Bases de Gröbner com coeficientes em anéis

Roberto Daniel Torrealba Fernandez

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura:_____

Roberto Daniel Torrealba Fernandez

Bases de Gröbner com coeficientes em anéis

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Matemática. *VERSÃO REVISADA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Daniel Levcovitz

USP – São Carlos
Outubro de 2015

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura:_____

Roberto Daniel Torrealba Fernandez

Gröbner bases with coefficients in rings

Master dissertation submitted to the Instituto de Ciências Matemáticas e de Computação - ICMC-USP, in partial fulfillment of the requirements for the degree of the Master Program in Mathematics. *FINAL VERSION*

Concentration Area: Mathematics

Advisor: Prof. Dr. Daniel Levcovitz

USP – São Carlos
October 2015

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados fornecidos pelo(a) autor(a)

Tb Torrealba, Roberto
Bases de Gröbner com Coeficientes em Anéis / Roberto Torrealba; orientador Daniel Levcovitz. -- São Carlos, 2015.
49 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2015.

1. Anéis noetherianos. 2. Anéis de operadores diferenciais. 3. Bases de Gröbner. I. Levcovitz, Daniel, orient. II. Título.

Resumo

Estudaremos a teoria de bases de Gröbner em anéis de polinômios comutativos com coeficientes em um anel noetheriano e em anéis de operadores diferencias. Apresentaremos, em ambos casos, uma generalização do algoritmo da divisão, do S-polinômio e do algoritmo de Buchberger para calcular bases de Gröbner.

Palavras chaves: Anéis noetheriano, Anéis de operadores diferenciais Bases de Gröbner.

Abstract

We study the theory of Gröbner bases for commutative polynomials rings over a noetherian ring and for rings of diferential operators. In both cases we exhibit a generalization of the division algorithm, the S -polynomial and the Buchberger algorithm for computing Gröbner bases.

Keywords: Notherian rings, Rings of diferentials operators, Gröbner bases.

Dedicatória

À minha Mãe Raquel Anubis Torrealba Fernandez. Te Amo.

Agradecimentos

Quero agradecer ao meu Deus Pai, que marcou meu caminho, me deu forças para seguir e sempre esteve do meu lado.

A minha mãe Raquel Anubis Torrealba Fernández que me apoiou sempre.

Ao Prof. Dr. Daniel Levcovitz, por suas orientacões, sugestões e ajuda nos momentos importantes do trabalho.

A minha namorada Yualy Morles, que luto, comigo mesmo na distancia nos momentos bons e nos momentos ruins. Seu apoio foi sempre muito importante para seguir.

Ao meu amigo, Glauco Lopéz, pelos seus conselhos e dicas importante no desenvolvimento do trabalho e na minha formação como mestre.

A minha amiga Letícia Melocro, por sua grande ajuda no momento de corrigir o português deste trabalho, sua paciência e sua dedicação para me ajudar foram quase infinitas e no final sempre tudo dá certo.

A minha família do Brasil, Liliam Merighe e Alex Pereira da Silva, por aqueles grandes momentos compartilhados juntos, estudos, risadas, piadas e muitos mais.

A minha república LF^3 os quais me aceitaram sem ter me conhecido e com o passar do tempo foram se convertendo em irmãos pra mim: Fernando Couto, Fernando Freitas, Lucas Fernando Castro, Tales Ronca, Guilherme Goncalves, Guilherme Pozzoli e em especial a Matheus Marquesi, quem respondeu aquela petição onde eu procurava onde morar e foi ele quem Deus usou para poder chegar aqui.

Aos meus demais familiares tios, tias, obrigado por seu apoio e por suas orações, primos e primas, obrigado por sempre me dar animo para seguir.

A todos e todas MUCHAS GRACIAS.

Lic. Roberto Daniel Torrealba Fernández

Sumário

Introdução

As bases de Gröbner foram descobertas por Bruno Buchberger em ([3]), que lhe deu este nome em homenagem ao seu orientador de doutorado, Wolfgang Gröbner. Buchberger inventou um algoritmo para calcular as bases de Gröbner em ([4]) que generaliza três algoritmos conhecidos: eliminação de Gauss para resolver sistemas de equações lineares; o algoritmo de Euclides para calcular o Máximo Divisor Comum; e o método Simplex para programação linear no caso bidimensional.

Podemos dizer que uma base de Gröbner é um conjunto de polinômios com propriedades algébricas desejáveis para resolver sistemas de equações gerais, ou seja, sistemas de equações em diversas variáveis, não necessariamente linear.

Alguns anos depois de que Bruno Buchberger publicou seu artigo principal sobre Bases de Gröbner para ideais de anéis comutativos de polinômios com coeficientes em um corpo, W. Trinks publicou uma generalização natural para anéis de polinômios com coeficientes em um anel noethereiano comutativo ([16]). Ele fez uma translação natural da noção de S-polinômio e de redução do caso de um corpo para o caso de um anel. Em 1984, Buchberger também fez uma aproximação para o caso de anéis de polinômios com coeficientes em anéis noetherianos em ([5]).

Pauer e Pfeifhofer apresentaram em 1988 um resultado muito próximo ao caso de coeficiente em um corpo, se considerarmos somente coeficientes em um domínio de ideias principais, ao invés de anéis noetherianos em geral ([15]). Outras propostas de bases de Gröbner com coeficientes em um anel foram feitas em, ([10]), ([11]) e ([12]).

Em 1992 Pauer ([13]), com a ideia de melhorar os cálculos de bases de Gröbner com coeficientes no corpo dos números racionais, usou o método de classes de restos, e assim, fez o estudo das bases de Gröbner sobre $\mathbb{Z}$, $\mathbb{Z}_p$ (p primo) e em $\mathbb{Z}_{p^l}$. Foi ele quem deu uma das primeiras definições para bases de Gröbner reduzidas.

Agora, no caso de anéis de operadores diferenciais (por exemplo uma álgebra de Weyl), a noção de bases de Gröbner foi introduzida em 1985 por Galligo em ([8]). Dois anos depois, Castro apresenta a noção de bases de Gröbner no anel de operadores diferenciais em ([6]). Mais tarde em 1998 motivados por problemas de teoria de sistemas, Insa e Pauer em ([9]) usaram o trabalho de Trinks para definir e calcular bases de Gröbner em uma grande classe de anéis de operadores diferenciais. Uma aplicação deste resultado é a apresentação de um método para verificar quando um módulo a esquerda finitamente gerado sobre certos anéis de operadores diferenciais é um módulo de torção ou não.

Nesta dissertação vamos estudar as bases de Gröbner em dois casos centrais: anéis de polinômios comutativos sobre um anel noetheriano (capítulo 1) e anéis de operadores diferenciais (capítulo 2).

No capítulo 1 seguimos de perto a exposição em [1], capítulo 4. Já para o caso de anéis de operadores diferenciais, nossas referências principais foram [9] e [14].

Avisamos ao leitor que não trataremos aqui do problema da unicidade das bases de Gröbner, isto é, das bases de Gröbner reduzidas. Embora este seja um tema interessante, sua discussão tornaria esta dissertação muito mais extensa e tecnicamente mais difícil.

Capítulo

1

Bases de Gröbner em Anéis de Polinômios

1.1 Definições básicas

Vamos começar apresentando a teoria de bases de Gröbner para polinômios com coeficientes em um anel comutativo noetheriano R, imitando a construção no caso tradicional, ou seja, quando os coeficientes estão em um corpo K. Para isso, $\preceq$ denotará uma ordem monomial (também chamada de ordem admissível) sobre o conjunto de todos os monômios $\mathfrak{M}$ nas indeterminadas $\{x_1, x_2, \ldots, x_n\}$. Trata-se de uma relação de ordem total que satisfaz as seguintes propriedades:

- $1 \preceq m$, para todo $m \in \mathfrak{M}$.
- Se $m_1 \preceq m_2$ então, $mm_1 \preceq mm_2$, para todo $m_1, m_2, m \in \mathfrak{M}$.

Note que $\preceq$ é uma ordem boa ordem.

