HOME EDITORA

BASE DE GRÖBNER: NOÇÕES E APLICAÇÕES

Marcos Pina

BASE GRÖBNER: NOÇÕES E APLICAÇÕES

"Acreditamos que um mundo melhor se faz com a difusão do conhecimento científico".

Equipe Home Editora

Marcos Flávio Oliveira Pina

BASE GRÖBNER: NOÇÕES E APLICAÇÕES

1ª Edição

Belém-PA
Home Editora
2024

Home Editora
CNPJ: 39.242.488/0002-80
www.homeeditora.com
contato@homeeditora.com
91988165332
Tv. Quintino Bocaiúva, 23011 - Batista Campos, Belém - PA, 66045-315

Editor-Chefe
Prof. Dr. Ednilson Ramalho
Projeto gráfico
homeeditora.com
Revisão, diagramação e capa
Autor
Bibliotecária
Janaina Karina Alves Trigo Ramos
CRB-8/009166
Produtor editorial
Laiane Borges

Catalogação na publicação
Elaborada por Bibliotecária Janaina Ramos – CRB-8/9166

P645b

Pina, Marcos Flávio Oliveira

Base Grobnër: noções e aplicações / Marcos Flávio Oliveira Pina. – Belém: Home, 2024.

Livro em PDF
68p.

ISBN 978-65-6089-047-3
DOI 10.46898/home. a4c20acc-afed-4b91-9d42-dbb5d8b1e8db

1. Álgebra computacional. I. Pina, Marcos Flávio Oliveira. II. Título.

CDD 512.243

Índice para catálogo sistemático

I. Álgebra computacional

Agradecimentos

A Deus.

A meu pai por todo apoio e suporte.

A minha filha Giovanna pela motivação.

A minha amiga, namorada e companheira, Rafaela, pelo apoio e paciência.

Ao professor André, meu orientador, pela ajuda, compreensão e paciência.

Aos professores da UFS, Zaqueu e Disson, e aos professores do IFS, Maikon, Crislene, Natanael, Tatiane, Adalgisa e Anselmo, pelo apoio e motivação.

Aos meus amigos Jirlan, João e Rodrigo por sempre me motivarem.

Prefácio

Neste livro estudaremos a teoria das bases de Gröbner no anel de polinômios em várias variáveis sobre um corpo k, o qual denotamos por $k[x_1, \ldots, x_n]$ ou simplesmente $k[\mathbf{x}]$, e no módulo livre $k[x_1, \ldots, x_n]^m$. Veremos também como aplicar essa teoria para determinar a dimensão de um ideal em $k[x_1, \ldots, x_n]$ e calcular o módulo Sizígia e uma resolução livre de um submódulo M em $k[x_1, \ldots, x_n]^m$. Também, usaremos a teoria para demonstrar o Teorema Sizígia de Hilbert, e após isto estenderemos para módulos graduados, usando ainda a teoria das bases de Gröbner.

Sumário

1 Preliminares **1**
1.1 Ordens Monomiais e Divisão em R 1
1.2 Ideais Monomiais 7
1.3 Base de Gröbner 9

2 Base de Gröbner para Submódulos em R^m **18**
2.1 Ordens Monomiais e Divisão em R^m 18
2.2 Base de Gröbner em R^m 23

3 Algumas Aplicações **27**
3.1 Dimensão de um Ideal 27
3.2 Sizígia 33
3.3 Resoluções Livres 42
3.4 Teorema Sizígia de Hilbert 48
3.5 Resoluções Graduadas 51

Introdução

Quando estudamos Estruturas Algébricas vemos que o anel de polinômios com uma variável sobre um corpo k, o qual denominamos por $k[x]$, é um domínio euclidiano e um domínio de ideais principais (DIP). Ou seja, se um ideal $I \subset k[x]$ possui um conjunto com t geradores, $\{f_1, \ldots, f_t\}$, então podemos calcular, usando o algoritmo de divisão, um polinômio $p = \text{MDC}(f_1, \ldots, f_t)$ tal que $I = < f_1, \ldots, f_t > = < p >$. Assim para saber se dado $f \in k[x]$ pertence também ao ideal I basta dividir o polinômio f pelo polinômio p, se o resto dessa divisão for zero, $f \in I$, se for diferente de zero, $f \notin I$.

Mas ao passarmos para o estudo do anel de polinômios em várias variáveis sobre um corpo k, o qual denominados por $k[x_1, \ldots, x_n] = k[\mathbf{x}]$, as coisas não são tão simples. Diferentemente do que vemos em $k[x]$, onde ordenamos os termos de acordo com seu grau, em $k[\mathbf{x}]$ não é bem assim. Por exemplo, em $k[x, y]$, como decidir quem é maior, x^4 ou y^4? Então, antes de pensarmos em um algoritmo de divisão, precisamos saber como ordenar os monômios em $k[\mathbf{x}]$.

Outro problema que também é encontrado ao trabalharmos no anel $k[\mathbf{x}]$ é o fato do mesmo não ser DIP. Ou seja, se $I \subset k[\mathbf{x}]$ é um ideal tal que I é gerado por s polinômios, $\{f_1, \ldots, f_s\}$, não podemos afirmar que exista um polinômio p tal que $p = \text{MDC}(f_1, \ldots, f_s)$ para assim podermos ter $I = < f_1, \ldots, f_s > = < p >$. Assim, para saber se dado $f \in k[\mathbf{x}]$ também pertence ao ideal $I \subset k[\mathbf{x}]$ precisamos dividir f pelo conjunto gerador $\{f_1, \ldots, f_s\}$, mas ao realizarmos essa divisão notamos que o resto não é único, independentemente de como se realize a divisão.

Buscando um conjunto de geradores para o ideal $I \subset k[\mathbf{x}]$, de modo que ao dividirmos dado $f \in k[\mathbf{x}]$ por esse conjunto obtenhamos a unicidade do resto, surge a teoria da base de Gröbner, introduzida em 1965 por Bruno Buchberger. Onde teremos um conjunto de geradores, $G = \{g_1, \ldots, g_s\}$, para I, de modo que f pertence a I se, e somente se, ao dividir f por G, o resto é zero.

O mesmo problema visto em $k[\mathbf{x}]$, também é encontrado no módulo livre sobre $k[\mathbf{x}]$. Isto é, dado um conjunto qualquer de geradores para um submódulo $M \subset k[\mathbf{x}]^m$, não teremos a unicidade do resto ao dividir um elemento $p \in k[\mathbf{x}]^m$ por qualquer conjunto gerador de M. Assim a teoria da base de Gröbner pôde também ser estendida para o módulo livre $k[\mathbf{x}]^m$, de modo a termos um conjunto de geradores para qualquer submódulo M, $H = \{h_1, \ldots, h_r\}$, onde ao dividir dado $f \in M$ por H, o resto sempre será zero.

A teoria possui aplicações nos mais diversos campos, aqui estaremos preocupados em suas aplicações na Álgebra Comutativa. Usaremos dela para calcular a dimensão de um ideal $I \subset k[\mathbf{x}]$ e como ferramenta para encontrar o Módulo Sizígia e uma Resolução Livre de qualquer submódulo $M \subset k[\mathbf{x}]^m$. E por fim a teoria será usada para demonstrar o Teorema

Sizígia de Hilbert.

No primeiro capítulo estudaremos ordens monomiais em $k[\mathbf{x}]$ e estenderemos o algoritmo de divisão visto em $k[x]$ para $k[\mathbf{x}]$. Após isso estudaremos ideais monomiais e as Bases de Gröbner com suas propriedades para $k[\mathbf{x}]$. Já no segundo capítulo, estenderemos a teoria da base de Gröbner para submódulos $M \subset k[\mathbf{x}]^m$, definindo uma ordem monomial em $k[\mathbf{x}]^m$, um algoritmo de divisão e as bases de Gröbner para qualquer submódulo $M \subset k[\mathbf{x}]^m$. E por fim, no terceiro capítulo, veremos as aplicações mencionadas, onde na última seção, estendemos as Resoluções Livres e o Teorema Sizígia de Hilbert para módulos graduados.

Capítulo 1

Preliminares

Ao longo deste capítulo veremos como estabelecer uma ordem monomial no anel de polinômios em n variáveis sobre um corpo k, $k[\mathbf{x}]$, e a partir dai, determinar um algoritmo de divisão e definir uma base de Gröbner para um ideal em $k[\mathbf{x}]$.

Antes disto relembremos que uma relação $\Re$ sobre um conjunto S é uma **relação de ordem** se

i. Para todo $x \in S$ temos $x\Re x$ ($\Re$ reflexiva);

ii. Para todo $x, y \in S$, se $x\Re y$ e $y\Re x$, então $x = y$ ($\Re$ é antissimétrica);

iii. Para todo $x, y, z \in S$, se $x\Re y$ e $y\Re z$ então $x\Re z$ ($\Re$ é transitiva).

Alguns exemplos de relação são $\leq$ e $\geq$ sobre $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$ e $|$ sobre $\mathbb{N}$.

Lembremos também que uma relação de ordem $\Re$ sobre um conjunto S é dita **relação de ordem total** se para qualquer $x, y \in S$, tivermos $x\Re y$ ou $y\Re x$.

Denotaremos R o anel $k[\mathbf{x}]$ e por $\mathbf{x}^\alpha$ o **monômio** $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ em $k[\mathbf{x}]$, onde $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_+^n$.

1.1 Ordens Monomiais e Divisão em R

Sabemos que no anel de polinômios com uma variável sobre um corpo k, $k[x]$, temos a divisão Euclidiana. Para estender esse algoritmo em R precisamos primeiramente considerar uma maneira de ordenar os monômios nele contidos.

Definição 1.1.1. *Uma **Ordem Monomial** em R é uma relação $>$ no conjunto de monômios $\mathbf{x}^\alpha$ em R (ou equivalentemente nos expoentes $\alpha \in \mathbb{Z}_+^n$) satisfazendo:*

i. $>$ é uma relação de ordem total;

ii. $>$ é compatível com a multiplicação em R, ou seja, se $\mathbf{x}^\alpha > \mathbf{x}^\beta$ e $\mathbf{x}^\lambda$ é qualquer monômio, então $\mathbf{x}^\alpha \mathbf{x}^\lambda > \mathbf{x}^\beta \mathbf{x}^\lambda$;

iii. $>$ é bem-ordenada, ou seja, toda coleção não vazia de monômios tem um elemento mínimo em $>$.

Lema 1.1.2. *Uma relação de ordem $>$ sobre $\mathbb{Z}_+^n$ é bem-ordenada se, e somente se, toda sequência estritamente decrescente em $\mathbb{Z}_+^n$*

$$\alpha_1 > \alpha_2 > \alpha_3 > \dots$$

é finita.

Demonstração. Mostraremos que existe uma sequência infinita estritamente decrescente em $\mathbb{Z}_+^n$ se, e somente se, $>$ não é bem-ordenada em $\mathbb{Z}_+^n$. Suponhamos primeiramente que $>$ não é bem-ordenada em $\mathbb{Z}_+^n$, então algum subconjunto não vazio $S \subset \mathbb{Z}_+^n$ não tem elemento minimal. Considere $\alpha_1 \in S$, como α_1 não é elemento minimal de S, temos que existe $\alpha_2 \in S$ tal que $\alpha_1 > \alpha_2$. Continuando esse processo, construiremos a sequência

$$\alpha_1 > \alpha_2 > \alpha_3 > \dots,$$

ou seja, uma sequência infinita estritamente decrescente.

Reciprocamente, suponhamos que $S = \{\alpha_1, \alpha_2, \alpha_3, \dots\} \subset \mathbb{Z}_+^n$ seja o conjunto formado pelos elementos da sequência infinita estritamente decrescente. Então S não tem um elemento mínimo, logo $>$ não é bem-ordenada. □

Temos assim que se $>$ é uma ordem monomial, então os monômios que aparecem em um polinômio $p \in R$ podem ser ordenados de forma crescente ou decrescente (por a) e em um processo de divisão (mais detalhes na Proposição 1.1.11), o mesmo possui um número finito de etapas (por c).

Temos abaixo algumas ordens monomiais usuais.

Definição 1.1.3 (**Ordem Lexicográfica**). *Sejam $\mathbf{x}^\alpha$ e $\mathbf{x}^\beta$ monômios em R. Dizemos que $\mathbf{x}^\alpha >_{lex} \mathbf{x}^\beta$ se na diferença $\alpha - \beta \in \mathbb{Z}^n$ a primeira entrada diferente de zero da esquerda para a direita é positiva.*

Definição 1.1.4 (**Ordem Lexicográfica Reversa**). *Sejam $\mathbf{x}^\alpha$ e $\mathbf{x}^\beta$ monômios em R. Dizemos que $\mathbf{x}^\alpha >_{revlex} \mathbf{x}^\beta$ se na diferença $\alpha - \beta \in \mathbb{Z}^n$ a primeira entrada diferente de zero da direita para a esquerda é positiva.*

Definição 1.1.5 (**Ordem Lexicográfica Graduada**). *Sejam $\mathbf{x}^\alpha$ e $\mathbf{x}^\beta$ monômios em R. Dizemos que $\mathbf{x}^\alpha >_{grlex} \mathbf{x}^\beta$ 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 $\mathbf{x}^\alpha >_{lex} \mathbf{x}^\beta$.*

Definição 1.1.6 (**Ordem Lexicográfica Graduada Reversa**). *Sejam $\mathbf{x}^\alpha$ e $\mathbf{x}^\beta$ monômios em R. Dizemos que $\mathbf{x}^\alpha >_{grevlex} \mathbf{x}^\beta$ 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 $\mathbf{x}^\alpha >_{revlex} \mathbf{x}^\beta$.*

Notemos que a ordem lexicográfica é análoga a ordem usada para ordenar as palavras no dicionário.

Exemplo 1.1.7. *Sejam x^3y^2z, $x^2y^6z^{12}$ e $x^2y^2z^2$ monômios em R, com $x > y > z$, logo:*

- $x^3y^2z >_{lex} x^2y^6z^{12} >_{lex} x^2y^2z^2$ *pois nas diferenças dos vetores expoentes,*

$$(3,2,1) - (2,6,12) = (1,-4,-11)$$

e

$$(2,6,12) - (2,2,2) = (0,4,10),$$

as primeiras coordenadas da esquerda para a direita são positivas;

- $x^2y^6z^{12} >_{revlex} x^2y^2z^2 >_{revlex} x^3y^2z$ *pois nas diferenças dos vetores expoentes*

$$(2,6,12) - (2,2,2) = (0,4,10)$$

e

$$(2,2,2) - (3,2,1) = (-1,0,1),$$

as primeiras coordenadas da direita para a esquerda são positivas;

- $x^2y^6z^{12} >_{grlex} x^3y^2z >_{grlex} x^2y^2z^2$ *pois na soma dos expoentes temos* $20 > 6$ *e na segunda relação temos*

$$3+2+1 = 2+2+2 \text{ e } x^3y^2z >_{lex} x^2y^2z^2;$$

- $x^2y^6z^{12} >_{grevlex} x^2y^2z^2 >_{grevlex} x^3y^2z$ *pois na soma dos expoentes temos* $20 > 6$ *e na segunda relação temos*

$$2+2+2 = 3+2+1 \text{ e } x^2y^2z^2 >_{revlex} x^3y^2z.$$

Definição 1.1.8. *Seja* $f = \sum a_\alpha \mathbf{x}^\alpha$ *um polinômio não nulo em* R *e* $>$ *uma ordenação monomial.*

i. O multigrau de f *é*

$$MG(f) := \max\{\alpha \in \mathbb{Z}_+^n; a_\alpha \neq 0\},$$

onde o máximo é escolhido com respeito a $>$*;*

ii. O coeficiente líder de f *é*

$$CL(f) := a_{MG(f)} \in k \ ;$$

iii. O monômio líder de f *é*

$$ML(f) := \mathbf{x}^{MG(f)};$$

iv. O termo líder de f *é*

$$TL(f) := CL(f).ML(f).$$

Definimos $CL(0) = ML(0) = TL(0) = 0$.

Exemplo 1.1.9. *Consideremos* $f = 4x^2yz^3 + 2x^2y^3z - 5x^3y + x^3z \in \mathbb{Q}[x, y, z]$, *com as variáveis ordenadas usualmente* $(x > y > z)$. *Usando a ordem lexicográfica temos que* $MG(f) = (3, 1, 0)$, $CL(F) = -5$, $ML(f) = x^3y$ *e* $TL(f) = -5x^3y$. *Agora usando a ordem lexicográfica reversa temos* $MG(f) = (3, 0, 1)$, $CL(F) = 1$, $ML(f) = x^3z$ *e* $TL(f) = x^3z$. *Na ordem lexicográfica graduada temos que* $MG(f) = (2, 2, 1)$, $CL(F) = 2$, $ML(f) = x^2y^3z$ *e* $TL(f) = 2x^3y^2$. *E na ordem lexicográfica graduada reversa temos* $MG(f) = (2, 1, 3)$, $CL(f) = 4$, $ML(f) = x^2yz^3$ *e* $TL(f) = 4x^2yz^3$.

Consideraremos que o anel de polinômios R estará sempre munido de uma ordenação das variáveis e de uma ordem monomial fixada.

Lema 1.1.10. *Sejam* $f, g \in R$ *polinômios não-nulos.*

a. $MG(f.g) = MG(f) + MG(g)$;

b. Se $f + g \neq 0$, *então* $MG(f + g) \leq \max\{MG(f), MG(g)\}$. *Além disso, se* $MG(f) \neq MG(g)$, *então*

$$MG(f + g) = \max\{MG(f), MG(g)\},$$

e, se $MG(f) = MG(g)$ *com* $TL(f) = -TL(g)$, *então*

$$MG(f + g) < \max\{MG(f), MG(g)\}.$$

Demonstração.

a. Podemos supor que $f = \sum_{i=1}^{n} a_i\mathbf{x}^{\alpha_i}$ e $g = \sum_{j=1}^{m} b_j\mathbf{x}^{\beta_j}$, onde $MG(f) = \alpha_1$ e $MG(g) = \beta_1$. Assim

$$\begin{aligned} f.g &= \sum_{i=1}^{n} a_i\mathbf{x}^{\alpha_i}.\sum_{j=1}^{m} b_j\mathbf{x}^{\beta_j} = \sum_{i=1}^{n}\sum_{j=1}^{m} a_ib_j\mathbf{x}^{\alpha_i+\beta_j} \\ &= \sum_{i=1}^{n} a_ib_1\mathbf{x}^{\alpha_i+\beta_1} + \sum_{i=1}^{n}\sum_{j=2}^{m} a_ib_j\mathbf{x}^{\alpha_i+\beta_j} \\ &= a_1b_1\mathbf{x}^{\alpha_1+\beta_1} + \sum_{i=2}^{n} a_ib_2\mathbf{x}^{\alpha_i+\beta_2} + \sum_{i=1}^{n}\sum_{j=2}^{m} a_ib_j\mathbf{x}^{\alpha_i+\beta_j}. \end{aligned}$$

Como $\alpha_1 + \beta_1 \geq \alpha_i + \beta_j$ para todo $1 \leq i \leq n$, $1 \leq j \leq m$ e $a_1b_1 \neq 0$ (pois k é corpo), então

$$MG(f.g) = \alpha_1 + \beta_1 = MG(f) + MG(g).$$

b. Se f e g são polinômios tais que $f+g \neq 0$, então o $MG(f+g)$ está definido. Suponhamos a princípio que $MG(f) \neq MG(g)$. Neste caso, é fácil ver que

$$MG(f + g) = \max\{MG(f), MG(g)\}.$$

Entretanto, se $MG(f) = MG(g)$ temos que analisar duas possibilidades:

1. $TL(f) = -TL(g)$.
   Neste caso, os termos líderes se anulam e, por isso,
   $$MG(f+g) < MG(f) = MG(g),$$
   ou seja,
   $$MG(f+g) < \max\{MG(f), MG(g)\}.$$
2. $TL(f) \neq -TL(g)$.
   Neste caso, os termos líderes não se anula e, por isso,
   $$MG(f+g) = MG(f) = MG(g).$$

□

Por fim, apresentaremos um algorítmo para a divisão em R.

Proposição 1.1.11. *Seja $F = \{f_1, \ldots, f_s\}$ um conjunto de polinômios não nulos em R. Então todo $f \in R$ pode ser escrito da forma*

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

onde $a_i \in R$ e $r = 0$ ou r é uma combinação linear de monômios com coeficientes em k, de modo que nenhum deles é divisível por algum termo líder de $f_1, \ldots, f_s$. Chamaremos r de resto de f numa divisão por F. Além disso,

$$ML(f) = \max\{\max\{ML(a_i)ML(f_i)\}, ML(r)\},$$

$i \in \{i, \ldots, s\}$.

Demonstração. Podemos ter as seguintes situações:

(A_1) existe $TL(f_i)$ que divide $TL(f)$;

(B_1) não existe $TL(f_i)$ que divida $TL(f)$,

onde $i = \{1, \ldots, s\}$. Caso ocorra (A_1) para mais de um f_i, seja f_{i_1} qualquer um deles. Definamos

$$p_1 = \begin{cases} f - \dfrac{TL(f)}{TL(f_{i_1})} f_{i_1}, & \textit{caso ocorra } (A_1) \\ f - TL(f), & \textit{caso ocorra } (B_1) \end{cases}.$$

Em todo caso, podemos escrever

$$f = a_{i_1} f_{i_1} + p_1 + r_1,$$

onde $a_{i_1} = \dfrac{TL(f)}{TL(f_{i_1})}$ e $r_1 = 0$, caso ocorra (A_1), ou $a_{i_1} = 0$ e $r_1 = TL(f)$, caso ocorra (B_1). Notemos que r_1 é uma combinação linear de monômios tais que nenhum deles é divisível por algum termo líder de $f_1, \ldots, f_s$.

Se $TL(f_i)$ não divide nenhum termo de p_1, para qualquer $i \in \{1, \ldots, s\}$, ou $p_1 = 0$, então a proposição fica provada, basta fazer $r = p_1 + r_1$. Caso contrário, temos as seguintes situações:

(A_2) existe $TL(f_i)$ que divide $TL(p_1)$;

(B_2) não existe $TL(f_i)$ que divida $TL(p_1)$.

Tomemos f_{i_2} do mesmo modo que f_{i_1} e definamos

$$p_2 = \begin{cases} p_1 - \dfrac{TL(p_1)}{TL(f_{i_2})} f_{i_2} & \textit{caso ocorra } (A_2) \\ p_1 - TL(p_1) & \textit{caso ocorra } (B_2) \end{cases}.$$

Em todo caso podemos escrever

$$f = a_{i_1} f_{i_1} + a_{i_2} f_{i_2} + p_2 + r_1 + r_2,$$

onde $a_{i_2} = \dfrac{TL(p_1)}{TL(f_{i_2})}$ e $r_2 = 0$, caso ocorra (A_2), ou $a_{i_2} = 0$ e $r_2 = TL(p_1)$, caso ocorra (B_2). Além disso, $r_1 + r_2$ tem a mesma propriedade do r_1 descrita acima.

Se $TL(f_i)$ não divide nenhum termo de p_2, para qualquer $i \in \{1, \ldots, s\}$, ou $p_2 = 0$, então a proposição está provada, bastando fazer $r = p_2 + r_1 + r_2$. Caso contrário, de maneira análoga construímos um p_3 e assim sucessivamente. Observemos que se $p_j = 0$ para algum $j \in \mathbb{Z}_+$ implica na proposição provada. Suponhamos então que esse processo não terminasse. Teríamos assim uma sequência de $p_j's$ tais que $p_j \neq 0$ para todo j, aplicando o Lema 1.1.10 e pela forma que os $p_j's$ são definidos, temos

$$MG(p_j) > MG(p_{j+1}).$$

Obtendo assim uma sequência infinita estritamente decrescente em $\mathbb{Z}_+^n$,

$$MG(p_1) > MG(p_2) > \ldots,$$

o que implica que $>$ não é bem-ordenada, pelo Lema 1.1.2. Gerando um absurdo, visto que a ordem monomial $>$ é bem-ordenada. Logo, devemos chegar a uma certa etapa l em que $p_l = 0$ e consequentemente, o processo de construção dos p_j deve encerrar nessa etapa e teremos $f = a_1 f_1 + \ldots + a_s f_s + r$, onde $r = r_1 + \ldots + r_s$.

Para a segunda parte, observemos que se A_1 ocorrer, então $ML(f) = ML(a_{i_1})ML(f_{i_1})$, e caso A_1 não ocorrer, temos $ML(f) = ML(r)$. □

Denotaremos por $\bar{f}^F$ o resto da divisão de f por F.

Exemplo 1.1.12. *Sejam $f = xy^2 - x$ e $I \subset \mathbb{C}[x, y]$ o ideal gerado por $\{xy + 1, y^2 - 1\}$. Considerando a ordem monomial lexicográfica e dividindo f por $f_1 = xy + 1$ e $f_2 = y^2 - 1$, temos duas possibilidades:*

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

e

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

O exemplo acima esclarece que o resto pode não ser único. Já que, um ideal não nulo admite mais de um conjunto de geradores. Uma pergunta natural seria saber se existe um conjunto de geradores do ideal de tal forma que tivéssemos a unicidade do resto. Tal pergunta será respondida na Proposição 1.3.3.

1.2 Ideais Monomiais

Os ideais que apresentaremos nesta seção desempenham um papel fundamental para encontrarmos um conjunto de geradores G para um ideal $I \subset R$, de tal forma que ao dividirmos dado $f \in R$ por G, obtermos a unicidade do resto.

Definição 1.2.1. *Um ideal $I \subset R$ é dito um **ideal monomial** quando admite um conjunto de monômios que geram I.*

Ou seja, existe um subconjunto $A \subset \mathbb{Z}_+^n$ de modo que I consiste de todos os polinômios que são somas finitas da forma $\sum_{\alpha \in A} h_\alpha \mathbf{x}^\alpha$, onde $h_\alpha \in R$, $\alpha \in A$. Escrevemos $I =< \mathbf{x}^\alpha; \alpha \in A >$.

