k}}{d_k} g_k = p_j - p_k. \end{aligned} \quad (2.3)$$

Usando esta equação e o fato que  $\sum_{i=1}^t c_i d_i = 0$ , a soma 2.2 acima pode ser escrita como

$$\begin{aligned} \sum_{i=1}^t c_i \underline{x}^{\alpha_i} g_i &= c_1 d_1 \underline{x}^{\delta - \gamma_{12}} S(g_1, g_2) + (c_1 d_1 + c_2 d_2) \underline{x}^{\delta - \gamma_{23}} S(g_2, g_3) + \cdots \\ &\cdots + (c_1 d_1 + \cdots + c_{t-1} d_{t-1}) \underline{x}^{\delta - \gamma_{t-1,t}} S(g_{t-1}, g_t), \end{aligned}$$

que é uma soma na forma desejada. Como  $p_j$  e  $p_k$  possuem multigráu  $\underline{\delta}$  e coeficiente líder 1, a diferença  $p_j - p_k$  possui multigráu estritamente menor que  $\underline{\delta}$ . Pela Equação (2.3), o mesmo vale para  $\underline{x}^{\delta - \gamma_{jk}} S(g_j, g_k)$  e o lema está provado.  $\square$

Usando este lema, podemos provar o critério de Buchberger que, conforme afirmamos antes nos dá uma caracterização das bases de Gröbner de um ideal  $I$ , bem como permite obter um processo bastante simples para produzirmos uma base de Gröbner de um ideal dado.

**Teorema 2.25 (Critério de Buchberger)** *Seja  $I \subset K[\underline{x}]$  um ideal. Então uma base  $G = \{g_1, \dots, g_t\}$  de  $I$  é uma base de Gröbner para  $I$  se, e somente se, para todo par  $i \neq j$ ,  $\frac{S(g_i, g_j)}{S(g_i, g_j)}^G = 0$ .*

**Demonstração:** ( $\Rightarrow$ ) Sendo  $G$  uma base de Gröbner e  $S(g_i, g_j) \in I$ , temos  $\overline{S(g_i, g_j)}^G = 0$ .

( $\Leftarrow$ ) Seja  $f \in I$  um polinômio não nulo e mostremos que, se todos os  $S$ -polinômios possuem resto zero na divisão por  $G$ , então

$$LT(f) \in \langle LT(g_1), \dots, LT(g_t) \rangle.$$

Antes apresentaremos a idéia da demonstração. Dado  $f \in \langle g_1, \dots, g_t \rangle$ , existem polinômios  $h_i \in K[x]$  tais que

$$f = \sum_{i=1}^t h_i g_i. \quad (2.4)$$

Assim,

$$\text{multigrau}(f) \leq \text{multigrau}(h_i g_i). \quad (2.5)$$

Se a igualdade não ocorrer, então algum cancelamento ocorre entre os termos líderes de (2.4). O Lema 2.24 nos permite, assim, reescrever esta expressão em termos dos  $S$ -polinômios e, deste modo, nossa hipótese de que  $\overline{S(g_i, g_j)}^G = 0$ ,  $i \neq j$ , nos permite trocar os  $S$ -polinômios por expressões que envolvem menos cancelamentos de termos líderes. Continuando neste caminho, conseguiremos uma expressão de  $f$  na forma (2.4) onde a igualdade em (2.5) vale. Então  $\text{multigrau}(f) = \text{multigrau}(h_i g_i)$  para algum  $i$  e, segue que  $LT(f)$  é divisível por  $LT(g_i)$ . Isto mostra que  $LT(f) \in \langle LT(g_1), \dots, LT(g_t) \rangle$ , provando o teorema.

Vejamos os detalhes da demonstração.

Dada uma expressão (2.4) para  $f$ , seja  $m_i = \text{multigrau}(h_i g_i)$  e  $\underline{\delta} = \max\{m_1, \dots, m_t\}$ . A inequação (2.5) se torna, então

$$\text{multigrau}(f) \leq \underline{\delta}.$$

Agora, consideremos todas as maneiras possíveis de escrever  $f$  na forma (2.4). Para cada uma destas expressões conseguimos um possível  $\underline{\delta}$  distinto. Como uma ordem monomial é uma boa ordem, podemos escolher uma expressão (2.4) para  $f$  com  $\underline{\delta}$  minimal.

Mostraremos que com esta escolha minimal, temos  $\text{multigrau}(f) = \underline{\delta}$ . Com isto a igualdade em (2.5) ocorre e, como foi observado,

$$LT(f) \in \langle LT(g_1), \dots, LT(g_t) \rangle.$$

Vejamos então que  $\text{multigrau}(f) = \underline{\delta}$ . Se isto não ocorrer então  $\text{multigrau}(f) < \underline{\delta}$ . Podemos escrever  $f$  na forma:

$$\begin{aligned} f &= \sum_{m_i = \underline{\delta}} h_i g_i + \sum_{m_i < \underline{\delta}} h_i g_i = \\ &= \sum_{m_i = \underline{\delta}} LT(h_i) g_i + \sum_{m_i < \underline{\delta}} (h_i - LT(h_i)) g_i + \sum_{m_i < \underline{\delta}} h_i g_i. \end{aligned} \quad (2.6)$$

Os monômios que aparecem nos segundo e terceiro somatórios possuem todos  $\text{multigrau}$  estritamente menor que  $\underline{\delta}$ . Assim, como assumimos  $\text{multigrau}(f) < \underline{\delta}$ , temos o primeiro somatório também com  $\text{multigrau}$  estritamente menor que  $\underline{\delta}$ .

Seja  $LT(h_i) = c_i \underline{x}^{\underline{\alpha}_i}$ . Então, a soma

$$\sum_{m_i=\underline{\delta}} LT(h_i)g_i = \sum_{m_i=\underline{\delta}} c_i \underline{x}^{\underline{\alpha}_i} g_i,$$

possui exatamente a forma descrita no Lema 2.24, pois  $c_i \underline{x}^{\underline{\alpha}_i} g_i$  possui multigrau  $\underline{\delta}$  e sua soma multigrau estritamente menor que  $\underline{\delta}$ . Portanto o Lema 2.24 implica

$$\sum_{m_i=\underline{\delta}} LT(h_i)g_i = \sum_{j,k} c_{jk} \underline{x}^{\underline{\delta}-\gamma_{jk}} S(g_j, g_k), \quad (2.7)$$

onde  $c_{j,k} \in K$  e  $\underline{x}^{\gamma_{jk}} = \text{MMC}(LM(g_j), LM(g_k))$ .

Usando a hipótese de que o resto de  $S(g_j, g_k)$  na divisão por  $g_1, \dots, g_t$  é zero. Pelo Algoritmo da Divisão, isto significa que cada  $S$ -polinômio pode ser escrito na forma

$$S(g_j, g_k) = \sum_{i=1}^t a_{ijk} g_i,$$

onde  $a_{ijk} \in K[\underline{x}]$ . O algoritmo ainda nos diz que

$$\text{multigrau}(a_{ijk} g_i) \leq \text{multigrau}(S(g_j, g_k)), \quad (2.8)$$

para todo  $i, j, k$ .

Multiplicando a expressão de  $S(g_j, g_k)$  por  $\underline{x}^{\underline{\delta}-\gamma_{jk}}$  obtemos

$$\underline{x}^{\underline{\delta}-\gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^t b_{ijk} g_i,$$

onde  $b_{ijk} = \underline{x}^{\underline{\delta}-\gamma_{jk}} a_{ijk}$ .

Então (2.8) e o Lema 2.24 nos garantem que

$$\text{multigrau}(b_{ijk} g_i) \leq \text{multigrau}(\underline{x}^{\underline{\delta}-\gamma_{jk}} S(g_j, g_k)) \leq \underline{\delta}. \quad (2.9)$$

Substituindo a expressão para  $\underline{x}^{\underline{\delta}-\gamma_{jk}} S(g_j, g_k)$  na equação (2.7), obtemos

$$\begin{aligned} \sum_{m_i=\underline{\delta}} LT(h_i)g_i &= \sum_{j,k} c_{jk} \underline{x}^{\underline{\delta}-\gamma_{jk}} S(g_j, g_k) = \\ &= \sum_{j,k} c_{jk} \left( \sum_{i=1}^t b_{ijk} g_i \right) = \sum_{i=1}^t \left( \sum_{j,k} c_{jk} b_{ijk} \right) g_i. \end{aligned}$$

Escrevendo esta última soma como  $\sum_{i=1}^t h'_i g_i$ , segue de (2.9) que

$$\text{multigrau}(h'_i g_i) < \underline{\delta},$$

pois os  $c_{jk}$  são constantes.

Para finalizar substituindo  $\sum_{m_i=\underline{\delta}} LT(h_i)g_i = \sum_{i=1}^t h'_i g_i$  na equação (2.6) e obtemos

$$f = \sum_{i=1}^t h'_i g_i + \sum_{m_i=\underline{\delta}} (h_i - LT(h_i))g_i + \sum_{m_i < \underline{\delta}} h_i g_i.$$

Assim, expressamos  $f$  como uma combinação polinomial dos  $g_i$ 's onde todos os termos possuem multigrado estritamente menor que  $\underline{\delta}$ . Isto contradiz a minimalidade de  $\underline{\delta}$  e completa a demonstração.  $\square$

Usando este critério, obtemos um processo muito simples para produzir uma base de Gröbner de um ideal dado, o qual descrevemos a seguir:

**Entrada:**  $F = (f_1, \dots, f_s)$

**Saída:** Uma base de Gröbner  $G = \{g_1, \dots, g_t\}$  para  $I = \langle F \rangle$ , com  $F \subset G$

$G := F$

REPITA

$G' := G$

PARA cada par  $p \neq q$  em  $G'$  FAÇA

$S := \overline{S(p, q)}^{G'}$

SE  $S \neq 0$  ENTÃO  $G := G \cup \{S\}$

ATÉ  $G = G'$

**Exemplo 2.26** Considere  $K[x, y]$  com a ordem *grlex* e  $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$ .

Note que  $\{f_1, f_2\}$  não é uma base de Gröbner de  $I$  pois,

$$S(f_1, f_2) = y(x^3 - 2xy) - x(x^2y - 2y^2 + x) = -x^2 \in I,$$

e  $LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle$ .

Usaremos o algoritmo para produzir uma base de Gröbner de  $I$ .

- No primeiro passo temos  $G' := \{f_1, f_2\}$  e  $\overline{S(f_1, f_2)}^{G'} = -x^2 \neq 0$ . Assim  $f_3 = -x^2$  é adicionado a  $G$  e o algoritmo continua.

- No segundo passo, determinaremos  $\overline{S(f_1, f_2)}^{G'}$ ,  $\overline{S(f_1, f_3)}^{G'}$ ,  $\overline{S(f_2, f_3)}^{G'}$  e, neste passo,  $G' = \{f_1, f_2, f_3\}$ .

$$S(f_1, f_2) = f_3 \text{ e, assim, } \overline{S(f_1, f_2)}^{G'} = 0.$$

$$S(f_1, f_3) = 1(x^3 - 2xy) - (-x)(-x^2) = -2xy \text{ e } \overline{S(f_1, f_3)}^{G'} = -2xy \neq 0. \text{ Logo } f_4 = -2xy \text{ é adicionado a } G.$$

$$S(f_2, f_3) = 1(x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x \text{ e } \overline{S(f_2, f_3)}^{G'} = -2y^2 + x \neq 0. \text{ Adicionando } f_5 = -2y^2 + x \text{ em } G.$$

Novamente  $G$  foi alterado e continuamos o processo.