Exemplos clássicos de ordens monomiais são:

Exemplo 1.1 (Ordem Lexicográfica)**.** *A ordem lexicográfica, denotada lex, deve seu nome a similaridade com a ordem do alfabeto habitual; se estabelece uma ordem entre as indeterminadas da seguinte maneira:*

$$x_i \prec x_j \quad para \quad i > j.$$

Agora, se

$$\mathfrak{m} = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \quad e \quad \mathfrak{n} = x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$$

então

$$\mathfrak{m} \prec_{Lex} \mathfrak{n},$$

se

$$i_1 = j_1, \quad i_2 = j_2, \ \ldots \ i_k = j_k, \quad i_{k+1} < j_{k+1}, \quad \textit{para algum} \quad k.$$

Em outras palavras,

$$\mathfrak{m} \prec_{Lex} \mathfrak{n}$$

se ao compararmos os expoentes na primeira indeterminada onde eles diferem, o expoente na indeterminada em $\mathfrak{m}$ é menor que o expoente na mesma indeterminada em $\mathfrak{n}$.

Exemplo 1.2 (Ordem Lexicográfica graduada)**.** *Na ordem lexicográfica em graus ou graduada, denotada por deglex, realizamos primeiro uma comparação dos graus dos monômios e se eles coincidem usamos a ordem lexicográfica, isto é, dados*

$$\mathfrak{m} = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \quad e \quad \mathfrak{n} = x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}$$

com

$$grau(\mathfrak{m}) = i_1 + i_2 + \cdots + i_n \quad e \quad grau(\mathfrak{n}) = j_1 + j_2 + \cdots + j_n.$$

Dizemos que

$$\mathfrak{m} \prec_{deglex} \mathfrak{n},$$

se

$$grau(\mathfrak{m}) < grau(\mathfrak{n}),$$

ou se

$$grau(\mathfrak{m}) = grau(\mathfrak{n}) \quad e \quad \mathfrak{m} \prec_{lex} \mathfrak{n}.$$

Observe que podemos ver uma ordem monomial $\preceq$ como uma ordem sobre $\mathbb{N}^n$, pois dado $m \in \mathfrak{M}$ com $m = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, existe uma única $n-$upla em $\mathbb{N}^n$ que representa m,

isto é,

$$\alpha := (\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Agora, dada $\prec$ uma ordem monomial sobre $\mathfrak{M}$ e $f \in R[x_1, x_2, \ldots, x_n]$ onde

$$f = c_1 m_1 + c_2 m_2 + \cdots + c_t m_t, \quad \text{com} \quad m_i \in \mathfrak{M},\ c_i \in R - \{0\}, \quad \text{para} \quad i = 1, 2, \ldots, t;$$

e $m_1 \prec m_2 \prec \cdots \prec m_t$. Definimos:

- Suporte de f: $supp(f) = \{m_i : i = 1, 2, \ldots, t\}$.
- Monômio líder de f: $lm(f) = m_t$.
- Coeficiente líder de f: $lc(f) = c_t$.
- Termo líder de f: $lt(f) = c_t m_t$.
- Grau de f: $deg(f) = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{N}^n$.

Além disso, se $f = 0$ então.

- $lm(f) = x^{(-\infty, -\infty, \ldots, -\infty)}$.
- $lc(f) = 0$.
- $deg(f) = (-\infty, -\infty, \ldots, -\infty) \in \mathbb{N}^n$.

Seguindo a construção tradicional da teoria de bases de Gröbner, devemos introduzir a noção da divisibilidade dos termos líderes. No caso em que os coeficientes estão num corpo K não temos com que nos preocupar, mas no nosso caso, como os coeficientes estão em um anel R, teremos um importante desafio.

Para afrontar este desafio, vamos apresentar a teoria de redução e bases de Gröbner generalizando as ideias do caso tradicional.

Assim, consideramos polinômios f e $f_1, f_2, \ldots, f_s$ em $R[x_1, x_2, \ldots, x_n]$ com $f_1, f_2, \ldots, f_s \neq 0$ e queremos dividir f por $f_1, f_2, \ldots, f_s$, isto é, queremos eliminar o termo líder de f usando os termos líderes de $f_1, f_2, \ldots, f_s$. Devemos usar cada f_i tal que $lm(f)$ é divisível por $lm(f_i)$. Isto implica que desejamos que o $lt(f)$ seja combinação linear dos $lt(f_i)$.

Definição 1.3 (Redução em um passo)**.** *Dados dois polinômios f e h e um conjunto de polinômios não nulos $F = \{f_1, f_2, \ldots, f_s\}$ em $R[x_1, x_2, \ldots, x_n]$, dizemos que f se reduz a h módulo F em um passo, denotado por*

$$f \xrightarrow{F} h$$

se, e somente se,

$$h = f - (c_1 X_1 f_1 + c_2 X_2 f_2 + \cdots + c_s X_s f_s)$$

para $c_1, c_2, \ldots, c_s \in R$ e monômios $X_1, X_2, \ldots, X_s$, onde, $lm(f) = X_i lm(f_i)$ para todo i tal que $c_i \neq 0$ e $lt(f) = c_1 X_1 lt(f_1) + c_2 X_2 lt(f_2) + \cdots + c_s X_s lt(f_s)$.

Exemplo 1.4. *Seja $R = \mathbb{Z}$ e sejam $f = xy - 1$, $f_1 = 7x + 3$, $f_2 = 11x^3 - 2y^2$ e $f_3 = 3y - 5$. Vamos usar a ordem deglex, com $x \prec y$.*
Considere $F = \{f_1, f_2, f_3\}$, vemos que $f \xrightarrow{F} h$ onde $h = -3y - 10x - 1$ pois,

$$h = f - yf_1 + xf_3 \quad e \quad xy = lt(f) = ylt(f_1) - 2xlt(f_3)$$

note que $c_2 = 0$ pois $lm(f) = xy$ não é divisível por $lm(f_2) = x^3$.

Por outro lado, seja $R = \mathbb{Z}_{10}$ com deglex $y \prec x$. Sejam $f = 3y$, $f_1 = 5x^2 + y$ e $f_2 = y$, então

$$lt(f) = 2lt(f_1) + 3lt(f_2) \quad e \quad lm(f) = lm(2f_1) = lm(3f_2) = y$$

e

$$h = f - (2f_1 + 3f_2) = -2y$$

que não se reduz.

Observação 1. *As condições*

$$lt(f) = c_1 X_1 lt(f_1) + c_2 X_2 lt(f_2) + \cdots + c_s X_s lt(f_s) \quad e \quad lm(f) = X_i lm(f_i)$$

$\forall i$ tal que $c_i \neq 0$, são a chave no processo de redução e não é equivalente a $lm(f) = lm(c_i X_i f_i)$ $\forall i$ tal que $c_i \neq 0$, como mostra o exemplo acima.

Um fato importante é apresentado no seguinte lema, que vai nos garantir que o processo de redução módulo um conjunto F termina depois de um número finito de passos.

Lema 1.5. *Com a notação da definição 1.3 temos que* $lm(h) \prec lm(f)$.

Demonstração:

Pela definição 1.3 temos que

$$h = f - (c_1X_1f_1 + c_2X_2f_2 + \cdots + c_sX_sf_s)$$

onde, $lm(f) = X_i lm(f_i)$ para todo i tal que $c_i \neq 0$ e

$$lt(f) = c_1X_1lt(f_1) + c_2X_2lt(f_2) + \cdots + c_sX_slt(f_s)$$

ou seja, o termo líder de f é eliminado no processo, assim o monômio líder de h é menor na ordem dada, isto é, $lm(h) \prec lm(f)$.