Lema 1.2.2. *Seja $I =< \mathbf{x}^\alpha; \alpha \in A >$ um ideal monomial. Um monômio $\mathbf{x}^\beta \in I$ se, e somente se, $\mathbf{x}^\beta$ é divisível por $\mathbf{x}^\alpha$, para algum $\alpha \in A \subset \mathbb{Z}_+^n$.*

Demonstração. Suponhamos que $\mathbf{x}^\beta$ é múltiplo de $\mathbf{x}^\alpha$, então, pela definição de ideal, $\mathbf{x}^\beta \in I$.

Reciprocamente, seja $\mathbf{x}^\beta \in I$, assim $\mathbf{x}^\beta = \sum_{i=1}^{s} h_i \mathbf{x}^{\alpha_i}$, onde $h_i \in R$ e $\alpha_i \in A$. Distribuindo os produtos, agrupando os termos semelhantes e eliminando os termos nulos, temos

$$\mathbf{x}^\beta = \sum_{j=1}^{t} a_{\gamma_j} \mathbf{x}^{\gamma_j},$$

onde $a_{\gamma_j} \in k$ e $\mathbf{x}^{\gamma_j}$ é divisível por algum $\mathbf{x}^{\alpha_i}$. Como o lado esquerdo da igualdade é um monômio, então o lado direito também é, assim $t = 1$ e $a_{\gamma_1} = 1$, ou seja,

$$\mathbf{x}^\beta = \mathbf{x}^{\gamma_1}.$$

Visto que algum $\mathbf{x}^{\alpha_i}$ divide $\mathbf{x}^{\gamma_1}$, segue que $\mathbf{x}^{\alpha_i}$ divide $\mathbf{x}^\beta$. □

Proposição 1.2.3. *Seja I um ideal monomial e seja $f \in R$. São equivalentes:*

a. $f \in I$;

b. Todo termo de f pertence a I;

c. f é uma combinação linear de monômios em I.

Demonstração. Notemos que as implicações $c \Rightarrow b \Rightarrow a$ são triviais, assim, basta mostrar que $a \Rightarrow c$.

Por hipótese, I é um ideal monomial. Suponhamos que $f \in I =< \mathbf{x}^\alpha; \alpha \in A \subset \mathbb{Z}_+^n >$, logo

$$f = \sum_{i=1}^{s} h_i \mathbf{x}^{\alpha_i},$$

onde $h_i \in R$ e $\alpha_i \in A$. Efetuando os produtos, agruparmos os termos semelhantes e eliminando os termos nulos, temos

$$f = \sum_{j=1}^{t} a_{\gamma_j} \mathbf{x}^{\gamma_j},$$

onde $a_{\gamma_j} \in k$ e cada termo do lado direito da igualdade é divisível por algum $\mathbf{x}^{\alpha_i}$. Assim, pelo Lema 1.2.2, cada parcela de f pertence a I, portanto f é uma combinação linear de monômios de I. □

Uma consequência da Proposição acima é

Corolário 1.2.4. *Dois ideais monomiais são iguais se, e somente se, contêm os mesmos monômios.*

Antes de seguimos com o próximo resultado, iremos lembrar do seguinte conceito: um anel A (comutativo) é dito **Noetheriano** quando todo ideal $I \subset A$ é finitamente gerado. Sabemos que todo corpo é Noetheriano, assim o Teorema da Base de Hilbert (mais detalhes, veja em [1], capítulo 7) nos garante que R é um anel Noetheriano.

Lema 1.2.5 (Lema de Dickson)**.** *Um ideal monomial* $I =< \mathbf{x}^{\alpha}; \alpha \in A >\subset R$ *pode ser escrito da forma*

$$I =< \mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_s} >,$$

onde $\alpha_1, \ldots, \alpha_s \in A \subset \mathbb{Z}_+^n$.

Demonstração. Sabemos que R é um anel Noetheriano, logo I é finitamente gerado. Seja então $I =< g_1, \ldots, g_t >$, onde $g_i \in R$, $i \in \{1, \ldots, t\}$. Como $g_i \in I =< \mathbf{x}^{\alpha}; \alpha \in A >$, então $g_i = \sum_{j=1}^{l_i} a_{i_j}\mathbf{x}^{\beta_{i_j}}$, com $a_{i_j} \in R$, ou seja, podemos tomar

$$I =< \mathbf{x}^{\beta_{1_1}}, \ldots, \mathbf{x}^{\beta_{1_{l_1}}}, \ldots, \mathbf{x}^{\beta_{t_1}}, \ldots, \mathbf{x}^{\beta_{t_{l_t}}} > .$$

Visto que $I \subset< \mathbf{x}^{\beta_{1_1}}, \ldots, \mathbf{x}^{\beta_{1_{l_1}}}, \ldots, \mathbf{x}^{\beta_{t_1}}, \ldots, \mathbf{x}^{\beta_{t_{l_t}}} >$ e que dado

$$f \in< \mathbf{x}^{\beta_{1_1}}, \ldots, \mathbf{x}^{\beta_{1_{l_1}}}, \ldots, \mathbf{x}^{\beta_{t_1}}, \ldots, \mathbf{x}^{\beta_{t_{l_t}}} >,$$

temos pela pela Proposição 1.2.3 que $f \in I$, ou seja,

$$< \mathbf{x}^{\beta_{1_1}}, \ldots, \mathbf{x}^{\beta_{1_{l_1}}}, \ldots, \mathbf{x}^{\beta_{t_1}}, \ldots, \mathbf{x}^{\beta_{t_{l_t}}} >\subset I.$$

Pelo Lema 1.2.2 temos que cada $\mathbf{x}^{\beta_{i_j}}$ é divisível por algum $\mathbf{x}^{\alpha}$, com $\alpha \in A$. Enumerando os $\alpha' s$ de 1 até s, segue que $I =< \mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_s} >$.

□

Definição 1.2.6. *Seja $I \subset R$ um ideal.*

i. Denotamos por $TL(I)$ o conjunto formado pelos termos líderes de I, isto é,

$$TL(I) = \{c\mathbf{x}^{\alpha}; \exists\ f \in I \text{ com } TL(f) = c\mathbf{x}^{\alpha}\};$$

ii. Denotamos por $< TL(I) >$ o ideal gerado pelos elementos de $TL(I)$.

Notemos que no caso de I ser o ideal nulo, temos $TL(I) = \{0\}$.

Proposição 1.2.7. *Seja $I \subset R$ um ideal.*

a. $< TL(I) >$ *é um ideal monomial;*

b. Existem $g_1, \ldots, g_s \in I$ *tais que* $< TL(I) >=< TL(g_1), \ldots, TL(g_s) >$.

Demonstração. Notemos que se I é o ideal nulo então a e b são triviais. Assim, seja I um ideal não nulo.

a. Os monômios líderes de elementos $f \in I - \{0\}$ geram o ideal monomial

$$< ML(f) : f \in I - \{0\} > .$$

Note que $TL(f)$ e $ML(f)$ se diferem apenas por uma constante não-nula, logo

$$< ML(f) : f \in I - \{0\} >=< TL(f) : f \in I - \{0\} >=< TL(I) >,$$

ou seja, $< TL(I) >$ é um ideal monomial.

b. Observemos que $< TL(I) >$ é gerado por monômios $ML(g)$, com $g \in I - \{0\}$. Assim, pelo Lema de Dickson, temos

$$< TL(I) >=< ML(g_1), \ldots, ML(g_s) >,$$

onde $g_i \in I$, $i \in \{i, \ldots, s\}$ Como $ML(g_i)$ e $TL(g_i)$ se diferem apenas por uma constante não-nula, concluímos que

$$< TL(I) >=< TL(g_1), \ldots, TL(g_s) > .$$

□

1.3 Base de Gröbner

Para resolvermos o problema de determinar se um elemento $f \in R$ pertence a um ideal $I \subset R$, o resto ser zero, ao dividir f por um conjunto qualquer de geradores de I, usando o algoritmo da divisão (Proposição 1.1.11), não é condição necessária. Contudo existe um conjunto gerador de I de modo que $r = 0$ independente da ordem que se realize no algoritmo da divisão. Ou seja, um conjunto gerador, onde não ocorra o que vimos no Exemplo 1.1.12.

Definição 1.3.1. *Seja* $I \subset R$ *um ideal não nulo. Uma* ***base de Gröbner*** *para* I *(com respeito a ordem monomial fixada) é uma coleção finita de polinômios* $G = \{g_1, \ldots, g_s\} \subset I$ *com a propriedade de que para todo* $f \in I$, $TL(f)$ *é divisível por* $TL(g_i)$ *para algum* $i \in \{1, \ldots, s\}$, *ou seja,*

$$< TL(g_1), \ldots, TL(g_s) >=< TL(I) > .$$

Se I é o ideal nulo, então tomamos $G = \emptyset$ por convenção.

Lema 1.3.2. *Todo ideal* $I \subset R$ *tem uma base de Gröbner. Além disso, se* $G = \{g_1, \ldots, g_s\}$ *é uma base de Gröbner para* I, *temos que* $I =< g_1, \ldots, g_s >$.

Demonstração. Se I é o ideal nulo, temos que $G = \emptyset$. Seja então I um ideal não nulo, notemos que por b da Proposição 1.2.7, existem $g_1, \ldots, g_s \in I$ tais que

$$< TL(I) >=< TL(g_1), \ldots, TL(g_s) > .$$

Assim provamos a existência de uma base de Gröbner.

Agora vamos provar a segunda parte do Lema. Observemos primeiramente que

$$< g_1, \ldots, g_s > \subset I,$$

pois cada $g_i \in I$. Reciprocamente, seja $f \in I$, então dividindo f por $g_1, \ldots, g_s$ chegaremos a uma expressão do tipo

$$f = a_1 g_1 + \ldots + a_s g_s + r,$$

onde $r = 0$ ou r é uma combinação linear de monômios com coeficientes em k, de modo que nenhum deles é divisível por algum termo líder de $g_1, \ldots, g_s$. Reescrevendo a expressão acima de modo conveniente, temos que

$$r = f - a_1 g_1 - \ldots - a_s g_s.$$

Se $r \neq 0$, então $TL(r) \in < TL(I) >=< TL(g_1), \ldots, TL(g_s) >$. Assim, pelo Lema 1.2.2 temos que $TL(r)$ é divisível por algum $TL(g_i)$, o que é uma contradição. Logo $r = 0$ e assim

$$f = a_1 g_1 + \ldots + a_s g_s,$$

ou seja, $f \in < g_1, \ldots, g_s >$, então $I \subset < g_1, \ldots, g_s >$. Portanto $I =< g_1, \ldots, g_s >$ □

A base de Gröbner possui a propriedade que nos permite identificar se dado elemento f em R pertence ou não a um ideal $I \subset R$.

Proposição 1.3.3. *Seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner para um ideal $I \subset R$ e seja $f \in R$. Então, existe um único $r \in R$ tal que:*

a. Nenhum termo de r é divisível por algum $TL(g_1), \ldots, TL(g_s)$;

b. 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 estão ordenados quando usamos o algorítmo da divisão.

Demonstração. Vamos mostrar a existência e a unicidade.

- *Existência:* Pelo algoritmo da divisão temos que

  $$f = a_1 g_1 + \ldots + a_s g_s + r.$$

  Assim r satisfaz a. Como $g_i \in I$, então $a_1 g_1 + \ldots + a_s g_s = g \in I$, logo $f = g + r$, o que verifica b.

- *Unicidade:* Suponhamos que existam g_1, g_2, r_1, r_2 tais que $f = g_1 + r_1 = g_2 + r_2$ satisfazendo a e b. Assim, $r_2 - r_1 = g_1 - g_2 \in I$. Se $r_1 \neq r_2$, então

$$TL(r_2 - r_1) \in < TL(I) > = < TL(g_1), \ldots, TL(g_s) > .$$

  Deste modo, pelo Lema 1.2.2, concluímos que $TL(r_2 - r_1)$ é divisível por algum $TL(g_i)$, $i \in \{1, \ldots, s\}$, o que é uma contradição, pois nenhum termo de r_1 ou r_2 é divisível por $TL(g_i)$. Assim, $r_1 - r_2 = 0$, ou seja, $r_1 = r_2$

□

Essa proposição nos garante que ao dividir $f \in I$ por uma base de Gröbner o resto é único. Mas os quocientes $a_i \in R$ produzidos na divisão, $f = a_1 g_1 + \ldots + a_s g_s$, podem ser diferentes.

Corolário 1.3.4. *Seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner para o ideal $I \subset R$ e seja $f \in R$. Então $f \in I$ se, e somente se, o resto da divisão de f por G é zero.*

Demonstração. Seja r o resto da divisão de f por G. Se $r = 0$, então $f = a_1 g_1 + \ldots + a_s g_s \in I$.

Reciprocamente, se $f \in I$, então da igualdade $f = f + 0$ e da Proposição 1.3.3, temos que o resto da divisão de f por G é zero. □

Definição 1.3.5. *Sejam $f, g \in R$ polinômios não nulos tais que*

$$TL(f) = c\mathbf{x}^\alpha \text{ e } TL(g) = d\mathbf{x}^\beta,$$

*onde $c, d \in k$ e $\alpha, \beta \in \mathbb{Z}_+^n$. Seja $\mathbf{x}^\gamma$ o mínimo múltiplo comum (*MMC*) de $\mathbf{x}^\alpha$ e $\mathbf{x}^\beta$. O* ***S-Polinômio*** *de f e g, denotado por $S(f, g)$, é o polinômio*

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

Exemplo 1.3.6. *Sejam $f = x^3y - 2x^2y^2 + x$ e $g = 3x^4 - y$ em $\mathbb{Q}[x, y]$. Usando a ordem monomial lexicográfica, temos que $TL(f) = x^3y$ e $TL(g) = 3x^4$, logo o* MMC$(x^3y, x^4) = x^4y$ *e assim*

$$\begin{aligned} S(f, g) &= \frac{x^4y}{x^3y}(x^3y - 2x^2y^2 + x) - \frac{x^4y}{3x^4}(3x^4 - y) \\ &= x(x^3y - 2x^2y^2 + x) - \frac{y}{3}(3x^4 - y) \\ &= x^4y - 2x^3y^2 + x^2 - x^4y + \frac{y^2}{3} \\ &= -2x^3y^2 + x^2 + \frac{y^2}{3}. \end{aligned}$$

Notemos que o S-polinômio $S(f, g)$ é constituído de modo que haja cancelamento de termos líderes.

Lema 1.3.7. *Considere a soma* $\sum_{i=1}^{s} c_i f_i$, *onde* $c_i \in k$ *e* $MG(f_i) = \delta \in \mathbb{Z}_+^n$ *para todo* $i = 1, \ldots, s$. *Se*

$$MG\left(\sum_{i=1}^{s} c_i f_i\right) < \delta,$$

então $\sum_{i=1}^{s} c_i f_i$ *é uma combinação linear com coeficientes em* k *dos S-polinômios* $S(f_j, f_t)$, *para* $1 \leq j, t \leq s$. *Além disso,* $MG(S(f_j, f_t)) < \delta$.

Demonstração. Seja $d_i = CL(f_i)$, para todo $i \in \{1, \ldots, s\}$, assim $c_i d_i$ é o coeficiente líder de $c_i f_i$. Visto que $MG(c_i f_i) = \delta$, para $c_i \neq 0$, e que $MG\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$, então o coeficiente relacionado a δ é zero, ou seja, $\sum_{i=1}^{s} c_i d_i = 0$.

Consideremos $p_i = \dfrac{f_i}{d_i}$ (observemos que $CL(p_i) = 1$) e a soma

$$\begin{aligned} \sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i d_i p_i \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \ldots + \\ &\quad (c_1 d_1 + \ldots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \ldots + c_s d_s) p_s. \end{aligned} \tag{1.1}$$

Por hipótese, $TL(f_i) = d_i \mathbf{x}^\delta$. Logo, o MMC$(ML(f_i), ML(f_t)) = \mathbf{x}^\delta$ e portanto

$$\begin{aligned} S(f_j, f_t) &= \frac{\mathbf{x}^\delta}{TL(f_j)} f_j - \frac{\mathbf{x}^\delta}{TL(f_t)} f_t \\ &= \frac{\mathbf{x}^\delta}{d_j \mathbf{x}^\delta} f_j - \frac{\mathbf{x}^\delta}{d_t \mathbf{x}^\delta} f_t \\ &= p_j - p_t. \end{aligned}$$

Usando esta equação e o fato de $\sum_{i=1}^{s} c_i d_i = 0$, temos que a soma 1.1 se torna

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \ldots + (c_1 d_1 + \ldots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s).$$

Para a segunda parte, como p_j e p_t têm multigrau δ e coeficiente líder 1, então $MG(p_j - p_t) < \delta$. Visto que $S(f_j, f_t) = p_j - p_t$, então $MG(S(f_j, f_t)) < \delta$. □

Proposição 1.3.8 (Critério de Buchberger)**.** *Seja* $I =< g_1, \ldots, g_s >$ *um ideal de* R. *Então* $G = \{g_1, \ldots, g_s\}$ *é uma base de Gröbner se, e somente se, para todo* $i \neq j$, *o resto da divisão de* $S(g_i, g_j)$ *por* G *(listados em qualquer ordem) é zero.*

Demonstração. Suponhamos que G é uma base de Gröbner, então, como $S(g_i, g_j) \in I$, o resto da divisão por G é zero, pelo Corolário 1.3.4.

Reciprocamente, suponha que o resto da divisão de cada S-polinômio por G seja zero. Nosso objetivo será mostrar que dado $f \in I - \{0\}$, então $TL(f) \in < TL(g_1), \ldots, TL(g_s) >$. Com efeito, como $f \in I =< g_1, \ldots, g_s >$, existem polinômios $h_i \in R$ tais que

$$f = \sum_{i=1}^{s} h_i g_i. \tag{1.2}$$

Pelo Lema 1.1.10, temos

$$MG(f) \leq \max\{MG(h_i g_i)\}. \tag{1.3}$$

Perceba que se a igualdade não ocorrer em 1.3, então deve ocorrer cancelamento de termos líderes em 1.2, e pelo Lema 1.3.7 todo cancelamento de termos líderes se dá por S–polinômios, então poderemos reescrever isto em termos destes. A ideia será utilizarmos a hipótese de que os S-polinômios possuem resto zero ao serem divididos por G, e isto nos permitirá substituí-los por expressões que envolvam menos cancelamento, ou seja, vamos obter uma expressão para f com menos cancelamentos dos termos líderes. Continuando esse processo, obteremos em alguma etapa uma expressão para f sem cancelamentos de termos líderes, tal que

$$MG(f) = \max\{MG(h_i g_i)\},$$

para algum i, ou seja, $TL(f)$ é divisível por $TL(g_i)$, daí concluiremos a demonstração.

Seja $\alpha_i = MG(h_i g_i)$ e defina $\delta = \max\{\alpha_1, \ldots, \alpha_s\}$. Assim

$$MG(f) \leq \delta.$$

Considere agora todos os possíveis modos de escrever f na forma $f = \sum_{i=1}^{s} h_i g_i$. Para cada possibilidade, temos possivelmente um δ diferente. Porém, como toda ordem monomial é uma boa ordenação, podemos escolher uma expressão para f tal que δ é mínimo. Devemos mostrar que para este δ mínimo escolhido, o $MG(f) = \delta$, pois assim, vale a igualdade de 1.3 e, consequentemente, $TL(f) \in < TL(g_1), \ldots, TL(g_s) >$.

Suponhamos por contradição que $MG(f) < \delta$ e escrevemos f convenientemente de modo a isolar os termos de multigrau δ

$$\begin{aligned} f &= \sum_{\alpha_i=\delta} h_i g_i + \sum_{\alpha_i<\delta} h_i g_i \\ &= \sum_{\alpha_i=\delta} (TL(h_i) + h_i - TL(h_i)) g_i + \sum_{\alpha_i<\delta} h_i g_i \\ &= \sum_{\alpha_i=\delta} TL(h_i) g_i + \sum_{\alpha_i=\delta} (h_i - TL(h_i)) g_i + \sum_{\alpha_i<\delta} h_i g_i. \end{aligned} \tag{1.4}$$

Note que todos os polinômios que aparecem na segunda e terceira soma da última igualdade têm $MG < \delta$. Deste modo, a hipótese de que $MG(f) < \delta$ implica que a primeira soma tem multigrau menor que δ, ou seja,

$$MG\left(\sum_{\alpha_i=\delta} TL(h_i) g_i\right) < \delta.$$

Seja $TL(h_i) = c_i\mathbf{x}^{\beta_i}$. Então

$$\sum_{\alpha_i=\delta} TL(h_i)g_i = \sum_{\alpha_i=\delta} c_i\mathbf{x}^{\beta_i}g_i$$

satisfaz as hipóteses do Lema 1.3.7 com $f_i = \mathbf{x}^{\beta_i}g_i$, e portanto este cancelamento pode ser escrito como uma combinação linear de S-polinômios $S(\mathbf{x}^{\alpha_j}g_j, \mathbf{x}^{\alpha_k}g_k)$. Contudo,

$$\begin{aligned} S(\mathbf{x}^{\beta_j}g_j, \mathbf{x}^{\beta_k}g_k) &= \frac{\mathbf{x}^{\delta}}{\mathbf{x}^{\beta_j}TL(g_j)}\mathbf{x}^{\beta_j}g_j - \frac{\mathbf{x}^{\delta}}{\mathbf{x}^{\beta_k}TL(g_k)}\mathbf{x}^{\beta_k}g_k \\ &= \frac{\mathbf{x}^{\delta}}{TL(g_j)}g_j - \frac{\mathbf{x}^{\delta}}{TL(g_k)}g_k \\ &= \frac{\mathbf{x}^{\delta-\gamma_{jk}+\gamma_{jk}}}{TL(g_j)}g_j - \frac{\mathbf{x}^{\delta-\gamma_{jk}+\gamma_{jk}}}{TL(g_k)}g_k \\ &= \mathbf{x}^{\delta-\gamma_{jk}}S(g_j, g_k), \end{aligned}$$

onde $\mathbf{x}^{\gamma_{jk}} = \text{MMC}(ML(g_j), ML(g_k))$. Logo, existem constantes $c_{jk} \in k$ tais que

$$\sum_{\alpha_i=\delta} TL(h_i)g_i = \sum_{jk} c_{jk}\mathbf{x}^{\delta-\gamma_{jk}}S(g_j, g_k). \tag{1.5}$$

O próximo passo é usar nossa hipótese de que o resto de $S(g_j, g_k)$ na divisão por $g_1, \ldots, g_s$ ser zero. Usando o algoritmo da divisão, isso significa que cada S-polinômio pode ser escrito na forma

$$S(g_j, g_k) = \sum_{v=1}^{s} a_{jk_v}g_v,$$

onde $a_{jk_v} \in R$.

Sabemos ainda, pelo algoritmo da divisão, que

$$MG(a_{jk_v}g_v) \leq MG(S(g_j, g_k)), \tag{1.6}$$

para todo j, k de 1.5 e $v \in \{1, \ldots, s\}$. Intuitivamente, isso mostra que quando o resto é zero, podemos encontrar uma expressão para $S(g_j, g_k)$ em termos de G onde nem todos os termos líderes se cancelam.

Para explorar isso, multipliquemos $S(g_j, g_k)$ por $\mathbf{x}^{\delta-\gamma_{jk}}$ para obter

$$\mathbf{x}^{\delta-\gamma_{jk}}S(g_j, g_k) = \sum_{l=1}^{s} b_{jk_l}g_l, \tag{1.7}$$

onde $b_{jk_l} = \mathbf{x}^{\delta-\gamma_{jk}}a_{jk_v}$. Então, novamente pelo Lema 1.3.7, temos

$$MG(b_{jk_l}g_l) \leq MG(\mathbf{x}^{\delta-\gamma_{jk}}S(g_j, g_k)) < \delta.$$

Substituindo a expressão 1.7 em 1.5 obtemos

$$\sum_{\alpha_i=\delta} TL(h_i)g_i = \sum_{jk} c_{jk}\mathbf{x}^{\delta-\gamma_{jk}}S(g_j, g_k) = \sum_{jk} c_{jk}\left(\sum_{l} b_{jk_l}g_l\right) = \sum_{i} \bar{h}_i g_i, \tag{1.8}$$

onde $\bar{h}_i \in R$, e concluímos assim que $MG(\bar{h}_i g_i) < \delta$, para todo i.

Finalmente, substituindo 1.8 em 1.4 obtemos uma expressão para f como combinação dos polinômios $g_i's$, onde todos têm multigrau menor que δ, o que contradiz a minimalidade de δ. Portando $MG(f) = \max\{MG(h_i g_i)\}$ e assim $TL(f) \in < TL(g_1), \ldots, TL(g_s) >$. □

O Critério de Buchberger, também é conhecido como *Critério dos S-pares de Buchberger*, é um dos resultados mais importantes na teoria das Bases de Gröbner. Através dele temos um método para identificar quando uma base é de Gröbner ou não.

Exemplo 1.3.9. *Seja* $I =< -y + x^2, -z + x^3 > \subset R$ *um ideal. Vamos mostrar que* $G = \{-y+x^2, -z+x^3\}$ *é uma base de Gröbner considerando a ordem lexicográfica com* $y > z > x$. *Considere* $f = -y + x^2$ *e* $g = -z + x^3$. *Notemos que* $TL(f) = -y$ *e* $TL(g) = -z$, *assim*

$$\text{MMC}(ML(f), ML(g)) = yz.$$

Logo, o S-polinômio $S(f, g)$ *é dado por*

$$\begin{aligned} S(f,g) &= \frac{yz}{(-y)}.(-y+x^2) - \frac{(yz)}{(-z)}.(-z+x^3) \\ &= yz - zx^2 - yz + yx^3 \\ &= yx^3 - zx^2. \end{aligned}$$

Dividindo $S(f, g)$ *por* f *e* g *temos*

$$yx^3 - zx^2 = -x^3(-y + x^2) + x^2(-z + x^3),$$

ou seja, o resto é zero. Logo pelo Critério de Buchberger, G *é uma base de Gröbner para o ideal* I.