- Neste passo, fazemos  $G' = \{f_1, f_2, f_3, f_4, f_5\}$ . Sabemos que

$$\overline{S(f_1, f_2)}^{G'} = \overline{S(f_1, f_3)}^{G'} = \overline{S(f_2, f_3)}^{G'} = 0.$$

Falta verificar quanto valem  $\overline{S(f_1, f_4)}^{G'}$ ,  $\overline{S(f_1, f_5)}^{G'}$ ,  $\overline{S(f_2, f_4)}^{G'}$ ,  $\overline{S(f_2, f_5)}^{G'}$ ,  $\overline{S(f_3, f_4)}^{G'}$ ,  $\overline{S(f_3, f_5)}^{G'}$ ,  $\overline{S(f_4, f_5)}^{G'}$ . Mais alguns cálculos (podemos usar um programa de computação algébrica, como veremos no Apêndice A) concluímos que eles são todos nulos e, deste modo,

$$f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x, f_3 = -x^2, f_4 = -2xy, f_5 = -2y^2 + x$$

formam uma base de Gröbner para  $I$ .

### 2.4.3 Base de Gröbner Reduzida

**Lema 2.27** *Seja  $G$  uma base de Gröbner para o ideal  $I \subset K[x]$ . Se  $p \in G$  é um polinômio tal que  $LT(p) \in \langle LT(G - \{p\}) \rangle$  então  $G - \{p\}$  é também uma base de Gröbner para  $I$ .*

**Demonstração:** Sabemos que  $\langle LT(G) \rangle = \langle LT(I) \rangle$ . Se  $LT(p) \in \langle LT(G - \{p\}) \rangle$ , então  $\langle LT(G - \{p\}) \rangle = \langle LT(G) \rangle$ . Pela definição, segue que  $G - \{p\}$  é uma base de Gröbner para  $I$ .  $\square$

Ajustando as constantes para que todo coeficiente líder seja 1 e removendo qualquer  $p$  tal que  $LT(p) \in LT(G) - \{p\}$  de  $G$ , chegamos ao que chamamos de base de Gröbner minimal.

**Definição 2.28** *Uma base de Gröbner minimal para um ideal  $I \subset K[x]$  é uma base de Gröbner  $G$  que satisfaz:*

- (i)  $LC(p) = 1$  para todo  $p \in G$ ;
- (ii) Para todo  $p \in G$ ,  $LT(p) \notin \langle LT(G) - \{p\} \rangle$ .

Aplicando o algoritmo de Buchberger e depois usando o Lema 2.27 para eliminar qualquer gerador desnecessário que possa ter sido incluído, podemos construir uma base de Gröbner minimal para um dado ideal não nulo. Para ilustrar o processo, voltemos ao ideal  $I$  estudado no Exemplo 2.26:

**Exemplo 2.29** *Lembrando que  $I = \langle f_1, f_2 \rangle$ , com  $f_1 = x^3 - 2xy$  e  $f_2 = x^2y - 2y^2 + x$ . Usando a ordem grlex encontramos uma base de Gröbner*

$$G = \{f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x, f_3 = -x^2, f_4 = -2xy, f_5 = -2y^2 + x\},$$

para  $I$ .

Como alguns coeficientes líderes são diferentes de 1, os polinômios serão multiplicados por constantes adequadas para que isto ocorra, obtendo uma nova base de Gröbner para  $I$ :

$$\tilde{G} = \{\tilde{f}_1 = x^3 - 2xy, \tilde{f}_2 = x^2y - 2y^2 + x, \tilde{f}_3 = -x^2, \tilde{f}_4 = -2xy, \tilde{f}_5 = -2y^2 + x\}.$$

Observando que  $LT(\tilde{f}_1) = x^3 = xLT(\tilde{f}_3)$  e que  $LT(\tilde{f}_2) = x^2y = xLT(\tilde{f}_4)$ , podemos dispensar  $\tilde{f}_1$  e  $\tilde{f}_2$  de  $\tilde{G}$ . Como não há outro caso onde o termo líder de um gerador divide o termo líder de outro, temos que

$$\tilde{f}_3 = x^2, \tilde{f}_4 = xy, \tilde{f}_5 = y^2 - \frac{1}{2}x$$

formam uma base de Gröbner minimal de  $I$ .

Infelizmente, um ideal dado pode ter muitas bases de Gröbner minimais. Por exemplo, no ideal  $I$  considerado acima os elementos

$$\hat{f}_3 = x^2 + axy, \hat{f}_4 = xy, \hat{f}_5 = y^2 - \frac{1}{2}x$$

também formam uma base de Gröbner minimal, onde  $a \in K$  é uma constante. Portanto, podemos produzir infinitas bases de Gröbner minimais (assumindo que  $K$  é infinito). Mas, felizmente, podemos escolher uma base de Gröbner minimal que é melhor que as outras, como veremos a seguir:

**Definição 2.30** Uma base de Gröbner reduzida para um ideal  $I \subset K[\underline{x}]$  é uma base de Gröbner minimal de  $I$  tal que para todo  $p \in G$ , nenhum monômio de  $p$  pertence a  $\langle LT(G - \{p\}) \rangle$ .

**Exemplo 2.31** Para o nosso ideal  $I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$  considerado anteriormente, temos que

$$\tilde{f}_3 = x^2, \tilde{f}_4 = xy, \tilde{f}_5 = y^2 - \frac{1}{2}x$$

forma a base de Gröbner reduzida de  $I$ .

As bases de Gröbner reduzidas possuem a seguinte propriedade:

**Proposição 2.32** Fixada uma ordem monomial  $>$  sobre  $K[\underline{x}]$ , cada ideal em  $K[\underline{x}]$  possui uma única base de Gröbner reduzida com respeito a  $>$ .

**Demonstração:** Seja  $G$  uma base de Gröbner minimal para  $I$ . Dizemos que  $g \in G$  é reduzido módulo  $G$  se nenhum monômio de  $G$  está em  $\langle LT(G - \{g\}) \rangle$ . Nosso objetivo é modificar  $G$  até que todos seus elementos sejam reduzidos.

Uma primeira observação é que se  $g$  é reduzido módulo  $G$ , então  $g$  é também reduzido módulo qualquer outra base de Gröbner minimal de  $I$  que contém  $g$  e possui o mesmo conjunto de termos líderes, pois a definição de elemento reduzido envolve apenas estes termos.

Agora, dado  $g \in G$  seja  $g' = \bar{g}^{G-\{g\}}$  e definindo  $G' = (G - \{g\}) \cup \{g'\}$ . Afirmamos que  $G'$  é uma base de Gröbner minimal para  $I$ . Notemos que  $LT(g') = LT(g)$ , pois quando dividimos  $g$  por  $G - \{g\}$ ,  $LT(g)$  vai para o resto por não ser divisível por qualquer elemento de  $LT(G - \{g\})$ .

Assim  $\langle LT(G') \rangle = \langle LT(G) \rangle$ . Como, claramente,  $G' \subset I$ , temos  $G'$  uma base de Gröbner para  $I$  que também é minimal. Finalmente,  $g'$  é reduzido módulo  $G'$  por construção.

Repetimos o processo acima até todos os elementos de  $G$  sejam reduzidos.

Observamos que a base de Gröbner pode mudar toda vez que aplicarmos o processo, mas pelo que vimos anteriormente, uma vez que o elemento é reduzido, ele permanece reduzido, pois nunca trocamos os termos líderes. Assim, terminamos o processo com uma base de Gröbner reduzida.

Para finalizar a demonstração falta verificarmos a unicidade. Suponhamos  $G$  e  $\tilde{G}$  bases de Gröbner reduzidas para  $I$ . Então, em particular,  $G$  e  $\tilde{G}$  são bases de Gröbner minimais e, assim,  $LT(G) = LT(\tilde{G})$ . Para verificarmos essa igualdade, observemos que  $\langle LT(G) \rangle = \langle LT(I) \rangle = \langle LT(\tilde{G}) \rangle$ . Deste modo, dado  $g \in G$ ,  $LT(g) \in \langle LT(\tilde{G}) \rangle$  e, com isto, existe  $\tilde{g} \in \tilde{G}$  tal que  $LT(\tilde{g})$  divide  $LT(g)$ . Por outro lado,  $LT(\tilde{g}) \in \langle LT(G) \rangle$  e, com isto, existe  $g' \in G$  tal que  $LT(g')$  divide  $LT(\tilde{g})$ . Se  $g \neq g'$ , temos  $LT(g) \in \langle LT(G - \{g\}) \rangle$  pois  $LT(g')$  divide  $LT(g)$ , o que é um absurdo. Portanto  $g = g'$  e  $LT(g) = LT(\tilde{g})$ . Analogamente podemos demonstrar que para todo  $\tilde{g} \in \tilde{G}$ , temos  $LT(\tilde{g}) \in LT(G)$  e, portanto,  $LT(G) = LT(\tilde{G})$ .

Com isto, dado  $g \in G$ , existe  $\tilde{g} \in \tilde{G}$  tal que  $LT(g) = LT(\tilde{g})$ . Se pudermos mostrar que  $g = \tilde{g}$ , mostramos que  $G = \tilde{G}$  e a unicidade está provada.

Para ver que  $g = \tilde{g}$ , consideremos  $g - \tilde{g}$ . Este é um elemento de  $I$  e, como  $G$  é uma base de Gröbner,  $\overline{g - \tilde{g}}^G = 0$ . Sabemos que  $LT(g) = LT(\tilde{g})$ , assim estes termos são cancelados em  $g - \tilde{g}$  e os termos restantes não são divisíveis pelos elementos de  $LT(G) = LT(\tilde{G})$ , pois  $G$  e  $\tilde{G}$  são bases reduzidas. Isto mostra que  $\overline{g - \tilde{g}}^G = g - \tilde{g}$  e, então,  $g - \tilde{g} = 0$ , o que completa a demonstração.  $\square$

## 2.5 Função de Hilbert de $S/I$ , com $I$ Ideal Monomial

Nesta seção denotaremos  $K[\underline{x}]$  por  $S$  e apresentaremos um processo para calcular a função de Hilbert de  $S/I$  com  $I$  ideal monomial e a função  $\lambda$  a dimensão. Antes porém, e até mesmo para ressaltar a importância deste procedimento apresentaremos um resultado que é decorrência natural do Teorema de Macaulay 2.20.

**Teorema 2.33** *Seja  $I$  um ideal homogêneo. Então a função de Hilbert de  $S/I$  é a mesma de  $S/\langle LT(I) \rangle$ .*

**Demonstração:** Sejam  $B = \{\text{monômios que não estão em } LT(I)\}$ ,  $S_d$  o conjunto de elementos de grau  $d$  de  $S = K[\underline{x}]$  e  $\bar{S}_d$  a imagem de  $S_d$  em  $S/I$ . Temos que  $H(S/I, d) = \dim_K \bar{S}_d = \#(S_d \cap B)$ . Pelo Teorema de Macaulay 2.20 e pelo fato de  $I$  ser homogêneo,  $H(S/\langle LT(I) \rangle, d) = \#\{m \in S_d \mid m \text{ monômio e } m \notin LT(I)\} = \#(S_d \cap B)$ .

Logo,  $H(S/I, d) = H(S/\langle LT(I) \rangle, d)$ .  $\square$

**Definição 2.34** *Seja  $I \subset S$  um ideal monomial, isto é,  $I = \langle m_1, \dots, m_r \rangle$ , 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  $m_i$  não divide  $m_j$ , para todo  $i, j \in \{1, \dots, r\}$ ,  $i \neq j$ .*

### 2.5.1 Processo para Calcular a Função de Hilbert de $S/I$ , com $I$ ideal monomial

Sejam  $I = \langle m_1, \dots, m_r \rangle$  ideal monomial de  $S$  e  $S_d$  o conjunto dos elementos de grau  $d$  de  $S$ .

Procedemos por indução sobre  $r$ .

Se  $r = 1$  então  $I = \langle m \rangle$ . Supondo grau de  $m = d$  temos, como vimos no Capítulo 1,

$$H\left(\frac{S}{\langle m \rangle}, i\right) = \dim_K \left(\frac{S}{\langle m \rangle}\right)_i.$$

Para  $i = 0, \dots, d-1$ ,  $(S/\langle m \rangle)_i \simeq S_i$  e, assim,  $\dim_K(S_i) = \binom{n+i-1}{n-1}$ ,  $i = 0, \dots, d-1$ . Também,  $\dim_K(S/\langle m \rangle)_d = \dim_K S_d - 1$  pois grau de  $m$  é  $d$ .