❑

Sejam $f \in R[x_1, x_2, \ldots, x_n]$ e $F = \{f_1, f_2, \ldots, f_s\}$ um conjunto de polinômios não nulos em $R[x_1, x_2, \ldots, x_n]$. Vamos determinar quando f se reduz módulo F. Primeiro determinamos o conjunto

$$J = \{j : lm(f_j) \text{ divide } lm(f), 1 \leq j \leq s\}.$$

Logo, vamos definir J pela propriedade: $lm(f) = X_i lm(f_i)$ da definição (1.3) e assim devemos resolver a equação

$$lc(f) = \sum_{j \in J} b_j lc(f_j) \tag{1.1}$$

para $b_j \in R$. Esta equação pode ser resolvida se, e somente se, $lc(f) \in (lc(f_j) : j \in J)_R$.

Uma vez obtidos os b_j's podemos fazer a redução de f,

$$f \xrightarrow{F} f - \sum_{j \in J} b_j \frac{lm(f)}{lm(f_j)} f_j.$$

Exemplo 1.6. *Tomemos o exemplo 1.4, temos* $lm(f) = xy$ *e assim,* $J = \{1, 3\}$. *Precisamos solucionar*

$$lc(f) = 1 = b_1 lc(f_1) + b_3 lc(f_3) = 7b_1 + 3b_3.$$

Para isso escolhemos a solução $b_1 = 1$ *e* $b_3 = -2$ *e reduzimos* f *da seguinte maneira*

$$\begin{aligned} h =& f - (b_1 X_1 f_1 + b_3 X_3 f_3) \\ =& f - (y f_1 - 2x f_3) \\ =& -3y - 10x - 1. \end{aligned}$$

Do exemplo anterior percebemos a importância de poder resolver equações lineares em R, o que motiva a seguinte definição.

Definição 1.7. *Dizemos que equações lineares são resolvidas em* R *se valem:*

i) Dados $a, a_1, a_2, \ldots, a_m \in R$ *existe um algoritmo para determinar quando* $a \in (a_1, a_2, \ldots, a_m)$, *e nesse caso o algoritmo calcula* $b_1, b_2, \ldots, b_m \in R$ *tais que*

$$a = b_1 a_1 + b_2 a_2 + \cdots + b_m a_m.$$

ii) Dados $a_1, a_2, \ldots, a_m \in R$ *existe um algoritmo para calcular um conjunto de geradores do* R*-módulo de syzygies*

$$Syz(a_1, a_2, \ldots, a_m) = \{(b_1, b_2, \ldots, b_m) \in R^m |\ a_1 b_1 + a_2 b_2 + \cdots + a_m b_m = 0\}.$$

Exemplos de tais anéis são $\mathbb{Z}$, $\mathbb{Z}_m$, $\mathbb{Q}[x_1, x_2, \ldots, x_m]$, $\mathbb{Z}[i]$, onde $i^2 = -1$ e $\mathbb{Z}[\sqrt{-5}]$.

Agora, vamos definir um dos processos chaves no cálculo de bases de Gröbner, o qual é a redução módulo um conjunto de polinômios não nulos.

Definição 1.8 (Redução módulo F)**.** *Sejam* f, h *e* $f_1, f_2, \ldots, f_s$ *polinômios em* $R[x_1, x_2, \ldots, x_n]$ *com cada um dos* $f_1, f_2, \ldots, f_s \neq 0$ *e seja* $F = \{f_1, f_2, \ldots, f_s\}$. *Dizemos que* f *se reduz a* h *módulo* F *denotado por*

$$f \xrightarrow{F}_{+} h$$

se, e somente se, existem polinômios $h_1, h_2, \ldots, h_{t-1} \in R[x_1, x_2, \ldots, x_n]$ *tais que*

$$f \xrightarrow{F} h_1 \xrightarrow{F} h_2 \xrightarrow{F} \cdots \xrightarrow{F} h_{t-1} \xrightarrow{F} h.$$

Notemos que se $f \xrightarrow{F}_+ h$, *então* $f - h \in (f_1, f_2, \ldots, f_s)$.

Exemplo 1.9. *Continuamos com o exemplo 1.4 onde* $R = \mathbb{Z}$ *e* $f = xy - 1$, $f_1 = 7x + 3$, $f_2 = 11x^3 - 2y^2 + 1$ *e* $f_3 = 3y - 5$ *com* $F = \{f_1, f_2, f_3\}$. *Note que* $f \xrightarrow{F}_+ -10x - 6$, *pois*

$$f \xrightarrow{F}_+ -3y - 10x - 1 \xrightarrow{F}_+ -10x - 6.$$

A primeira redução é obtida do exemplo 1.6 e a segunda redução é obtida somando f_3 *a* $-3y - 10x - 1$.

No caso tradicional, temos um algoritmo de divisão para o cálculo de bases de Gröbner e com ele obtemos um polinômio que usualmente é chamado de resto. Agora, no nosso caso também obtemos tal polinômio, uma vez que o processo de redução módulo um conjunto tenha acabado. Chamaremos tal polinômio de minimal.

Definição 1.10. *Um polinômio* r *é chamado minimal com respeito a um conjunto de polinômios não nulos* $F = \{f_1, f_2, \ldots, f_s\}$ *se* r *não pode ser reduzido módulo* F.

Notação: Para um conjunto $W \subset R[x_1, x_2, \ldots, x_n]$. O ideal gerado pelos termos líderes de W é denotado por

$$Lt(W) = (\{lt(w) : w \in W\}).$$

Uma condição necessária e suficiente para que um polinômio seja minimal é apresentada a seguir.

Lema 1.11. *Um polinômio* $r \in R[x_1, x_2, \ldots, x_n]$ *com* $r \neq 0$ *é minimal com respeito a um conjunto de polinômios não nulos* $F = \{f_1, f_2, \ldots, f_s\} \subset R[x_1, x_2, \ldots, x_n]$ *se, e somente se,* $lt(r) \notin Lt(F)$.

Demonstração:

Suponha que r não seja minimial, isto é, r pode ser reduzido módulo F, ou seja, existe pelo menos um $r' \in R[x_1, x_2, \ldots, x_n]$ tal que

$$r' = r - (c_1 X_1 f_1 + c_2 X_2 f_2 + \cdots + c_s X_s f_s).$$

Isto implica, $lm(r) = X_i lm(f_i)$ para todo i tal que $c_i \neq 0$ e

$$lt(r) = c_1 X_1 lt(f_1) + c_2 X_2 lt(f_2) + \cdots + c_s X_s lt(f_s)$$

ou seja, $lt(r) \in Lt(F)$.

Reciprocamente, se $lt(r) \in Lt(F)$ então $lt(r) = h_1 lt(f_1) + h_2 lt(f_2) + \cdots + h_s lt(f_s)$ para alguns polinômios $h_i \in R[x_1, x_2, \ldots, x_n]$. Se expandimos esta equação em termos individuais, temos que somente um monômio pode ter coeficiente não nulo: $lp(r)$. Assim, podemos assumir que os polinômios h_i são termos, isto é, $h_i = c_i X_i$. Logo, é claro que

$$r - c_1 X_1 f_1 + c_2 X_2 f_2 + \cdots + c_s X_s f_s$$

é uma redução de r. ❑

Note que no exemplo 1.9 o polinômio $r = -10x - 6$ é minimal com respeito a $F = \{f_1, f_2, f_3\}$, pois somente f_1 tem a propriedade que $lm(f_1)$ divide $lm(r)$, mas $lc(r) = -10 \notin (lc(f_1))_{\mathbb{Z}} = (7)_{\mathbb{Z}}$.

Um dos ingredientes importantes para o cálculo de bases de Gröbner é o algoritmo da divisão, que será apresentado, no nosso caso, a seguir.

Teorema 1.12. *[Teorema de Divisão] Sejam $f, f_1, f_2, \ldots, f_s \in R[x_1, x_2, \ldots, x_n]$ com $f_1, f_2, \ldots, f_s \neq 0$ e seja $F = \{f_1, f_2, \ldots, f_s\}$. Então existe $r \in R[x_1, x_2, \ldots, x_n]$ minimal com respeito a F, tal que $f \xrightarrow{F}_+ r$. Além disso, existem $h_1, h_2, \ldots, h_s \in R[x_1, x_2, \ldots, x_n]$ tais que*

$$f = h_1 f_1 + h_2 f_2 + \cdots + h_s f_s + r$$

com

$$lm(f) = \max(\max_{1\leq i\leq s}(lm(h_i)lm(f_i)), lm(r)).$$

Se as equações lineares são resolvidas em R então os h_i's e r podem ser computados.