Até agora sabemos dizer se um conjunto de geradores é uma base de Gröbner ou não. Mas cabe perguntar, como produzir uma base de Gröbner. Para isto, temos o Algoritmo de Buchberger, que nos ajudará a encontrar uma base de Gröbner para um ideal de R.

A ideia central do **Algoritmo de Buchberger** é tentar expandir o conjunto original de geradores, $F_0 = \{f_1, \ldots, f_t\}$, a uma base de Gröbner, adicionando os restos não nulos de $S(f_i, f_j)$, $i \neq j$, na divisão por F, onde F é o conjunto de geradores em um determinado momento do processo.

Observemos que o processo é finito, pois caso contrário, teríamos em cada etapa que o resto de algum $S(f_i, f_j)$ na divisão por F é diferente de zero, ou seja, $\overline{S(f_i, f_j)}^F \neq 0$, e assim fazendo $f_s = \overline{S(f_i, f_j)}^F$ e o acrescentando a F, obteríamos um novo conjunto, F_1, de geradores. E consequentemente poderíamos obter um conjunto infinito de geradores para o ideal I, contrariando o fato de R ser Noetheriano.

Exemplo 1.3.10. *No exemplo 1.1.12 vimos que ao dividir* $f = xy^2 - x$ *por* $f_1 = xy + 1$ *e* $f_2 = y^2 - 1$ *o resto não era único, ou seja,* $\{f_1, f_2\}$ *não é uma base de Gröbner. Notemos então que, sendo* $S(f_1, f_2) = x + y$ *e como nenhum monômio de* $S(f_1, f_2)$ *é divisível pelos termos líderes de* f_1 *e* f_2, *então* $\overline{S(f_1, f_2)}^F = x + y$. *Adicionando* $f_3 = x + y$ *a* F, *temos assim* $\overline{S(f_1, f_2)}^F = 0$, *como gostaríamos.*

Agora também temos que calcular $S(f_1, f_3)$ *e* $S(f_2, f_3)$.

$$\begin{array}{rcccl} S(f_1, f_3) & = & -y^2 + 1 & = & -f_2 \\ S(f_2, f_3) & = & -y^3 - x & = & -yf_2 - f_3, \end{array}$$

ou seja, $\overline{S(f_1, f_3)}^F = 0$ *e* $\overline{S(f_2, f_3)}^F = 0$. *Portando* $F = \{f_1, f_2, f_3\}$ *é uma base de Gröbner.*

Exemplo 1.3.11. *Seja* I *o ideal gerado por* $F = \{f_1, f_2\}$, *onde* $f_1 = x^2y - 1$ *e* $f_2 = xy^2 - x$, *em* $\mathbb{C}[x, y]$. *Consideremos a ordem lexicográfica com* $x > y$, *logo* $\text{MMC}(TL(f_1), TL(f_2)) = x^2y^2$ *e assim*

$$S(f_1, f_2) = \frac{x^2y^2}{x^2y}(x^2y - 1) - \frac{x^2y^2}{xy^2}(xy^2 - x) = x^2 - y.$$

Notemos que não podemos dividir $S(f_1, f_2)$ *pelor termos líderes de* f_1 *e* f_2, *logo,* $\overline{S(f_1, f_2)}^F = x^2 - y$. *Porém ao adicionarmos* $f_3 = x^2 - y$ *ao conjunto original de geradores* F, *temos* $\overline{S(f_1, f_2)}^F = 0$.

Calculando $S(f_1, f_3)$ *temos*

$$S(f_1, f_3) = \frac{x^2y}{x^2y}(x^2y - 1) - \frac{x^2y}{x^2}(x^2 - y) = y^2 - 1,$$

que também não é divisível por nenhum termo líder de $F = \{f_1, f_2, f_3\}$, *logo* $\overline{S(f_1, f_3)}^F = y^2 - 1$, *então acrescentamos* $f_4 = y^2 - 1$ *à base de geradores de* I, *ou seja, a* F, *assim,* $\overline{S(f_1, f_3)}^F = 0$.

Notemos ainda que

$$\begin{array}{rcccl} S(f_1, f_4) & = & x^2 - y & = & f_3; \\ S(f_2, f_3) & = & -x^2 + y^3 & = & -f_3 + yf_4; \\ S(f_2, f_4) & = & -x + x & = & 0; \\ S(f_3, f_4) & = & x^2 - y^3 & = & f_3 - yf_4. \end{array}$$

Ou seja, $\overline{S(f_1, f_4)}^F = \overline{S(f_2, f_3)}^F = \overline{S(f_2, f_4)}^F = \overline{S(f_3, f_4)}^F = 0$, *e assim,* $F = \{f_1, f_2, f_3, f_4\}$ *é uma base de Gröbner para o ideal* I.

Notemos que em geral as bases de Gröbner construídas usando o algorítmo de Buchberger são maiores que o necessário, para resolver isso, temos

Proposição 1.3.12. *Seja* G *uma base de Gröbner do ideal* $I \subset R$ *e* $p \in G$ *um polinômio tal que* $TL(p) \in < TL(G - \{p\}) >$. *Então* $G - \{p\}$ *também é uma base de Gröbner para* I.

Demonstração. Já sabemos que $< TL(G) > = < TL(I) >$. Suponhamos que

$$TL(p) \in < TL(G - \{p\}) >,$$

então $< TL(G - \{p\}) > = < TL(G) >$. Logo, por definição, $G - \{p\}$ também é uma base de Gröbner para I. □

Definição 1.3.13. *Uma* ***Base de Gröbner Minimal*** *para um ideal* $I \subset R$ *é uma base de Gröbner* G *de* I *tal que:*

i. $CL(p) = 1$, *para todo* $p \in G$;

ii. Para todo $p \in G$ *temos que* $TL(p)$ *não pertence a* $< TL(G - \{p\}) >$.

Exemplo 1.3.14. *No Exemplo 1.3.11 vimos que* $f_1 = x^2y - 1$, $f_2 = xy^2 - x$, $f_3 = x^2 - y$ *e* $f_4 = y^2 - 1$. *Notemos que* $TL(f_1) = x^2y = yTL(f_3)$, *então pela Proposição 1.3.12, podemos retirar* f_1. *Do mesmo modo* $TL(f_2) = xy^2 = xTL(f_4)$ *e assim podemos também retirar* f_2. *Logo* $\{f_3, f_4\}$ *formam uma base de Gröbner minimal de* I.

Observemos que na base de Gröbner minimal, pode existir algum $p \in G$ tal que $TL(p) \notin < TL(G - \{p\}) >$, mas algum monômio de p (diferente de $TL(p)$) pode estar em $< TL(G - \{p\}) >$.

Definição 1.3.15. *Uma* ***Base de Gröbner reduzida*** *para um ideal* $I \subset R$ *é uma base de Gröbner* G *para* I *tal que:*

i. $CL(p) = 1$, *para todo* $p \in G$;

ii. Para todo $p \in G$, *nenhum monômio de* p *pertence a* $< TL(G - \{p\}) >$.

Exemplo 1.3.16. *Vimos no Exemplo 1.3.10 que* $F = \{f_1, f_2, f_3\}$ *é uma base de Gröbner para o ideal* $I \subset \mathbb{C}[x, y]$. *Observemos agora que* $xy + 1 = -(y^2 - 1) + y(x + y)$, *ou seja,* $f_1 \in I =< f_2, f_3 >\subset \mathbb{C}[x, y]$. *Logo, podemos tomar* $F = \{f_2, f_3\}$, *que satisfaz as duas condições para uma base de Gröbner reduzida.*

Observemos que um ideal pode ter mais de uma base de Gröbner. Se no Exemplo 1.3.9 tivéssemos considerado a ordem lexicográfica graduada com $x > y > z$, então o conjunto $\{x^2 - y, xy - z, xz - y^2, y^3 - z^2\}$ formaria uma base de Gröbner reduzida para I, e não o conjunto $\{-y + x^2, -z + x^3\}$.

Capítulo 2

Base de Gröbner para Submódulos em R^m

Neste capítulo vamos expandir a teoria vista no capítulo anterior para o R-módulo livre R^m, ou seja, determinar um algoritmo de divisão e um conjunto gerador G para um submódulo $M \subset R^m$, tal que, ao dividir dado elemento $f \in M$, o resto sempre será zero. E assim podermos determinar se um elemento $f \in R^m$ pertence ou não a um submódulo $M \subset R^m$.

2.1 Ordens Monomiais e Divisão em R^m

Um **monômio m** em R^m é um elemento da forma $\mathbf{x}^\alpha e_i$ para algum $i \in \{1, \ldots, m\}$, onde $\mathbf{m}$ contêm o vetor canônico e_i. Todo elemento $f \in R^m$ pode ser escrito de maneira única como uma combinação linear de monômios com coeficientes em k (*k-combinação linear*),

$$f = \sum_{i=1}^{n} c_i \mathbf{m}_i, \tag{2.1}$$

onde $c_i \in k$ e $c_i \neq 0$ (Proposição 1.6 do Capítulo 5 de [1]).

Exemplo 2.1.1. *Em $k[x, y]^3$,*

$$f = \begin{bmatrix} 5xy^2 - y^{10} + 3 \\ 4x^3 + 2y \\ 16x \end{bmatrix} = 5\begin{bmatrix} xy^2 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} y^{10} \\ 0 \\ 0 \end{bmatrix} + 3\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + 4\begin{bmatrix} 0 \\ x^3 \\ 0 \end{bmatrix} + 2\begin{bmatrix} 0 \\ y \\ 0 \end{bmatrix} + 16\begin{bmatrix} 0 \\ 0 \\ x \end{bmatrix}$$

$$= 5xy^2 e_1 - y^{10} e_1 + 3e_1 + 4x^3 e_2 + 2ye_2 + 16xe_3,$$

que é uma k-combinação linear de monômios.

Em alguns momentos, denotaremos um elemento $f \in R^m$, onde

$$f = \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_m \end{bmatrix} = f_1 e_1 + f_2 e_2 + \ldots + f_m e_m,$$

por $(f_1, f_2, \ldots, f_m)$, tal que $f_i \in R$, $i \in \{1, \ldots, m\}$.

O produto $c\mathbf{m}$ de um monômio $\mathbf{m}$ por um elemento $c \in k$ é chamado de **termo** e c é chamado de **coeficiente**. Dado $f \in R^m$, dizemos que os termos $c_i\mathbf{m}_i$, $c_i \neq 0$, e os monômios correspondentes $\mathbf{m}_i$, *pertencem* a f (ver 2.1).

Sejam $\mathbf{m}$ e $\mathbf{n}$ monômios em R^m, onde $\mathbf{m} = \mathbf{x}^\alpha e_i$ e $\mathbf{n} = \mathbf{x}^\beta e_j$, dizemos que $\mathbf{n}$ *divide* $\mathbf{m}$ (ou $\mathbf{m}$ é *divisível* por $\mathbf{n}$) se, e somente se, $i = j$ e $\mathbf{x}^\beta$ divide $\mathbf{x}^\alpha$.

Se $\mathbf{n}$ divide $\mathbf{m}$ definimos o *quociente* $\mathbf{m}/\mathbf{n}$ com $\mathbf{x}^\alpha/\mathbf{x}^\beta \in R$ (ou seja, $\mathbf{m}/\mathbf{n} = \mathbf{x}^{\alpha-\beta}$). Note que o quociente é um elemento do anel R, e se $\mathbf{n}$ divide $\mathbf{m}$, temos $(\mathbf{m}/\mathbf{n})\mathbf{n} = \mathbf{m}$, como se deseja. Se $\mathbf{m}$ e $\mathbf{n}$ são monômios contendo o mesmo elemento da base canônica e_i, definimos o *máximo divisor comum*, $\mathrm{MDC}(\mathbf{m}, \mathbf{n})$, e o *mínimo múltiplo comum*, $\mathrm{MMC}(\mathbf{m}, \mathbf{n})$, ambos em R^m, para serem o maior divisor comum e o menor múltiplo comum, respectivamente, de $\mathbf{x}^\alpha$ e $\mathbf{x}^\beta$ em e_i. Se $\mathbf{m}$, $\mathbf{n}$ contêm diferentes vetores canônicos, $\mathrm{MMC}(\mathbf{m}, \mathbf{n}) = 0$.

Dizemos que um submódulo $M \subset R^m$ é um **submódulo monomial** se M pode ser gerado por uma coleção de monômios.

Vimos que nos ideais monomiais, para saber se $f \in R$ pertence ou não ao ideal, bastava checar se todo termo de f pertence ao ideal. Veremos que os submódulos monomiais também tem uma propriedade similar a essa.

Proposição 2.1.2.

a. Todo submódulo monomial de R^m é gerado por uma coleção finita de monômios.

b. Toda cadeia ascendente infinita $M_1 \subset M_2 \subset \ldots$ de submódulos monomiais de R^m estabiliza. Ou seja, existe um N tal que $M_N = M_{N+1} = \ldots = M_{N+l} = \ldots$ para todo $l \geq 0$.

Demonstração.

a. Notemos que R^m é finitamente gerado como R-módulo, logo R^m é Noetheriano e assim, M é finitamente gerado (mais detalhes em [1], capítulo 6). Seja $M =< g_1, \ldots, g_t >$, com $g_i \in R^m$, $i \in \{1, \ldots, t\}$. Como $g_i \in M$, então $g_i = \sum_{j=1}^{l_i} a_{i_j}\mathbf{m}_{i_j}$, com $a_{i_j} \in R$, ou seja, podemos tomar

$$M =< \mathbf{m}_{1_1}, \ldots, \mathbf{m}_{1_{l_1}}, \ldots, \mathbf{m}_{t_1}, \ldots, \mathbf{m}_{t_{l_t}} > .$$

Nos restringindo aos $\mathbf{m}_{ij}$ tais que os vetores canônicos são os mesmos, podemos usar o Lema 1.2.2 (pois $M_s = M \cap Re_s = I_s e_s$, com $I_s e_s \cong I_s$ um ideal em R), e assim temos que para cada $\mathbf{m}_{ij} = \mathbf{x}^{\beta_{i_j}} e_s$ existe um $\mathbf{m}_k = \mathbf{x}^{\alpha_k} e_s \in M$, tal que $\mathbf{x}^{\alpha_k}$ divide $\mathbf{x}^{\beta_{i_j}}$, ou seja, $\mathbf{m}_k$ divide $\mathbf{m}_{i_j}$. Enumerando os m_k de 1 até r e eliminando os termos repetidos, temos $M =< \mathbf{m}_1, \ldots, \mathbf{m}_r >$.

b. Segue do fato de R^m ser um módulo Noetheriano.

□

Vimos na demonstração da parte a da Proposição 2.1.2 que sendo $M =< \mathbf{m}_1, \ldots, \mathbf{m}_t >$ um submódulo monomial e dado $f \in R^m$, então $f \in M$ se, e somente se, todos termos de f forem divisíveis por algum $\mathbf{m}_i$, $i \in \{1, \ldots, t\}$. Logo se estamos estudando submódulos monomiais, já sabemos resolver o problema de um elemento pertencer ou não ao submódulo.

Para estendermos a teoria das bases de Gröbner para submódulos de R^m, precisamos definir uma ordem nos monômios, ter um algoritmo de divisão e estender o algoritmo de Buchberger para R^m.

Definição 2.1.3. *Uma ordem monomial em R^m é uma relação de ordem $>$ nos monômios de R^m satisfazendo:*

i. $>$ *é uma ordem total;*

ii. Para todo par de monômios $\boldsymbol{m}, \boldsymbol{n} \in R^m$ com $\boldsymbol{m} > \boldsymbol{n}$, temos $\mathbf{x}^\alpha \boldsymbol{m} > \mathbf{x}^\alpha \boldsymbol{n}$ para todo $\mathbf{x}^\alpha \neq 0 \in R$;

iii. $\mathbf{x}^\alpha \boldsymbol{m} > \boldsymbol{m}$ para todos monômios $\boldsymbol{m} \neq 0 \in R^m$ e todos monômios $\mathbf{x}^\alpha \neq 0 \in R$ tal que $\mathbf{x}^\alpha \neq 1$.

Proposição 2.1.4. *Toda ordem monomial em R^m é bem-ordenada.*

Demonstração. Vamos demonstrar por redução ao absurdo. Suponhamos que exista uma coleção não vazia de monômios que não possui termo mínimo, ou seja, não é bem-ordenada. Logo existe uma sequência infinita

$$\mathbf{x}^{\alpha_1} e_{i_1} > \mathbf{x}^{\alpha_2} e_{i_2} > \mathbf{x}^{\alpha_3} e_{i_3} > \ldots, \tag{2.2}$$

onde e_{i_j} são vetores da base canônica de R^m. Definindo os submódulos, $M_1 =< \mathbf{x}^{\alpha_1} e_{i_1} >$, $M_2 =< \mathbf{x}^{\alpha_1} e_{i_1}, \mathbf{x}^{\alpha_2} e_{i_2} >$, $M_3 =< \mathbf{x}^{\alpha_1} e_{i_1}, \mathbf{x}^{\alpha_2} e_{i_2}, \mathbf{x}^{\alpha_3} e_{i_3} >$, e assim por diante. Temos que

$$M_1 \subset M_2 \subset M_3 \subset \ldots,$$

onde as inclusões são próprias, visto que se para algum j tivermos $M_j = M_{j+1}$, então

$$< \mathbf{x}^{\alpha_1} e_{i_1}, \ldots, \mathbf{x}^{\alpha_j} e_{i_j} >=< \mathbf{x}^{\alpha_1} e_{i_1}, \ldots, \mathbf{x}^{\alpha_j} e_{i_j}, \mathbf{x}^{\alpha_{j+1}} e_{i_{j+1}} >,$$

isto é, $\mathbf{x}^{\alpha_{j+1}} e_{i_{j+1}} = \mathbf{x}^{\alpha_l} e_{i_l}$, para algum $l \in \{1, \ldots, j\}$, contrariando 2.2. Assim temos uma cadeia ascendente de submódulos que não estabiliza, absurdo pelo item b da Proposição 2.1.2. □

As ordens monomiais em R^m mais comuns são extensões das ordens monomiais em R. Existem duas maneiras naturais de fazer isto, desde que escolhemos uma ordem nos vetores da base canônica. Sempre usaremos a ordem decrescente nas entradas de uma coluna

$$e_1 > e_2 > \ldots > e_m,$$

embora qualquer outra ordem também possa ser usada.

Definição 2.1.5. *Seja $>$ uma ordem monomial em R.*

i. (extensão TSP de >) Dizemos que $\mathbf{x}^\alpha e_i >_{TSP} \mathbf{x}^\beta e_j$ *se* $\mathbf{x}^\alpha > \mathbf{x}^\beta$ *ou se* $\mathbf{x}^\alpha = \mathbf{x}^\beta$ *e* $i < j$.

ii. (extensão PST de >) Dizemos que $\mathbf{x}^\alpha e_i >_{PST} \mathbf{x}^\beta e_j$ *se* $i < j$ *ou se* $i = j$ *e* $\mathbf{x}^\alpha > \mathbf{x}^\beta$.

Os termos TSP e PST significam *termo sobre posição* e *posição sobre termo*, respectivamente.

Observação 2.1.6. *Para qualquer ordem monomial > em R, ambos* $>_{TSP}$ *e* $>_{PST}$ *definem ordens monomiais em* R^m.

Exemplo 2.1.7. *Se estendermos a ordem lexicográfica em* $k[x, y]$ *com* $x > y$ *usando TSP em* $k[x, y]^3$, *obtemos uma ordem* $>_1$ *tal que os termos do exemplo 2.1.1 são ordenados da seguinte maneira:*

$$\begin{bmatrix} 0 \\ x^3 \\ 0 \end{bmatrix} >_1 \begin{bmatrix} xy^2 \\ 0 \\ 0 \end{bmatrix} >_1 \begin{bmatrix} 0 \\ 0 \\ x \end{bmatrix} >_1 \begin{bmatrix} y^{10} \\ 0 \\ 0 \end{bmatrix} >_1 \begin{bmatrix} 0 \\ y \\ 0 \end{bmatrix} >_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Se estendermos agora usando PST temos $>_2$, *onde*

$$\begin{bmatrix} xy^2 \\ 0 \\ 0 \end{bmatrix} >_2 \begin{bmatrix} y^{10} \\ 0 \\ 0 \end{bmatrix} >_2 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} >_2 \begin{bmatrix} 0 \\ x^3 \\ 0 \end{bmatrix} >_2 \begin{bmatrix} 0 \\ y \\ 0 \end{bmatrix} >_2 \begin{bmatrix} 0 \\ 0 \\ x \end{bmatrix}.$$

Nos dois casos temos $e_1 > e_2$.

Uma vez que tenhamos uma ordenação $>$ em monômios, podemos escrever qualquer elemento $f \in R^m$ como a soma de termos

$$f = \sum_{i=1}^{t} c_i \mathbf{m}_i, \tag{2.3}$$

com $c_i \neq 0$ e $\mathbf{m}_1 > \mathbf{m}_2 > \ldots > \mathbf{m}_t$.

Definição 2.1.8. *Seja* $>$ *uma ordenação monomial e* $f = \sum_{i=1}^{t} c_i \boldsymbol{m}_i$ *um elemento não nulo em* R^m *como descrito em 2.3.*

i. O coeficiente líder de f é

$$CL(f) = c_1;$$

ii. O monômio líder de f é

$$ML(f) = \boldsymbol{m}_1;$$

iii. O termo líder de f é

$$TL(f) = c_1 \boldsymbol{m}_1.$$

Exemplo 2.1.9. *Seja*

$$f = (5xy^2 - y^{10} + 3)e_1 + (4x^3 + 2y)e_2 + 16xe_3 \in k[x, y]^3$$

como no exemplo 2.1.1, e usando a extensão TSP da ordem lexicográfica em $k[x, y]$, $(x > y)$, então $CL(f) = 4$, $ML(f) = x^3e_2$ e $TL(f) = 4x^3e_2$. Similarmente usando a extensão PST temos $CL(f) = 5$, $ML(f) = xy^2e_1$ e $TL(f) = 5xy^2e_1$.

Como já temos uma ordem monomial em R^m, agora podemos estender o algoritmo da divisão visto em R (Proposição 1.1.11) para o módulo livre R^m.

Lema 2.1.10 (Algorítmo da Divisão em R^m)**.** *Fixe uma ordem monomial em R^m e seja $F = \{f_1, \ldots, f_s\}$ uma s-tupla de elementos de R^m. Então todo $f \in R^m$ pode ser escrito como*

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

*onde $a_i \in R$, $r \in R^m$, $TL(a_if_i) \leq TL(f)$ para todo i, e, ou $r = 0$ ou r é uma k-combinação linear de monômios que não são divisíveis por nenhum dos $ML(f_1), \ldots, ML(f_s)$. Chamamos r de **resto** da divisão por F.*

Demonstração. A prova desse lema é exatamente a mesma que a prova do Lema 1.1.11, exceto que ao invés de utilizar a Proposição 1.1.10 para mostrar que o processo de construção dos $p's$ termina, usamos b da Proposição 2.1.2. Ou seja, se o processo não terminasse e tomando $M_1 =< TL(p_1) >$, $M_2 =< TL(p_1), TL(p_2) >$, $M_3 =< TL(p_1), TL(p_2), TL(p_3) >$, e assim por diante, teríamos

$$M_1 \subset M_2 \subset M_3 \subset \ldots,$$

onde as inclusões são próprias, pois caso contrário teríamos algum M_i tal que $M_i = M_{i+1}$, isto é, $TL(p_{i+1})$ é divisível por algum $TL(p_l)$, para algum $l \in \{1, \ldots, i\}$, contrariando a definição dos $p_i's$. □

Exemplo 2.1.11. *Sejam*

$$\begin{aligned} f &= (5xy^2 - y^{10} + 3)e_1 + (4x^3 + 2y)e_2 + 16xe_3; \\ f_1 &= (xy + 4x)e_1 + y^2e_3; \\ f_2 &= (y - 1)e_2 + (x - 2)e_3, \end{aligned}$$

em $k[x, y]$. Seja também $>$ a extensão PST da ordem lexicográfica em $k[x, y]$ com $x > y$. Então $TL(f) = 5xy^2$, $TL(f_1) = xye_1$ e $TL(f_2) = ye_2$.

Tomando p como o dividendo intermediário em cada etapa do algorítmo, onde $p = f$ e $a_1 = a_2 = r = 0$ para começar. Seguindo o algorítmo, teremos no final que

$$\begin{aligned} a_1 &= 5y - 20; \\ a_2 &= 2; \\ r &= 80xe_1 - y^10e_1 + 3e_1 + 4x^3e_2 + 2e_2 + 14xe_3 - ry^3e_3 + 20y^2e_3 + 4e_3. \end{aligned}$$

Isto é, $f = a_1f_1 + a_2f_2 + r$.

2.2 Base de Gröbner em R^m

Agora já podemos estender a definição de Base de Gröbner para o R-módulo livre R^m.

Definição 2.2.1. *Sejam M um submódulo de R^m e $>$ uma ordem monomial.*

i. Definimos $< TL(M) >$ como o submódulo monomial gerado pelos termos líderes de todos $f \in M$ com respeito a $>$.

*ii. Uma coleção finita $G = \{g_1, \ldots, g_s\} \subset M$ é chamada uma **base de Gröbner** para M se $< TL(M) >=< TL(g_1), \ldots, TL(g_s) >$.*

Observação 2.2.2. *Observemos que dado $f \in R^m$, $TL(f)$ se difere de $ML(f)$ apenas por uma constante não nula. Logo*

$$< ML(M) >=< TL(M) >=< TL(g_1), \ldots, TL(g_s) >=< ML(g_1), \ldots, ML(g_s) > .$$

*Ou seja, um conjunto não nulo $G = \{g_1, \ldots, , g_s\}$ contido no submódulo M é chamado uma **base de Gröbner** para M se, e somente se, para todo $f \in M$, existe $i \in \{1, \ldots, s\}$ tal que $ML(g_i)$ divide $ML(f)$.*

Muitas propriedades da base de Gröbner para ideais são também estendidas para R^m .