Seja  $i > d$ , então existe  $u \in \mathbb{N}$  tal que  $i = d + u$ . Como queremos calcular a dimensão de  $(S/\langle m \rangle)_i$ , nos interessa saber o número de monômios de grau  $i$  de  $S$  que não são múltiplos de  $m$ . Logo  $\dim_K(S/\langle m \rangle)_i = \dim_K S_i - \dim_K S_u$ , pois se  $v \in S_u$ , então  $vm \in S_i$  e, portanto, temos que eliminar todos os monômios da forma  $vm$ , com  $v \in S_u$ . Assim,  $\dim(S/\langle m \rangle)_i = \binom{n+i-1}{n-1} - \binom{i-d+n-1}{n-1}$ ,  $i \geq d$ , de onde segue que

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

e, portanto, sabemos calcular a Função de Hilbert de  $S/\langle m \rangle$ .

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

Seja  $I = \langle m_1, \dots, m_r \rangle$ , onde  $\{m_1, \dots, m_r\}$  é um conjunto minimal de geradores e seja  $m$  um desses geradores, que, sem perda de generalidade podemos supor seja  $m_r$ . Logo  $I = \langle m, I' \rangle$ , onde  $I' = \langle m_1, \dots, m_{r-1} \rangle$ . Supondo grau de  $m$  igual a  $d$  temos uma seqüência exata

$$0 \rightarrow \text{Ker } \varphi \rightarrow S(-d) \xrightarrow{\varphi} \frac{S}{I'} \xrightarrow{\pi} \frac{S}{I} \rightarrow 0, \quad (2.10)$$

onde  $\varphi(r) = \overline{sm}$ ,  $S(-d) = \bigoplus S'_i$  e  $S'_i = S_{i-d}$ .

Tal seqüência exata é de grau zero, isto é, se  $x \in S_i$ , então  $\varphi(x) \in (S/I')$ , pois se  $x \in S'_i$  tem-se  $x \in S_{i-d}$  ou ainda  $mx \in S_i$  e, portanto,  $\overline{mx} \in (S/I')_i$ .

Temos que

$$\begin{aligned} \text{Ker } \varphi &= \{u \in S(-d) \mid \varphi(u) = \overline{0}\} \\ &= \{u \in S(-d) \mid \overline{um} = \overline{0}\} \\ &= \{u \in S(-d) \mid um \in I'\}. \end{aligned}$$

Como  $S(-d) \subset S$  e levando em consideração a alteração nos graus,

$$\text{Ker } \varphi = \{u \in S \mid um \in I'\} = (I' : m).$$

Mas,  $I'$  é ideal de  $S$  e  $I' = \langle m_1, \dots, m_{r-1} \rangle$ , então

$$J = (I' : m) = \left( \frac{m_1}{\text{mdc}(m_1, m)}, \dots, \frac{m_{r-1}}{\text{mdc}(m_{r-1}, m)} \right).$$

Logo a seqüência exata (2.10) induz a seguinte seqüência exata, também de grau zero, da forma

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

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

$$0 \rightarrow \left(\frac{S}{J}\right)_{i-d} \rightarrow \left(\frac{S}{I'}\right)_i \rightarrow \left(\frac{S}{I}\right)_i \rightarrow 0. \quad (2.11)$$

Porém  $J$  e  $I'$  possuem menos geradores do que  $I$  e, por hipótese de indução, sabemos calcular suas funções de Hilbert. Logo de (2.11) temos que

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

Com isto obtemos um processo recursivo para calcular a função de Hilbert de  $S/I$ .

**Exemplo 2.35** Para ilustrar o processo, calcularemos a Função de Hilbert de

$$R = \frac{K[x, y, z]}{\langle xy, xz, yz \rangle}.$$

Tomando  $m = yz$  e  $I' = \langle xy, xz \rangle$  temos

$$J = (I' : m) = \left\langle \frac{xy}{\text{MDC}(xy, yz)}, \frac{xz}{\text{MDC}(xz, yz)} \right\rangle = \left\langle \frac{xy}{y}, \frac{xz}{z} \right\rangle = \langle x \rangle.$$

Assim,  $S/J \simeq K[y, z]$ . Pelo que vimos,

$$H(R, i) = H\left(\frac{S}{I'}, i\right) - H\left(\frac{S}{J}, i-2\right).$$

Para calcular  $H(S/I', i)$  repetimos o processo para  $J' = (I'' : m_1)$ , onde  $m_1 = xz$  e  $I'' = \langle xy \rangle$ . Agora

$$J' = (I'' : m_1) = \left\langle \frac{xy}{\text{MDC}(xy, xz)} \right\rangle = \langle y \rangle \text{ e, portanto,}$$

$$H\left(\frac{S}{I'}, i\right) = H\left(\frac{S}{\langle xy \rangle}, i\right) - H(K(x, z), i-2),$$

de onde segue que

$$H\left(\frac{S}{I}, i\right) = H\left(\frac{S}{I'}, i\right) - H\left(\frac{S}{J}, i-2\right) = H\left(\frac{S}{\langle xy \rangle}, i\right) - H\left(\frac{S}{J'}, i-2\right) - H\left(\frac{S}{J}, i-2\right),$$

onde  $J = \langle x \rangle$  e  $J' = \langle y \rangle$ . Deste modo

$$H\left(\frac{S}{J}, i\right) = H\left(\frac{S}{J'}, i\right) = \begin{cases} 1, & i = 0 \\ \binom{2+i}{2} - \binom{1+i}{2}, & i \geq 1. \end{cases}$$

Assim,

$$H\left(\frac{S}{J}, i-2\right) = \begin{cases} 0, & 0 \leq i < 2 \\ 1, & i = 2 \\ \binom{i}{2} - \binom{i-1}{2}, & i \geq 3. \end{cases}$$

Mas

$$\begin{aligned} \binom{i}{2} - \binom{i-1}{2} &= \frac{i!}{(i-2)!2} - \frac{(i-1)!}{(i-3)!2} = \frac{i! - (i-1)!(i-2)}{(i-2)!2} = \\ &= \frac{i(i-1) - (i-2)(i-1)}{2} = i-1, \end{aligned}$$

ou seja,

$$H\left(\frac{S}{J}, i-2\right) = \begin{cases} 0, & i = 0 \\ i-1, & i \geq 1. \end{cases}$$

Temos também que

$$H\left(\frac{S}{\langle xy \rangle}, i\right) = \begin{cases} \binom{i+2}{2}, & 0 \leq i < 2 \\ \binom{2+i}{2} - \binom{i}{2}, & i \geq 2. \end{cases}$$

De forma similar ao que fizemos para  $H(S/J)$  obtemos que  $H(S/\langle xy \rangle, i) = 2i + 1$ , para  $i \geq 0$ .

Portanto, no caso  $i = 0$ , temos  $H(R, i) = 2 \cdot 0 + 1 - 0 - 0 = 1$  e, se  $i \geq 1$ , temos  $H(R, i) = 2i + 1 - (i-1) - (i-1)$ , ou seja,

$$H(R, i) = \begin{cases} 1, & i = 0 \\ 3, & i \geq 1. \end{cases}$$

## 2.6 Anéis de Stanley-Reisner

Os anéis de Stanley-Reisner são objeto central de estudo da chamada Álgebra Comutativa Combinatória criada por Hochster e Stanley em meados dos anos 70. Estes anéis estão associados aos chamados complexos simpliciais e são exemplos importantes de aplicações em geometria algébrica e álgebra comutativa, onde podemos calcular a função de Hilbert a partir do complexo simplicial associado ao anel.

Nesta seção veremos como o número de faces de um complexo simplicial está relacionado com a série de Hilbert do correspondente anel de Stanley-Reisner.

**Definição 2.36** *Seja  $V = \{v_1, \dots, v_n\}$  um conjunto finito. Um complexo simplicial (finito)  $\Delta$  sobre  $V$  é uma coleção de subconjuntos de  $V$  tal que*

(i)  $F \in \Delta$  sempre que  $F \subset G$  para algum  $G \in \Delta$ ;

(ii)  $\{v_i\} \in \Delta$ , para  $i = 1, \dots, n$ .

Os elementos de  $\Delta$  são chamados de faces.

**Definição 2.37** Sejam  $\Delta$  um complexo simplicial sobre  $V = \{v_1, \dots, v_n\}$  e  $F \in \Delta$ . Chamamos de dimensão de  $F$  e denotamos por  $\dim F$  o número de elementos de  $F$  menos um, ou seja,  $\dim F = \#F - 1$ . A dimensão do complexo simplicial,  $\dim \Delta$ , é igual ao máximo das dimensões de suas faces, isto é,  $\dim \Delta = \max\{\dim F \mid F \in \Delta\}$ .

**Exemplo 2.38** Seja  $V = \{x_1, x_2, x_3, x_4\}$ , considere

$$\Delta = \{\emptyset, \{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_1, x_2\}, \{x_2, x_3\}, \{x_3, x_4\}\}.$$

Podemos representar  $\Delta$  graficamente da seguinte forma:

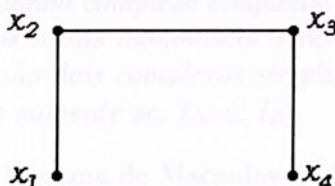


Figura 2.1: Complexo Simplicial

### Observações 2.39

- (i) O conjunto  $\emptyset$  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 de arestas. As faces maximais em relação a inclusão são ditas facetas do complexo simplicial.

A codificação algébrica de um complexo simplicial pode ser feita da forma descrita a seguir:

Primeiramente, estabelecemos uma bijeção ordenada entre o conjunto dos vértices do complexo simplicial  $\Delta$  e um conjunto de indeterminadas  $\underline{x}$ :  $x_1, \dots, x_n$  sobre um corpo (fixo)  $K$ .

Em seguida, queremos introduzir um ideal do anel  $K[\underline{x}]$  que reflita propriedades do complexo simplicial  $\Delta$ . Após vencer o primeiro impulso de fazer corresponder monômios às faces de  $\Delta$ , temos a seguinte definição:

**Definição 2.40** Sejam  $\Delta$  um complexo simplicial sobre  $V = \{v_1, \dots, v_n\}$  e  $K$  um anel. O anel de Stanley-Reisner do complexo simplicial  $\Delta$  com respeito a  $K$  é a  $K$ -álgebra homogênea definida por:

$$K[\Delta] := K[\underline{x}] / I_\Delta,$$

onde  $I_\Delta$  é gerado por todos os monômios  $x_{i_1}^{\alpha_{i_1}} \cdots x_{i_s}^{\alpha_{i_s}}$ , com  $\alpha_{i_j} > 0$ , tais que  $\{v_{i_1}, \dots, v_{i_s}\} \notin \Delta$ .

### Observações 2.41

- (i) A escolha da letra  $K$  na definição indica que, salvo exceções, sempre teremos um corpo para o anel dos coeficientes.

(ii) Lembremos que o suporte de um monômio  $\underline{x}^\alpha$  é o conjunto

$$\text{supp } \underline{x}^\alpha = \{x_{i_1}, \dots, x_{i_s} \mid \alpha_{i_j} \neq 0, j = 1, \dots, s\}.$$

Segundo a Definição 2.40  $I_\Delta$  é gerado por todos os monômios  $x_{i_1}^{\alpha_{i_1}} \cdots x_{i_s}^{\alpha_{i_s}}$ , com  $\alpha_{i_j} > 0$ , tais que  $\{v_{i_1}, \dots, v_{i_s}\} \notin \Delta$ , assim, para facilitar a leitura, indicaremos, no que segue, o fato que  $\{v_{i_1}, \dots, v_{i_s}\} \in \Delta$  também por  $\text{supp } \underline{x}^\alpha \in \Delta$  e

$$\mathcal{F}(\Delta) := \{\underline{x}^\alpha \mid \text{supp}(\underline{x}^\alpha) \in \Delta\}$$

(iii) Note que o ideal das faces  $I_\Delta$  é gerado, minimamente, por monômios livres de quadrados. Por outro lado, se  $I \subset (x_1, \dots, x_n)^2$  é ideal gerado por monômios livres de quadrados, então  $K[\underline{x}]/I \simeq K[\Delta]$  para algum complexo simplicial  $\Delta$ , o que nos dá uma bijeção entre os complexos simpliciais e os ideais monomiais livres de quadrados. Tal bijeção inverte inclusão, isto é, se  $\Delta$  e  $\Delta'$  são dois complexos simpliciais sobre um mesmo conjunto de vértices, então  $\Delta \subset \Delta'$  se, e somente se,  $I_{\Delta'} \subset I_\Delta$ .