Demonstração:

Se f não pode ser reduzido módulo F, ou seja, $lt(f) \notin Lt(F)$. Então tomamos $r = f$ e $h_1 = h_2 = \cdots = h_s = 0$. Neste caso, $lm(f) = lm(r)$. Por outro lado, se f pode ser reduzido módulo F temos que

$$f \xrightarrow{F} r_1$$

isto é, $r_1 = f - (c_{1,1}X_{1,1}f_1 + c_{2,1}X_{2,1}f_2 + \cdots + c_{s,1}X_{s,1}f_s)$ com $lm(r_1) \prec lm(f)$. Agora, Se r_1 não pode ser reduzido módulo F, ou seja, r_1 é minimal para F, então tomamos $r = r_1$ e $h_i = c_{i,1}X_{i,1}$ para todo $i = 1, 2, \ldots, s$ e como $lm(f) = X_{i,1}lm(f_i)$ para todo i tal que $c_{i,1} \neq 0$ temos que

$$lm(f) = \max(\max_{1\leq i\leq s}(lm(h_i)lm(f_i)), lm(r)).$$

Além disso, $f = (c_{1,1}X_{1,1}f_1 + c_{2,1}X_{2,1}f_2 + \cdots + c_{s,1}X_{s,1}f_s) + r_1$.

Novamente, se r_1 pode ser reduzido módulo F, temos que existe um r_2 tal que

$$r_1 \xrightarrow{F} r_2,$$

ou seja, $r_2 = r_1 - (c_{1,2}X_{1,2}f_1 + c_{2,2}X_{2,2}f_2 + \cdots + c_{s,2}X_{s,2}f_s)$ com $lm(r_2) \prec lm(r_1)$. Agora, se r_2 não pode ser reduzido módulo F, repetimos o procedimento anterior e notemos que

$$r_1 = (c_{1,2}X_{1,2}f_1 + c_{2,2}X_{2,2}f_2 + \cdots + c_{s,2}X_{s,2}f_s) + r_2.$$

Mas pelo passo anterior $r_1 = f - (c_{1,1}X_{1,1}f_1 + c_{2,1}X_{2,1}f_2 + \cdots + c_{s,1}X_{s,1}f_s)$, ou seja,

$$f = ((c_{1,1}X_{1,1} + c_{1,2}X_{1,2})f_1 + (c_{2,1}X_{2,1} + c_{2,2}X_{2,2})f_2 + \cdots + (c_{s,1}X_{s,1} + c_{s,2}X_{s,2})f_s) + r_2$$

como queríamos. Caso contrário, r_2 pode ser reduzido. Fazemos a redução repetindo o processo até chegar a $r \in R[x_1, x_2, \ldots, x_n]$ que seja minimal e obtemos

$$f \xrightarrow{F} r_1 \xrightarrow{F} r_2 \xrightarrow{F} \cdots \xrightarrow{F} r_{t-1} \xrightarrow{F} r.$$

O processo termina pois $lm(f) \succ lm(r_1) \succ lm(r_2) \succ \cdots \succ lm(r)$ é uma sequência decrescente finita de monômios e $\succ$ é uma boa ordem. Logo reagrupando os termos, obtemos

$$f = h_1 f_1 + h_2 f_2 + \cdots + h_s f_s + r$$

com

$$lm(f) = \max(\max_{1 \leq i \leq s}(lm(h_i)lm(f_i)), lm(r)).$$

❑

Assim, temos o seguinte algoritmo:

Algoritmo 1.

Entrada: $f, f_1, f_2, \ldots, f_s \in R[x_1, x_2, \ldots, x_n]$ *com* $f_i \neq 0$, $1 \leq i \leq s$.

Saída: $h_1, h_2, \ldots, h_s, r$ *onde* $f = h_1 f_1 + h_2 f_2 + \cdots + h_s f_s + r$ *com* $lm(f) = \max(\max_{1 \leq i \leq s}(lm(h_i)lm(f_i)), lm(r))$ *e* r *é minimal com respeito a* $\{f_1, f_2, \ldots, f_s\}$.

Inicialização $h_1 := 0, h_2 := 0, \ldots, h_s := 0, r := f$.

Enquanto *Exista um* i *tal que* $lm(f_i)$ *divide* $lm(r)$ *e existam* $c_1, c_2, \ldots, c_s \in R$ *e monômios* $X_1, X_2, \ldots, X_s$ *tais que* $lt(r) = c_1 X_1 lt(f_1) + c_2 X_2 lt(f_2) + \cdots + c_s X_s lt(f_s)$ *e* $lm(r) = X_i lm(f_i)$ *para todo* $c_i \neq 0$ ***faça***

$r := r - (c_1 X_1 f_1 + c_2 X_2 f_2 + \cdots + c_s X_s f_s)$.

Para $i = 1$ *até* s ***faça***

$h_i := h_i + c_i X_i$.

Vejamos como funciona o algoritmo.

Exemplo 1.13. *Lembremos o exemplo 1.4 e o exemplo 1.9. Usando o algoritmo temos:*

O primeiro passo do loop "enquanto" foi feito no exemplo 1.4 e obtivemos

$$r = f - (yf_1 + (-2x)f_3) = -3y - 10x - 1, \quad h_1 = y, h_2 = 0 \quad e \quad h_3 = -2x$$

e o segundo passo do loop "enquanto" foi feito no exemplo 1.9 e obtivemos

$$r = (-3y - 10x - 1) - (-f_3) = -10x - 6, \quad h_1 = y, h_2 = 0 \quad e \quad h_3 = -2x - 1.$$

O loop "enquanto" termina pois somente $lm(f_1)$ divide $lm(r)$, mas não existe $c \in R = \mathbb{Z}$ tal que $-10x = lt(r) = c(7x)$. Assim,

$$f = yf_1 + (-2x - 1)f_3 + (-10x - 6).$$

Veremos agora o principal teorema deste capítulo. Ele nos proporcionará a definição de bases de Gröbner para ideais de anéis de polinômios com coeficientes em um anel.

Teorema 1.14. *Seja I um ideal de $R[x_1, x_2, \ldots, x_n]$ e $G = \{g_1, g_2, \ldots, g_t\}$ um conjunto de polinômios não nulos em I. Então as seguintes propriedades são equivalentes:*

i) $Lt(G) = Lt(I)$.

ii) Para qualquer polinômio $f \in R[x_1, x_2, \ldots, x_n]$ temos

$$f \in I \quad \text{se, somente se,} \quad f \xrightarrow{G}_{+} 0.$$

iii) Para todo $f \in I$ temos que $f = h_1g_1 + h_2g_2 + \cdots + h_tg_t$, para alguns polinômios $h_1, h_2, \ldots, h_t \in R[x_1, x_2, \ldots, x_n]$ tais que $lm(f) = \max_{1 \leq i \leq s}(lm(h_i)lm(g_i))$.

Demonstração:

$i) \Rightarrow ii)$ $(\Rightarrow)$ Note que se $f \in I$ então $lt(f) \in Lt(I)$, portanto $lt(f) \in Lt(G)$. Assim, f pode ser reduzido módulo G a um polinômio $h \in R[x_1, x_2, \ldots, x_n]$, isto é,

$$h = f - \sum_{i=1}^{t} c_i X_i g_i.$$

Como $f, g_1, g_2, \ldots, g_t \in I$ temos que $h \in I$, portanto $lt(h) \in Lt(I)$ e assim, $lt(h) \in Lt(G)$. Novamente h pode ser reduzido módulo G a um $h_1 \in R[x_1, x_2, \ldots, x_n]$ tal que $h_1 \in I$ e portanto $lt(h_1) \in Lt(I)$. Após fazer reduções sucessivas obtemos $f \xrightarrow{G}_+ 0$.