Proposição 2.2.3. *Seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner para um submódulo $M \subset R^m$.*

a. $f \in M$ se, e somente se, o resto na divisão por G é zero.

b. Uma base de Gröbner para M gera M como submódulo, ou seja, $M =< g_1, \ldots, g_s >$.

Demonstração.

a. Se o resto é zero, então $f = a_1 g_1 + \ldots + a_s g_s$, onde $a_i \in R$ e $i \in \{1, \ldots, s\}$, logo $f \in M$.

   Reciprocamente, seja $f \in M$. Então ao dividir f por G usando o algoritmo de Divisão, temos que $f = a_1 g_1 + \ldots + a_s g_s + r$. Suponhamos que $r \neq 0$, logo $r = f - a_1 g_1 - \ldots - a_s g_s$, assim, $r \in M$. Visto que G é uma base de Gröbner, então $TL(g_i)$ divide $TL(r)$ para algum $i \in \{1, \ldots, s\}$. Assim pela Observação 2.2.2, então $ML(g_i)$ divide $ML(r)$, gerando um absurdo, pois pelo algorítmo da divisão $ML(g_i)$ não divide nenhum monômio de r.

b. Observemos primeiramente que todo submódulo $M \subset R^m$ possui uma base de Gröbner, pois $< TL(M) >$ é um submódulo monomial, e por a da Proposição 2.1.2 e pela Observação 2.2.2, existem $g_1, \ldots, g_s$ em M tais que $< TL(M) >=< TL(g_1), \ldots, TL(g_s) >$.

   Agora vamos mostrar que $M =< g_1, \ldots, g_s >$, notemos que $< g_1, \ldots, g_s > \subset M$, pois cada $g_i \in M$, $i \in \{1, \ldots, s\}$. Reciprocamente, seja $f \in M$, dividindo f por G, temos

$$f = a_1 g_1 + \ldots + a_s g_s + r,$$

onde $a_i \in R$ e $r = 0$ ou r é uma *k-combinação linear* de monômios, de modo que nenhum deles é divisível por por algum monômio líder de $g_1, \ldots, g_s$. Reescrevendo a expressão acima, temos que

$$r = f - a_1 g_1 - \ldots - a_s g_s.$$

Se $r \neq 0$ então $ML(r) \in < ML(M) > = < ML(g_1), \ldots, ML(g_s) >$, ou seja, o monômio líder de r é divisível por algum $ML(g_i)$, o que é uma contradição. Logo $r = 0$ e $f = a_1 g_1 + \ldots + a_s g_s \in < g_1, \ldots, g_s >$. Portando $M \subset < g_1, \ldots, g_s >$.

□

Normalmente, não é verdade que uma base de Gröbner seja uma base para o submódulo M (ou seja, um conjunto linearmente independente) como um R-módulo. Uma base de Gröbner é um conjunto de geradores para M, mas não é necessariamente linearmente independente sobre R. Contudo, existem bases de Gröbner para todos os submódulos de R^m (como vimos na demonstração da parte b da Proposição 2.2.3.

Agora podemos determinar se um elemento de R^m pertence ou não a um submódulo $M \subset R^m$. Para isso, basta dividir o elemento pela base de Gröbner, se o resto for zero, o elemento pertence ao submódulo M. Mas como vimos em R, precisamos de método para saber se o conjunto gerador de M é uma base de Gröbner e um algoritmo para encontra-la. Para isso vamos estender a definição de S-polinômios, do critério de Buchberger e o algoritmo de Buchberger.

Definição 2.2.4. *Fixe uma ordem monomial em R^m e seja $f, g \in R^m$. O S-vetor de f e g, denotado por $S(f, g)$, é o seguinte elemento de R^m:*

$$S(f, g) = \frac{\boldsymbol{m}}{TL(f)} f - \frac{\boldsymbol{m}}{TL(g)} g$$

onde $\boldsymbol{m} = \text{MMC}(TL(f), TL(g))$.

Exemplo 2.2.5. *Seja $f = (xy - x)e_1 + (x^3 - y)e_2$ e $g = (x^2 + 2y^2)e_1 + (x^2 - y^2)e_2$ em $k[x, y]^2$. Usando a extensão PST da ordem lexicográfica em $k[x, y]$ com $x > y$, temos*

$$\begin{aligned} S(f, g) &= \frac{x^2 y}{xy}(xy - x, x^3 + y) - \frac{x^2 y}{x^2}(x^2 + 2y^2 . x^2 - y^2) \\ &= (x^2 y - x^2, x^4 + xy) - (x^2 y + 2y^3, x^2 y - y^3) \\ &= (-x^2 - 2y^3, x^4 - x^2 y - xy + y^3). \end{aligned}$$

Lema 2.2.6 (Critério de Buchberger para submódulos)**.** *Um conjunto $G = \{g_1, \ldots, g_s\} \subset R^m$ é uma base de Gröbner para o módulo que ele gera se, e somente se, para todo $i \neq j$ o resto da divisão de $S(g_i, g_j)$ por G é 0.*

Demonstração. A demonstração é análoga ao Critério de Buchberger para ideais (Proposição 1.3.8). □

Exemplo 2.2.7. *Do Exemplo 2.1.11 temos que $f_1 = (xy + 4x, o, y^2) = xye_1 + 4xe_1 + y^2 e_3$ e $f_2 = (0, y - 1, x - 2) = ye_2 - e_2 + xe_3 - 2e_3$. Onde e_1, e_2, e_3 são os vetores canônicos em R^3. Logo $\boldsymbol{m} = \text{MMC}(TL(f_1), TL(f_2)) = 0$, pois os f_1 e f_2 possuem vetores canônicos diferentes em seus termos líderes. Portanto $S(f_1, f_2) = 0$.*

O **Algoritmo de Buchberger** para submódulos segue a mesma ideia do Algoritmo de Buchberger para ideais que vimos na seção 1.2.

Exemplo 2.2.8. *Sejam*

$$f_1 = (0, y, x), f_2 = (0, x, xy - x), f_3 = (x, y^2, 0), f_4 = (y, 0, x)$$

vetores de $(\mathbb{Q}[x, y])^3$. *Usando a ordem monomial lexicográfica graduada em* $\mathbb{Q}[x, y]$ *com* $x > y$ *e a extensão* TSP *em* $(\mathbb{Q}[x, y])^3$ *com* $e_1 > e_2 > e_3$, *vamos calcular a base de Gröbner para* $M =< f_1, f_2, f_3, f_4 >$ *usando o algoritmo de Buchberger para submódulos. Tomemos* $G = \{f_1, f_2, f_3, f_4\}$ *inicialmente. Observemos que:*

$$\begin{aligned} f_1 &= xe_3 + ye_2; \\ f_2 &= xye_3 + xe_2 - xe_3; \\ f_3 &= y^2e_2 + xe_1; \\ f_4 &= xe_3 + ye_1. \end{aligned}$$

Assim, só podemos calcular $S(f_1, f_2)$, $S(f_1, f_4)$ *e* $S(f_2, f_4)$.

- $S(f_1, f_2) = yf_1 - f_2 = (0, y^2 - x, x)$,

que dividido por G *se têm* $\overline{S(f_1, f_2)}^G = (-x, -x - y, 0)$. *Logo fazemos* $f_5 = (-x, -x - y, 0) = -xe_1 - xe_2 - ye_2$ *e adicionamos a* G;

- $S(f_1, f_4) = f_1 - f_4 = (-y, y, 0)$,

que dividido por G, *se têm* $\overline{S(f_1, f_4)}^G = (-y, y, 0)$. *Logo fazemos* $f_6 = (-y, y, 0) = -ye_1 + ye_2$ *e adicionamos a* G;

- $S(f_2, f_4) = f_2 - yf_4 = (-y^2, x, -x)$,

que dividido por G *se têm* $\overline{S(f_2, f_4)}^G = 0$. *Temos agora que considerar* $S(f_5, f_6)$.

- $S(f_5, f_6) = yf_5 - xf_6 = (0, -2xy - y^2, 0)$,

que dividido por G *se têm* $\overline{S(f_5, f_6)}^G = (00, -2xy - x - y, 0)$ *e fazemos* $f_7 = (0, -2xy - x - y, 0) = -2xye_2 - xe_2 - ye_2$ *e adicionamos a* G. *Vamos agora também considerar* $S(f_3, f_7)$.

- $S(f_3, f_7) = 2xf_3 + yf_7 = (2x^2, -xy - -y^2, 0)$,

que dividido por G *se têm* $\overline{S(f_3, f_7)}^G = (0, -2x^2 + \frac{1}{2}x + \frac{1}{2}y, 0)$ *e fazemos* $f_8 = (0, -2x^2 + \frac{1}{2}x + \frac{1}{2}y, 0) = -2x^2e_2 + \frac{1}{2}xe_2 + \frac{1}{2}ye_2$ *e adicionamos a* G. *Assim, ainda temos que considerar* $S(f_3, f_8)$ *e* $S(f_7, f_8)$.

- $S(f_3, f_8) = 2x^2f_3 + y^2f_8 = (2x^3, \frac{1}{2}xy^2 + \frac{1}{2}y^3, 0)$,

que dividido por G *se têm* $\overline{S(f_3, f_8)}^G = 0$.

- $S(f_7, f_8) = xf_7 - yf_8 = (0, -x^2 - \frac{3}{2}xy - \frac{1}{2}y^2, 0)$,

que dividido por G se têm $\overline{S(f_7, f_8)}^G = 0$.

Dessa forma, $G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$ é uma base de Gröbner para M.

Após o Exemplo 2.2.8, poderíamos questionar se existe uma base de Gröbner com menos elementos, como vimos na Seção 1.2, assim podemos expandir a Definição 1.3.15 para submódulos.

Definição 2.2.9. *Uma base de Gröbner $G = \{g_1, \ldots, g_s\} \subset R^m$ é uma **Base de Gröbner reduzida** para um submódulo $M \subset R^m$ se para todo $i \in \{1, \ldots, s\}$ temos*

i. $CL(g_i) = 1$;

ii. Nenhum monômio de g_i pertence a $< TL(G - \{g_i\}) >$.

Exemplo 2.2.10. *Voltando ao Exemplo 2.2.8, vimos que $G = \{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8\}$ é uma base de Gröbner para M, onde*

$$\begin{aligned}
g_1 &= xe_3 + ye_2 \\
g_2 &= xye_3 + xe_2 - xe_3 \\
g_3 &= y^2e_2 + xe_1 \\
g_4 &= xe_3 + ye_1 \\
g_5 &= xe_1 + xe_2 + ye_2 \\
g_6 &= ye_1 - ye_2 \\
g_7 &= xye_2 + \tfrac{1}{2}xe_2 + \tfrac{1}{2}ye_2 \\
g_8 &= x^2e_2 - \tfrac{1}{4}xe_2 - \tfrac{1}{4}ye_2
\end{aligned}$$

Observemos primeiramente que $ML(g_1)$ divide $ML(g_2)$ e $ML(g_4)$, assim, podemos eliminar g_2 e g_4. Observemos também que o monômio xe_1 em f_3 pertence a $< TL(G - \{f_3\}) >$, pois $TL(f_5) = xe_1$, logo, dividindo g_3 por g_5 temos como resto $y^2e_2 - xe_2 - ye_2$, assim, tomemos $g_3 = (0, y^2 - x - y, 0)$. Portanto $G = \{g_1, g_3, g_5, g_6, g_7, g_8\}$ formam uma base de Gröbner reduzida para M.

Capítulo 3

Algumas Aplicações

Veremos agora algumas aplicações da base de Gröbner. Ela nos ajudará a determinar a dimensão de um ideal $I \subset R$ e a calcular o Módulo Sizígia e Resoluções Livres de um módulo $M \subset R^m$. Além disso iremos demonstrar o Teorema Sizígia de Hilbert e estenderemos Resoluções Livres e o Teorema Sizígia de Hilbert para módulos graduados.

3.1 Dimensão de um Ideal

Seja $t[x_1, \ldots, x_n]$ o conjunto de todos os termos nas variáveis $x_1, \ldots, x_n$. Se o conjunto $\{u_1, \ldots, u_r\} \subset \{x_1, \ldots, x_n\}$, então $t[u_1, \ldots, u_r]$ é o conjunto de todos os termos em $t[x_1, \ldots, x_n]$ contendo somente variáveis em $\{u_1, \ldots, u_r\}$, com a convenção de que $t[\emptyset] = \{1\}$. $k[u_1, \ldots, u_r]$ é o subanel de $k[\mathbf{x}]$ contendo todos polinômios $f \in k[\mathbf{x}]$ tal que todos os termos de f pertencem a $t[u_1, \ldots, u_r]$, em particular, $k[\emptyset] = k$. Similarmente, seja $\{v_1, \ldots, v_l\} = \{x_1, \ldots, x_n\} - \{u_1, \ldots, u_r\}$, então $t[v_1, \ldots, v_l]$ denotará o conjunto de todos os termos em $t[x_1, \ldots, x_n]$ que contém somente as variáveis $\{v_1, \ldots, v_l\}$.

Denotaremos por $U = \{u_1, \ldots, u_r\}$, $X = \{x_1, \ldots, x_n\}$, $T = t[x_1, \ldots, x_n]$, $T_U = t[u_1, \ldots, u_r]$, $T_f = t(f)$ o conjunto dos termos de $f \in R$ e $R_U = k[u_1, \ldots, u_r]$.

Observemos que se $I \subset R$ é um ideal e $U \subset X$, então $I \cap R_U$ é um ideal do anel R_U.

Definição 3.1.1. *Seja $I \subset R$ um ideal e $U \subset X$. O ideal $I \cap R_U$ é chamado de **ideal de eliminação** de I com respeito a U e é denotado por I_U.*

Observação 3.1.2. *Seja $>$ uma ordem monomial sobre os termos de T e $U \subset X$, escrevemos*

$$X - U \ggg U$$

se $g > f$ para todo $f \in T_U$ e $1 \neq g \in T_{X-U}$.

Notemos que sempre podemos encontrar uma ordem monomial $>$ em T satisfazendo $X - U \ggg U$, basta tomar a ordem lexicográfica onde todas as variáveis em U são menores que todas de $X - U$.

Lema 3.1.3. *Suponha $U \subset X$ e $>$ uma ordem monomial satisfazendo $X - U \ggg U$. Logo:*

a. Se $f \in T$ e $g \in T_U$ com $g > f$, então $f \in T_U$;

b. *Seja $f, p \in R$ polinômios não nulos. Pelo algoritmo da divisão, existem $q, r \in R$ tais que $f = qp + r$. Se $f \in R_U$ e $q \neq 0$, então $p, r \in R_U$.*

Demonstração.

a. Suponhamos que $f \notin T_U$. Então podemos escrever $f = f_1 f_2$ com $1 \neq f_2 \in T_{X-U}$. Por hipótese $X - U \ggg U$, assim

$$f_2 > g > f.$$

Multiplicando pelo monômio f_1 e por b da Definição 1.1.1, temos que

$$f_1 f_2 > f_1 g > f_1 f,$$

ou seja, $f > f_1 f$, absurdo. Logo $f \in T_U$.

b. Observemos que $TL(p)$ divide algum $f_i \in T_f$, pois $q \neq 0$, logo $TL(p) \in T_U$ e assim $T_p \subset T_U$ por a, ou seja, $p \in R_U$. Visto que $r = f - qp$ e que $q \in R_U$ (pois cada termo de q divide algum termo de f), segue imediatamente que $r \in R_U$.

□

Nossa próxima proposição nos dará uma maneira de calcular ideais de eliminação. Relembremos que por convenção o ideal $< \emptyset >= \{o\}$. Assim o conjunto vazio é uma base de Gröbner para o ideal nulo.

Proposição 3.1.4. *Seja $I \subset R$ um ideal e $U \subset X$. Suponha que $>$ é uma ordem monomial em T que satisfaz $X - U \ggg U$ e G uma base de Gröbner para I com relação a ordem $>$. Então $G \cap R_U$ é uma base de Gröbner para o ideal de eliminação I_U.*

Demonstração. Considere $G = \{g_1, \ldots, g_s\}$, se $TL(g_i) \in T_u$, $i \in \{1, \ldots, s\}$, então por a do Lema 3.1.3, $T_{g_i} \subset T_U$, logo $g_i \in G \cap R_U$.

Vamos mostrar que, sendo $G \cap R_U = \{g_{U_1}, \ldots, g_{U_r}\}$, então

$$< TL(I_U) >=< TL(g_{U_1}), \ldots, TL(g_{U_r}) > .$$

Notemos que $< TL(g_{U_1}), \ldots, TL(g_{U_r}) > \subset < TL(I_U) >$, pois $g_{U_j} \in I_U$, $j \in \{1, \ldots, r\}$. Seja agora $f \in I_U$, logo $TL(f) \in < TL(I_U) >$, e pela definição de Base de Gröbner, existe algum $g_i \in G$, $i \in \{1, \ldots, s\}$, tal que $TL(g_i)$ divide $TL(f)$. Assim, podemos ter $TL(f) = TL(g_i)$ ou $TL(f) > TL(g_i)$. Se $TL(f) = TL(g_i)$, então temos que $g_i = g_{U_j} \in G \cap R_U$ e $TL(f) \in < TL(g_{U_1}), \ldots, TL(g_{U_r}) >$. E se $TL(f) > TL(g_i)$ temos por a do Lema 3.1.3 que $TL(g_i) \in T_U$, e consequentemente, para algum j, $g_i = g_{U_j} \in G \cap R_U = G_U$ e $TL(f) \in < TL(g_{U_1}), \ldots, TL(g_{U_r}) >$. Portando $< TL(I_U) > \subset < TL(g_{U_1}), \ldots, TL(g_{U_r}) >$. □

Poderíamos perguntar se $F \cap R_U$ é um conjunto gerador para I_U, sendo F um conjunto gerador qualquer de um ideal $I \subset R$, tal que as hipóteses sejam satisfeitas. Como veremos no exemplo abaixo, a resposta é não.

Exemplo 3.1.5. *Dos Exemplos 1.3.11 e 1.3.14 vimos que o ideal $I \subset R$ gerado por $F = \{x^2 y - 1, xy^2 - x\}$ tem sua base de Gröbner reduzida $G = \{x^2 - y, y^2 - 1\}$, usando a ordem lexicográfica com $x > y$. Observemos que as hipóteses da proposição acima são satisfeitas e que $F \cap k[y] = \{\emptyset\}$ e $G \cap k[y] = \{y^2 - 1\}$. Logo a base de Gröbner do ideal de eliminação I_U, com $U = \{y\}$ é $\{y^2 - 1\}$ e assim $I_U =< y^2 - 1 >$.*

Antes de prosseguimos, observemos que a Proposição 3.1.4 aplicada para $U = \emptyset$ diz que o ideal de eliminação $I \cap R_U = I \cap k$ é gerado por $G \cap k$ para toda base de Gröbner G de I satisfazendo as hipóteses. Visto que k é um corpo, esse ideal de eliminação só pode ser $\{0\}$ ou k. Assim $G \cap k \neq \{\emptyset\}$ se, e somente se, $I = R$.

Definição 3.1.6. *Seja $I \subset R$ um ideal próprio e $U \subset X$. Então U é chamado de* ***conjunto independente*** *de I se $I_U = \{0\}$. Mais ainda, U é chamado de* ***conjunto independente maximal*** *de I se ele é um conjunto independente de I e não está contido propriamente em qualquer outro conjunto independente de I.*

Definição 3.1.7. *Seja $I \subset R$ um ideal próprio e $U \subset X$ um conjunto independente de I. A* ***dimensão*** *de I, denotada por* $\dim(I)$*, é definida da seguinte maneira,*

$$\dim(I) = \max\{|U|; U \subset X \text{ seja um conjunto independente de } I\}. \tag{3.1}$$

Um ideal $I \subset R$ será chamado de **zero-dimensional** se ele é próprio e possui dimensão zero.

Usando a Proposição 3.1.4 e o fato de $< \emptyset >= \{0\}$, temos que, sendo $I \subset R$ um ideal próprio e $U \subset X$ um conjunto independente de I, então $G \cap R_U = \{\emptyset\}$ para toda base de Gröbner G de I, considerando uma ordem monomial satisfazendo $X - U \ggg U$.

Exemplo 3.1.8. *Seja $R = \mathbb{Q}[x, y, z]$ e $I \subset R$ um ideal gerado por $G = \{xz + z, yz + z\}$, onde G é uma base de Gröbner. Considerando a ordem lexicográfica e $x > y > z$, temos que xz e yz são os termos líderes, respectivamente, dos dois polinômios. Logo para todo $f \in I$, o $TL(f)$ é divisível por xz ou yz. Assim podemos concluir que $I \cap k[x] = I \cap k[y] = I \cap k[z] = I \cap k[x, y] = \{0\}$. Ou seja, os conjuntos independentes de I são $\{x\}$, $\{y\}$, $\{z\}$, e $\{x, y\}$, onde, desses, $\{z\}$ e $\{x, y\}$ são independentes maximais, assim,* $\dim(I) = 2$.

Poderíamos nos perguntar o que aconteceria se as variáveis fossem ordenadas diferentes, ou seja, se por exemplo, $z > y > x$. Notemos que em todo caso G ainda seria uma base de Gröbner e os termos líderes dos elementos de G seria xz e yz.

Lema 3.1.9. *Se I e J são ideais próprios de R com $I \subset J$, então* $\dim(J) \leq \dim(I)$.

Demonstração. Segue direto das definições, visto que se $U \subset X$ é um conjunto independente de J, então também será um conjunto independente de I. □

Lema 3.1.10. *Seja $I \subset R$ um ideal próprio. Então*

a. *$I \subset k[\mathbf{x}]$ é um ideal zero-dimensional se, e somente se, para cada variável, I contém um polinômio de grau positivo que depende somente dessa variável;*

b. *Sejam I, J ideais próprios tais que J contém I e $U \subset X$ um subconjunto qualquer. Se I é zero-dimensional, então J e I_U também são.*

Demonstração.

a. Observemos que se I contém um polinômio de grau positivo de somente uma variável, para cada variável, então $I \cap R[x_i] \neq \{0\}$, para todo $i \in \{1, \ldots, n\}$. Seja $f_i \in I \cap R[x_i]$,

dado $U \subset X$ não vazio, ou seja, existe $x_i \in U$, temos que $f_i \in I \cap R_U$, isto é, $I \cap R_U \neq \{0\}$. Logo I é zero-dimensional.

Reciprocamente, se I é zero dimensional, então $U = \{x_i\}$ não é conjunto independente de I, para todo $i \in \{1, \ldots, n\}$, assim $I \cap k[x_i] \neq \{0\}$. Como I é ideal próprio, I contém um polinômio de grau positivo que depende de somente uma variável, para cada variável.

b. Pelo Lema 3.1.9 segue que $\dim(J) = 0$. Como I é zero-dimensional, todo ideal de eliminação de I com respeito a qualquer conjunto formado por variáveis é diferente de $\{0\}$. Veremos que $\dim(I_U) = 0$, ou seja, $(I_U)_{U'} \neq \{0\}$, para todo $U' \subset U$. De fato,

$$(I_U)_{U'} = I_U \cap R_{U'} = I \cap R_U \cap R_{U'} = I \cap R_{U'} \neq \{0\},$$

pois $\dim(I) = 0$.

□

Seja $>$ é uma ordem monomial sobre os termos de T, então o conjunto de **termos reduzidos** sobre I é definido como $T - TL(I)$ e será denotada por $TR(I)$.

Lema 3.1.11. *Seja $>$ uma ordem monomial sobre T e $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner de I com respeito a $>$. Então*

$$\begin{aligned} TR(I) &= \{f \in T; g \nmid f \text{ para todo } g \in TL(I)\} \\ &= \{f \in T; g \nmid f \text{ para todo } g \in TL(G)\}, \end{aligned}$$

onde $TL(G) = \{TL(g_1), \ldots, TL(g_s)\}$.

Demonstração. Seja $\text{mult}(TL(I)) = \{ph; p \in T \text{ e } h \in TL(I)\}$. Observemos que se $f \in I$ e $g \in T$, então $gf \in I$ e $TL(gf) = g.TL(f)$, assim $TL(I) = \text{mult}(TL(I))$. Logo $TR(I) = T - \text{mult}(TL(I))$, ou seja,

$$TR(I) = \{f \in T; g \nmid f \text{ para todo } g \in TL(I)\}.$$

Para a segunda parte, basta observar que $\text{mult}(TL(G)) = TL(I)$, visto que sendo $G = \{g_1, \ldots, g_s\}$, se $f \in \text{mult}(TL(G))$, então $f = pTL(g_i)$, com $i \in \{i, \ldots, s\}$ e $p \in T$. Como $TL(g_i) \in TL(I)$, $f \in TL(I)$. Reciprocamente, se $f \in TL(I)$, então existe i tal que $TL(g_i)$ divide $TL(f)$, ou seja, $TL(f) = pTL(g_i)$, com $p \in T$, logo $f \in \text{mult}(TL(G))$. E assim temos que

$$TR(I) = T - TL(I) = T - \text{mult}(TL(G)) = \{f \in T; g \nmid f \text{ para todo } g \in TL(G)\}.$$

□

Estabeleceremos agora uma conexão entre a dimensão de I, o conjunto dos termos líderes de I (usando uma ordem monomial qualquer) e a dimensão do k-espaço vetorial R/I.

Iremos denotar a classe de resíduos $g + I \in R/I$ de um elemento $g \in R$ por $\overline{g}$. Analogamente se $A \subset R$, então $\overline{A} = \{\overline{g}; g \in A\}$.