Um resultado que decorre do Teorema de Macaulay 2.20 é:

**Proposição 2.42** *Seja  $\Delta$  um complexo simplicial. Os resíduos em  $K[\Delta]$  dos elementos de  $\mathcal{F}(\Delta)$  constituem uma  $K$ -base vetorial de  $K[\Delta]$ .*

**Corolário 2.43** *Se  $\Delta$  é um complexo simplicial e  $F \in \Delta$ , então os resíduos dos vértices de  $F$  são algebricamente independentes sobre  $K$ .*

**Corolário 2.44** *Se  $\Delta$  é um complexo simplicial, vale  $\dim K[\Delta] = \dim \Delta + 1$ .*

**Exemplo 2.45** *Para o complexo simplicial do exemplo anterior, temos  $I_\Delta = \langle x_1x_3, x_1x_4, x_2x_4 \rangle$  (minimamente gerado) e  $K[\Delta]$  é gerado pelas  $K$ -combinações lineares dos resíduos de*

$$1, x_1, x_1^2, \dots, x_2, x_2^2, \dots, x_3, x_3^2, \dots, x_4, x_4^2, \dots, \\ x_1x_2, x_1^2x_2, x_1x_2^2, \dots, x_2x_3, x_2^2x_3, x_2x_3^2, \dots, x_3x_4, x_3^2x_4, x_3x_4^2, \dots$$

Neste caso, temos que  $\dim K[\Delta] = \dim \Delta + 1 = 1 + 1 = 2$ .

### 2.6.1 Função e Série de Hilbert de um Anel de Stanley-Reisner

**Definição 2.46** *Dado um complexo simplicial  $\Delta$  de dimensão  $d - 1$ , chamamos de  $f$ -vetor (do complexo simplicial  $\Delta$ ) o vetor  $(f_0, f_1, \dots, f_{d-1})$ , onde  $f_i := \#\{F \in \Delta \mid \dim F = i\}$ ,  $-1 \leq i \leq d - 1$ .*

**Observação 2.47** *Note que dado o  $f$ -vetor do complexo simplicial  $\Delta$ ,  $(f_0, f_1, \dots, f_{d-1})$ , sempre temos  $f_{-1} = 1$  e  $f_0$  é número de vértices de  $\Delta$ .*

**Exemplo 2.48** *Para o complexo simplicial*

$$\Delta = \{\emptyset, \{x_1\}, \{x_2\}, \{x_3\}, \{x_4\}, \{x_1, x_2\}, \{x_2, x_3\}, \{x_3, x_4\}\}$$

sobre  $V = \{x_1, x_2, x_3, x_4\}$ , considerado no Exemplo 2.38, temos o seguinte  $f$ -vetor:  $(4, 3)$ .

Para  $\Delta$  um complexo simplicial, a função de Hilbert de  $K[\Delta]$  associada à dimensão é  $H(K[\Delta], -) : \mathbb{N} \rightarrow \mathbb{N}$ , onde  $m \mapsto \dim K[\Delta]_m$  e  $K[\Delta]_m$  denota o subespaço vetorial de  $K[\Delta]$  cujos elementos são resíduos dos polinômios homogêneos de grau  $m$  e a série de Hilbert de  $K[\Delta]$  associada à dimensão é a série formal

$$F(K[\Delta], z) := \sum_{m \geq 0} H(K[\Delta], m) z^m.$$

**Proposição 2.49** *Seja  $\Delta$  um complexo simplicial de dimensão  $d-1$  e  $f$  vetor  $(f_0, f_1, \dots, f_{d-1})$ , então*

$$H(K[\Delta], m) = \begin{cases} 1 & , m = 0 \\ \sum_{i=0}^{d-1} f_i \binom{m-1}{i} & , m \geq 1. \end{cases}$$

**Demonstração:** De acordo com a Proposição 2.42, uma base para  $K[\Delta]_m$  é dada pelos resíduos dos monômios cujos suportes são faces de  $\Delta$ . Assim, para uma face  $\{x_{i_1}, \dots, x_{i_{i+1}}\}$  fixa de dimensão  $i \leq m$ , devemos contar o número de monômios  $x_{i_1}^{r_1} \dots x_{i_{i+1}}^{r_{i+1}}$  de grau  $m$  tais que  $r_j \neq 0$ ,  $1 \leq j \leq i+1$ . Mas este número é  $\binom{m-1}{i}$ , mostrando o resultado.  $\square$

**Corolário 2.50** *Seja  $\Delta$  um complexo com  $f$ -vetor  $(f_0, f_1, \dots, f_n)$ , então*

$$F(K[\Delta], z) = \sum_{i=-1}^{d-1} \frac{f_i z^{i+1}}{(1-z)^{i+1}}.$$

**Exemplo 2.51** *Retornando ao Exemplo 2.35 vemos que o ideal  $I = \langle xy, xz, yz \rangle$  é livre de quadrados e, assim, podemos associá-lo a um complexo simplicial e calcularmos sua função de Hilbert.*

Vejamos qual é o complexo com  $V = \{x, y, z\}$  e  $I_\Delta = \langle xy, xz, yz \rangle$  gerado pelas não faces. Logo  $\Delta = \{\emptyset, \{x\}, \{y\}, \{z\}\}$  e, com isto,  $f_{-1} = 1$ ,  $f_0 = 3$ ,  $f_1 = 0$  e  $f_2 = 0$ .

Portanto a função de Hilbert de  $K[x, y, z]/I_\Delta$  é dada por

$$H\left(\frac{K[x, y, z]}{I_\Delta}, m\right) = \begin{cases} 1 & , m = 0 \\ \sum_{i=0}^2 f_i \binom{m-1}{i} = f_0 + \binom{m-1}{1} f_1 + \binom{m-1}{2} f_2 = & , m \geq 1. \\ 3 + 0 + 0 = 3 & \end{cases}$$

## Capítulo 3

### Teorema de Macaulay

Nos dois primeiros capítulos estudamos a função de Hilbert. Vimos que se trata de uma função numérica. Uma pergunta natural é: “Quando uma função numérica é a função de Hilbert de algum anel ou módulo graduado?”

Neste capítulo apresentaremos o 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.

Vejamos, inicialmente, alguns resultados preliminares que nos auxiliarão na demonstração do teorema principal.

Seja  $R = \bigoplus_{n \geq 0} R_n$  uma  $K$ -álgebra homogênea onde  $R_0 = K$  é um corpo. Mostraremos que  $R$  possui uma  $K$ -base constituída de monômios em uma base  $y_1, \dots, y_m$  de  $R_1$ . Consideraremos no que segue:  $\pi : K[x_1, \dots, x_m] \rightarrow R$  o homomorfismo sobrejetor de  $K$ -álgebras com  $\pi(x_i) = y_i$ , mas antes uma definição.

**Definição 3.1** Um conjunto não vazio  $M$  de monômios nas indeterminadas  $x_1, \dots, x_m$  é chamado ideal de ordem de monômios se dado  $m \in M$  e um monômio  $m'$  que divide  $m$ , então  $m' \in M$ . Equivalentemente, se  $x_1^{a_1} \cdots x_m^{a_m} \in M$  e  $0 \leq b_i \leq a_i$  para  $i = 1, \dots, m$ , então  $x_1^{b_1} \cdots x_m^{b_m} \in M$ .

**Observação 3.2** Um ideal de ordem de monômios  $M$  não é uma  $K$ -base de um ideal, por outro lado, denotando por  $M'$  o complementar de  $M$  no conjunto de todos os monômios, então  $M'$  é uma  $K$ -base do ideal gerado pelos monômios  $m \in M' = \mathbb{M} - M$ , onde  $\mathbb{M}$  representa o conjunto de todos os monômios.

O resultado que apresentaremos a seguir, nos mostra que  $R$  possui uma  $K$ -base formada por monômios.

**Teorema 3.3 (Macaulay)** Sejam  $R$  uma  $K$ -álgebra homogênea,  $K$  um corpo,  $y_1, \dots, y_m$  uma  $K$ -base para  $R_1$  e  $\pi : K[x_1, \dots, x_m] \rightarrow R$  o  $K$ -homomorfismo com  $\pi(x_i) = y_i$ , para  $i = 1, \dots, m$ . Então existe um ideal de ordem de monômios  $M$  tal que  $\pi(M)$  é uma  $K$ -base de  $R$ .

**Demonstração:** Seja  $\mathbb{M}$  o conjunto de todos os monômios nas indeterminadas  $x_1, \dots, x_m$  e consideremos a ordem lexicográfica graduada reversa (*grevlex*) sobre  $\mathbb{M}$ . Seja a sequência de monômios  $u_1, u_2, \dots$  definida recursivamente por:  $u_1 = 1$  e assumindo  $u_1, \dots, u_i$  determinados,



T. 1403/05



então  $u_{i+1}$  é o menor elemento na *grevlex* 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, a seqüência termina em  $u_i$ .

Afirmamos que  $M = \{u_1, u_2, \dots\}$  é o ideal de ordem de monômios desejado. Por construção temos que  $\pi(M)$  é um conjunto L.I. e gera  $R$  como um  $K$ -espaço vetorial, ou seja, é uma  $K$ -base de  $R$ .

Vejamos então, que  $M$  é um ideal de ordem de monômios. Assumindo que não, existem  $u_{i_0} \in M$  e  $u \in \mathbb{M} - M$  tais que  $u_{i_0} = ux_j$  para algum  $x_j$ . Como  $u \notin M$ , podemos escrever  $\pi(u) = \sum \lambda_i \pi(u_i)$  com  $u_i \in M$ ,  $u_i < u$  e  $\lambda_i \in K$ . Deste modo  $\pi(u_{i_0}) = \pi(ux_j) = \pi(u)\pi(x_j) = \sum \lambda_i \pi(u_i x_j)$  e  $u_i x_j < u_{i_0}$  para todo  $i$  na soma. Porém  $\pi(u_i x_j) = \sum_{r_{ij}} \beta_{ij} \pi(u_{r_{ij}})$ , com  $u_{r_{ij}} \leq u_i x_j$ .

Logo  $\pi(u_{i_0}) = \sum \gamma_s \pi(u_s)$ , com  $u_s \in M$  e  $u_s < u_{i_0}$  o que é um absurdo, pela construção de  $M$ .  $\square$

Vimos nessa demonstração que nossa  $K$ -base  $\pi(u_1), \pi(u_2), \dots$  de  $R$  possui a seguinte propriedade:  $u \in \mathcal{L}$  e escrevendo  $\pi(u) = \sum_{\lambda_i \neq 0} \lambda_i \pi(u_i)$ , então  $u_i \leq u$ , para todo  $i$  e, se  $u \notin M$ , essas inequações são estritas.