$(\Leftarrow)$ Se $f \xrightarrow{G}_+ 0$, então $f = h_1 g_1 + h_2 g_2 + \cdots + h_t g_t$. Como $g_i \in I$ para todo $i = 1, 2, \ldots, t$ temos que $f \in I$.

$ii) \Rightarrow iii)$ É claro pelo teorema 1.12.

$iii) \Rightarrow i)$ Temos que $Lt(G) \subset Lt(I)$. Vamos mostrar que $Lt(I) \subset Lt(G)$.
Seja $f \in I$. Por hipótese existem polinômios $h_1, h_2, \ldots, h_t \in R[x_1, x_2, \ldots, x_n]$ tais que $f = h_1 g_1 + h_2 g_2 + \cdots + h_t g_t$ com $lm(f) = \max_{1 \leq i \leq t}(lm(h_i) lm(g_i))$, assim renomeando se necessário temos,

$$lt(f) = c_1 X_1 lt(g_1) + c_2 X_2 lt(g_2) + \cdots + c_s X_s lt(g_s),$$

para algum $s \leq t$, portanto $lt(f) \in Lt(G)$.

❑

Na literatura existem diferentes definições de bases de Gröbner para ideais de anéis de polinômios com coeficientes em um anel. Vamos apresentar a seguinte definição, a qual foi tomada de [1], que é a mais usada e tradicional na literatura. No próximo capítulo, apresentaremos uma outra definição que foi usada em [9].

Definição 1.15. *Um conjunto finito G de polinômios não nulos contido em um ideal I é chamado uma base de Gröbner para I se G satisfaz qualquer uma das três propriedades equivalentes do teorema 1.14. Um conjunto G de polinômios não nulos contido em*

$R[x_1, x_2, \ldots, x_n]$ é chamado uma base de Gröbner, se G for uma base de Gröbner para (G).

Exemplo 1.16. *Seja $R = \mathbb{Z}$ e $A = \mathbb{Z}[x, y]$ com a ordem deglex e $x \prec y$. Seja $f_1 = 4x+1$, $f_2 = 6y + 1$ e $I = (f_1, f_2)$. Então $3yf_1 - 2xf_2 = 3y - 2x \in I$, mas $lt(3y - 2x) = 3y \notin (lt(f_1), lt(f_2)) = (4x, 6y)$ e assim, $\{f_1, f_2\}$ não é uma base de Gröbner para I.*

Considere agora, $g_1 = 2x + 1$, $g_2 = 3y + 1$ e seja $I' = (g_1, g_2)$. Então fazendo todas as combinações lineares de g_1 e g_2 é fácil ver que $Lt(I') = (2x, 3y, xy) = (2x, 3y) = (lt(g_1), lt(g_2))$ e assim $\{g_1, g_2\}$ é uma base de Gröbner para I'.

Corolário 1.17. *Se G é uma base de Gröbner para o ideal I em $R[x_1, x_2, \ldots, x_n]$ então $I = (G)$.*

Demonstração:

Seja $G = \{g_1, g_2, \ldots, g_t\}$ uma Base de Gröbner para o ideal I em $R[x_1, x_2, \ldots, x_n]$. Então, pela propriedade *iii*) do teorema 1.14, temos que

$$f = h_1 g_1 + h_2 g_2 + \cdots + h_t g_t,$$

para todo $f \in I$. Portanto $f \in (G)$ e segue-se que $I = (G)$.

❑

Note que o resto r obtido pelo teorema 1.12 não é necessariamente único, mesmo que F seja uma base de Gröbner. No entanto, pelo teorema 1.14 temos que se G é uma base de Gröbner e $f \in (G)$, o único resto possível para f com respeito a G é 0.

Corolário 1.18. *Se G é uma base de Gröbner e $f \in (G)$ com $f \xrightarrow{G}_+ r$ onde r é minimal, então $r = 0$.*

Demonstração:

Como $f \in (G)$ temos que $r \in (G)$, pois G é uma base de Gröbner. Assim, se $r \neq 0$ então pelo lema (1.11) r não pode ser minimal.

❑

Corolário 1.19. *Seja $I \subset R[x_1, x_2, \ldots, x_n]$ um ideal não nulo, então I tem uma base de Gröbner finita.*

Demonstração:

Como R é noetheriano, então pelo teorema da base de Hilbert, $R[x_1, x_2, \ldots, x_n]$ é noetheriano também. Considere $Lt(I) \subset R[x_1, x_2, \ldots, x_n]$. Então $Lt(I)$ é finitamente gerado, digamos por $\{r_1, r_2, \ldots, r_t\}$. Tome $g_i \in I$ tal que $lt(g_i) = r_i$. Então, $G = \{g_1, g_2, \ldots, g_t\}$ é uma base de Gröbner, pois $Lt(G) = Lt(I)$.

❑

1.2 Calculando bases de Gröbner

1.2.1 Syzygies

Definição 1.20. *Seja $F = (f_1, f_2, \ldots, f_s)$ uma $s-$upla de elementos não nulos de $R[x_1, x_2, \ldots, x_n]$. Um syzygy nos termos líderes $lt(f_1), lt(f_2), \ldots, lt(f_s)$ de F é uma s-upla de polinômios $S = (h_1, h_2, \ldots, h_s) \in R[x_1, x_2, \ldots, x_n]^s$ tal que*

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

Consideremos $Syz(F)$ o subconjunto de $(R[x_1, x_2, \ldots, x_n])^s$ que consiste de todos os syzygies nos termos líderes de F.

Exemplo 1.21. *Seja $F = (x, x^2 + z, y + z)$. Usando a ordem lexicográfica com $x \succ y \succ z$ vemos que $S = (-x + y, 1, -x) \in (\mathbb{Q}[x, y, z])^3$ é um syzygy em $Syz(F)$ pois:*

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

Seja $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Q}[x_1, x_2, \ldots, x_n]^s$ o i-ésimo vetor canônico. Então um syzygy $S \in Syz(F)$ pode ser escrito como

$$S = \sum_{i=1}^{s} h_i e_i.$$

Exemplo 1.22. *Considere os syzygies que vem dos $S-$polinômios no caso que $R = K$ é um corpo. Ou seja, dado um par $\{f_i, f_j\} \subset F$ onde $i < j$, seja X^γ o mínimo múltiplo comum dos monômios líderes de f_i e f_j então:*

$$S_{ij} = \frac{X^\gamma}{lt(f_i)} e_i - \frac{X^\gamma}{lt(f_j)} e_j \tag{1.2}$$

é um syzygy nos termos líderes de $F = (f_i, f_j)$.

Com efeito, o nome $S-$Polinômio é de fato uma abreviação para syzygy-polinômio.

Note que o conjunto dos syzygies é um $R[x_1, x_2, \ldots, x_n]$-submódulo do módulo livre $R[x_1, x_2, \ldots, x_n]^s$. Assim, sendo um submódulo do $R[x_1, x_2, \ldots, x_n]$-módulo noetheriano $R[x_1, x_2, \ldots, x_n]^s$, $Syz(F)$ possui um conjunto finito de geradores, isto é, existe uma coleção finita de syzygies tais que cada syzygy é uma combinação linear com coeficientes polinomiais dos syzygies geradores.

No entanto, precisamos de um conjunto de geradores homogêneos.

Definição 1.23. *Um elemento $S \in Syz(F)$ é dito homogêneo de grau α, onde $\alpha \in \mathbb{N}^n$ se*

$$S = (c_1 X^{\alpha(1)}, c_2 X^{\alpha(2)}, \ldots, c_s X^{\alpha(s)})$$

onde $c_i \in R$ e $\alpha(i) + deg(f_i) = \alpha$ sempre que $c_i \neq 0$.

Um resultado importante sobre a estrutura de $Syz(F)$ é o seguinte lema.