Proposição 3.1.12. *Sejam $>$ qualquer ordem monomial sobre T, $I \subset R$ um ideal e $B = \overline{TR(I)} \subset R/I$. Então B é uma base para k-espaço vetorial R/I.*

Demonstração. Recordemos que a multiplicação por escalar em R/I é definido por $a \cdot \overline{f} = \overline{af}$. Mostraremos primeiramente que B gera R/I. Suponha que G seja uma base de Gröbner sobre I com respeito a $>$. Seja $f \in R$ e h o resto ao dividir f por G. Então $\overline{f} = \overline{h}$ e $T_h \subset TR(I)$. Daí

$$\begin{aligned} \overline{f} &= \overline{h} \\ &= \overline{\sum_{p \in T_h} a_p p} \ \ (a_p \in k) \\ &= \sum_{p \in T_h} \overline{a_p p} \\ &= \sum_{p \in T_h} a_p \overline{p}. \end{aligned}$$

Vamos mostrar agora que B é linearmente independente. Assuma que exista uma combinação linear

$$0 = \sum_{i=1}^{r} a_i \cdot \overline{t_i} \ \ (a_i \in k, \ t_i \in TR(I)),$$

onde nem todos a_i, $i \in \{1, \ldots, r\}$, são zero. Sem perda de generalidade, suponhamos que $a_1 \neq 0$ e $t_1 > t_i$ para $i \in \{2, \ldots, r\}$. Se tomarmos

$$h = \sum_{i=1}^{r} a_i t_i,$$

então $h \neq 0$ e $TL(h) = a_1 t_1$, e além disso, $h \in I$, pois $\overline{h} = 0$. Logo existe um $s \in TL(G)$ tal que s divide $TL(h) = a_1 t_1$, contradizendo $t_1 \in TR(I)$ (Lema 3.1.11). □

Até o momento vimos que para saber a dimensão de um ideal temos que calcular as bases de Gröbner usando uma ordem monomial que satisfaça $X - U \ggg U$. Isto pode se tornar trabalhoso, pois, para cada U que queremos saber se o mesmo é um conjunto independente, temos que usar uma ordem que satisfazendo $X - U \ggg U$ e calcular novamente uma base de Gröbner. O Lema abaixo nos permitira dizer, usando qualquer ordem monomial, se a dimensão de um ideal é zero ou não.

Lema 3.1.13. *Seja I um ideal próprio de R. Então são equivalentes:*

a. $\dim(I) = 0$*;*

b. Existe uma ordem monomial $>$ sobre T e uma base de Gröbner G de I com respeito a $>$ tal que, para cada $i \in \{1, \ldots, n\}$, existe um $g_i \in G$ com $TL(g_i) = x_i^{\alpha_i}$, para algum $0 < \alpha_i \in \mathbb{Z}_+$;

c. Para toda ordem monomial $>$ sobre T e toda base de Gröbner G de I com respeito a $>$, existe (a menos de ordenação e multiplicação por constante), para cada $i \in \{1, \ldots, n\}$, um $g_i \in G$, com $TL(g_i) = x_i^{\alpha_i}$, para algum $0 < \alpha_i \in \mathbb{Z}_+$.

Demonstração. Vamos mostrar que $a \Leftrightarrow c$ e $b \Leftrightarrow c$.

- $(a \Rightarrow c)$ Se $\dim(I) = 0$, então por a do Lema 3.1.10, I contém um polinômio de grau positivo que depende somente da variável x_i, $p_i = \sum_{j=1}^{r_i} a_j x_i^j$, com $r_i > 0$ e $i \in \{1, \ldots, n\}$. Seja G uma base de Gröbner qualquer de I, com respeito a qualquer ordem monomial. Como $TL(p_i) = a_i x_i^{r_i}$ e $TL(p_i) \in < TL(I) > = < TL(G) >$, então existe $g_j \in G$ tal que $TL(g_j) = c_i x_i^{\alpha_i}$ para algum $0 < \alpha_i \in \mathbb{Z}_+$.

- $(c \Rightarrow a)$Suponhamos que $\dim(I) \neq 0$, logo existe algum conjunto $U = \{u_1, \ldots, u_r\} \subset X$ tal que $I \cap R_U = \{0\}$. Seja $>$ uma ordem monomial que satisfaça $X - U \ggg U$ e G uma base de Gröbner de I. Pela Proposição 3.1.4 temos $G \cap R_U = \{\emptyset\}$. Ou seja, $TL(g_i) \neq u_j^{\alpha}$, para todo $g_i \in G$ e $u_j \in U$, pois, caso $TL(g_i) = u_j^{\alpha}$, para algum $g_i \in G$ e $u_j \in U$, teríamos que $g_i \in G \cap R_U$, visto que $X - U \ggg U$. Logo $\dim(I) = 0$.

- $(b \Rightarrow c)$ Observemos que se para alguma ordem monomial $>$ e alguma base de Gröbner G tivermos $TL(g_i) = x_i^{\alpha_i}$, então $x_i^{\alpha_k} \notin TR(I)$, para $\alpha_k \geq \alpha_i$ e assim, pela Proposição 3.1.12, o k-espaço vetorial R/I gerado por $\overline{TR(I)}$ tem dimensão finita. Suponhamos agora que exista alguma ordem monomial $>$ e uma base de Gröbner G tal que, para algum $i \in \{1, \ldots, n\}$ $TL(g_j) \neq x_i^{\alpha_i}$, para todo $g_j \in G$. Então $x_i^{\alpha_i} \in TR(I)$ para todo $0 < \alpha_i \in \mathbb{Z}_+$, logo R/I tem dimensão infinita como k-espaço vetorial, contrariando o fato do k-espaço vetorial R/I ter dimensão finita.

- $(c \Rightarrow b)$ Trivial.

□

Sabemos que sendo $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner de um ideal $I \subset R$, então dado $f \in I$, $TL(g_i)$ divide $TL(f)$, para algum $i \in \{i, \ldots, s\}$. Assim, podemos enunciar o seguinte corolário:

Corolário 3.1.14. *Seja I um ideal próprio de R. Então são equivalentes:*

a. $\dim(I) = 0$*;*

b. Existe uma ordem monomial $>$ sobre T, tal que, para cada $i \in \{1, \ldots, n\}$, existe $g_i \in I$, com $TL(g_i) = x_i^{\alpha_i}$, para algum $0 < \alpha_i \in \mathbb{N}$;

c. Para toda ordem monomial $>$ sobre T, existe, para cada $i \in \{1, \ldots, n\}$, um $g_i \in I$, com $TL(g_i) = x_i^{\alpha_i}$, para algum $0 < \alpha_i \in \mathbb{N}$.

Exemplo 3.1.15. *Seja $k = \mathbb{Q}$, $n = 2$ e $I = < f_1, f_2 >$, com $f_1 = x^2 + y + 1$ e $f_2 = 2xy + y$. Usando a ordem lexicográfica com $x > y$, temos que uma base de Gröbner reduzida para I é*

$$G = \{x^2 + y + 1, xy + \frac{y}{2}, y^2 + \frac{5}{4}y\},$$

visto que $TL(x^2 + y + 1) = x^2$ e $TL(y^2 + \frac{5}{4}y) = y^2$, então, pela Proposição 3.1.13, temos $\dim(I) = 0$.

3.2 Sizígia

Sizígia é o termo utilizado em astronomia para designar o alinhamento de três corpos celestes, mas em matemática é o termo utilizado para designar o núcleo de um homomorfismo de R-módulos.

Seja $I =< f_1, \ldots, f_s > \subset R$ um ideal. Consideremos o homomorfismo de R-módulo φ definido da forma:

$$\varphi : R^s \longrightarrow I$$

tal que

$$(h_1, \ldots, h_s) \longmapsto \sum_{i=1}^{s} h_i f_i.$$

Definição 3.2.1. *O núcleo da aplicação φ é chamado de **módulo Sizígia** da matriz*

$$\left[\begin{array}{ccc} f_1 & \ldots & f_s \end{array}\right]_{1\times s}.$$

O qual é denotado por $\mathrm{Syz}(f_1, \ldots, f_s)$. *Um elemento* $(h_1, \ldots, h_s)$ *de* $\mathrm{Syz}(f_1, \ldots, f_s)$ *é chamado de uma sizígia de* $\left[\begin{array}{ccc} f_1 & \ldots & f_s \end{array}\right]$, *ou seja, ele satisfaz*

$$h_1 f_1 + \ldots + h_s f_s = 0.$$

Observação 3.2.2. *Podemos também dizer que* $\mathrm{Syz}(f_1, \ldots, f_s)$ *é o conjunto solução da equação linear*

$$f_1\chi_1 + \ldots f_s\chi_s = 0,$$

onde os f_i's são os coeficientes da equação e $\chi_i \in R$.

Notemos também que a aplicação φ pode ser vista como uma multiplicação de matriz

$$\varphi(h_1, \ldots, h_s) = \left[\begin{array}{ccc} f_1 & \ldots & f_s \end{array}\right] \left[\begin{array}{c} h_1 \\ \vdots \\ h_s \end{array}\right] = \sum_{i=1}^{s} h_i f_i.$$

Isto é, se F é a matriz $\left[\begin{array}{ccc} f_1 & \ldots & f_s \end{array}\right]$, e $h = \left[\begin{array}{c} h_1 \\ \vdots \\ h_s \end{array}\right] \in R^s$, então $\varphi(h_1, \ldots, h_s) = Fh$ e $\mathrm{Syz}(f_1, \ldots, f_s)$ é o conjunto de todas soluções h da equação linear $Fh = 0$.

Exemplo 3.2.3. *Seja $R = \mathbb{Q}[x, y, z, w]$, e $I =< x^2 - yw, xy - wz, y^2 - xz >$. Podemos assim definir a aplicação $\varphi : R^3 \longrightarrow I$ dada por*

$$(h_1, h_2, h_3) \longmapsto h_1(x^2 - yw) + h_2(xy - wz) + h_3(y^2 - xz),$$

onde $(y, -x, w)$ e $(-z, y, -x)$ são ambos sizígias de

$$\left[\begin{array}{ccc} x^2 - yw & xy - wz & y^2 - xz \end{array}\right],$$

pois

$$y(x^2 - yw) - x(xy - wz) + w(y^2 - xz) = 0$$

e

$$-z(x^2 - yw) + y(xy - wz) - x(y^2 - xz) = 0.$$

De maneira semelhante podemos definir uma Sizígia para submódulos de R^m.

Definição 3.2.4. *Sejam $f_1, \ldots, f_s \in R^m$. Uma **Sizígia** da matriz $F = \begin{bmatrix} f_1 & \ldots & f_s \end{bmatrix}_{m\times s}$ é um vetor $(h_1, \ldots, h_s) \in R^s$ tal que*

$$\sum_{i=1}^{s} h_i f_i = 0.$$

O conjunto de todas sizígias é chamado o módulo Sizígia de F e é denotada por $\mathrm{Syz}(f_1, \ldots, f_s)$ *ou* $\mathrm{Syz}(F)$.

Em outras palavras, $\mathrm{Syz}(F) = \mathrm{Syz}(f_1, \ldots, f_s)$ pode ser visto como o conjunto de todas soluções $h \in R^s$ de um sistema de equações lineares homogêneas **Fh=0** com coeficientes polinomiais. Ou seja, se $f_1 = (f_{11}, \ldots, f_{m1}), \ldots, f_s = (f_{1s}, \ldots, f_{ms})$, então $\mathrm{Syz}(f_1, \ldots, f_s)$ é o conjunto de todas soluções do sistema

$$\begin{cases} f_{11}\chi_1 + \ldots + f_{1s}\chi_s &= 0 \\ f_{21}\chi_1 + \ldots + f_{2s}\chi_s &= 0 \\ \vdots & \vdots \ \vdots \\ f_{m1}\chi_1 + \ldots + f_{ms}\chi_s &= 0 \end{cases}$$

Seja M um módulo dado por t geradores $f_1, \ldots, f_t$, a **matriz de apresentação** para M é qualquer matriz cujas colunas geram $\mathrm{Syz}(f_1, \ldots, f_t) \subset R^t$.

Proposição 3.2.5. *Sejam $\{\boldsymbol{m}_1, \ldots \boldsymbol{m}_t\}$ um conjunto de geradores monomiais para um submódulo monomial de R^m e $\varepsilon_1, \ldots, \varepsilon_t$ os vetores da base canônica de R^t. Seja também $\boldsymbol{m}_{ij} = \mathrm{MMC}(\boldsymbol{m}_i, \boldsymbol{m}_j)$. O módulo Sizígia, $\mathrm{Syz}(\boldsymbol{m}_1, \ldots, \boldsymbol{m}_t)$, é gerado pelas sizígias*

$$\sigma_{ij} = \frac{\boldsymbol{m}_{ij}}{\boldsymbol{m}_i}\,\varepsilon_i - \frac{\boldsymbol{m}_{ij}}{\boldsymbol{m}_j}\,\varepsilon_j,$$

para todo $1 \leq i < j \leq t$ (se m_i e m_j contêm diferentes vetores canônicos, $\sigma_{ij} = 0$).

Demonstração. Definamos

$$\sigma_{ij} = \frac{\mathbf{m}_{ij}}{\mathbf{m}_i}\,\varepsilon_i - \frac{\mathbf{m}_{ij}}{\mathbf{m}_j}\,\varepsilon_j,$$

vamos provar que $\mathrm{Syz}(\mathbf{m}_1, \ldots, \mathbf{m}_t) =< \sigma_{ij}; 1 \leq i < j \leq t >$. Observemos que sendo $\mathbf{m}_i = \mathbf{x}^\alpha e_l$ e $\mathbf{m}_j = \mathbf{x}^\beta e_r$, então $\mathrm{MMC}(\mathbf{m}_i, \mathbf{m}_j) = \mathbf{m}_{ij} = \mathbf{x}^\gamma$ se $l = r$ ou $\mathrm{MMC}(\mathbf{m}_i, \mathbf{m}_j) = 0$ se $l \neq r$. Assim, se $l \neq r$, temos $\sigma_{ij} = (0, \ldots, 0)$ e $\sigma_{ij} \in \mathrm{Syz}(\mathbf{m}_1, \ldots, \mathbf{m}_t)$, suponhamos $l = r$, então

$$\sigma_{ij} = (0, 0, \ldots, 0, \frac{\mathbf{x}^\gamma}{\mathbf{x}^\alpha}, 0, \ldots, o, -\frac{\mathbf{x}^\gamma}{\mathbf{x}^\beta}, 0, \ldots, 0),$$

onde $\dfrac{\mathbf{x}^\gamma}{\mathbf{x}^\alpha}$ está na i-ésima posição e $-\dfrac{\mathbf{x}^\gamma}{\mathbf{x}^\beta}$ está na j-ésima posição. Assim

$$\begin{bmatrix} \mathbf{m}_1 & \mathbf{m}_2 & \cdots & \mathbf{m}_t \end{bmatrix} \begin{bmatrix} 0 & \cdots & 0 & \dfrac{\mathbf{x}^\gamma}{\mathbf{x}^\alpha} & 0 & \cdots & 0 & -\dfrac{\mathbf{x}^\gamma}{\mathbf{x}^\beta} & 0 & \cdots & 0 \end{bmatrix}^T = 0,$$

logo $\sigma_{ij} \in \mathrm{Syz}(\mathbf{m}_i, \ldots, \mathbf{m}_t)$, portanto $< \sigma_{ij}; 1 \leq i < j \leq t > \subset \mathrm{Syz}(\mathbf{m}_i, \ldots, \mathbf{m}_t)$.

Vamos agora provar que $\mathrm{Syz}(\mathbf{m}_i, \ldots, \mathbf{m}_t) \subset < \sigma_{ij}; 1 \leq i < j \leq t >$. Seja $(a_1, \ldots, a_t) \in \mathrm{Syz}(\mathbf{m}_i, \ldots, \mathbf{m}_t)$, expandindo em termos da base canônica de R^m, temos

$$0 = a_1\mathbf{m}_1 + \ldots + a_t\mathbf{m}_t = f_1e_1 + \ldots + f_me_m, \tag{3.2}$$

assim $f_1 = \ldots = f_m = 0$. Logo podemos restringir e considerar apenas as coleções de monômios contendo o mesmo e_i. Sem perda de generalidade, suponhamos

$$\mathbf{m}_1 = \mathbf{x}^{\alpha_1}e_i, \ldots, \mathbf{m}_s = \mathbf{x}^{\alpha_s}e_i \ ,$$

com $s \leq t$, assim $(a_1, \ldots, a_s) \in \mathrm{Syz}(\mathbf{m}_1, \ldots, \mathbf{m}_s)$. Observemos que pela igualdade de polinômios e por $a_1\mathbf{m}_1 + \ldots + a_s\mathbf{m}_s = 0$, temos

$$0 = a_1\mathbf{m}_1 + \ldots + a_s\mathbf{m}_s = c_1\mathbf{x}^{\lambda} + \ldots + c_s\mathbf{x}^{\lambda},$$

onde $c_i \in k$ e $a_i = \mathbf{x}^{\lambda-\alpha_i}$, $i \in \{1, \ldots, s\}$. Assim

$$(a_1, \ldots, a_s) = (c_1\mathbf{x}^{\lambda-\alpha_1}, \ldots, c_s\mathbf{x}^{\lambda-\alpha_s}),$$

com $c_1 + \ldots + c_s = 0$. Tal sizígia é chamada uma **Sizígia Homogênea**, e como vimos, todas sizígias são somas de sizígias homogêneas.

Observemos também que

$$\begin{aligned}(c_1\mathbf{x}^{\lambda-\alpha_1}, \ldots, c_s^{\lambda-\alpha_s}) = \ & (c_1\mathbf{x}^{\lambda-\alpha_1}, -c_1\mathbf{x}^{\lambda-\alpha_2}, 0, \ldots, 0)+ \\ & (0, (c_1 + c_2 + c_4 + \ldots + c_s)\mathbf{x}^{\lambda-\alpha_2}, c_3\mathbf{x}^{\lambda-\alpha_3}, 0 \ldots, 0) + \ldots + \\ & (0, -c_i\mathbf{x}^{\lambda-\alpha_2}, 0, \ldots, 0, c_i\mathbf{x}^{\lambda-\alpha_i}, 0, \ldots, 0) + \ldots + \\ & (0, -c_s\mathbf{x}^{\lambda-\alpha_2}, 0, \ldots, 0, c_s\mathbf{x}^{\lambda-\alpha_s}),\end{aligned}$$

onde

$$(c_1\mathbf{x}^{\lambda-\alpha_1}, -c_1\mathbf{x}^{\lambda-\alpha_2}, 0, \ldots, 0) = c_1(\mathbf{x}^{\lambda-\alpha_1}, -\mathbf{x}^{\lambda-\alpha_2}, 0, \ldots, 0)$$

é uma sizígia sobre o par $\mathbf{x}^{\alpha_1}$ e $\mathbf{x}^{\alpha_2}$,

$$\begin{aligned}((c_1 + c_2 + c_4 + \ldots + c_s)\mathbf{x}^{\lambda-\alpha_2}, c_3\mathbf{x}^{\lambda-\alpha_3}, 0 \ldots, 0) &= (-c_3\mathbf{x}^{\lambda-\alpha_2}, c_3\mathbf{x}^{\lambda-\alpha_3}, 0 \ldots, 0) \\ &= -c_3(\mathbf{x}^{\lambda-\alpha_2}, -\mathbf{x}^{\lambda-\alpha_3}, 0 \ldots, 0)\end{aligned}$$

é uma sizígia sobre o par $\mathbf{x}^{\alpha_2}$ e $\mathbf{x}^{\alpha_3}$,

$$(0, -c_i\mathbf{x}^{\lambda-\alpha_2}, 0, \ldots, 0, c_i\mathbf{x}^{\lambda-\alpha_i}, 0 \ldots, 0) = -c_i(0, \mathbf{x}^{\lambda-\alpha_2}, 0, \ldots, 0, -\mathbf{x}^{\lambda-\alpha_i}, 0, \ldots, 0)$$

é uma sizígia sobre o par $\mathbf{x}^{\alpha_2}$ e $\mathbf{x}^{\alpha_i}$, e

$$(0, -c_s\mathbf{x}^{\lambda-\alpha_2}, 0, \ldots, 0, c_s\mathbf{x}^{\lambda-\alpha_s}) = -c_s(0, \mathbf{x}^{\lambda-\alpha_2}, 0, \ldots, 0, -\mathbf{x}^{\lambda-\alpha_s})$$

é uma sizígia sobre o par $\mathbf{x}^{\alpha_2}$ e $\mathbf{x}^{\alpha_s}$ (notemos que essa é uma, entre varias outras, maneiras de se escrever $(c_1\mathbf{x}^{\lambda-\alpha_1}, \ldots, c_s^{\lambda-\alpha_s})$ como uma soma de sizígias entre os pares de monômios).

Visto que dados dois monômios $\mathbf{x}^{\alpha}$ e $\mathbf{x}^{\beta}$ e $\mathbf{x}^{\gamma} = \mathrm{MMC}(\mathbf{x}^{\alpha}, \mathbf{x}^{\beta})$, então a sizígia $(\mathbf{x}^{\gamma-\alpha}, -\mathbf{x}^{\gamma-\beta})$ é o mesmo que

$$\sigma = \left(\frac{\mathrm{MMC}(\mathbf{x}^{\alpha}, \mathbf{x}^{\beta})}{\mathbf{x}^{\alpha}}, -\frac{\mathrm{MMC}(\mathbf{x}^{\alpha}, \mathbf{x}^{\beta})}{\mathbf{x}^{\beta}}\right).$$

Assim $(a_1, \ldots, a_s) \in < \sigma_{ij}; 1 \leq i < j \leq s >$, e como vimos em 3.2, $(a_1, \ldots, a_t)$ é a soma de sizígias contendo o mesmo vetor canônico e_i, consequentemente

$$(a_1, \ldots, a_t) \in < \sigma_{ij}; 1 \leq i < j \leq t >,$$

ou seja, $\text{Syz}(\mathbf{m}_1, \ldots, \mathbf{m}_t) \subset < \sigma_{ij}; 1 \leq i < j \leq t >$. Portanto $\text{Syz}(\mathbf{m}_1, \ldots, \mathbf{m}_t) = < \sigma_{ij}; 1 \leq i < j \leq t >$.

□

Agora começaremos o estudo das Sizígias em um conjunto de elementos de um módulo, com o intuito de resolver o seguinte problema: dado uma s-upla de elementos ordenados $\{f_1, \ldots, f_s\}$ de R^m(por exemplo, um conjunto ordenado de geradores), encontrar um conjunto de geradores para o módulo Sizígia $\text{Syz}(f_1, \ldots, f_s) \subset R^s$.

Seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner para um submódulo $M \subset R^m$ com uma ordem monomial $>$ fixada. Como G é uma base de Gröbner, pelo Lema 2.2.6, o resto de $S(g_i, g_j)$ na divisão por G é zero, assim

$$S(g_i, g_j) = \sum_{l=1}^{s} a_{ij_l} g_l, \tag{3.3}$$

onde $a_{ij_l} \in R$, e $TL(a_{ij_l} g_l) \leq TL(S(g_i, g_j))$ para todo i, j, l.

Considere $\varepsilon_1, \ldots, \varepsilon_s$ a base canônica de R^s. Seja $\mathbf{m}_{ij} = \text{MMC}(TL(g_i), TL(g_j))$, e seja $a_{ij} \in R^s$ o vetor coluna definido por

$$a_{ij} = a_{ij_1}\varepsilon_1 + a_{ij_2}\varepsilon_2 + \ldots + a_{ij_s}\varepsilon_s \in R^s.$$

Para o par (i, j), tal que $\mathbf{m}_{ij} \neq 0$, defina $s_{ij} \in R^s$ da seguinte forma:

$$s_{ij} = \frac{\mathbf{m}_{ij}}{TL(g_i)}\varepsilon_i - \frac{\mathbf{m}_{ij}}{TL(g_j)}\varepsilon_j - a_{ij} \tag{3.4}$$

em R^s, e seja $s_{ij} = 0$ caso $\mathbf{m}_{ij} = 0$.

Proposição 3.2.6. *Com a notação acima, a coleção $\{s_{ij}; 1 \leq i < j \leq t\}$ é um conjunto gerador para* $\text{Syz}(G) = \text{Syz}(g_1, \ldots, g_s)$.

Demonstração. Observemos primeiramente que

$$\begin{aligned} s_{ij} &= \frac{\mathbf{m}_{ij}}{TL(g_i)}\varepsilon_i - \frac{\mathbf{m}_{ij}}{TL(g_j)}\varepsilon_j - a_{ij} \\ &= \frac{\mathbf{m}_{ij}}{TL(g_i)}\varepsilon_i - \frac{\mathbf{m}_{ij}}{TL(g_j)}\varepsilon_j - (a_{ij_1}\varepsilon_1 + a_{ij_2}\varepsilon_2 + \ldots + a_{ij_s}\varepsilon_s) \\ &= (-a_{ij_1})\,\varepsilon_1 + \ldots + \left(\frac{\mathbf{m}_{ij}}{TL(g_i)} - a_{ij_i}\right)\varepsilon_i + \ldots + \left(-\frac{\mathbf{m}_{ij}}{TL(g_j)} - a_{ij_j}\right)\varepsilon_j + \ldots + (-a_{ij_s})\,\varepsilon_s\,. \end{aligned}$$

E que

$$\begin{bmatrix} g_1 & \ldots & g_s \end{bmatrix} \begin{bmatrix} (-a_{ij_1}) & \ldots & \left(\frac{\mathbf{m}_{ij}}{TL(g_i)} - a_{ij_i}\right) & \ldots & \left(-\frac{\mathbf{m}_{ij}}{TL(g_j)} - a_{ij_j}\right) & \ldots & (-a_{ij_s}) \end{bmatrix}^T$$

é igual a

$$(-a_{ij_1}g_1)+\ldots+\left(\frac{\mathbf{m}_{ij}}{TL(g_i)}g_i-a_{ij_i}g_i\right)+\ldots+\left(-\frac{\mathbf{m}_{ij}}{TL(g_j)}g_j-a_{ij_j}g_j\right)+\ldots+(-a_{ij_s}g_j) \;=$$
$$\left(\frac{\mathbf{m}_{ij}}{TL(g_i)}g_i-\frac{\mathbf{m}_{ij}}{TL(g_j)}g_j\right)-\left(\sum_{l=1}^{s}a_{ij_l}g_l\right)=S(g_i,g_j)-S(g_i,g_j)=0,$$

pela Definição 2.2.4 e por 3.3. Logo $s_{ij}\in \mathrm{Syz}(G)$ e $<\{s_{ij};1\leq i<j\leq t>\subset \mathrm{Syz}(G)$.