Como consequência imediata do Teorema 3.3 e da Observação 3.2 temos:

**Corolário 3.4** *Seja  $J$  o ideal que é gerado pelos monômios em  $M'$ . Então a  $K$ -álgebra  $R$  e  $K[x_1, \dots, x_m]/J$  possuem a mesma função de Hilbert.*  $\square$

O conjunto de monômios  $M'$  associado a  $R$  pode ser descrito de outra forma. Seja  $I = \text{Ker } \pi$  e, desta forma,  $M' = LM_{\text{grevlex}}(I)$ . De fato, se  $f \in LM_{\text{grevlex}}(I)$ , escolhendo  $f \in I$ ,  $f = \sum_{i=1}^n \lambda v_i$  com monômios  $v_i$  tais que  $v = LM_{\text{grevlex}}(f) = v_n$ . Se  $v_n \notin M'$ , então  $v_n \in M$  e, com isto,

$$0 \neq \pi(v_n) = - \sum_{i=1}^n \lambda_n \lambda_i \pi(v_i).$$

Cada  $\pi(v_i)$  é uma combinação linear  $\sum \alpha_{ij} \pi(u_j)$ ,  $\alpha_{ij} \in K$ ,  $u_j \in M$ ,  $u_j \leq v_i < v_n$ . Trocando os  $\pi(v_i)$  na equação acima pela sua combinação linear, obtemos a representação como uma combinação linear não nula de elementos em  $\pi(M)$  e isto contradiz o Teorema 3.3.

Por outro lado, supondo  $v \in M'$ , então  $\pi(v) = \sum \lambda_i \pi(u_i)$ , com  $u_i \in M$ ,  $u_i < v$ . Assim, fazendo  $f = v - \sum \lambda_i u_i$  temos  $\pi(f) = 0$  e  $LM_{\text{grevlex}}(f) = v$ .

**Definição 3.5** *Tomando um monômio  $u$  de grau  $d$ , ou seja,  $u \in S_d$ , definimos*

$$\mathcal{L}_u := \{v \in S_d \mid v \text{ é monômio e } v < u\},$$

$$\mathcal{R}_u := \{v \in S_d \mid v \text{ é monômio e } v \geq u\}.$$

Note que  $\mathcal{R}_{x_1} = \{x_1, \dots, x_m\}$ .

**Lema 3.6** *Nas condições e com as notações dos parágrafos anteriores, dado  $u \in S_d$ , temos  $\mathcal{R}_{x_1} \mathcal{R}_u = \mathcal{R}_{x_1 u}$ .*

**Demonstração:** Seja  $v \in \mathcal{R}_u$ , então  $x_1 v \geq x_1 v \geq x_1 u$ . Por outro lado, seja  $v \in \mathcal{R}_{x_1 u}$ . Podemos assumir que  $x_1$  não divide  $v$ , então  $v \geq x_1 u$ . Sejam  $u = x_1^{a_1} \dots x_m^{a_m}$ ,  $v = x_1^{b_1} \dots x_m^{b_m}$  e  $i$  o maior inteiro tal que  $b_i > a_i$ . Se existe  $j < i$  com  $b_j > 0$ , então  $x_j^{-1} v \in \mathcal{R}_u$ , caso contrário,  $x_i^{-1} \in \mathcal{R}_u$ . Nos dois casos segue que  $v \in \mathcal{R}_{x_1} \mathcal{R}_u$ .  $\square$

**Lema 3.7** Dado  $u \in S_d$ ,  $u = x_{j(1)}x_{j(2)} \cdots x_{j(d)}$  temos

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

onde  $[x_1, \dots, x_i]_d$  denota o conjunto de todos os monômios de grau  $d$  nas variáveis  $x_1, \dots, x_i$ .

**Demonstração:** O conjunto  $\mathcal{L}_u$  admite uma decomposição natural: seja  $i$  o maior inteiro tal que  $x_i$  divide  $u$ . Então podemos escrever  $\mathcal{L}_u = \mathcal{L}'_u \dot{\cup} \mathcal{L}''_u x_i$ , onde  $x_i$  não divide elementos de  $\mathcal{L}'_u$ . Esta união é disjunta visto que  $\mathcal{L}'_u$  consiste de todos os monômios de grau  $d$  nas variáveis  $x_1, \dots, x_{i-1}$  e que  $\mathcal{L}''_u = \mathcal{L}_{x_i^{-1}u}$ .

Usando a mesma idéia podemos decompor  $\mathcal{L}''_u$  e assim por diante. Deste modo, se escrevermos

$$u = x_{j(1)}x_{j(2)} \cdots x_{j(d)},$$

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

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

Continuando com este raciocínio, terminamos com uma união disjunta

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

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

Vejamos um exemplo:

**Exemplo 3.8** Seja  $S = K[x_1, x_2, x_3, x_4]$  e  $u = x_2^2 x_3$ . Então,

$$\begin{aligned} \mathcal{L}_u &= \{x_1^3, x_1^2 x_2, x_1 x_2^2, x_2^3, x_1^2 x_3, x_1 x_2, x_3\}, \\ \mathcal{L}'_u &= \{x_1^3, x_1^2 x_2, x_1 x_2^2, x_2^3\} \\ \mathcal{L}''_u &= \{x_1^2, x_1 x_2\} = \mathcal{L}_{x_2} \end{aligned}$$

**Observação 3.9** Com a decomposição natural de  $\mathcal{L}_u$  temos que

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

Agora,  $|[x_1, \dots, x_{j(i)-1}]_i| = \binom{j(i)-1+i-1}{j(i)-1-1} = \binom{j(i)+i-1}{j(i)-2} = \binom{j(i)+i-2}{i}$ . Logo,

$$|\mathcal{L}_u| = \sum_{i=1}^d \binom{k(i)}{i},$$

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

Pelo exposto anteriormente, os números inteiros não negativos  $|\mathcal{L}_u|$  podem ser escritos como um somatório de números binomiais. Este resultado é mais geral como pode ser visto no lema a seguir.

**Lema 3.10** *Seja  $d$  um inteiro positivo. Todo  $a \in \mathbb{N}$  pode ser escrito unicamente na forma*

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

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

Assumiremos que  $\binom{k}{l} = 0$  para  $0 \leq k < l$ .

**Demonstração:** Para mostrarmos a existência procederemos por indução sobre  $a$ , para  $a = 1$  temos que

$$a = \binom{d}{d} + \binom{d-2}{d-1} + \cdots + \binom{0}{1}.$$

Suponhamos que o resultado seja válido para qualquer número menor do que  $a$  e escolhamos  $k(d)$  o maior natural tal que  $\binom{k(d)}{d} \leq a$ . Se  $a = \binom{k(d)}{d}$ , então  $a = \sum_{i=1}^d \binom{k(i)}{i}$ , com  $k(i) = i - 1$ ,  $i = 1, \dots, d - 1$ . Agora se  $\binom{k(d)}{d} < a$  então  $a' = a - \binom{k(d)}{d} > 0$  e, pela hipótese de indução, temos  $a' = \sum_{i=1}^{d-1} \binom{k(i)}{i}$ , com  $k(d-1) > \cdots > k(1) \geq 0$ .

Falta mostrar que  $k(d) > k(d-1)$ .

Temos  $\binom{k(d)+1}{d} > a$ , então

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

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

de onde segue que  $k(d) > k(d-1)$ .

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

Para vermos 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  $\binom{k'(d)}{d} \leq a$  tem-se  $k(d) \leq k'(d)$ . Do mesmo modo tem-se  $k(d) \leq k'(d)$ . Portanto  $k(d) = k'(d)$ . Procedendo com raciocínio análogo chegamos a  $k(i) = k'(i)$  para todo  $i = 1, \dots, d$ .  $\square$

Chamaremos a soma do Lema 3.10 de  $d$ -ésima representação de Macaulay de  $a$ , e chamaremos  $k(d), \dots, k(1)$  de  $d$ -ésimos coeficientes de Macaulay de  $a$ . Note que para todo  $i \leq d$  o coeficiente  $k(i)$  é determinado pelo fato de ser o maior inteiro  $j$  tal que

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

Os  $d$ -ésimos coeficientes de Macaulay possuem a seguinte propriedade:

**Lema 3.11** *Sejam  $k(d), \dots, k(1)$  e  $k'(d), \dots, k'(1)$ , respectivamente, os  $d$ -ésimos coeficientes de Macaulay de  $a$  e  $a'$ . Então  $a > a'$  se, e somente se,  $(k(d), \dots, k(1)) >_{\text{lex}} (k'(d), \dots, k'(1))$ .*

**Demonstração:** Mostraremos as duas implicações por indução sobre  $d$ . Para  $d = 1$  a afirmação é clara. Agora, assumindo  $d > 1$ , se  $k(d) = k'(d)$ , então  $k(d-1), \dots, k(1)$  e  $k'(d-1), \dots, k'(1)$  são, respectivamente, os  $d-1$ -ésimos coeficientes de Macaulay de  $a - \binom{k(d)}{d}$  e  $a' - \binom{k'(d)}{d}$ . Aplicando a hipótese de indução obtemos o resultado. Agora, se  $k(d) \neq k'(d)$ , a caracterização dos  $d$ -ésimos coeficientes de Macaulay, vista no Lema 3.10 nos assegura que  $k(d) > k'(d)$  se, e somente se,  $a > a'$ .  $\square$

Descartando as parcelas que são zero na  $d$ -ésima representação de Macaulay de  $a$ , obtemos a seguinte expansão (única):

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

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

**Definição 3.12** *Dado  $a \in \mathbb{N}$  e sua representação de Macaulay, como anteriormente, definimos*

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

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

Este número goza das seguintes propriedades:

**Lema 3.13** *Sejam  $a, a'$  e  $d$  inteiros positivos.*

(i) *Se  $a \leq a'$ , então  $a^{(d)} \leq a'^{(d)}$ .*

(ii) *Sejam  $k(d), \dots, k(1)$  os  $d$ -ésimos coeficientes de Macaulay de  $a$  e  $j = \min\{i \mid k(i) \geq i\}$ . 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. Usando a hipótese e o Lema 3.11 temos  $(k(d), \dots, k(1)) <_{\text{lex}} (k'(d), \dots, k'(1))$  e, assim,  $a^{(d)} < a'^{(d)}$ .

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

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

$$a+1 = \binom{k(d)}{d} + \dots + \binom{k(j)}{j} + 1 = \binom{k(d)}{d} + \dots + \binom{k(j-1)}{j-1}, \quad \text{e}$$

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

Agora, para  $j = 1$ , seja  $i$  o maior inteiro tal que  $k(i) = k(1) + i - 1$ . Então

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

uma vez que  $\sum_{r=1}^i \binom{k(1)+r-1}{r} = \binom{k(1)+i}{i} - 1$ .

Deste modo,

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

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

Assim,

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

Portanto,

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

como queríamos.  $\square$

**Proposição 3.14** *Seja  $u$  um monômio de grau  $d$  em  $S$ . Então  $|\mathcal{L}_{x_1 u}| = |\mathcal{L}_u|^{(d)}$ .*

**Demonstração:** Seja  $\mathcal{L}_u = \dot{\cup}_{i=1}^d [x_1, \dots, x_{j(i)-1}]_{i+1} x_{j(i+1)} \cdots x_{j(d)}$  a decomposição natural de  $\mathcal{L}_u$ . Afirmamos que

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

é a decomposição canônica de  $\mathcal{L}_{x_1 u}$ . Além disso, a decomposição natural de  $\mathcal{L}_u$  é completamente determinada pela seqüência  $j(1), \dots, j(d)$ , relacionada a  $u$ . Sejam  $l(1), \dots, l(d+1)$  a seqüência correspondente a  $x_1 u$ , então  $l(1) = 1$  e  $l(i) = j(i-1)$  para  $i = 2, \dots, d+1$ . Como se trata de união disjunta, segue o resultado.  $\square$

**Definição 3.15** Ainda usando os  $d$ -coeficientes de Macaulay de um número positivo 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 que se seguirão:

**Lema 3.16** Sejam  $a, a', d$  e  $b$  números naturais.

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

**Demonstração:** (i) Segue do que foi observado anteriormente e do Lema 3.11.

(ii) Procederemos por indução sobre  $d$ . Se  $d = 1$  e  $a \neq 1$  temos  $a = \binom{a}{1}$  e  $\binom{a-1}{1} = a - 1$ . Logo  $a_{\langle 1 \rangle} > (a-1)_{\langle 1 \rangle}$ .

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

(1) Se  $k'(d) = k(d)$ , tomamos  $a' = a - \binom{k(d)}{d}$ , temos  $a' - 1 > 0$ , pois se  $a' = 1$ , então  $a = \binom{k(d)}{d} + \binom{d-1}{d-1}$  (absurdo pois estamos supondo  $k(j) \neq j$ ).