Lema 1.24. *$Syz(F)$ tem um conjunto finito de geradores homogêneos, i.e. existe um conjunto finito $C_F \subset Syz(F)$ tal que cada elemento de C_F é homogêneo e $Syz(F) = (C_F)$.*

Demonstração:

Já vimos que $Syz(F)$ é finitamente gerado. Assim, é suficiente mostrar que dado $S = (h_1, h_2, \ldots, h_s) \in Syz(F)$, podemos escrever S como uma soma de syzygies homogêneos. Fixe um expoente $\alpha \in \mathbb{N}^n$ e seja $h_{i\alpha}$ o termo de h_i tal que $h_{i\alpha} lt(f_i)$ tem grau α. Então temos que $\sum_{i=1}^s h_{i\alpha} lt(f_i) = 0$, pois os $h_{i\alpha} lt(f_i)$ são os termos de grau α na soma $\sum_{i=1}^s h_i lt(f_i) = 0$. Então $S_\alpha = (h_{1\alpha}, h_{2\alpha}, \ldots, h_{s\alpha})$ é um elemento homogêneo de $Syz(F)$ de grau α e $S = \sum_\alpha S_\alpha$.

❑

1.2.2 Algoritmo de Buchberger

Nesta seção vamos apresentar uma generalização do algoritmo de Buchberger para calcular bases de Gröbner em anéis de polinômios sobre anéis noetherianos comutativos.

Teorema 1.25. *[Critério de Buchberger] Seja $G = \{g_1, g_2, \ldots, g_t\}$ um conjunto de polinômios não nulos em $R[x_1, x_2, \ldots, x_n]$. Seja B um conjunto de geradores homogêneos para $Syz(g_1, g_2, \ldots, g_t)$. Então G é uma base de Gröbner para o ideal $I = (g_1, g_2, \ldots, g_t)$ se, e somente se, para todo $(h_1, h_2, \ldots, h_t) \in B$, temos que:*

$$h_1g_1 + h_2g_2 + \cdots + h_tg_t \xrightarrow{G}_+ 0.$$

Demonstração:

($\Rightarrow$) Dado um syzygy homogêneo $(h_1, \cdots, h_t) \in B$, então

$$f := h_1g_1 + h_2g_2 + \cdots + h_tg_t \in I.$$

Logo, pelo teorema (1.14),

$$f = h_1g_1 + h_2g_2 + \cdots + h_tg_t \xrightarrow{G}_+ 0.$$

($\Leftarrow$) Dado $g \in (G)$ temos que

$$g = u_1g_1 + u_2g_2 + \cdots + u_tg_t, \quad u_i \in R[x_1, \ldots, x_n]. \tag{1.3}$$

Escolha uma representação de $g \in (G)$ como acima tal que $X = \max_{1\leq i\leq t}(lm(u_i)lm(g_i))$ seja mínimo com respeito a $\prec$. Afirmamos que, para uma tal representação, tem-se $X = lm(g)$, o que conclui a prova pelo teorema (1.14). Vamos supor por contradição que $lm(g) \prec X$.

Seja $E = \{i \in \{1, 2, \ldots, t\} | lm(u_i)lm(g_i) = X\}$. Assim,

$$\sum_{i\in E} lt(u_i)lt(g_i) = 0.$$

Seja

$$h = \sum_{i \in E} lt(u_i)e_i$$

onde $e_1, e_2, \ldots, e_t$ é a base canônica do módulo $(R[x_1x_2, \ldots, x_n])^t$. Logo, $h \in Syz(G)$ e h é homogêneo de grau $deg(X)$. Agora, pelo lema (1.24), $Syz(G)$ tem um conjunto de geradores homogêneos, digamos $B = \{h_1, h_2, \ldots, h_l\}$ onde, para cada $j = 1, 2, \ldots, l$, $h_j = (h_{1j}, h_{2j}, \ldots, h_{tj})$. Escrevemos

$$h = \sum_{j=1}^{l} a_j h_j, \quad a_j \in R[x_1, \ldots, x_n].$$

Como h é um syzygy homogêneo de grau X, temos que, para cada $j = 1, 2, \ldots, l$ e $i = 1, 2, \ldots, t$, $lm(a_j)lm(h_{ij})lm(g_i) = X$ sempre que $lm(a_j)lm(h_{ij}) \neq 0$. Logo, por hipótese, para cada j temos

$$\sum_{i=1}^{t} h_{ij}g_i \xrightarrow{G}_{+} 0.$$

Pelo teorema (1.12), para cada j existe uma família $v_{1j}, v_{2j}, \ldots, v_{tj}$ em $R[x_1, x_2, \ldots, x_n]$ tal que

$$\sum_{i=1}^{t} h_{ij}g_i = \sum_{i=1}^{t} v_{ij}g_i,$$

e $\max_{1 \leq i \leq t} (lm(v_{ij})lm(g_i)) = lm(\sum_{i=1}^{t} h_{ij}g_i)$. Como $\sum_{i=1}^{t} h_{ij}lt(g_i) = 0$ segue que $lm(\sum_{i=1}^{t} h_{ij}g_i) \prec \max_{1 \leq i \leq t} lm(h_{ij})lm(g_i)$. Agora,

$$\begin{aligned} g =& u_1g_1 + u_2g_2 + \cdots + u_tg_t \\ =& \sum_{i \in E} lt(u_i)g_i + \sum_{i \in E} (u_i - lt(u_i))g_i + \sum_{i \notin E} u_ig_i. \end{aligned}$$

Note que todos os termos em $\sum_{i \in E} (u_i - lt(u_i))g_i + \sum_{i \notin E} u_ig_i$ são menores que X

com respeito a $\prec$. Logo,

$$\begin{aligned} g &= \sum_{j=1}^{l}\sum_{i=1}^{t} a_j h_{ij} g_i + \text{termos menores que } X \text{ com respeito a } \prec \\ &= \sum_{j=1}^{l}\sum_{i=1}^{t} a_j v_{ij} g_i + \text{termos menores que } X \text{ com respeito a } \prec. \end{aligned}$$

Finalmente,

$$\max_{i,j}\left(lm(a_j)lm(v_{ij})lm(g_i)\right) \prec \max_{i,j}\left(lm(a_j)lm(h_{ij})lm(g_i)\right) = X,$$

contradizendo a minimalidade de X. Portanto $lm(g) = X$ e segue que G é uma base de Gröbner para I.

❑

Podemos considerar $h_1g_1 + h_2g_2 + \cdots + h_tg_t$ como uma generalização dos S-polinômios no caso tradicional. De fato, nessa expressão o termo líder se cancela. Agora, estamos prontos para dar uma generalização do algoritmo de Buchberger pois temos um processo de redução (definição (1.8)) e os S-polinômios, os quais são necessário para calcular bases de Gröbner. Mas antes de apresentar tal generalização, vamos apresentar um método para construir um conjunto de geradores homogêneos para o módulo de syzygies dos termos líderes.

Queremos construir um conjunto de geradores homogêneos para $Syz(G)$. Em geral, dado um conjunto de monômios $\{X_1, X_2, \ldots, X_s\}$ e elementos não nulos $c_1, c_2, \ldots, c_s \in R$, como construir um conjunto de geradores homogêneos para $Syz(c_1X_1, c_2X_2, \ldots, c_sX_s)$?

Definição 1.26. *Para cada subconjunto $J \subseteq \{1, 2, \ldots, s\}$, seja $X_J = mmc(X_j | j \in J)$. Dizemos que J é saturado com respeito a $X_1, X_2, \ldots, X_s$ se:*

- *Para todo $j \in \{1, 2, \ldots, s\}$ tal que X_j divide X_J então $j \in J$.*

Para qualquer subconjunto $J \subseteq \{1, 2, \ldots, s\}$ chamamos a saturação de J ao conjunto J' o qual consiste de todos os $j \in J$ tal que X_j divide X_J.

Note que se J é saturado então $J = J'$.

Exemplo 1.27. *Seja* $X_1, = xy$, $X_2 = x^2$, $X_3 = y$, *e* $X_4 = x^4$. *Se* $J = \{1, 2\}$ *temos que* $X_J = x^2y$. *Note que* $X_3 = y$ *divide* $X_J = x^2y$, *mas* $3 \notin J$, *portanto* J *não é saturado. Por outro lado, se* $J = \{1, 2, 3\}$ *temos que* $X_J = x^2y$. *Como* $X_4 = x^4$ *não divide* X_J *e* 4 *é o único elemento de* $\{1, 2, 3, 4\}$ *tal que* $4 \notin J$, *logo* J *é saturado. Assim* $\{1, 2, 3\}$ *é a saturação de* $\{1, 2\}$.