Agora vamos mostrar que $\mathrm{Syz}(g)\subset<\{s_{ij};1\leq i<j\leq t\}$. Suponha o contrário, que existe $(u_1,\ldots,u_s)$ tal que

$$(u_1,\ldots,u_s)\in \mathrm{Syz}(g_1,\ldots,g_s)-<s_{ij};1\leq i<j\leq s>.$$

Seja $\mathbf{m}=max_{1\leq i\leq s}\{ML(u_i)ML(g_i)\}$, e definamos

$$S=\{i\in\{1,\ldots,s\};ML(u_i)ML(g_i)=\mathbf{m}\}.$$

Para cada $i\in\{1,\ldots,s\}$ definamos também u_i' da seguinte maneira:

$$u_i'=\begin{cases} u_i, se\ i\notin S \\ u_i-TL(u_i),\ se\ i\in S. \end{cases}$$

Notemos que para $i\in S$, $TL(u_i)=c_i\mathbf{m}_i$, onde $c_i\in k$ e $\mathbf{m}_i\in R$ é um monômio. Como $(u_1,\ldots,u_s)\in \mathrm{Syz}(g_1,\ldots,g_s)$, vemos que

$$\sum_{i\in S}c_i\mathbf{m}_iTL(g_i)=0,$$

então

$$\sum_{i\in S}c_i\mathbf{m}_i\varepsilon_i\in \mathrm{Syz}(TL(g_i);i\in S).$$

Sem perda de generalidade, podemos supor que $TL(g_i)=ML(g_i)$, pois se diferem apenas por uma constante não nula, assim, por c da Proposição 2.1.2, temos

$$\sum_{i\in S}c_i\mathbf{m}_i\varepsilon_i=\sum_{\substack{i<j\\ i,j\in S}}b_{ij}\left(\frac{\mathbf{m}_{ij}}{TL(g_i)}\varepsilon_i-\frac{\mathbf{m}_{ij}}{TL(g_j)}\varepsilon_j\right),$$

para algum $b_{ij}\in R$. Visto que $\mathbf{m}_iTL(g_i)=\mathbf{m}_iML(g_i)=ML(u_i)ML(g_i)=\mathbf{m}$, então podemos escrever $b_{ij}=d_{ij}\dfrac{\mathbf{m}}{\mathbf{m}_{ij}}$, com d_{ij} sendo uma constante em k. Logo, temos que

$$\begin{aligned}(u_1,\ldots,u_s) &= \sum_{i\in S}\left(c_i\mathbf{m}_i\varepsilon_i\right)+(u_1',\ldots,u_s')\\ &= \sum_{\substack{i<j\\ i,j\in S}}\left(b_{ij}\left(\frac{\mathbf{m}_{ij}}{TL(g_i)}\varepsilon_i-\frac{\mathbf{m}_{ij}}{TL(g_j)}\varepsilon_j\right)\right)+(u_i',\ldots,u_s')\\ &= \sum_{\substack{i<j\\ i,j\in S}}(b_{ij}s_{ij})+(u_i',\ldots,u_s')+\sum_{\substack{i<j\\ i,j\in S}}\left((b_{ij})(a_{ij_1},\ldots,a_{ij_s})\right),\end{aligned}$$

pela Equação 3.4. Seja $(v_1,\ldots,v_s)=(u'_i,\ldots,u'_s)+\sum_{\substack{i<j\\ i,j\in S}}\big((b_{ij})(a_{ij_1},\ldots,a_{ij_s})\big)$, assim

$$(u_1,\ldots,u_s)-\sum_{\substack{i<j\\ i,j\in S}}(b_{ij}s_{ij})=(v_1,\ldots,v_s).$$

Observemos que $(u_1,\ldots,u_s),s_{ij}\in \mathrm{Syz}(g_1,\ldots,g_s)$ e $(u_1,\ldots,u_s)\notin< s_{ij};1\leq i<j\leq s>$, assim $(v_1,\ldots,v_s)\in \mathrm{Syz}(g_1,\ldots,g_s)-<s_{ij};1\leq i<j\leq s>$, então basta provar que $\max_{1\leq k\leq s}\{ML(v_k)ML(g_k)\}<\mathbf{m}$ e teremos uma contradição. Para cada $k\in\{1,\ldots,s\}$, temos

$$\begin{aligned} ML(v_k)ML(g_k) &= ML\big(u'_k+\sum_{\substack{i<j\\ i,j\in S}}\big((b_{ij})(a_{ij_1})\big)\big)TL(g_k)\\ &\leq max\{ML(u'_k),\max_{1\leq k\leq s}\{ML(b_{ij})ML(a_{ij_k}))\}\}TL(g_k)\end{aligned}$$

Mas por definição de u'_k temos

$$ML(u'_k)ML(g_k)<\mathbf{m}$$

e também

$$ML(b_{ij})ML(a_{ij_k})TL(g_k)=\frac{\mathbf{m}}{\mathbf{m}_{ij}}ML(a_{ij_k})TL(g_k)\leq\frac{\mathbf{m}}{\mathbf{m}_{ij}}ML(S(g_i,g_j))<\mathbf{m},$$

para todo $i,j\in S$, $i<j$ (pois, se $\frac{\mathbf{m}}{\mathbf{m}_{ij}}ML(S(g_i,g_j))\geq\mathbf{m}$ então $ML(S(g_i,g_j))\geq\mathbf{m}_{ij}$, absurdo, visto que $S(g_i,g_j)$ cancela os termos líderes de g_i e g_j).

Portanto $ML(v_k)ML(g_k)<\mathbf{m}$ para cada $k\in\{i,\ldots,s\}$, gerando uma contradição da condição de $\mathbf{m}=max_{1\leq i\leq s}\{ML(u_i)ML(g_i)\}$.

□

Exemplo 3.2.7. *Voltemos ao Exemplo 2.2.10. Vemos que o conjunto* $\{g_1,g_2,g_3,g_4,g_5,g_6\}$ *é uma base de Gröbner reduzida com respeito a ordem lexicográfica graduada em* $\mathbb{Q}[x,y]$ *com* $x>y$ *e a ordem TSP em* $(\mathbb{Q}[x,y])^3$ *com* $e_1>e_2>e_3$*, onde*

$$\begin{aligned} g_1&=(0,y,x)=xe_3+ye_2\\ g_2&=(0,y^2-x-y,0)=y^2e_2-xe_2-ye_2\\ g_3&=(x,x+y,0)=xe_1+xe_2+ye_2\\ g_4&=(y,-y,0)=ye_1-ye_2\\ g_5&=(0,xy+\frac{1}{2}x+\frac{1}{2}y,0)=xye_2+\frac{1}{2}xe_2+\frac{1}{2}ye_2\\ g_6&=(0,x^2-\frac{1}{4}x-\frac{1}{4}y,0)=x^2e_2-\frac{1}{4}xe_2-\frac{1}{4}ye_2.\end{aligned}$$

Logo

- $S(g_2,g_5)=-\frac{1}{2}g_2-\frac{3}{2}g_5-g_6\Longrightarrow a_{25}=\left(0,-\frac{1}{2},0,0,-\frac{3}{2},-1\right)$.

- $S(g_2, g_6) = \left(\frac{1}{4}y + \frac{1}{8}\right) g_2 + \left(-x + \frac{1}{4}y + \frac{3}{8}\right) g_5 + \left(-x + \frac{1}{4}\right) g_6 \Longrightarrow a_{26} =$
$$\left(0, \frac{1}{4}y + \frac{1}{8}, 0, 0, -x + \frac{1}{4}y + \frac{3}{8}, -x + \frac{1}{4}\right)$$
- $S(g_5, g_6) = \frac{1}{4}g_2 - \frac{1}{4}g_3 + \frac{3}{4}g_5 + \frac{1}{2}g_6 \Longrightarrow a_{56} = \left(0, \frac{1}{4}, -\frac{1}{4}, 0, \frac{3}{4}, \frac{1}{2}\right)$.
- $S(g_3, g_4) = g_2 - g_3 + 2g_5 \Longrightarrow a_{34} = (0, 1, -1, 0, 2, 0)$.

Portanto

- $s_{25} = x\varepsilon_2 - y\varepsilon_5 - a_{25} = \left(0, x + \frac{1}{2}, 0, 0, -y + \frac{3}{2}, 1\right)$;
- $s_{26} = x^2\varepsilon_2 - y^2\varepsilon_6 - a_{26} = \left(0, x^2 - \frac{1}{4}y - \frac{1}{8}, 0, 0, x - \frac{1}{4}y - \frac{3}{8}, -y^2 + x - \frac{1}{4}\right)$;
- $s_{56} = x\varepsilon_5 - y\varepsilon_6 - a_{56} = \left(0, -\frac{1}{4}, \frac{1}{4}, 0, x - \frac{3}{4}, -y - \frac{1}{2}\right)$;
- $s_{34} = y\varepsilon_3 - x\varepsilon_4 - a_{34} = (0, -1, y + 1, -x, -2, 0)$.

Lema 3.2.8. *Sejam $g_1, \ldots, g_s$ vetores não nulos em R^m e $>$ uma ordem monomial em R^m. Definamos uma ordem $>_G$ nos monômios de R^s da seguinte maneira:*

$$\mathbf{x}^\alpha e_i >_G \mathbf{x}^\beta e_j \Longleftrightarrow \begin{cases} ML(\mathbf{x}^\alpha g_i) > ML(\mathbf{x}^\beta g_j) \text{ ou} \\ ML(\mathbf{x}^\alpha g_i) = ML(\mathbf{x}^\beta g_j) \text{ e } i < j. \end{cases}$$

Então $>_G$ é uma ordem monomial em R^s.

Demonstração. Primeiro mostraremos que $>_G$ é uma ordem total. Seja $\mathbf{x}^\alpha, \mathbf{x}^\beta$ monômios em R, se $i \neq j \in \{i, \ldots, s\}$, então $ML(\mathbf{x}^\alpha g_i) = ML(\mathbf{x}^\beta g_j)$ e $i < j$ ou $j < i$, ou $ML(\mathbf{x}^\alpha g_i) > ML(\mathbf{x}^\beta g_j)$ ou $ML(\mathbf{x}^\beta g_j) > ML(\mathbf{x}^\alpha g_i)$. Em qualquer caso, temos $\mathbf{x}^\alpha e_i >_G \mathbf{x}^\beta e_j$ ou $\mathbf{x}^\beta e_j >_G \mathbf{x}^\alpha e_i$. Se $i = j \in \{i, \ldots, s\}$ e $\mathbf{x}^\alpha \neq \mathbf{x}^\beta$, então $ML(\mathbf{x}^\alpha g_i) > ML(\mathbf{x}^\beta g_i)$ ou $ML(\mathbf{x}^\beta e_i) > ML(\mathbf{x}^\alpha e_i)$, por outro lado, se $ML(\mathbf{x}^\alpha g_i) = ML(\mathbf{x}^\beta g_i)$, então

$$\mathbf{x}^\alpha ML(g_i) = ML(\mathbf{x}^\alpha g_i) = ML(\mathbf{x}^\beta g_i) = \mathbf{x}^\beta ML(g_i),$$

e temos $\mathbf{x}^\alpha = \mathbf{x}^\beta$, pois $g_i \neq 0$. Assim temos, $\mathbf{x}^\alpha e_i >_G \mathbf{x}^\beta e_i$ ou $\mathbf{x}^\beta e_i >_G \mathbf{x}^\alpha e_i$.

Agora sejam $\mathbf{x}^\alpha, \mathbf{x}^\beta, \mathbf{x}^\gamma$ monômios em R, e seja $i, j \in \{i, \ldots, s\}$. Assumamos que $\mathbf{x}^\alpha e_i >_G \mathbf{x}^\beta e_j$. Se $ML(\mathbf{x}^\alpha g_i) > ML(\mathbf{x}^\beta g_j)$, então

$$ML(\mathbf{x}^\gamma \mathbf{x}^\alpha g_i) = \mathbf{x}^\gamma ML(\mathbf{x}^\gamma g_i) > \mathbf{x}^\gamma ML(\mathbf{x}^\beta g_j) = ML(\mathbf{x}^\gamma \mathbf{x}^\beta g_j),$$

logo $\mathbf{x}^\gamma \mathbf{x}^\alpha e_i >_G \mathbf{x}^\gamma \mathbf{x}^\beta e_j$. Se $ML(\mathbf{x}^\alpha g_i) = ML(\mathbf{x}^\beta g_j)$ e $i < j$, então

$$ML(\mathbf{x}^\gamma \mathbf{x}^\alpha g_i) = \mathbf{x}^\gamma ML(\mathbf{x}^\alpha g_i) = \mathbf{x}^\gamma ML(\mathbf{x}^\beta g_j) = ML(\mathbf{x}^\gamma \mathbf{x}^\beta g_j)$$

e $i < j$, então $\mathbf{x}^\gamma \mathbf{x}^\alpha >_G \mathbf{x}^\gamma \mathbf{x}^\beta e_j$.

Por fim, seja $\mathbf{x}^\alpha, \mathbf{x}^\gamma$ monômios em R tal que $\mathbf{x}^\gamma \neq 1$. Seja $i \in \{1, \ldots, s\}$. Então $ML(\mathbf{x}^\gamma \mathbf{x}^\alpha g_i) = \mathbf{x}^\gamma ML(\mathbf{x}^\alpha g_i) > ML(\mathbf{x}^\alpha g_i) >$, logo $\mathbf{x}^\gamma \mathbf{x}^\alpha e_i >_G \mathbf{x}^\alpha e_i$ □

Definição 3.2.9. *A ordem monomial definida no Lema 3.2.8 é chamada de* ***ordem em*** R^s ***induzida por*** $\begin{bmatrix} g_1 & \dots & g_s \end{bmatrix}$.

Teorema 3.2.10 (Teorema de Schreyer)**.** *Seja* $G = \{g_1, \dots, g_s\} \subset R^m$ *uma base de Gröbner com respeito a uma ordem monomial* $>$ *em* R^m*. Os* s_{ij} *formam uma base de Gröbner para o módulo Sizígia* $M = \mathrm{Syz}(g_1, \dots, g_s)$ *com respeito a ordem monomial* $>_G$ *em* R^s*.*

Demonstração. Observemos que $S(g_i, g_j) = -S(g_j, g_i)$, então é suficiente considerar os s_{ij} para $i < j$ somente. Seja então $i < j$, logo

$$TL_{>_G}(s_{ij}) = \frac{\mathbf{m}_{ij}}{TL(g_i)}\varepsilon_i$$

na ordem $>_G$. Pois, como $ML\left(\frac{\mathbf{m}_{ij}}{TL(g_i)}g_i\right) = ML\left(\frac{\mathbf{m}_{ij}}{TL(g_j)}g_j\right)$ e $i < j$ então $\frac{\mathbf{m}_{ij}}{TL(g_i)}\varepsilon_i$ é maior que $\frac{\mathbf{m}_{ij}}{TL(g_j)}\varepsilon_j$. E visto que os a_{ij} são obtidos pelo algoritmo da divisão, dividindo $S(g_i, g_j)$ por G, temos $TL_>(S(g_i, g_j)) \geq TL_>(a_{ij_l}g_l)$ para todo $l = 1, \dots, s$ em R^s. Contudo, pela definição de S-vetor,

$$TL_>\left(\frac{\mathbf{m}_{ij}}{TL(g_i)}g_i\right) > TL_>\left(S(g_i, g_j)\right),$$

pois nos S-vetores há a cancelação dos termos líderes. Logo $\frac{\mathbf{m}_{ij}}{TL(g_i)}\varepsilon_i$ é maior que a_{ij}.

Mostraremos agora que $\{s_{ij}; 1 \leq i < j \leq s\}$ é uma base de Gröbner para $\mathrm{Syz}(g_1, \dots, g_s)$ com respeito a $>_G$. Seja $f \in M$, pela Definição de base de Gröbner para submódulos e pela observação 2.2.2 (página 23) precisamos mostrar que existem i, j, $1 \leq i < j \leq s$, tal que $ML(s_{ij})$ divide $ML(f)$. Escrevamos $f = \sum_{l=1}^{s} h_l\varepsilon_l$ onde $h_l \in R$. Seja $\mathbf{x}^{\alpha_l} = ML(h_l)$ e $c_l = CL(h_l)$. Note que $ML(f) = \mathbf{x}^{\alpha_r}\varepsilon_r$ para algum $r \in \{1, \dots, s\}$. Para esse r fixado, definamos

$$S = \{l \in \{1, \dots, s\}; ML(\mathbf{x}^{\alpha_l}g_l) = ML(\mathbf{x}^{\alpha_r}g_r)\}.$$

Observemos que se $l \in S$, então $r \leq l$, pela definição de $>_G$. Definamos

$$f' = \sum_{l \in S} c_l\mathbf{x}^{\alpha_l}\varepsilon_l.$$

Como f é uma sizígia de $\begin{bmatrix} g_1 & \dots & g_s \end{bmatrix}$, temos

$$\sum_{l \in S} c_l\mathbf{x}^{\alpha_l}TL(g_l) = 0.$$

Dessa forma, f' é uma sizígia de $\begin{bmatrix} TL(g_1) & \dots & TL(g_s) \end{bmatrix}$. Note que o índice das coordenadas não nulas de f' estão em S, logo, pela Proposição 3 (submódulos monomiais gerados pelos sigmas) temos que f' pertence ao submódulo de R^s gerado por

$$\sigma_{kv} = \frac{\mathbf{m}_{kv}}{\mathbf{m}_k}\varepsilon_k - \frac{\mathbf{m}_{kv}}{\mathbf{m}_v}\varepsilon_v \ , \ \forall\ 1 \leq k < v \leq s,$$

onde $\mathbf{m}_k = ML(g_k)$, $\mathbf{m}_v = ML(g_v)$ e $\mathbf{m}_{kv} = \text{MMC}(ML(g_k), ML(g_v))$. Assim, temos que

$$f' = \sum_{k,v \in S; k<v} b_{kv}\sigma_{kv} = b_{kv}\left(\frac{\mathbf{m}_{kv}}{\mathbf{m}_k}\,\varepsilon_k - \frac{\mathbf{m}_{kv}}{\mathbf{m}_v}\,\varepsilon_v\right),$$

para $b_{kv} \in R$. Como $ML(f') = ML(f) = \mathbf{x}^{\alpha_r}\varepsilon_r$ e $r < j$ para todo $r \neq j \in S$, vemos que

$$\mathbf{x}^{\alpha_r}\varepsilon_r = ML(f') = ML(b_{rt})\frac{\mathbf{m}_{rt}}{\mathbf{m}_r}\varepsilon_r,$$

para algum $t \in S$, $t \neq r$. Visto que $\dfrac{\mathbf{m}_{rt}}{\mathbf{m}_r}\varepsilon_r = \dfrac{\mathbf{m}_{rt}}{ML(g_r)}\varepsilon_r = ML(s_{rt})$ para algum $t \in S$, então

$$ML(f') = ML(b_{rt})ML(s_{rt}).$$

Logo $ML(s_{rt})$ divide $ML(f)$. □

Como vemos, os módulos Sizígia podem ser encontrado basicamente em dois passos, o primeiro consiste em encontrar uma base de Gröbner, $G = \{g_1, \ldots, g_s\}$, para o submódulo $M \subset R^m$ (observemos que quando $m = 1$, M é um ideal de R), e o segundo passo consiste em calcular um conjunto gerador pata $\text{Syz}(g_1, \ldots, g_s)$ usando o Teorema de Schreyer.

Exemplo 3.2.11. *Seja M um submódulo de $R^3 = (\mathbb{Q}[x,y])^3$ gerado por $F = \{f_1, f_2, f_3, f_4\}$, onde $f_1 = (xy, y, x)$, $f_2 = (x^2 + x, y + x^2, y)$, $f_3 = (-y, x, y)$ e $f_4 = (x^2, x, y)$. Usaremos a ordem lexicográfica em R com $y > x$ e a extensão TSP com $e_1 > e_2 > e_3$ em R^3. Assim podemos escrever*

$$\begin{aligned} f_1 &= xye_1 + ye_2 + xe_3 \\ f_2 &= ye_2 + ye_3 + x^2e_1 + x^2e_2 + xe_1 \\ f_3 &= -ye_1 + ye_3 + xe_2 \\ f_4 &= ye_3 + x^2e_1 + xe_2. \end{aligned}$$

A base de Gröbner reduzida para M é $G = \{g_1, g_2, g_3, g_4, g_5, g_6\}$, onde

$$\begin{aligned} g_1 &= (x^3 + x, x^2 - x, -x) = x^3e_1 + x^2e_2 + xe_1 - xe_2 - xe_3; \\ g_2 &= (x, y + x^2 - x, 0) = ye_2 + x^2e_2 + xe_1 - xe_2; \\ g_3 &= (y + x^2, 0, 0) = ye_1 + x^2e_1; \\ g_4 &= (x^2, x, y) = ye_3 + xe_1 + xe_2; \\ g_5 &= (x^2, x^3, -x^3) = x^3e_2 - x^3e_3 + x^2e_1; \\ g_6 &= (x^2 - 2x, -x^2 + 2x, x^5 - x^4 - 3x^3 + x^2 + 2x) = \\ &\quad x^5e_3 - x^4e_3 - 3x^3e_3 + x^2e_1 - x^2e_2 + x^2e_3 - 2xe_1 + 2xe_2 + 2xe_3. \end{aligned}$$

Assim, podemos calcular $S(g_1, g_3)$, $S(g_2, g_5)$ e $S(g_4, g_6)$ e assim obtermos

$$\begin{aligned} s_{13} &= (y + x^2, -x^2 + x, -x^3 - x, x, -1, 0) \\ s_{25} &= (-x^2 + x + 2, -x^3, -x^2, x^3, y + x^2 - x - 2, 1) \\ s_{46} &= (x^4 - x^3 - 4x^2 + 2x + 4, x^2 - 2x, \\ &\quad -x^2 + 2x, -x^5 + x^4 + 3x^3 - x^2 - 2x, x^2 - x - 2, y + 2). \end{aligned}$$

Que ordenando usando a ordem $>_G$ temos

$$\begin{aligned} s_{13} &= y\,\varepsilon_1 - x^3\,\varepsilon_3 - x^2\,\varepsilon_2 - x\,\varepsilon_3 + x\,\varepsilon_2 + x\,\varepsilon_4 + x^2\,\varepsilon_1 - \varepsilon_5 \\ s_{25} &= -x^3\,\varepsilon_2 + y\,\varepsilon_5 + x^3\,\varepsilon_4 - x^2\,\varepsilon_3 - x^2\,\varepsilon_1 + x^2\,\varepsilon_5 + \varepsilon_6 + x\,\varepsilon_1 - x\,\varepsilon_5 + 2\,\varepsilon_1 - 2\,\varepsilon_5 \\ s_{46} &= -x^5\,\varepsilon_4 + y\,\varepsilon_6 + x^4\,\varepsilon_4 + 3x^3\,\varepsilon_4 - x^2\,\varepsilon_3 + x^2\,\varepsilon_2 - x^2\,\varepsilon_4 + 2x\,\varepsilon_3 - 2x\,\varepsilon_2 \\ &\quad -2x\,\varepsilon_4 + x^4\,\varepsilon_1 - x^3\,\varepsilon_1 - 4x^2\,\varepsilon_1 + x^2\,\varepsilon_5 + 2\,\varepsilon_6 + 2x\,\varepsilon_1 - x\,\varepsilon_5 + 4\,\varepsilon_1 - 2\,\varepsilon_5, \end{aligned}$$

onde $\{\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6\}$ é a base canônica de R^6.

3.3 Resoluções Livres

Veremos nesta seção como a Base de Gröbner, $G = \{g_1, \ldots, g_s\}$, de um submódulo $M \subset R^m$ e o seu módulo Sizígia, $\mathrm{Syz}(g_1, \ldots, g_s)$, pode nos auxiliar a calcular a Resolução Livre de M.

Definição 3.3.1. *Considere uma sequência de R-módulos e homomorfismos*

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots$$

i. Dizemos que a ***sequência é exata em*** M_i *se* $\mathrm{Im}(\varphi_{i+1}) = \mathrm{Ker}(\varphi_i)$*;*

ii. Dizemos que a ***sequência é exata*** *se for exata em cada M_i.*

Observação 3.3.2. *Em particular temos que:*

- $M \xrightarrow{\varphi} N \longrightarrow 0$ *é exata* $\iff \varphi : M \longrightarrow N$ *é sobrejetiva;*
- $0 \longrightarrow M \xrightarrow{\varphi} N$ *é exata* $\iff \varphi : M \longrightarrow N$ *é injetiva;*
- $0 \longrightarrow M \longrightarrow N \longrightarrow 0$ *é exata* $\iff \varphi : M \longrightarrow N$ *é um isomorfismo.*
- $0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$ *é exata* $\iff \varphi$ *é injetiva,* ψ *é sobrejetiva e* ψ *induz um isomorfismo de* $\mathrm{Coker}(\varphi) = N/\varphi(M)$ *sobre* P*.*

Exemplo 3.3.3. *Dado um homomorfismo de R-módulos ou um par de módulos, Q e P, tal que $Q \subset P$, obtemos sequências exatas associadas da seguinte maneira:*

- *Para qualquer homomorfismo de Módulos $\varphi : M \longrightarrow N$, temos uma sequência exata*

  $$0 \longrightarrow \mathrm{Ker}(\varphi) \xrightarrow{\tau} M \xrightarrow{\varphi} N \xrightarrow{\psi} \mathrm{Coker}(\varphi) \longrightarrow 0,$$

  onde $\tau : \mathrm{Ker}(\varphi) \longrightarrow M$ é a aplicação inclusão e $\psi : N \longrightarrow \mathrm{Coker}(\varphi) = N/\mathrm{Im}(\varphi)$ é o homomorfismo natural no módulo quociente;

- *Se Q e P são submódulos de um R-módulo tais que $Q \subset P$, então temos uma sequência exata*

  $$0 \longrightarrow Q \xrightarrow{\sigma} P \xrightarrow{\upsilon} P/Q \longrightarrow 0$$

  onde $\sigma : Q \longrightarrow P$ é a aplicação inclusão e υ é o homomorfismo natural no módulo quociente.