Logo,  $a' - 1 > 0$ . Agora,  $a'$  tem como  $(d-1)$ -ésimos coeficientes de Macaulay  $k(d-1), k(d-2), \dots, k(1)$  e  $a' - 1$  tem como  $(d-1)$ -coeficientes de Macaulay os números  $k'(d-1), k'(d-2), \dots, k'(1)$ . Porém,  $a'$  satisfaz as condições do item (ii) deste teorema e, por hipótese de indução,  $(a' - 1)_{\langle d-1 \rangle} < a'_{\langle d-1 \rangle}$ , 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  $a_{\langle d \rangle} = a'_{\langle d-1 \rangle} + \binom{k(d)-1}{d}$  e  $(a-1)_{\langle d \rangle} = (a' - 1)_{\langle d-1 \rangle} + \binom{k(d)-1}{d}$ , segue o resultado.

(2) Se  $k(d) > k'(d)$ ,  $k(d) - 1 > k'(d) - 1$  e, assim,  $(a-1)_{\langle d \rangle} < a_{\langle d \rangle}$ .

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

$$b = \binom{k(d)}{d} + \cdots + \binom{k(j)}{j},$$

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  $c_{\langle d \rangle} = b$ . Assim, se mostrarmos que  $a \geq c$ , teremos  $a_{\langle d \rangle} \geq c_{\langle d \rangle} = b$ . Supondo que  $a < c$ ,

$$a < \binom{k(d)+1}{d} + \cdots + \binom{k(j)+1}{j},$$

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

Distinguimos dois casos:

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

Desta forma

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

Agora, por hipótese,  $b \leq b_{(d)} + (a - b)_{(d-1)}$  e, portanto,

$$\begin{aligned} b &\leq \binom{k(d)-1}{d} + \cdots + \binom{k(1)-1}{1} + \binom{k(d)-1}{d-1} + \cdots + \binom{k(2)-1}{1} = \\ &= \binom{k(d)}{d} + \cdots + \binom{k(2)}{2} + \binom{k(1)-1}{1} < b. \text{ (Absurdo!)} \end{aligned}$$

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

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

O próximo teorema é a chave para a demonstração do Teorema de Macaulay. Porém, antes de enunciá-lo, apresentaremos algumas noções de geometria algébrica que nos ajudarão a demonstrá-lo. Para maiores detalhes veja [3].

**Definição 3.17** *Sejam  $K$  um corpo,  $S = K[x_1, \dots, x_n]$  e  $I \subset S$  ideal.*

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

(ii)  *$V(I) = \{(a_1, \dots, a_n) \in A^n(K) \mid f(a_1, \dots, a_n) = 0, \forall f \in I\}$  é chamado variedade do ideal  $I$ .*

Temos as seguintes propriedades:

(i) Se  $(I_\lambda)_{\lambda \in \Omega}$  é uma família de ideais de  $S$  então  $\cap_{\lambda \in \Omega} V(I_\lambda) = V(\sum I_\lambda)$ .

(ii) Para  $I_j \in S$ ,  $j = 1, \dots, n$ ,  $\cup_{j=1}^n V(I_j) = V(\cap_{j=1}^n I_j)$ .

Com estas propriedades  $A^n(K)$  é um espaço topológico, onde os fechados são da forma  $F = V(I)$  com  $I$  ideal de  $S$ .

Mais ainda, para  $K$  corpo infinito,  $A^n(K)$  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 3.18

(i) *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  $y_i = x_i + I$  com  $I$  o ideal homogêneo de  $S$  que define  $R$ .*

- (ii) Se  $R_1$  é espaço topológico irredutível, então todo aberto é denso em  $R_1$ .
- (iii) Dada  $P$  uma propriedade definida nas formas lineares de  $R_1$ , dizemos que  $h \in R_1$  é genérico em relação a  $P$  se existe  $U \subseteq R_1$ ,  $h \in U$  tais que  $P$  vale para toda forma linear de  $U$ .

**Teorema 3.19 (Green-Forma Algébrica)** *Sejam  $R$  uma  $K$ -álgebra homogênea,  $K$  um corpo infinito e  $n \geq 1$  um inteiro. Então*

$$H(R/hR, n) \leq H(R, n)_{\langle n \rangle},$$

para uma forma linear genérica  $h$ .

**Demonstração:** Seja  $s = \sup\{\dim_K hR_{n-1} \mid h \in R_1\}$ . Então  $\dim_K hR_{n-1} = s$  para alguma forma linear  $h$ . De fato, seja  $U \subset R_1$  o subconjunto dos elementos  $h \in R_1$  tais que  $\dim_K hR_{n-1} = s$ . Temos  $U \neq \emptyset$  e para vermos que  $U$  é aberto, escolhemos uma base  $\{y_1, \dots, y_m\}$  de  $R_1$  e  $\{u_1, \dots, u_r\}$ ,  $\{v_1, \dots, v_l\}$  bases de  $R_{n-1}$  e de  $R_n$ , respectivamente. Se  $h \in R_1$ , então  $h = \sum_{i=1}^m a_i y_i$ , considerando os  $a_i$  variáveis sobre  $K$ . A aplicação multiplicação por  $h$ ,  $\varphi_h : R_{n-1} \rightarrow R_n$ , dada por  $\varphi_h(f) = hf$  pode ser descrita por uma matriz  $[\varphi_h]$  de formas lineares em  $a_1, \dots, a_m$ . Trocando os  $w_i$  por indeterminadas, produzimos uma matriz  $A$  de polinômios lineares com coeficientes em  $K$ . Mostraremos que  $U = R_1 - V(I_s(A))$ , onde  $I_s(A)$  é o ideal gerado pelos determinantes dos menores  $s \times s$  de  $A$ .

Observamos que se  $h \in V(I_s(A))$ , então o determinante de qualquer menor  $s \times s$  de  $\varphi_h$  é nulo e portanto  $\dim_K hR_{n-1} < s$ .

$U$  é um conjunto aberto (complementar de fechado) e todo elemento  $h \in U$  é genérico.

Sejam  $h \in U$  e  $S = R/hR$ . Afirmamos que  $H(S, n) \leq H(R, n)_{\langle n \rangle}$  e provaremos esta afirmação por indução sobre  $n$  e  $\dim_K R_1$ . Se  $n = 1$  e  $\dim_K R_1$  é qualquer temos que  $H(R/hR, 1) = \dim_K (R/hR)_1 = \dim_K R_1/hR_0 = \dim_K R/Kh = \dim_K R_1 - 1$ ,  $H(R, 1) = \dim_K R_1$  e  $H(R, 1)_{\langle 1 \rangle} = \dim_K R_1 - 1$ .

Portanto  $H(R/hR, 1) \leq H(R, 1)_{\langle 1 \rangle}$ .

Se, ainda,  $\dim_K R_1 = 1$  e  $n$  é qualquer, como  $R = K[y_1, \dots, y_m]$  com  $y_i = x_i + I$ , podemos supor que  $y_1$  gera  $R_1$ . Assim, dado  $y_i \in R$ ,  $i \neq 1$  temos  $y_i = c_i y_1$  e, portanto,  $x_i - c_i x_1 \in I$ . Daí, substituindo  $R = K[y_1, \dots, y_m]$  por  $K[x_1, x_2 - c_2 x_1, \dots, x_m - c_m x_1]$  temos:

$$\frac{K[x_1, x_2 - c_2 x_1, \dots, x_m - c_m x_1]}{I} \simeq \frac{K[y_1]}{(y_1^i)} = K[y_1].$$

$$\text{Assim } \dim_K R_j = \begin{cases} 1, & \text{se } j = 0 \\ 0, & \text{se } j \leq 1. \end{cases}$$

Como  $h \in R_1$  temos  $(R/hR)_n = 0$  para todo  $n$  e, portanto,  $0 = H(R/hR, n) \leq H(R, n)_{\langle n \rangle}$ .

Logo, se  $n = 1$  e  $\dim_K R_1$  é qualquer ou se  $\dim_K R_1 = 1$  e  $n$  é qualquer o resultado vale.

Façamos, agora, a seguinte hipótese de indução:  $n > 1$ ,  $\dim_K R_1 > 1$  e que o resultado valha para um número menor do que  $n$  e  $\dim_K R_1$  qualquer. Seja  $V \subset S_1 = R_1/hR_0$  o subconjunto de formas lineares  $g$  nas quais  $\dim_K gS_{n-1}$  é máxima e denotemos por  $\varphi$  o epimorfismo canônico  $\varphi : R \rightarrow S$ ,  $\varphi(f) = f + hR = \bar{f}$ . Consideremos o subconjunto de  $R_1$

$$W = (U - Kh) \cap \varphi^{-1}(V)$$

de  $R_1$ . O conjunto  $W$  é não vazio, pois  $R_1$  é irredutível e ambos  $\varphi^{-1}(V)$  e  $(U - Kh)$  são não vazios. De fato, suponhamos  $U \subset Kh$ . Então, como  $U$  é denso e  $Kh$  é fechado em  $R_1$ , segue que  $R_1 = Kh$ , contradizendo  $\dim_K R_1 > 1$ . Agora  $W$  é aberto pois  $\varphi|_{R_1} : R_1 \rightarrow S_1$  é contínua na topologia de Zariski e, portanto,  $\varphi^{-1}(V)$  é aberto, uma vez que  $V$  é aberto (a demonstração deste fato é análoga àquela apresentada para  $U$ ). Além disso  $U - Kh$  é também um conjunto aberto.

Escolhendo  $h^* \in W$  e consideremos a seguinte sequência exata:

$$0 \rightarrow \bar{h}^* S_{n-1} \rightarrow S_n \rightarrow \frac{S_n}{\bar{h}^* S_{n-1}} \rightarrow 0.$$

Então

$$H(S, n) = \dim_K(S_n/h^* S_{n-1}) + \dim_K h^* S_{n-1}. \quad (3.1)$$

Como  $\dim_K S_1 < \dim_K R_1$  e  $h^* \in \varphi^{-1}(V)$  por hipótese de indução, temos

$$\dim_K(S_n/\bar{h}^* S_{n-1}) \leq H(S, n)_{(n)}.$$

Para obtermos uma cota superior para a segunda parcela de 3.1 notemos que

$$\dim_K \bar{h}^* S_{n-1} \leq \dim_K(h^* R_{n-1}/h(h^* R_{n-1})) = \dim_K(h R_{n-1}/h^*(h R_{n-2})),$$

uma vez que a sequência exata

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

$$\text{nos dá } \dim_K h^* R_{n-1} = \dim_K \frac{h^* R_{n-1}}{h h^* R_{n-2}} + \dim_K h h^* R_{n-2}.$$

Agora, da sequência exata

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

$$\text{temos } \dim_K h R_{n-1} = \dim_K \frac{h R_{n-1}}{h^* h R_{n-2}} + \dim_K h h^* R_{n-2}.$$

$$\text{Como } h, h^* \in U \text{ temos que } \dim_K h R_{n-1} = \dim_K h^* R_{n-1} \text{ e, assim, } \dim_K \frac{h^* R_{n-1}}{h h^* R_{n-2}} = \dim_K \frac{h R_{n-1}}{h^* h R_{n-2}}.$$

Escolhendo  $h^*$  tal que  $h^*(h R_{n-2})$  tenha dimensão máxima, consideremos  $J = \text{Ann } h$  e  $P = R/\text{Ann } h$ .  $J$  é um ideal homogêneo,

$$\dim_K \frac{h R_{n-1}}{h h^* R_{n-2}} = \dim_K \frac{\left(\frac{R_{n-1}}{J_{n-1}}\right)}{h^* \left(\frac{R_{n-2}}{J_{n-2}}\right)} = H\left(\frac{P}{h^* P}, n-1\right)$$

e, por hipótese de indução  $H(P/h^* P, n-1) \leq H(P, n-1)_{(n-1)}$ .