Teorema 1.28. *Sejam* $\{X_1, \ldots, X_s\}$ *um conjunto de monômios e* $c_1, \ldots, c_s \in R$. *Para cada subconjunto* $J \subseteq \{1, 2, \ldots, s\}$, *o qual é saturado com respeito a* $X_1, X_2 \ldots, X_s$, *seja* $B_J = \{\mathbf{b}_{1J}, \mathbf{b}_{2J}, \ldots, \mathbf{b}_{v_J J}\}$ *um conjunto de geradores do* R*-módulo de syzygies* $Syz_R(c_j | j \in J)$, $(\mathbf{b}_{v_J J} \in R^{|J|})$. *Para cada* $\mathbf{b}_{vJ}$ *denote sua* j*-ésima coordenada por* $\mathbf{b}_{j_v J}$ $(j \in J)$. *Seja*

$$\mathbf{s}_{vJ} = \sum_{j \in J} b_{j_v J} \frac{X_J}{X_j} e_j \quad (\mathbf{s}_{vJ} \in R^s).$$

Então o conjunto de vetores $\mathbf{s}_{v,J}$, *para* J *percorrendo todos os subconjuntos saturados de* $\{1, 2, \ldots, s\}$ *e* $1 \leq v \leq v_J$, *formam um conjunto de geradores homogêneos para o módulo de syzygies* $Syz(c_1X_1, c_2X_2, \ldots, c_sX_s)$.

Demonstração:

Primeiramente é claro que $\mathbf{s}_{vJ}$ é homogêneo de grau $deg(X_j)$. Além disso, $\mathbf{s}_{vJ}$ é um syzygy de $(c_1X_1, c_2X_2, \ldots, c_sX_s)$, pois

$$\begin{aligned}(c_1X_1, c_2X_2, \ldots, c_sX_s) \cdot s_{vJ} =& (c_1X_1, c_2X_2, \ldots, c_sX_s) \cdot \sum_{j \in J} b_{j_v J} \frac{X_J}{X_j} e_j \\ =& \sum_{j \in J} b_{j_v J} \frac{X_J}{X_j} c_j X_j = X_J \sum_{j \in J} b_{j_v J} c_j = 0,\end{aligned}$$

já que $\mathbf{b}_{vJ}$ é um syzygy de $(c_j, j \in J)$.

Agora, seja $\mathbf{h} = (h_1, h_2, \ldots h_s) \in Syz(c_1X_1, c_2X_2, \ldots, c_sX_s)$. Pelo lema (1.24) o módulo de syzygies $Syz(c_1X_1, c_2X_2, \ldots, c_sX_s)$ é gerado por um conjunto de syzygies homogêneos. Portanto é suficiente mostrar que $\mathbf{h}$ é combinação linear dos $\mathbf{s}_{vJ}$, no caso que $\mathbf{h}$ é homogêneo de grau $deg(Y)$. Escrevemos $\mathbf{h} = (d_1Y_1, d_2Y_2, \ldots, d_sY_s)$ para $d_1, d_2, \ldots, d_s \in R$ e monômios $Y_1, Y_2, \ldots, Y_s$. Seja $J = \{j : d_j \neq 0\}$ e J' a saturação de J. Temos que $Y_jX_j = Y$, para todo $j \in J$, pois $\mathbf{h}$ é homogêneo de grau $deg(Y)$. Como $\mathbf{h}$ é um syzygy

de $(c_1X_1, c_2X_2, \ldots, c_sX_s)$ temos que

$$\sum_{j\in J} d_jY_jc_jX_j = Y\sum_{j\in J} d_jc_j = 0.$$

Logo, $(d_j|j \in J')$ é um syzygy de $(c_j|j \in J')$ e portanto, pela hipótese,

$$(d_j|j \in J') = \sum_{v=1}^{v_{J'}} r_v\mathbf{b}_{vJ'}, \quad (r_v \in R).$$

Olhando para as componentes dos vetores acima, temos que, para cada $j \in J'$,

$$d_j = \sum_{v=1}^{v_{J'}} r_v b_{j_vJ'}.$$

Agora, como $Y_jX_j = Y$, cada X_j divide Y e portanto $X_J = X_{J'}$ divide Y. Logo,

$$\begin{aligned}
\sum_{v=1}^{v_{J'}} r_v\frac{Y}{X_{J'}}s_{vJ'} =& \sum_{v=1}^{v_{J'}}\sum_{j\in J} r_v\frac{Y}{X_{J'}}\frac{X_{J'}}{X_J}b_{j_vJ'}e_j \\
=& \sum_{j\in J'}\left(\sum_{v=1}^{v_{J'}} r_v b_{j_vJ'}\right)Y_je_j \\
=& \sum_{j\in J'} d_jY_je_j \\
=& \sum_{j=1}^{s} d_jY_je_j \quad (j \notin J' \Rightarrow j \notin J \Rightarrow d_j = 0) \\
=& \mathbf{h},
\end{aligned}$$

como queríamos.

❑

Exemplo 1.29. *Considere $R = \mathbb{Z}$. Sejam $c_1X_1 = 2xyz$, $c_2X_2 = 5xy^2$, $c_3X_3 = 85y^2$ e $c_4X_4 = 6x^2z$. Note que em $\mathbb{Z}$ podemos resolver equações lineares. Agora, os subconjuntos saturados de $\{1,2,3,4\}$ são: $\{1\}$, $\{3\}$, $\{4\}$, $\{1,4\}$, $\{2,3\}$, $\{1,2,3\}$ e $\{1,2,3,4\}$. Veja que $\{2\}$ não é saturado, pois X_3 divide X_2 e $3 \notin \{2\}$. Como $R = \mathbb{Z}$ é um domínio de integridade, os syzygies relacionados com $\{1\}$, $\{3\}$ e $\{4\}$ são todos nulos.*

- $J = \{1, 4\}$. *Resolvendo a equação*

$$2b_1 + 6b_4 = 0, \tag{1.4}$$

temos que o conjunto de soluções para (1.4) é gerado por $\{(-3, 1)\}$. *Como* $X_J = x^2yz$, *o correspondente syzygy é*

$$-3\frac{x^2yz}{xyz}e_1 + \frac{x^2yz}{x^2z}e_4 = (-3x, 0, 0, y).$$

- $J = \{2, 3\}$. *Resolvendo a equação*

$$5b_2 + 85b_3 = 0, \tag{1.5}$$

temos que o conjunto de soluções para (1.5) é gerado por $\{(-17, 1)\}$. *Como* $X_J = xy^2$, *o correspondente syzygy é*

$$-17\frac{xy^2}{xy^2}e_2 + \frac{xy^2}{y^2}e_3 = (0, -17, x, 0).$$

- $J = \{1, 2, 3\}$. *Resolvendo a equação*

$$2b_1 + 5b_2 + 85b_3 = 0, \tag{1.6}$$

temos que o conjunto de soluções para (1.6) é gerado pelos dois elementos $\{(-40, -1, 1)\}$ *e* $(-5, 2, 0)$. *Como* $X_J = xy^2z$, *os correspondentes syzygies são*

$$-40\frac{xy^2z}{xyz}e_1 - \frac{xy^2z}{xy^2}e_2 + \frac{xy^2z}{y^2}e_3 = (-40y, -z, xz, 0)$$

e

$$-5\frac{xy^2z}{xyz}e_1 + 2\frac{xy^2z}{xy^2}e_2 = (-5y, 2z, 0, 0).$$

Finalmente para $J = \{1, 2, 3, 4\}$ *obtemos os geradores* $(-40, -1, 1, 0)$, $(-5, 2, 0, 0)$ *e* $(-3, 0, 0, 1)$. *Esse syzygies já foram obtidos e portanto já estão em nosso conjuntos de*

geradores. Assim, obtemos

$$Syz(2xyz, 5xy^2, 85y^2, 6x^2z) = ((-3x, 0, 0, y), (0, -17, x, 0), (-40y, -z, xz, 0), (-5y, 2z, 0, 0)).$$

Finalmente vamos apresentar o algoritmo principal de este capitulo, uma generalização do algoritmo de Buchberguer.