Lema 3.3.4. *Seja M um R-módulo.*

a. *Escolher um elemento de M é equivalente a escolher um homomorfismo $R \longrightarrow M$.*

b. *Escolher t elementos de M é equivalente a escolher um homomorfismo $R^t \longrightarrow M$.*

c. *Escolher um conjunto de t geradores de M é equivalente a escolher um homomorfismo $R^t \longrightarrow M$ sobrejetivo (ou seja, a sequência $R^t \longrightarrow M \longrightarrow 0$ é exata).*

d. *Se M é livre com base finita, escolher uma base (isto é, um conjunto gerador que é R-linearmente independente) com t elementos é equivalente a escolher um isomorfismo $R^t \longrightarrow M$.*

Demonstração.

a. Dado $f \in M$, podemos tomar um homomorfismo de R-módulo $\varphi : R \longrightarrow M$, dado por $\varphi(g) = gf$, com $g \in R$, satisfazendo $\varphi(1) = f$, onde $\varphi(1)$ determina todos os valores de φ para todo $g \in R$:
$$\varphi(g) = \varphi(g.1) = g.\varphi(1) = gf.$$

b. A escolha de t elementos em M pode ser vista como a escolha de t homomorfismo de R-módulos de R em M ou, equivalentemente, como a escolha de um homomorfismo de R-módulos, de R^t em M, de modo que, sendo $e_1, \ldots, e_t$ a base canônica de R^t, temos $\varphi(e_i) = f_i$, $i \in \{1, \ldots, t\}$.

c. Seja $M =< f_1, \ldots, f_t >$. Tomando o homomorfismo tal como vimos no item b, ou seja, $\varphi(e_i) = f_i$, $i \in \{1, \ldots, t\}$, logo $\mathrm{Im}(\varphi) = M$, isto é, φ é sobrejetiva.

d. Como M é livre com base finita, seja $< f_1, \ldots, f_t >$ uma base para M, logo, usando o item c, $\varphi(a_1, \ldots, a_t) = 0$ se, e somente se, $a_i = 0$, para todo $i \in \{1, \ldots, t\}$. Ou seja, φ é injetiva, e assim, φ é um isomorfismo.

□

Vimos então que podemos descrever um homomorfismo de R-módulos, escolhendo apenas elementos de um R-módulo M.

Definição 3.3.5. *Seja M um R-módulo livre. Quando temos um conjunto gerador para M, $f_1, \ldots, f_t$, e um conjunto gerador para o módulo Sizígia* $\mathrm{Syz}(f_1, \ldots, f_t)$*, dizemos que temos uma* ***apresentação*** *para M.*

Obtemos uma **matriz de apresentação** para um módulo $M =< f_1, \ldots, f_t > \subset R^m$, organizando os geradores de $\mathrm{Syz}(f_1, \ldots, f_t)$ como colunas. Sendo
$$\mathrm{Syz}(f_1, \ldots, f_t) =< g_1, \ldots, g_s > \subset R^t,$$
onde $f_i = (f_{i1}, \ldots, f_{im})$ e $g_j = (g_{j1}, \ldots, g_{jt})$, para $i \in \{1, \ldots, m\}$ e $j \in \{1, \ldots, t\}$, então a matriz de apresentação é
$$\begin{bmatrix} g_{11} & \cdots & g_{s1} \\ \vdots & \vdots & \vdots \\ g_{1t} & \cdots & g_{st} \end{bmatrix}. \tag{3.5}$$

Logo podemos formar uma sequência exata

$$R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \longrightarrow 0,$$

onde o homomorfismo $\psi : R^s \longrightarrow R^t$ é dado pela matriz 3.5 e o homomorfismo φ é dado pela matriz

$$\begin{bmatrix} f_1 & \dots & f_t \end{bmatrix} \tag{3.6}$$

Assim, temos que $\mathrm{Syz}(f_1, \dots, f_t) = \ker(\varphi) = \mathrm{Im}(\psi)$. Ou seja, uma matriz de apresentação, nos informa uma apresentação para M.

Vamos destacar oque vimos acima na seguinte observação:

Observação 3.3.6. *Temos por c da Proposição* 3.3.4 *que escolher um conjunto de geradores do módulo Sizígia corresponde a escolher um homomorfismo ψ de R^s em $\mathrm{Ker}(\varphi) = \mathrm{Syz}(f_1, \dots, f_t)$. Mas sendo φ sobrejetiva, temos $\mathrm{Im}(\psi) = \mathrm{Ker}(\varphi)$, logo temos uma sequência exata em R^t,*

$$R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \longrightarrow 0. \tag{3.7}$$

Isso mostra que uma apresentação para M é equivalente a uma sequência exata da forma 3.7. Observemos também que a matriz de ψ com relação às base canônica de R^s e R^t é uma matriz de apresentação para M.

A seguir, veremos que todo R-módulo finitamente gerado tem uma apresentação.

Proposição 3.3.7. *Seja M um R-módulo finitamente gerado.*

a. *M tem uma apresentação da forma $R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \longrightarrow 0$.*

b. *M é a imagem homomórfica de um R-módulo livre. Ou seja, se $f_1, \dots, f_t$ é um conjunto de geradores de M, então $M \cong R^t/S$, onde S é o submódulo de R^t dado por $S = \mathrm{Syz}(f_1, \dots, f_t)$. Alternativamente, se deixarmos a matriz A representar ψ em*

$$R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \longrightarrow 0,$$

então $AR^s = \mathrm{Im}(\psi)$ e $M \cong R^t/AR^s$.

Demonstração. Seja $M =< f_1, \dots, f_t >$.

a. Sabemos que todo submódulo de R^t é finitamente gerado, em particular

$$\mathrm{Syz}(f_1, \dots, f_t) \subset R^t.$$

Logo podemos escolher um conjunto finito de geradores para o módulo Sizígia, e assim pela Observação 3.3.6, temos a sequência exata desejada.

b. Segue de a e da definição de Sizígia.

□

Exemplo 3.3.8. *Seja* $I =< x^2 - x, xy, y^2 - y > \subset R = k[x, y]$ *um ideal. Seja*

$$A = \begin{bmatrix} x^2 - x & xy & y^2 - y \end{bmatrix}$$

e

$$B = \begin{bmatrix} y & 0 \\ -x + 1 & y - 1 \\ 0 & -x \end{bmatrix}.$$

Considerando $\mathrm{Syz}(I) = \mathrm{Syz}(x^2 - x, xy, y^2 - y)$ *temos que:*

- *Se tomarmos os homomorfismos* φ *e* ψ*, definidos pelas matrizes* A *e* B *respectivamente, então podemos construir a sequencia exata*

  $$R^2 \xrightarrow{\psi} R^3 \xrightarrow{\varphi} I \longrightarrow 0,$$

  pois o produto de matrizes AB *é igual à matriz zero* 1×2*, assim* $\mathrm{Im}(\psi) \subset \mathrm{Ker}(\varphi)$*. E como*

  $$\ker(\varphi) =< (y, -x + 1, 0), (y^2 - y, 0, -x^2 + x), (0, y - 1, -x) >$$

  e $(y^2 - y, 0, -x^2 + x) \in < (y, -x + 1, 0), (0, y - 1, -x) >$*, temos que* $\ker(\varphi) \subset \mathrm{Im}(\psi)$*, logo,* $\mathrm{Im}(\psi) = \mathrm{Ker}(\varphi)$*.*

- *Visto que os geradores de* I*,* $F = \{f_1, f_2, f_3\}$*, formam uma base de Gröbner usando a ordem lexicográfica, pois*

  $$\begin{array}{lcll} S(f_1, f_2) & = & -xy & \Longrightarrow \overline{S(f_1, f_2)}^F = 0; \\ S(f_1, f_3) & = & (x - y)xy & \Longrightarrow \overline{S(f_1, f_3)}^F = 0 \\ S(f_2, f_3) & = & xy & \Longrightarrow \overline{S(f_2, f_3)}^F = 0, \end{array}$$

  então podemos usar o Teorema de Schreyer(Teorema 3.2.10. Notemos que $a_{12} = (0, -1, 0)$*,* $a_{13} = (0, x - y, 0)$ *e* $a_{23} = (0, 1, 0)$*, assim* $s_{12} = (y, -x + 1, 0)$*,* $s_{13} = (y^2, y - x, -x^2)$ *e* $s_{23} = (0, y - 1, -x)$*.*

  Como $(y^2, y - x, -x^2) = y(y, -x + 1, 0) + x(0, y - 1, -x)$*, então* $s_{13} \in < s_{12}, s_{23} >$ *e com isso,* $\mathrm{Syz}(I) =< (y, -x + 1, 0), (0, y - 1, -x) >$*.*

Logo, $I \cong R^3/\mathrm{Syz}(I)$*.*

Seja M um R-módulo finitamente gerado pelo conjunto G. Tomando $S_1 = \mathrm{Syz}(G)$, temos que S_1 também é finitamente gerado, suponhamos agora pelo conjunto G_1, logo também podemos definir $S_2 = \mathrm{Syz}(G_1)$, que é chamada de **segunda Sizígia**, que também é finitamente gerada, suponhamos por um conjunto finito, G_2, logo podemos definir $S_3 = \mathrm{Syz}(G_2)$ como a **terceira Sizígia**, e assim por diante.

No Exemplo 3.3.8, há uma relação entre os geradores s_{ij} de $\mathrm{Syz}(x^2 - x, xy, y^2 - y)$, a saber

$$ys_{12} - s_{13} + xs_{23} = 0,$$

logo $\begin{bmatrix} y & -1 & x \end{bmatrix}^T \in R^3$ deve pertencer a segunda Sizígia.

A conexão entre um R-módulo M e suas Sizígias podem também ser formuladas em termos de uma sequência exata de módulos e os homomorfismos dados pelas matrizes de apresentação de M e de cada módulo Sizígia de M. A ideia é simples, apenas repetimos a construção da sequência exata dando uma apresentação. Por exemplo, iniciando da sequência vista na Proposição 3.3.7, correspondente a uma apresentação para M, se também queremos conhecer a Segunda sizígia, precisamos de mais um homomorfismo de R-módulos na sequência, a saber,

$$R^r \xrightarrow{\lambda} R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \longrightarrow 0,$$

onde agora a imagem de $\lambda : R^r \longrightarrow R^s$ é igual ao núcleo de ψ (o segundo módulo Sizígia). Continuando da mesma maneira para a terceira e superior sizígias, produzimos sequências exatas longas. Acabamos assim construindo uma **resolução livre** de M. A definição precisa é a seguinte:

Definição 3.3.9. *Seja M um R-módulo. Uma **resolução livre** de M é uma sequência exata da forma*

$$\ldots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

*onde, para todo i, $F_i \cong R^{r_t}$ é um R-módulo livre. Se existir um l tal que $F_{l+1} = F_{l+2} = \ldots = 0$, mas $F_l \neq 0$, então dizemos que a resolução é **finita**, de comprimento l. Em uma resolução finita de comprimento l, geralmente escrevemos a resolução como*

$$0 \longrightarrow F_l \longrightarrow F_{l-1} \longrightarrow \ldots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0.$$

Exemplo 3.3.10. *Considere a apresentação*

$$R^2 \xrightarrow{\psi} R^3 \xrightarrow{\varphi} I \longrightarrow 0$$

para $I =< x^2 - x, xy, y^2 - y >$ em $R = k[x, y]$, como visto no Exemplo 3.3.8. Já sabemos que o primeiro módulo Sizígia,

$$S = \mathrm{Syz}(x^2 - x, xy, y^2 - y) =< (y, -x + 1, 0), (0, y - 1, -x) > \subset R^3,$$

e o segundo módulo Sizígia,

$$S_1 = \mathrm{Syz}((y, -x + 1, 0), (0, y - 1, -x)) = \{0\} \subset R^2,$$

são módulos livres, onde $\{(y, -x+1, 0), (0, y-1, -x)\}$ é uma base de Gröbner para S. Como resultado, podemos estender a sequência acima para a sequência exata

$$0 \longrightarrow R^2 \xrightarrow{\psi} R^3 \xrightarrow{\varphi} I \longrightarrow 0,$$

onde φ e ψ são os homomorfismos dados pelas matrizes

$$\begin{bmatrix} x^2 - x & xy & y^2 - y \end{bmatrix} \; e \; \begin{bmatrix} y & 0 \\ -x + 1 & y - 1 \\ 0 & -x \end{bmatrix},$$

respectivamente.

E de acordo com a definição de resolução livre dada acima, está é uma resolução livre de comprimento 1 para I.

Agora, se tomarmos o primeiro módulo Sizígia sendo gerado por s_{12}, s_{13} e s_{23}, ou seja,

$$S = \mathrm{Syz}(x^2 - x, xy, y^2 - y) =< (y, -x + 1, 0), (y^2, -x + y, -x^2), (0, y - 1, -x) >\subset R^3,$$

que também é uma base de Gröbner para S, temos que o segundo módulo Sizígia possui um gerador não-nulo, ou seja,

$$S_1 = \mathrm{Syz}(< s_{12}, s_{13}, s_{23} >) =< (y, -1, x) > \subset R^3,$$

onde $< (y, -1, x) >$ é uma base de Gröbner (obtida usando o Teorema de Schreyer) para S_1, logo, podemos tomar a terceira sizígia,

$$S_2 = \mathrm{Syz}((y, -1, x)) \subset R,$$

e assim, podemos estender para a sequência exata

$$0 \longrightarrow R \xrightarrow{\lambda} R^3 \xrightarrow{\psi} R^3 \xrightarrow{\varphi} I \longrightarrow 0,$$

onde φ, ψ e λ são os homomorfismos dados por

$$\begin{bmatrix} x^2 - x & xy & y^2 - y \end{bmatrix}, \begin{bmatrix} y & y^2 & 0 \\ -x + 1 & -x + y & y - 1 \\ 0 & -x^2 & -x \end{bmatrix} e \begin{bmatrix} y \\ -1 \\ x \end{bmatrix},$$

respectivamente.

Neste caso temos uma resolução livre de comprimento 2 para o mesmo submódulo.

Proposição 3.3.11. *Em uma resolução livre finita*

$$0 \longrightarrow F_l \xrightarrow{\varphi_l} F_{l-1} \xrightarrow{\varphi_{l-1}} \ldots \xrightarrow{\varphi_{l-2}} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

temos que $\mathrm{Ker}(\varphi_{l-1})$ é um módulo livre. Por outro lado, se M tiver uma resolução livre na qual $\mathrm{Ker}(\varphi_{l-1})$ é um módulo livre para algum l, então M tem uma resolução livre finita de comprimento l.

Demonstração. Observemos primeiramente que φ_l é injetiva, assim se temos uma resolução livre finita de comprimento l, então $\mathrm{Im}(\varphi_l) = \ker(\varphi_{l-1})$ é um módulo livre.

Reciprocamente, se $\ker(\varphi_{l-1})$ é um módulo livre então a resolução parcial

$$F_{l-1} \xrightarrow{\varphi_{l-1}} F_{l-2} \longrightarrow \ldots \longrightarrow F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

pode ser completada para uma resolução finita de comprimento l

$$0 \longrightarrow F_l \xrightarrow{\varphi_l} F_{l-1} \xrightarrow{\varphi_{l-1}} F_{l-2} \longrightarrow \ldots \longrightarrow F_0 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

tomando F_l como sendo $\ker(\varphi_{l-1})$ e φ_l a aplicação inclusão. □

Observação 3.3.12. *O Teorema de Schreyer (3.2.10) forma a base de um algorítmo para encontrar os homomorfismos de R-módulos em uma resolução livre.*

Pode-se perguntar se sempre existirá resoluções livres finitas, vejamos o exemplo abaixo.

Exemplo 3.3.13. *Sejam* $R = k[x]/ < x^2 >$ *e* $M =< \bar{x} >\subset R$. *Tomemos o homomorfismo* $\varphi : R \longrightarrow M$ *dado pela multiplicação por* $\bar{x}$. *Observemos agora que* $\ker(\varphi) =< \bar{x} >= M$, *pois* $\bar{x}^2 = \bar{0}$. *Observemos também que toda resolução livre de* M *é infinita e da forma*

$$\ldots \xrightarrow{\varphi} R \xrightarrow{\varphi} R \xrightarrow{\varphi} R \xrightarrow{\varphi} M \longrightarrow 0.$$

Visto que, caso contrário, existiria uma resolução livre finita de M *de comprimento* l

$$0 \longrightarrow R \xrightarrow{\varphi_l} \ldots \xrightarrow{\varphi_2} R \xrightarrow{\varphi_1} R \xrightarrow{\varphi_0} M \longrightarrow 0,$$

onde $\varphi_0 = \varphi$ *e* $\ker(\varphi_l) = \{\bar{0}\}$. *Assim, como* $\ker(\varphi_i) = \mathrm{Im}(\varphi_{i+1})$, $i \in \{0, \ldots, l-1\}$, *temos* $\varphi_j = \varphi$, *para todo* $j \in \{0, \ldots, l\}$, *e assim* $\ker(\varphi_l) =< \bar{x} >$, *contrariando o fato de* $\ker(\varphi_l) = \{\bar{0}\}$. *Portanto, toda resolução livre de* M *é infinita.*

Vemos assim que nem sempre poderemos obter uma resolução livre finita.

3.4 Teorema Sizígia de Hilbert

Na seção passada vimos que dado um R-módulo, não podemos afirmar que o mesmo possuirá uma resolução livre finita, como vimos no Exemplo 3.3.13. Mas quando consideramos R o anel de polinômios em n variáveis sobre um corpo k, $R = k[\mathbf{x}]$, a situação, como veremos, é melhor.

Para enunciarmos o próximo lema, seja G uma base de Gröbner para um submódulo $M \subset R^t$ e organizemos os elementos de G de forma a ter uma s-upla ordenada $G = \{g_1, \ldots, g_s\}$ tal que, se $TL(g_i)$ e $TL(g_j)$ contêm o mesmo vetor da base canônica e_k e $i < j$, então $ML(g_i)/e_k >_{lex} ML(g_j)/e_k$, onde $>_{lex}$ é a ordem lexicográfica em R com $x_1 > \ldots > x_n$.

Lema 3.4.1. *Se as variáveis* $x_1, \ldots, x_m$ *não aparecem nos termos líderes de* G, *então as variáveis* $x_1, \ldots, x_{m+1}$ *não aparecerão nos termos líderes de* $s_{ij} \in \mathrm{Syz}(G)$ *usando a ordem* $>_G$ *definida no Lema 3.2.8.*

Demonstração. Vimos na demonstração do Teorema de Schreyer (3.2.10) que

$$TL_{>_G}(s_{ij}) = \frac{\mathbf{m}_{ij}}{TL(g_i)}\epsilon_i, \tag{3.8}$$

onde $\mathbf{m}_{ij} = \mathrm{MMC}(TL(g_i), TL(g_j))$ e ϵ_i é um vetor da base canônica de R^s. Como sempre, é suficiente considerar somente os s_{ij} tais que $TL(g_i)$ e $TL(g_j)$ contenham o mesmo vetor canônico e_k em R^t e $i < j$. Pela hipótese da ordenação dos elementos de G, $ML(g_i)/e_k >_{lex} ML(g_j)/e_k$. Como $x_1, \ldots, x_m$ não aparecem nos termos líderes da base de Gröbner G, então podemos escrever

$$ML(g_i)/e_k = x_{m+1}^a n_i \text{ e } ML(g_j)/e_k = x_{m+1}^b n_j,$$

onde $a \geq b$, e n_i, n_j são monômios em R contendo somente as variáveis $x_{m+2}, \ldots, x_n$. Mas então, $\mathrm{MMC}(TL(g_i), TL(g_j))$ contém x_{m+1}^a, e por 3.8, $TL_{>_G}(s_{ij})$ não contém $x_1, \ldots, x_{m+1}$. □

Exemplo 3.4.2. *Seja M o submódulo de $R^3 = (\mathbb{Q}[x,y])^3$ do Exemplo 3.2.11. Sabemos que $\{g_1, g_2, g_3, g_4, g_5, g_6\}$ forma uma base de Gröbner usando a ordem TSP em R^3, com $e_1 > e_2 > e_3$ e com a ordem lexicográfica em R, com $y > x$, onde*

$$\begin{aligned} g_1 &= (x^3+x, x^2-x, -x) \\ g_2 &= (x, y+x^2-x, 0) \\ g_3 &= (y+x^2, 0, 0) \\ g_4 &= (x^2, x, y) \\ g_5 &= (x^2, x^3, -x^3) \\ g_6 &= (x^2-2x, -x^2+2x, x^5-x^4-3x^3+x^2+2x). \end{aligned}$$

Reordenando os g_i's como o Lema 3.4.1 requer, com $y > x$, temos

$$\begin{aligned} g_1 &= (y+x^2, 0, 0) \\ g_2 &= (x^3+x, x^2-x, -x) \\ g_3 &= (x, y+x^2-x, 0) \\ g_4 &= (x^2, x^3, -x^3) \\ g_5 &= (x^2, x, y) \\ g_6 &= (x^2-2x, -x^2+2x, x^5-x^4-3x^3+x^2+2x), \end{aligned}$$

onde

$$\begin{aligned} TL(g_1) &= ye_1 \\ TL(g_2) &= x^3e_1 \\ TL(g_3) &= ye_2 \\ TL(g_4) &= x^3e_2 \\ TL(g_5) &= ye_3 \\ TL(g_6) &= x^5e_3. \end{aligned}$$

Temos agora as Sizígias

$$\begin{aligned} s_{12} &= (x^3+x, -y-x^2, x^2-x, 1, -x, 0) \\ s_{34} &= (x^2, x^2-x-2, x^3, -y-x^2+x+2, -x^3, -1) \\ s_{56} &= (x^2-2x, -x^4+x^3+4x^2-2x-4, -x^2+2x, \\ &\quad -x^2+x+2, x^5-x^4-3x^3+x^2+2x, -y-2). \end{aligned}$$

Usando a ordem $>_G$ temos

$$\begin{aligned} TL(s_{12}) &= x^3\,\varepsilon_1 \\ TL(s_{34}) &= x^3\,\varepsilon_3 \\ TL(s_{56}) &= x^5\,\varepsilon_5\,. \end{aligned}$$

Observemos que a variável y não aparece nos termos líderes das Sizígias.

Teorema 3.4.3 (Teorema Sizígia de Hilbert)**.** *Seja $R = k[\mathbf{x}]$. Todo R-módulo finitamente gerado possui uma resolução livre finita de comprimento no máximo n.*

Demonstração. Como M é finitamente gerado como um R-módulo, temos pela Observação 3.3.6 uma apresentação para M da forma 3.7. Ou seja,

$$F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0, \tag{3.9}$$

correspondendo à escolha de um conjunto gerador $\{f_1, \ldots, f_{r_0}\}$ para M, e uma base de Gröbner $G_0 = \{g_1, \ldots, g_{r_1}\}$ para $\mathrm{Syz}(f_1, \ldots, f_{r_0}) = \mathrm{Im}(\varphi_1) \subset F_0 = R^{r_0}$ (com uma ordem monomial fixada em F_0). Podemos assumir que as bases de Gröbner que obtivermos são sempre reduzidas. Assim, ordenemos G_0 como no Lema 3.4.1 e apliquemos o Teorema de Schreyer para calcular a base de Gröbner G_1 para o módulo $\mathrm{Syz}(G_0) \subset F_1 = R^{r_1}$ (usando a ordem $>_G$). Pelo Lema 3.4.1 novamente, pelo menos x_1 não estará em G_1. Além disso, se a base de Gröbner G_1 contém r_2 elementos, então obtemos a sequência exata

$$F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0,$$

com $F_2 = R^{r_2}$ e $\mathrm{Im}(\varphi_2) = \mathrm{Syz}(G_1)$. Agora podemos repetir o processo fazendo $\varphi_i : F_i \longrightarrow F_{i-1}$, onde $\mathrm{Im}(\varphi_i) = \mathrm{Syz}(G_{i-1})$ e $G_i \subset R^{r_i}$ é uma base de Gröbner para $\mathrm{Syz}(G_{i-1})$.

Observemos que em cada etapa, ordenamos G_i como na hipótese do Lema 3.4.1. Assim, o número de variáveis presente nos termos líderes dos elementos das bases de Gröbner obtidas, diminui a cada etapa, então, após $l \leq n$ etapas, os termos líderes de cada elemento da base de Gröbner G_l são da forma e_s, para algum $s \in \{1, \ldots, r_l\}$. Até esse momento estendemos a sequência 3.9 para

$$F_l \xrightarrow{\varphi_l} F_{l-1} \xrightarrow{\varphi_{l-1}} \ldots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0. \tag{3.10}$$

Suponhamos que $G_l = \{h_1, \ldots, h_v\}$, observemos agora que se e_s é o termo líder de algum elemento $h_i \in G_l$, então e_s é o termo líder de exatamente um elemento de G_l. De fato, caso existissem h_i, h_j em G_l tal que $TL(h_i) = TL(h_j) = e_s$, com $i < j$, então existe $h_j \in G_l$ tal que $ML(h_j) \in < TL(G_l - \{h_j\}) >$, contrariando o fato de G_l ser uma base de Gröbner reduzida. Tomando o homomorfismo

$$\psi : k^v \longrightarrow G_l$$

tal que $\psi(a_1, \ldots, a_v) = a_1 h_1 + \ldots + a_v h_v$, onde $(a_1, \ldots, a_v) \in k^v$, temos que $\mathrm{Syz}(G_l) = \{0\}$ e $G_l \cong k^v$, ou seja, G_l é um módulo libre. Assim, tomando $F_l = G_l$ temos que $\ker(\varphi_{l-1}) = \mathrm{Im}(\varphi_l)$ é um módulo livre, então pela Proposição 3.3.11 podemos estender a sequência 3.10 para a

$$0 \longrightarrow F_l \xrightarrow{\varphi_l} F_{l-1} \xrightarrow{\varphi_{l-1}} \ldots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0. \tag{3.11}$$

Portanto obtemos uma resolução livre de comprimento $l \leq n$. □

Exemplo 3.4.4. *Seja* $I =< g_1, g_2, g_3 > \subset R = k[x, y, z, w]$ *um ideal tal que* $g_1 = xz - y^2$, $g_2 = xw - yz$ *e* $g_3 = yw - z^2$. *Usando a ordem lexicográfica graduada reversa,* $S(g_1, g_2) = -yg_3$, $S(g_1, g_3) = z^2 g_1 - y^2 g_3$ *e* $S(g_2, g_3) = zg_1$, *ou seja,* $\{g_1, g_2, g_3\}$ *é uma base de Gröbner para* I. *Pelo Teorema de Schreyer, temos que*

$$\begin{aligned} s_{12} &= we_1 - ze_2 + ye_3 \\ s_{13} &= ywe_1 - xze_3 + y^2 e_3 - z^2 e_1 \\ s_{23} &= ye_2 - xe_3 - ze_1 \end{aligned}$$

formam uma base de Gröbner para $\mathrm{Syz}(g_1, g_2, g_3)$, *onde* $\{e_1, e_2, e_3\}$ *é a base canônica de* R^3. *Notemos que* $s_{13} = yf_1 + zf_3$ *e que* $\{s_{12}, s_{23}\}$ *forma uma base de Gröbner reduzida para* $\mathrm{Syz}(g_1, g_2, g_3)$. *Assim, temos a resolução livre*

$$0 \longrightarrow R^2 \xrightarrow{\varphi_1} R^3 \xrightarrow{\varphi_0} I \longrightarrow 0,$$

onde $\varphi_0 : R^3 \longrightarrow I$ *é tal que* $\varphi_0(f_1, f_2, f_3) = f_1g_1 + f_2g_2 + f_3g_3$, *com* $(f_1, f_2, f_3) \in R^3$ *e* $\varphi_1 : R^2 \longrightarrow R^3$ *é tal que* $\varphi_1(h_1, h_2) = h_1s_{12} + h_2s_{23}$, *com* $(h_1, h_2) \in R^2$.