Porém,  $H(P, n-1) = \dim_K R_{n-1}/J_{n-1} = \dim_K hR_{n-1} = \dim_K R_n - \dim_K R_n/hR_{n-1}$ . Logo  $H(P, n-1) = H(R, n) - H(S, n)$  e concluímos que  $\bar{h}^* S_{n-1} \leq (H(R, n) - H(S, n))_{\langle n-1 \rangle}$ .

Assim  $H(S, n) \leq H(S, n)_{\langle n \rangle} + (H(R, n) - H(S, n))_{\langle n-1 \rangle}$  e, usando Lema 3.16 (iii), segue que

$$H(S, n) \leq H(R, n)_{\langle n \rangle}. \quad \square$$

Agora, apresentaremos o principal teorema:

**Teorema 3.20 (Macaulay)** *Sejam  $K$  um corpo e  $h : \mathbb{N} \rightarrow \mathbb{N}$  uma função numérica. As seguintes condições são equivalentes:*

- (i) *Existe uma  $K$ -álgebra homogênea  $R$  com função de Hilbert  $H(R, n) = h(n)$ , para todo  $n \geq 0$ .*
- (ii) *Existe uma  $K$ -álgebra homogênea  $R$  com relações monomiais e com função de Hilbert  $H(R, n) = h(n)$ , para todo  $n \geq 0$ .*
- (iii)  *$h(0) = 1$  e  $h(n+1) \leq [h(n)]^{(n)}$  para  $n \geq 1$ .*
- (iv) *Seja  $m = h(1)$  e para cada  $n \geq 0$  seja  $M_n$  o conjunto dos primeiros  $h(n)$  monômios de grau  $n$  nas variáveis  $x_1, \dots, x_m$  (na ordem lexicográfica graduada reversa). Definindo  $M = \cup_{n \geq 0} M_n$ , temos que  $M$  é um ideal de ordem de monômios.*

**Demonstração:** (i)  $\Leftrightarrow$  (ii) foi vista no Corolário 3.10.

(iv)  $\Rightarrow$  (ii) Trivial.

(iii)  $\Rightarrow$  (iv) Por hipótese  $h(n+1) \leq [h(n)]^{(n)}$  para todo  $n \geq 1$ . Assim, se  $h(1) = m$  então  $h(n) \leq \binom{m+n-1}{n}$ . Suponhamos que  $h(n+1) = \binom{n+m}{n+1}$ , então  $h(n) = \binom{n+m+1}{n}$  e, assim,  $M_i = [x_1, \dots, x_m]_i$  para  $i = n$  e  $i = n+1$ . Logo, se  $u \in M_{n+1}$  e  $x_i$  divide  $u$ , então  $x_i^{-1}u \in M_n$ . Agora supomos que  $h(n+1) \leq \binom{n+m}{n+1}$ , então existe um monômio  $u_{n+1}$  tal que  $M_{n+1} = \mathcal{L}_{u_{n+1}}$ . Se como antes,  $M_n = [x_1, \dots, x_m]_n$ , não há nada a mostrar. De outro modo, existe um monômio  $u_n$  tal que  $M_n = \mathcal{L}_{u_n}$ . A condição (iii) e a Proposição 3.14 implicam  $\mathcal{R}_{x_1} \mathcal{R}_{u_n} \subset \mathcal{R}_{u_{n+1}}$ . Portanto, se  $u \in M_{n+1}$  e  $x_i$  divide  $u$  temos  $x_i^{-1}u \in M_n$ . Em outras palavras,  $M = \cup_{n \geq 0} M_n$  é um ideal de ordem de monômios.

Até agora vimos que (iii)  $\Rightarrow$  (iv)  $\Rightarrow$  (ii)  $\Leftrightarrow$  (i). Para fechar o ciclo mostraremos que (i)  $\Rightarrow$  (iii).

(i)  $\Rightarrow$  (iii) Podemos assumir que  $K$  é infinito, pois se necessário, trocamos  $R$  por  $L \otimes_K R$ , onde  $L$  é uma extensão infinita de  $K$ .

Sejam  $g$  uma forma linear e  $S = R/gR$ . A seqüência exata

$$0 \rightarrow gR_n \rightarrow R_{n+1} \rightarrow S_{n+1} \rightarrow 0$$

nos dá a inequação  $H(R, n+1) \leq H(R, n) + H(S, n+1)$ . Fazendo  $a = H(R, n)$  e  $b = H(R, n+1)$ . Para uma forma linear genérica  $g$  a inequação e o Teorema de Green 3.19 nos garantem que  $b \leq a + b_{\langle n+1 \rangle}$ . Sejam  $k(n+1), \dots, k(1)$  os  $(n+1)$ -coeficientes de Macaulay de  $b$ . Então

$$b = \binom{k(n+1)-1}{n+1} + \dots + \binom{k(1)-1}{1}, \text{ e, assim,}$$

$$a \geq \binom{k(n+1)-1}{n} + \cdots + \binom{k(2)-1}{1} + \binom{k(1)-1}{0}.$$

Seja  $j = \min\{i \mid k(i) \geq i\}$ . Se  $j > 1$ , então  $k(1) = 0$  e

$$a^{(n)} \geq \binom{k(n+1)}{n+1} + \cdots + \binom{k(2)}{2} = b$$

e, portanto,  $b = H(R, n+1) = h(n+1) \leq H(R, n)^{(n)} = h(n)^{(n)}$  como queríamos demonstrar. Se  $j = 1$ , então, pelo Lema 3.13,

$$a^{(n)} \geq \binom{k(n+1)}{n+1} + \cdots + \binom{k(3)}{3} + \binom{k(2)}{2} + k(2).$$

Mas  $k(2) > k(1)$  e, portanto,  $a^{(n)} > b$ .  $\square$

**Exemplo 3.21** Seja  $h : \mathbb{N} \rightarrow \mathbb{N}$  dada inicialmente por  $h(0) = 1$ ,  $h(1) = 3$ ,  $h(2) = 4$ ,  $h(3) = 5$  e  $h(4) = 7$ .  $h$  não pode ser a função de Hilbert de uma  $K$ -álgebra homogênea pois

$$\bullet \ 5 = \binom{4}{3} + \binom{2}{2};$$

$$\bullet \ 5^{(3)} = \binom{5}{4} + \binom{3}{3};$$

$$\bullet \ h(4) = 7 > 6 = 5^{(3)} = h(3)^{(3)}.$$

**Corolário 3.22** Sejam  $R$  uma  $K$ -álgebra homogênea e  $K$  um corpo. Então  $H(R, n+1) = H(R, n)^{(n)}$  para  $n$  suficientemente grande.

**Demonstração:** Tomando  $R = S/I$ , onde  $S = K[x_1, \dots, x_m]$ , pelo item (iv) do Teorema de Macaulay 3.20, existe um ideal de ordem de monômios  $M = \cup_{n \geq 0} M_n$  em  $S$  tal que  $H(R, n) = H(S/J, n)$  para todo  $n$ , onde  $J$  é o ideal gerado por todos os monômios que não estão em  $M$ . Além disso, a escolha de  $M$  foi tal que  $M$  consiste de todos os monômios de grau  $n$  se  $I_n = 0$  e  $M_n = \mathcal{L}_{u_n}$  para um monômio  $u_n$  apropriado caso contrário. Como  $J$  é finitamente gerado, existe um inteiro  $r$  tal que  $\mathcal{R}_{u_{n+1}} = \mathcal{R}_{x_1} \mathcal{R}_{u_n}$  para todo  $n \geq r$  e o resultado segue da Proposição 3.14.  $\square$

# Apêndice A

## Exemplos Utilizando o CoCoA

Utilizaremos o WinCoCoA, que é a versão com interface gráfica que acompanha o CoCoA 4.2, pois facilita a utilização do mesmo.

### A.1 Introdução ao CoCoA

Todos os nomes de comandos, palavras chave e variáveis no CoCoA devem começar com letras maiúsculas e as linhas de comando dever ser terminadas com ponto e vírgula (;).

#### A.1.1 Ambiente Anel

Antes de fazermos cálculos utilizando polinômios precisamos especificar o anel que usaremos com o comando **Use**. O operador especial  $::=$  armazena, em uma variável, um anel.

- $\mathbb{Q}[x,y,z]$ ; – coeficientes em  $\mathbb{Q}$  e indeterminadas  $x, y$  e  $z$ .

- $\mathbb{Z}/(23)[x,y,z]$ ; – coeficientes em  $\mathbb{Z}/23\mathbb{Z}$ .

- $\mathbb{Q}[x,y,z], \text{Lex}$ ; – ordem lexicográfica.

O padrão é a ordem lexicográfica reversa (**DegRevLex**), ou seja, se nenhuma ordem monomial for colocada no comando, o CoCoA utilizará a ordem lexicográfica reversa. Para ordem lexicográfica graduada use **DegLex**.

- $\mathbb{Q}[x[1..8]]$ ; – indeterminadas indexadas.

- $S ::= \mathbb{Q}[x,y]$ ; – armazena o anel na variável  $S$ .

- **Use S**; – usa o anel armazenado em  $S$ .

- **Use S ::=  $\mathbb{Q}[x,y]$** ; – armazena o anel na variável  $S$  e o usa.

- **Use  $\mathbb{Q}[x,y,z]$** ; – usa o anel que acabou de ser criado.

- **CurrentRing()**; – exibe o anel em uso.

### A.1.2 Estruturas de Programação

Seguem as sintaxes das estruturas de programação mais comuns. As palavras chave estão em *tipewriter* e, em *itálico*, descrevemos a classe de expressões que ocupam seu lugar.

- *If condições Then comandos EndIf;*
- *If condições Then comandos Else comandos EndIf;*
- *While condições Do comandos EndWhile;*
- *For variável := inicial To final Do comandos EndFor;*  
*inicial e final são inteiros e se inicial > final, então o laço de repetição termina sem executar o(s) comando(s) de comandos.*

### A.1.3 Lista de Comandos

A seguir, listamos alguns comandos do CoCoA que utilizaremos para ilustrar os exemplos do que foi visto no Capítulo 2.

Depois do nome do comando, segue a sintaxe, uma breve descrição e exemplos de sua utilização. Na sintaxe temos o comando e a descrição de seus argumentos. Os argumentos são variáveis, cujo tipo está indicado após o nome da variável. Tipos de variáveis que usaremos: POLY (polinômios), LIST de POLY (lista de polinômios), IDEAL (ideal), INT (inteiro) e RING (anel)

#### DivAlg

##### SINTAXE

*DivAlg(X:POLY,L:LIST de POLY)*

Esta função aplica o algoritmo da divisão sobre  $X$  com respeito a  $L$ , retornando dois campos: 'Quotients' com uma lista de polinômios e 'Remainder' com o resto da divisão de  $X$  por  $L$ .

##### EXEMPLO

```
Use R := Q[x,y,z];
F := x^2y+xy^2+y^2;
L := [xy-1,y^2-1];
DivAlg(F,[xy-1,y^2-1]);
Record[Quotients = [x + y, 1], Remainder = x + y + 1]
```

-----

**GBasis**

## SINTAXE

GBasis(M: IDEAL)

Esta função retorna uma lista cujos componentes formam uma base de Gröbner de M com respeito a ordem monomial do anel corrente. Para um base de Gröbner reduzida, usamos o comando 'ReducedGBasis'. O anel dos coeficientes necessita ser um corpo.

## EXEMPLO

```
Use R ::= Q[t,x,y];
I := Ideal(t^3-x,t^4-y);
GBasis(I);
[t^3 - x, -tx + y, t^2y - x^2, x^3 - ty^2]
```

**GCD, LCM**

## SINTAXE

```
GCD(F_1:INT,...,F_n:INT)
GCD(L:LIST de INT)
LCM(F_1:INT,...,F_n:INT)
LCM(L:LIST de INT)
GCD(F_1:POLY,...,F_n:POLY)
GCD(L:LIST de POLY)
LCM(F_1:POLY,...,F_n:POLY)
LCM(L:LIST de POLY)
```

Estas funções retornam, respectivamente, o máximo divisor comum e o mínimo divisor comum de  $F_1, \dots, F_n$  ou os elementos na lista L. Para o cálculo do MDC e do MMC de polinômios, o anel dos coeficientes precisa ser um corpo.

## EXEMPLO

```
Use R ::= Q[x,y];
F := x^2-y^2;
G := (x+y)^3;
GCD(F,G);
x + y
-----
LCM(F,G);
1/4x^4 + 1/2x^3y - 1/2xy^3 - 1/4y^4
-----
4It = (x+y)^3(x-y);
TRUE
```

```
-----
GCD(3*4,3*8,6*16);
```

```
12
-----
```

```
GCD([3*4,3*8,6*16]);
```

```
12
-----
```

## Hilbert

### SINTAXE

```
Hilbert(R:RING)
```

```
Hilbert(R:RING,N:INT)
```

A primeira forma desta função calcula a Função de Hilbert de R. A segunda forma calcula o N-ésimo valor da Função de Hilbert de R. O anel dos coeficientes precisa ser um corpo.

### EXEMPLO

```
Use R ::= Q[t,x,y,z];
```

```
Hilbert(R/Ideal(z^2-xy,xz^2+t^3));
```

```
H(0) = 1
```

```
H(1) = 4
```

```
H(t) = 6t-3 for t >= 2
```

```
-----
Hilbert(R/Ideal(z^2-xy,xz^2+t^3),2);
```

```
9
-----
```

## Ideal

### SINTAXE

```
Ideal(P_1:POLY,...,P_n:POLY)
```

```
Ideal(L:LIST de POLY)
```

A primeira forma retorna o ideal gerado por  $P_1, \dots, P_n$  e a segunda forma o ideal gerado pelos polinômios em L.

### EXEMPLO

```
Use R ::= Q[x,y,z];
```

```
I := Ideal(x-y^2,xy-z);
```

```
I;
```

```
Ideal(-y^2 + x, xy - z)
```

```
L := [xy-z,x-y^2];
J := Ideal(L);
I = J;
TRUE
```

---

## LC

### SINTAXE

LC(F:POLY)

Esta função retorna o coeficiente líder de F com relação a ordem monomial do anel que F pertence.

### EXEMPLO

```
Use R ::= Q[x,y];
LC(x+3x^2-5y^2);
3
```

---

## LM

### SINTAXE

LM(P:POLY)

Cuidado, esta função retorna, pela nossa teoria, o termo líder de P e não o monômio líder, ou seja, o monômio e o coeficiente líderes. Para obter o monômio líder, veja o comando LT.

### EXEMPLO

```
Use R ::= Q[x,y];
LM(3x^2y+y);
3x^2y
```

---

## LT

### SINTAXE

LT(E:IDEAL ou POLY)

Se E é um polinômio, esta função retorna o monômio líder (e não o termo líder!) do polinômio E com respeito a ordem monomial do anel corrente. Se E é um ideal, esta função retorna o ideal gerado pelos monômios líderes de todos os elementos de E. Para obter o termo líder, veja o comando LM.

### EXEMPLO

```

Use R ::= Q[x,y,z]; -- a ordem monomial padrão é a DegRevLex
LT(y^2-xz);
y^2
-----
Use R ::= Q[x,y,z], Lex;
LT(y^2-xz);
xz
-----
Use R ::= Q[x,y,z];
I := Ideal(x-y,x-z^2);
LT(I);
Ideal(x, z^2)
-----

```

**NF****SINTAXE**

**NF(F:POLY,I:IDEAL)**

Esta função retorna a forma normal de F com respeito a I. Também computará uma base de Gröbner de I se uma tal base ainda não tiver sido computada. O anel dos coeficientes precisa ser um corpo.

**EXEMPLO**

```

Use R ::= Q[x,y,z];
I := Ideal(z);
NF(x^2+xy+xz+y^2+yz+z^2,I);
x^2 + xy + y^2
-----

```

**ReducedGBasis****SINTAXE**

**ReducedGBasis(I:IDEAL)**

Esta função retorna uma lista cujas componentes formam a Base de Gröbner Reduzida de I com respeito à ordem monomial do anel corrente. O anel dos coeficientes precisa ser um corpo.

**EXEMPLO**

```

Use R ::= Q[t,x,y,z];
ReducedGBasis(I);
[t^3 - x, tx - y, ty - z, y^2 - xz, x^2 - tz, t^2z - xy]
-----

```

Use

### SINTAXE

Use N:RING

'Use' é o comando usado para tornar um anel ativo. O comando

Use N ::= E;

onde E é um anel é o meio prático para

N ::= E;

Use N;

### EXEMPLO

```
Use S ::= Q[x,y,z];
```

```
-----
T ::= Z/(3)[a,b];
```

```
Use T;
```

```
CurrentRing();
```

```
Z/(3)[a,b]
```

## A.2 Exemplos

Utilizaremos o CoCoA para computar

### A.2.1 Exemplo 2.8 - Algoritmo da Divisão

Utilizando  $K = \mathbb{Q}$ , dividiremos  $f = xy^3z^2 + xyz^2$  por  $f_1 = xy - 1$  e  $f_2 = yz^2 - 1$ :

```
Use S::=Q[x,y,z],Lex;
```

```
DivAlg(x*y^3*z^2+x*y*z^2,[x*y-1,y*z^2-1]);
```

```
Record[Quotients = [y^2z^2 + z^2, y], Remainder = y + z^2]
```

Obtendo o resultado esperado. Agora mudamos a ordem da divisão, ou seja, dividiremos  $f = xy^3z^2 + xyz^2$  por  $f_2 = yz^2 - 1$  e  $f_1 = xy - 1$ :

```
Use S::=Q[x,y,z],Lex;
```

```
DivAlg(x*y^3*z^2+x*y*z^2,[y*z^2-1,x*y-1]);
```

```
Record[Quotients = [xy^2 + x, y], Remainder = x + y]
```

Novamente com o resultado esperado.

### A.2.2 Exemplo 2.26

No Exemplo 2.26 ilustramos o algoritmo de Buchberger calculando uma base de Gröbner para  $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$ . Em alguns casos, o processo para de verificação pode tornar-se inviável devido o número de cálculos que serão exigidos. No exemplo em questão, não tínhamos verificado que o resto da divisão de  $S(f_i, f_j)$ , para  $i = 1, 2, 3, 4$  e  $j = i + 1, \dots, 5$  por  $G' = \{f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x, f_3 = -x^2, f_4 = -2xy, f_5 = -2y^2 + x\}$  é zero. Seguem os comandos e o resultado obtido, garantindo que todos os restos são nulos.

```
Use S:=Q[x,y];
F:=[x^3-2*x*y,x^2*y-2*y^2+x,-x^2,-2*x*y,-2*y^2+x];
I:=Ideal(x^3-2*x*y,x^2*y-2*y^2+x,-x^2,-2*x*y,-2*y^2+x);
PrintLn(' ');
For K := 1 To 4 Do
  For J := K+1 To 5 Do
    A:=(LCM(LT(F[K]),LT(F[J]))/LM(F[K]))*F[K] -
      (LCM(LT(F[K]),LT(F[J]))/LM(F[J]))*F[J];
    PrintLn('S(F[' ,K,'],F[' ,J,']) = ',A);
    B:=NF(A,I);
    PrintLn('FN(S(F[' ,K,'],F[' ,J,'])) = ',B);
    PrintLn(' ');
  EndFor;
EndFor;
Print('Onde FN indica a forma normal com respeito ao ideal I.');
```

```
-----
S(F[1],F[2])) = -x^2
FN(S(F[1],F[2])) = 0
```

```
S(F[1],F[3])) = -2xy
FN(S(F[1],F[3])) = 0
```

```
S(F[1],F[4])) = -2xy^2
FN(S(F[1],F[4])) = 0
```

```
S(F[1],F[5])) = 1/2x^4 - 2xy^3
FN(S(F[1],F[5])) = 0
```

```
S(F[2],F[3])) = -2y^2 + x
FN(S(F[2],F[3])) = 0
```

```
S(F[2],F[4])) = -2y^2 + x
FN(S(F[2],F[4])) = 0
```

```
S(F[2],F[5])) = 1/2x^3 - 2y^3 + xy
```

$$\text{FN}(\text{S}(\text{F}[2], \text{F}[5])) = 0$$

$$\text{S}(\text{F}[3], \text{F}[4])) = 0$$

$$\text{FN}(\text{S}(\text{F}[3], \text{F}[4])) = 0$$

$$\text{S}(\text{F}[3], \text{F}[5])) = 1/2x^3$$

$$\text{FN}(\text{S}(\text{F}[3], \text{F}[5])) = 0$$

$$\text{S}(\text{F}[4], \text{F}[5])) = 1/2x^2$$

$$\text{FN}(\text{S}(\text{F}[4], \text{F}[5])) = 0$$

-----  
 Onde FN indica a forma normal com respeito ao ideal I.  
 -----

### A.2.3 Exemplos 2.35 e 2.51

Vimos nos Exemplos 2.35 e 2.51 que a função de Hilbert de  $R = \frac{K[x, y, z]}{\langle xy, xz, yz \rangle}$  é dada por

$$H(R, i) = \begin{cases} 1, & i = 0 \\ 3, & i \geq 1. \end{cases}$$

Seguem os comandos e o resultado obtido utilizando o WinCoCoA, com  $K = \mathbb{Q}$ :

```
Use S:=Q[x,y,z];
I:=Ideal(x*y,x*z,y*z);
R:=S/I;
Hilbert(R);
```

$$H(0) = 1$$

$$H(t) = 3 \quad \text{for } t \geq 1$$

-----

## Referências Bibliográficas

- [1] Atiah, M. F. & MacDonald, J. G., *Introduction to Commutative Algebra*, Adson-Weasley, Reading, 1969.
- [2] Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics 150, Springer-Verlang, New York, 1994.
- [3] Kunz, E., *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser Boston, 1985.
- [4] Cox, D. & Little, J. & O'Shea, D. *Ideals, Varieties and Algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, 1991.
- [5] Bruns, W. & Herzog, J., *Cohen-Macaulay rings*, Cambridge University Press 39, 1993.
- [6] Cox, D. & Little, J. & O'Shea, D. *Using Algebraic Geometry*, Graduate Texts in Mathematics, Springer, 1998.
- [7] Simis, A., *Combinatória Algébrica*, Impa, Rio de Janeiro, 1991.
- [8] Becker, T., Weispfenning, V., Kredel, H., *Gröbner Bases - A Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1993.

## Referências Bibliográficas

- [1] Atiah, M. F. & MacDonald, J. G., *Introduction to Commutative Algebra*, Adson-Weasley, Reading, 1969.
- [2] Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics 150, Springer-Verlang, New York, 1994.
- [3] Kunz, E., *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser Boston, 1985.
- [4] Cox, D. & Little, J. & O'Shea, D. *Ideals, Varieties and Algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, 1991.
- [5] Bruns, W. & Herzog, J., *Cohen-Macaulay rings*, Cambridge University Press 39, 1993.
- [6] Cox, D. & Little, J. & O'Shea, D. *Using Algebraic Geometry*, Graduate Texts in Mathematics, Springer, 1998.
- [7] Simis, A., *Combinatória Algébrica*, Impa, Rio de Janeiro, 1991.
- [8] Becker, T., Weispfenning, V., Kredel, H., *Gröbner Bases - A Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1993.

Lemos, Robinson Alves.

Alguns aspectos computacionais em álgebra comutativa : bases de Gröbner e função de Hilbert / Robinson Alves Lemos - São José do Rio Preto : [s.n.], 2005

71 f. ; 1 il. ; 30 cm.

Orientador: Aparecida Francisco da Silva

Dissertação (mestrado) - Universidade Estadual Paulista. Instituto de Biociências, Letras e Ciências Exatas

1. Álgebra comutativa. 2. Hilbert, Funções de. 3. Gröbner, Bases de. 4. Macaulay, Teorema de. I. Silva, Aparecida Francisco da. II. Universidade Estadual Paulista. Instituto de Biociências, Letras e Ciências Exatas. III. Título.

CDU - 512.71