Exemplo 3.4.5. *Seja* $M =< z^3 - yw^2, yz - xw, y^3 - x^2z, xz^2 - y^2w >\subset R$ *um ideal, onde* $\{z^3 - yw^2, yz - xw, y^3 - x^2z, xz^2 - y^2w\}$ *é uma base de Gröbner para* M. *Calculando as sizígias usando a Proposição 3.2.6 e usando a ordem dada pelo Lema 3.2.8, temos o módulo sizígia* $\mathrm{Syz}(M) =< g_1, g_2, g_3, g_4 >= M_1$, *tal que*

$$\begin{aligned} g_1 &= -xe_1 + ywe_2 + ze_4 \\ g_2 &= -xze_2 + we_3 + ye_4 \\ g_3 &= -z^2e_2 - we_4 + ye_1 \\ g_4 &= -ze_3 - xe_4 + y^2e_2, \end{aligned}$$

onde $\{e_1, e_2, e_3, e_4\}$ *é a base canônica de* R^4 *e* $\{g_1, g_2, g_3, g_4\}$ *uma base de Gröbner para* $\mathrm{Syz}(M)$.

De forma semelhante, encontramos a sizígia de M_1, *assim* $\mathrm{Syz}(M_1) =< h_1 >= M_2$, *onde* $h_1 = -ze_2 + xe_3 - we_4 + ye_1$. *Logo, temos a resolução*

$$0 \longrightarrow R \xrightarrow{\varphi_2} R^4 \xrightarrow{\varphi_1} R^4 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

onde, φ_0, φ_1 *e* φ_2 *são dadas por*

$$\varphi_0 = \begin{bmatrix} z^3 - yw^2 & ys - xw & y^3 - x^2z & xz^2 - y^2w \end{bmatrix},$$

$$\varphi_1 = \begin{bmatrix} -x & 0 & y & 0 \\ yw & -xz & -z^2 & y^2 \\ 0 & w & 0 & -z \\ z & y & -w & -x \end{bmatrix}$$

e

$$\varphi_2 = \begin{bmatrix} y \\ -z \\ x \\ -w \end{bmatrix}.$$

3.5 Resoluções Graduadas

Estenderemos agora o estudo feito nas Seções 3.3 e 3.4 para Módulos Graduados.

Denotaremos por $R_s = k[\mathbf{x}]_s$ os polinômios homogêneos em R de grau total s, juntamente com 0.

Exemplo 3.5.1. *Seja* $R = k[x, y, z]$, *então* $1 \in R_0$, $xy - yz \in R_2$, $x^2z + y^3 - yz^2 \in R_3$ *e* $x^7y - z^8 \in R_8$.

Definição 3.5.2. *Um módulo graduado sobre* R *é um módulo* M *com uma família de subgrupos* $\{M_t : t \in \mathbb{Z}\}$ *do grupo aditivo* M *satisfazendo as seguintes propriedades:*

a. Como grupos aditivos,

$$M = \bigoplus_{t \in \mathbb{Z}} M_t;$$

b. A decomposição de M na parte a é compatível com a multiplicação por elementos de R no sentido de que $R_s M_t \subset M_{s+t}$ para todo $s \geq 0$ e todo $t \in \mathbb{Z}$.

Os elementos de M_t são chamados de elementos homogêneos de grau t.

Sendo M um R-módulo graduado, então qualquer elemento $f \in M$ pode ser escrito de maneira única como uma soma $\sum_{t\in\mathbb{Z}} f_t$, onde $f_t \in M_t$ para todo $t \in \mathbb{Z}$, e todos, exceto um número finito de f_t, são 0. As componentes f_t não nulas são chamadas de *componentes homogêneas* de f.

Notemos que M_t é um módulo sobre o subanel $R_0 = k \subset R$, assim, ele é um k-subespaço vetorial de M. Se M é finitamente gerado, os M_t tem dimensão finita sobre k.

Exemplo 3.5.3. *Sendo $R = k[\mathbf{x}]$, então R é um R-módulo graduado, definindo R_s como acima, ou seja, $R = \bigoplus_{s\geq 0} R_s$.*

Lembremos que um ideal é *homogêneo* se dado $f \in I$, os componentes homogêneos de f estão todos em I.

Exemplo 3.5.4. *Seja $I =< y - x^2 > \subset k[x, y]$. Os componentes homogêneos de $f = y - x^2$ são $f_1 = y$ e $f_2 = -x^2$. Notemos que nenhum desses polinômios está em I, logo I não é um ideal homogêneo.*

Algumas propriedades importantes dos ideais homogêneos são resumidas a seguir.
Seja $I \subset k[\mathbf{x}]$ um ideal. Então são equivalentes:

I. I é um ideal homogêneo;

II. $I =< f_1, \ldots, f_s >$, onde f_i são polinômios homogêneos;

III. Uma base de Gröbner reduzida para I (com respeito a qualquer ordem monomial) consiste de polinômios homogêneos.

(Mais detalhes em [4], Teorema 2 do Capítulo 8, seção 3)

Sendo I um ideal homogêneo, temos que I tem uma estrutura de módulo graduado fazendo $I_t = I \cap R_t$, para $t \geq 0$ (esse é o conjunto de todos os elementos homogêneos de grau total t em I, junto com o 0) e $I_t = \{0\}$ para $t < 0$. Assim, $I = \bigoplus_{t\in\mathbb{Z}} I_t$ e $R_s I_t \subset I_{s+t}$, consequência direta da definição de um ideal e as propriedades de multiplicação de polinômios.

Observemos que $(R^m)_t = (R_t)^m$, assim os módulos livres R^m também são módulos graduados sobre R. Chamamos isto de uma *estrutura canônica de módulos graduados* sobre R^m. Podemos assim escrever

$$R^m = \left(\bigoplus_{t_1\geq 0} R_{t_1} e_1\right) \oplus \ldots \oplus \left(\bigoplus_{t_m\geq 0} R_{t_m} e_m\right).$$

Proposição 3.5.5. *Seja $M \subset R^m$ um submódulo. Então são equivalentes:*

a. *A graduação canônica em R^m induz uma estrutura de módulo graduado sobre M, dado por $M_t = (R_t)^m \cap M$, o conjunto de elementos em M onde cada componente é um polinômio homogêneo de grau t, $t \geq 0$;*

b. *$M =< f_1, \ldots, f_r > \subset R^m$, onde cada f_i é polinômios homogêneos de grau d_i;*

c. *Existe uma base de Gröbner reduzida (usando qualquer ordem monomial em R^m) consiste de polinômios homogêneos.*

Demonstração.

- $(a \Rightarrow b)$ Já que, R^m é Noetheriano, M é finitamente gerado. Suponhamos que $M =< h_1, \ldots, h_s >$, como M tem estrutura de módulo graduado, ou seja, $M = \bigoplus_{t \geq 0} M_t$, então

$$h_i = \sum_{j=1}^{t_i} h_{ij},$$

onde cada h_{ij} pertence a algum M_t, isto é, os h_{ij} são polinômios homogêneos. Seja M' o módulo gerado pelos h_{ij}, logo $M \subset M'$. Por outro lado $M' \subset M$, pois cada $h_{ij} \in M_t \subset M$. Portanto $M = M'$. Enumerando os h_{ij} de 1 a r temos $M =< f_1, \ldots, f_r >$.

- $(b \Rightarrow c)$ Seja $F = \{f_1, \ldots, f_r\}$, então, dados $f_i, f_j \in F$, observemos que $S(f_i, f_j)$ é um polinômio homogêneo, assim pelo algorítmo de Buchberger temos uma base de Gröbner para M formada por polinômios homogêneos, $G = \{g_1, \ldots, g_s\}$. Para obtermos a base de Gröbner reduzida, notemos que:

  i. Se $CL(g_i) = c \neq 1$ então multiplicamos g_i por c^{-1}, $i \in \{1, \ldots, s\}$;

  ii. Se algum termo de $g_i = \sum_{j=1}^{t_i} g_{ij}$ pertence a $< TL(G - \{g_i\}) >$, então $g_{ij} = \sum_{k=i}^{t_{ij}} a_{ijk} TL(g_k)$, com $k \in \{1, \ldots, s\} - \{i\}$ e $a_{ijk} \in R^m$. Pela igualdade de polinômios, e como o grau total de g_{ij} é d_i (pois g_i é um polinômio homogêneo de grau d_i), então, o grau total do resto da divisão de g_i por $G - \{g_i\}$ é d_i ou 0. Assim podemos dividir g_i por $G - \{g_i\}$ e teremos que o resto, r_i, terá grau d_i se for diferente de zero, e assim o acrescentamos a $G - \{g_i\}$.

  Logo, temos uma base de Gröbner reduzida constituída de polinômios homogêneos.

- $(c \Rightarrow a)$ Seja $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner reduzida para M, onde cada g_i é um polinômio homogêneo de grau d_i. Seja G_i o k-subespaço vetorial gerado por g_i, e fazendo

$$M_t = \sum_{i=1}^{s} R_{t-d_i} G_i$$

Temos que $M = \bigoplus_{t \geq 0} M_t$, onde os M_t são grupos aditivos, e $R_s M_t \subset M_{s+t}$. Além disso, $M_t = (R_t)^m \cap M$ e concluímos a demonstração.

□

Definição 3.5.6. *Se M é um módulo graduado e N é um submódulo de M, então dizemos que N é um submódulo graduado se o subgrupo aditivo $N_t = M_t \cap N$ para cada $t \in \mathbb{Z}$, define uma estrutura de módulo graduado em N.*

Dada uma coleção de módulos graduados $M_1, \ldots, M_m$, podemos produzir a soma direta $N = M_1 \oplus \ldots \oplus M_m$ fazendo $N_t = (M_1)_t \oplus \ldots \oplus (M_m)_t$, definindo assim uma estrutura de módulo graduado em N.

Se $N \subset M$ é um submódulo graduado de um módulo graduado M, então o anel quociente M/N também tem uma estrutura de módulo graduado, definida pela coleção de subgrupos aditivos $(N/M)_t = M_t/N_t = M_t/(M_t \cap N)$.

Proposição 3.5.7. *Sejam M um R-módulo graduado e d um inteiro. Defina $M(d)$ a soma direta*

$$M(d) = \bigoplus_{t \in \mathbb{Z}} M(d)_t,$$

onde $M(d)_t = M_{d+t}$. Temos que $M(d)$ é um R-módulo graduado.

Demonstração. Observemos que os $M(d)_t = M_{d+t}$ são grupos aditivos e que $R_s M(d)_t = R_s M_{d+t} \subset M_{s+d+t} = M(d)_{s+t}$, para todo $s \geq 0$ e todo $t \in \mathbb{Z}$, assim pela Definição 3.5.2, temos que $M(d)$ é um R–módulo graduado. □

Os módulos $(R^m)(d) = R(d)^m$ são chamados de *módulos livres graduados deslocados* (ou torcidos) sobre R. Os vetores e_i da base canônica de R^m formam uma base para o módulo $R(d)^m$, mas eles são agora considerados elementos homogêneos de grau $-d$ na graduação (iremos em alguns momentos denota-los por e_i^{-d}, para $i \in \{1, \ldots, m\}$), visto que $R(d)_{-d} = R_0$, ou seja,

$$R(d)^m = R(d)e_1^{-d} \oplus \ldots \oplus R(d)e_m^{-d} = \left(\bigoplus_{t_1 \geq 0} R(d)_{t_1} e_1^{-d} \right) \oplus \ldots \oplus \left(\bigoplus_{t_m \geq 0} R(d)_{t_m} e_m^{-d} \right).$$

Exemplo 3.5.8. *Seja $d = 3$ e $m = 2$, logo*

$$R(3)^2 = \left(\bigoplus_{t_1 \geq 0} R(3)_{t_1} e_1^{-3} \right) \oplus \left(\bigoplus_{t_2 \geq 0} R(3)_{t_2} e_2^{-3} \right).$$

Visto que $R(3)_{t_1} = R_{3+t_1}$, assim

$$\begin{array}{rcrcccccc} t_1 & = & -3 & \Longrightarrow & R_{3-3}e_1^{-3} & = & R_0 e_1^{-3} & = & R'_{-3} \\ t_1 & = & -2 & \Longrightarrow & R_{3-2}e_1^{-3} & = & R_1 e_1^{-3} & = & R'_{-2} \\ t_1 & = & -1 & \Longrightarrow & R_{3-1}e_1^{-3} & = & R_2 e_1^{-3} & = & R'_{-1} \\ t_1 & = & 0 & \Longrightarrow & R_{3+0}e_1^{-3} & = & R_3 e_1^{-3} & = & R'_0 \\ t_1 & = & 1 & \Longrightarrow & R_{3+1}e_1^{-3} & = & R_4 e_1^{-3} & = & R'_1 \\ \vdots & & \vdots & & \vdots & & \vdots & & \end{array} \tag{3.12}$$

Analogamente para t_2, temos

$$\begin{array}{rcrcrcrcl} t_2 & = & -3 & \Longrightarrow & R_{3-3}e_2^{-3} & = & R_0e_2^{-3} & = & R''_{-3} \\ t_2 & = & -2 & \Longrightarrow & R_{3-2}e_2^{-3} & = & R_1e_2^{-3} & = & R''_{-2} \\ t_2 & = & -1 & \Longrightarrow & R_{3-1}e_2^{-3} & = & R_2e_2^{-3} & = & R''_{-1} \\ t_2 & = & 0 & \Longrightarrow & R_{3+0}e_2^{-3} & = & R_3e_2^{-3} & = & R''_0 \\ t_2 & = & 1 & \Longrightarrow & R_{3+1}e_2^{-3} & = & R_4e_2^{-3} & = & R''_1 \\ \vdots & & \vdots & & \vdots & & \vdots & & \end{array} \tag{3.13}$$

Logo $R(3)^2 = \left(\bigoplus_{s_1 \geq 0} R'_{s_1}\right) \oplus \left(\bigoplus_{s_2 \geq 0} R''_{s_2}\right)$*, onde os* R'_{s_1} *e* R''_{s_2}*, são definidos como em 3.12 e 3.13.*

Para simplificar, omitiremos os e_i, ou seja,

$$R(d)^m = R(d) \oplus \ldots \oplus R(d).$$

Do mesmo modo podemos considerar módulos livres graduados deslocados da forma

$$R(d_1) \oplus \ldots \oplus R(d_m)$$

para qualquer m-upla de inteiros $d_1, \ldots, d_m$, onde os vetores e_i da base canônica são homogêneos de grau $-d_i$ para cada i.

Definição 3.5.9. *Seja M, N módulos graduados sobre R. Um homomorfismo $\varphi : M \longrightarrow N$ é dito um homomorfismo graduado de grau d se $\varphi(M_t) \subset N_{t+d}$ para todo $t \in \mathbb{Z}$.*

Exemplo 3.5.10. *Suponha que M é um R-módulo graduado gerado pelos elementos homogêneos $f_1, \ldots, f_m$ de graus $d_1, \ldots, d_m$, respectivamente. Então temos um homomorfismo graduado*

$$\varphi : R(-d_1) \oplus \ldots \oplus R(-d_m) \longrightarrow M$$

que envia os elementos da base canônica e_i em $f_i \in M$. Já que e_i tem grau d_i, segue que φ tem grau zero.

Outro exemplo de homomorfismo graduado é dado por uma matriz $A_{m \times p}$ cujas entradas são polinômios homogêneos de grau d no anel R. Então A define um homomorfismo graduado φ de grau d pela multiplicação de matriz

$$\begin{array}{rcl} \varphi : R^p & \longrightarrow & R_m \\ f & \longmapsto & Af. \end{array}$$

Também podemos considera A definindo um homomorfismo graduado de grau zero do módulo graduado deslocado $R(-d)^p$ para R^m. Da mesma forma, se as entradas da j-ésima coluna são polinômios homogêneos de grau d_j, mas o grau varia com a coluna, então A define um homomorfismo graduado de grau zero

$$R(-d_1) \oplus \ldots \oplus R(-d_p) \longrightarrow R^m.$$

Ainda mais geral, um homomorfismo graduado de grau zero

$$R(-d_1) \oplus \ldots \oplus R(-d_p) \longrightarrow R(-c_1) \oplus \ldots \oplus R(-c_m)$$

é definido por uma matriz $A_{m\times p}$ onde as entradas $a_{ij} \in R$ são homogêneas de grau $d_j - c_i$ para todo i, j. Chamaremos a matriz A satisfazendo esta condição para alguma coleção d_j, de graus de colunas, e alguma coleção c_i, de graus de linhas, uma *matriz graduada* sobre R.

A razão para discutimos matrizes graduadas é que elas aparecem nas resoluções livres de módulos graduados sobre R.

Exemplo 3.5.11. *Consideremos a resolução do ideal homogêneo*

$$M =< z^3 - yw^2, yz - xw, y^3 - x^2z, xz^2 - y^2w >$$

em R do Exemplo 3.4.5. M é a imagem do homomorfismos graduado de grau zero

$$R(-3) \oplus R(-2) \oplus R(-3)^2 \longrightarrow R.$$

Observemos que

$$\varphi_1 = \begin{bmatrix} -x & 0 & y & 0 \\ yw & -xz & -z^2 & y^2 \\ 0 & w & 0 & -z \\ z & y & -w & -x \end{bmatrix}$$

(onde as colunas geram o módulo sizígia, $\mathrm{Syz}(M)$*), define também um homomorfismo graduado de grau zero*

$$R(-4)^4 \xrightarrow{\varphi_1} R(-3) \oplus R(-2) \oplus R(-3)^2.$$

Notemos que $d_j = 4$, $j = \{1, 2, 3, 4\}$, $c_1 = c_3 = c_4 = 3$ e $c_2 = 2$ na notação acima, então todas as entradas das linhas 1, 3 e 4 da matriz de φ_1 são polinômios homogêneos de graus $4 - 3 = 1$ e os da linha 2 são de grau $4 - 2 = 2$.

Definição 3.5.12. *Seja M um R-módulo graduado. Uma resolução graduada de M é uma resolução da forma*

$$\ldots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

onde cada F_l é um módulo graduado livre deslocado $R(-d_1) \oplus \ldots \oplus R(-d_p)$ e cada homomorfismo φ_l é um homomorfismo graduado de grau zero (de modo que os φ_l são dados por matrizes graduadas como definidas acima).

Teorema 3.5.13 (Teorema Sizígia de Hilbert Graduado)**.** *Seja $R = k[\mathbf{x}]$. Então todo R-módulo graduado finitamente gerado tem uma resolução graduada finita de comprimento no máximo n.*

Demonstração. A demonstração é análoga a do Teorema Sizígia de Hilbert (Teorema 3.4.3), com algumas pequenas mudanças. Usaremos a Proposição 3.5.5 sobre M, para termos uma base de Gröbner reduzida formada por polinômios homogêneos $\{g_1, \ldots, g_t\}$ e mostraremos que a base de Gröbner do módulo Sizígia de M, obtida usando o Teorema de Schreyer (Teorema 3.2.10), é também um submódulo graduado do módulo livre graduado deslocado $R(-d_1) \oplus \ldots \oplus R(-d_t)$ formado por polinômios homogêneos.

Observemos então que dados $g_i, g_j \in \{g_1, \ldots, g_s\}$, $1 \leq i < j \leq s$, temos

$$\begin{aligned} S(g_i, g_j) &= \frac{\mathbf{m}_{ij}}{TL(g_i)} g_i - \frac{\mathbf{m}_{ij}}{TL(g_j)} g_j \\ &= \mathbf{m}_{ij_i} g_i - \mathbf{m}_{ij_j} g_j, \end{aligned} \tag{3.14}$$

onde $\mathbf{m}_{ij} = \text{MMC}(TL(g_i), TL(g_j))$, $\mathbf{m}_{ij_i} = \dfrac{\mathbf{m}_{ij}}{TL(g_i)}$ e $\mathbf{m}_{ij_j} = \dfrac{\mathbf{m}_{ij}}{TL(g_j)}$. Visto que $\{g_1, \ldots, g_s\}$ é uma base de Gröbner reduzida formada por polinômios homogêneos de graus $d_1, \ldots, d_t$, respectivamente, então $\mathbf{m}_{ij_i}$ tem grau $d_{ij} - d_i$ e $\mathbf{m}_{ij_j}$ tem grau $d_{ij} - d_j$, onde d_{ij} é o grau de $\mathbf{m}_{ij}$. Sendo $g_k = g_{k_1} + \ldots + g_{k_{t_k}}$, $k \in \{1, \ldots, s\}$ e estendendo 3.14 temos

$$S(g_i, g_j) = \mathbf{m}_{ij_i} g_{i_1} + \ldots + \mathbf{m}_{ij_i} g_{i_{t_i}} - (\mathbf{m}_{ij_j} g_{j_1} + \ldots + \mathbf{m}_{ij_j} g_{j_{t_j}}), \tag{3.15}$$

onde cada termo da soma de 3.15 tem grau d_{ij}, logo $S(g_i, g_j)$ é um polinômio homogêneo de grau total d_{ij}.

Visto que, pelo Critério de Buchberger, $S(g_i, g_j) = a_{ij1} g_1 + \ldots + a_{ijt} g_t$, então o grau total de a_{ijk} é $d_{ij} - d_k$, assim

$$a_{ij} = a_{ij1} e_1^{d_1} + \ldots + a_{ijt} e_t^{d_t}$$

é um polinômio homogêneo de grau total também d_{ij}, onde $e_1^{d_1}, \ldots, e_t^{d_t}$ é a base canônica de $R(-d_1) \oplus \ldots \oplus R(-d_t)$.

Portanto

$$\begin{aligned} s_{ij} &= \frac{\mathbf{m}_{ij}}{TL(g_i)} e_i^{d_i} - \frac{\mathbf{m}_{ij}}{TL(g_j)} e_j^{d_j} - a_{ij} \\ &= \mathbf{m}_{ij_i} e_1^{d_1} - \mathbf{m}_{ij_j} e_j^{d_j} - (a_{ij1} e_1^{d_1} + \ldots + a_{ijt} e_t^{d_t}) \end{aligned}$$

são polinômios homogêneos.

□

Exemplo 3.5.14. *Do Exemplo 3.4.5, observemos que podemos ter a resolução graduada*

$$0 \longrightarrow R(-5) \xrightarrow{\varphi_2} R(-4)^4 \xrightarrow{\varphi_1} R(-3) \oplus R(-2) \oplus R(-3)^2 \xrightarrow{\varphi_0} M \longrightarrow 0,$$

onde φ_2, φ_1 e φ_0 são homomorfismo graduados de grau zero.

Referências Bibliográficas

[1] ADAMS, W. W.; LOUSTAUNAU, P. *An Introduction to Gröbner Bases.* AMS, Providence RI, 1994

[2] ATIYAH, M. F.; MACDONALD, I. G. *Introduction to Commutative Algebra.* Addison-Wesley, Reading, 1969.

[3] BECKER, T.; WEISPFENNING, V. *Gröbner Bases*, Springer-Verlag, New York, 1993.

[4] COX, D. J.;LITTLE, J.; O'SHEA, D. *Ideals, Varieties, and Algorithms.* 4nd edition, Springer-Verlag, New York, 2015.

[5] COX, D. J.;LITTLE, J.; O'SHEA, D. *Using Algebraic Geometry.* 2nd edition, Springer-Verlag, New York, 2005.

[6] VILANOVA, F.F. *Sistemas de equações polinomiais e base de Gröbner* / Dissertação. São Cristóvão-SE, 2015.

BASE GRÖBNER: NOÇÕES E APLICAÇÕES

Neste livro estudaremos a teoria das bases de Gröbner no anel de polinômios em várias variáveis sobre um corpo k e no módulo livre sobre k. Veremos também como aplicar essa teoria para determinar a dimensão de um ideal e calcular o módulo Sizígia e uma resolução livre de um submódulo M. Também, usaremos a teoria para demonstrar o Teorema Sizígia de Hilbert, e após isto estenderemos para módulos graduados, usando ainda a teoria das bases de Gröbner.

Home Editora
CNPJ: 39.242.488/0002-80
www.homeeditora.com
contato@homeeditora.com
91988165332
Tv. Quintino Bocaiúva, 23011 - Batista Campos, Belém - PA, 66045-315

9 786560 890473 >