Algoritmo 2.

Entrada: $F = \{f_1, f_2, \ldots, f_s\} \subset R[x_1, x_2, \ldots, x_n]$.

Saída: $G = \{g_1, g_2, \ldots, g_t\}$ *uma base de Gröbner para* $(f_1, f_2, \ldots, f_s)$.

Inicialização: $G := \emptyset$, $G' := F$.

Enquanto $G' \neq G$ ***faça***

$G := G'$

Considere os elementos de G *e*

calcule um conjunto C_G *de geradores homogêneos*

para $Syz(G)$

Para *cada* $h \in C_G$ ***faça***

Reduza $\sum_{i=1}^{\#G} h_i g_i \xrightarrow{G'}_+ r$ *com* r *minimal con respeito a* G'

Se $r \neq 0$ ***então***

$G' := G' \cup \{r\}$.

Vamos provar que o algoritmo termina em um número finito de passos e calcula uma base de Gröbner para $I = (f_1, \ldots, f_s)$. Primeiro note que, para cada $h \in C_G$ o algoritmo produz um novo conjunto de geradores de I sempre que o resto da redução de $\sum_{i=1}^{\#G} h_i g_i \xrightarrow{G'}_+ r$ por G' é não nulo. Assim, suponhamos que $G_0 = G'$ e que G_j é o conjunto de geradores resultante ao final do j-ésimo passo. Então, $G_{j+1} = G_j \cup \{r_{j+1}\}$; onde r_{j+1} é o resto da divisão de algum $\sum_{i=1}^{\#G} h_i g_i \xrightarrow{G'}_+ r$ por G_j. Logo, temos

$$Lt(G_0) \subset Lt(G_1) \subset Lt(G_2) \subset \cdots \subset Lt(G_j) \subset \cdots$$

Como $R[x_1, x_2, \ldots, x_n]$ é noetheriano temos que a cadeia é estacionária, portanto existe um $k \in \mathbb{N}$ tal que $Lt(G_k) = Lt(G_t)$ para todo $t \leq k$. Assim, $lt(r_t) \in Lt(G_k)$ e portanto $r_t = 0$ para todo $t > k$. Logo, o algoritmo termina em um número finito de passos. Por outra parte, pelo teorema (1.26) o algoritmo calcula uma base de Gröbner para I.

❑

Encerraremos o capítulo com um exemplo onde podamos calcular uma base de Gröbner com ajuda do algoritmo de buchberger

Exemplo 1.30. *Sejam $R = \mathbb{Z}$, $A = \mathbb{Z}[x, y]$ a ordem deglex com $x \prec y$ e $g_1 = 2x + 1$, $g_2 = 3y + 1$ como no Exemplo (1.6). Considere $I' = (g_1, g_2)$. Vamos mostrar que de fato $\{g_1, g_2\}$ é uma base de Gröbner para I.*

O passo 1 pelo algoritmo é calcular um conjunto de geradores homogêneos de $Syz(G)$, para isso temos que $Syz(G)$ é gerado por $\{(3y, -2x)\}$ logo pelo Teorema (1.28) temos que o conjunto $\{(3y, -2x)\}$ é um conjunto de geradores homogêneos.

O passo 2 é calcular o S-polinômio associado a $(3y, -2x)$, ou seja,

$$Spoly = 3y(2x + 1) - 2x(3y + 1) = 3y - 2x$$

O passo 3 é reduzir o Spoly módulo G,

$$Spoly = 3y - 2x \xrightarrow{G}_{+} 0$$

Por tanto $G = \{g_1 = 2x + 1, g_2 = 3y + 1\}$ é uma base de Gröbner para o ideal I.

Capítulo

2

Bases de Gröbner em Anéis de Operadores Diferenciais

Neste capítulo vamos estudar anéis (não comutativos) de operadores diferenciais. Apresentaremos um algoritmo de divisão, uma definição de bases de Gröbner e uma generalização do algoritmo de Buchberger ([14]).

2.1 Algoritmo de divisão

Seja R um anel noetheriano comutativo de modo que possamos resolver equações lineares sobre R, i.e.

- para todo $z \in R$ e para todo subconjunto finito $S \subseteq R$ podemos decidir quando z é um elemento do ideal gerado por S e se sim, podemos calcular uma família $(d_s)_{s\in S}$ em R tal que $z = \sum_{s\in S} d_s s$.

- para todo subconjunto finito $S \subseteq R$ podemos calcular um conjunto finito de geradores do R-módulo $\{(c_s)_{s\in S} \in R^{\#S} : \sum_{s\in S} c_s s = 0\}$ dos syzygies de S.

Exemplos importantes são $\mathbb{Z}$, $\mathbb{Z}_m$, anéis de polinômios com coeficientes num corpo e certos subanéis do corpo de funções racionais com coeficientes sobre um corpo K, por exemplo

$$\left\{\frac{p}{q} : p, q \in K[y_1, y_2, \ldots, y_n], q(a) \neq 0\right\} \quad \text{onde} \quad a \in K^n.$$

Seja A um anel associativo noetheriano à esquerda com unidade contendo R como um subanel e elementos $x_1, x_2, \ldots, x_n \in A$ tais que

- Os elementos $x_1, x_2, \ldots, x_n$ comutam entre si, isto é, $x_i x_j = x_j x_i$ para todos $1 \leq i, j \leq n$.
- A é um R-módulo livre à esquerda e a família $(x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n})_{\alpha \in \mathbb{N}^n}$ é uma R-base do R-módulo A, i.e., cada elemento de A pode ser escrito unicamente como $\sum_{\alpha \in \mathbb{N}} c_\alpha x^\alpha$, $c_\alpha \in R$, onde somente um número finito de c_α são não nulos.

Um exemplo bem conhecido de A é:

- Anéis de operadores diferenciais: seja K um corpo de característica zero, n um inteiro positivo e $K(y_1, y_2, \ldots, y_n)$ o corpo das funções racionais em n indeterminadas sobre K. Seja $\frac{\partial}{\partial y_i} : K(y_1, y_2, \ldots, y_n) \to K(y_1, y_2, \ldots, y_n)$ a derivada parcial em y_i, $1 \leq i \leq n$. Seja R uma K-subálgebra noetheriana de $K(y_1, y_2, \ldots, y_n)$, a qual é estável por $\frac{\partial}{\partial y_i}$, $1 \leq i \leq n$. Denotamos por D_i a restrição de $\frac{\partial}{\partial y_i}$ a R, $1 \leq i \leq n$. Seja $A = R[D] = R[D_1, D_2, \ldots, D_n] = R[x_1, x_2, \ldots x_n]$ a R-subálgebra de $End_K(R)$ gerada por $id_R = 1$ e $D_1, D_2, \ldots, D_n$. O anel $R[D]$ é chamado **anel de operadores diferenciais** com coeficientes em R ([2]). Tais anéis são K-álgebras não comutativas que satisfazem as seguintes relações:

$$y_i y_j = y_j y_i, \quad D_i D_j = D_j D_i, \quad y_i D_j - D_j y_i = -\delta_{ij} \quad \text{para} \quad 1 \leq i, j \leq n,$$

onde δ_{ij} é o delta de Kronecker.

Os elementos de $R[D]$ podem ser escritos unicamente como somas finitas

$$\sum_{(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n} r_{i_1, i_2, \ldots, i_n} D_1^{i_1} D_2^{i_2} \cdots D_n^{i_n} \quad \text{onde} \quad r_{i_1, i_2, \ldots, i_n} \in R,$$

ou resumidamente, como

$$\sum_{i \in \mathbb{N}^n} r_i D^i, \quad \text{onde } i = (i_1, i_2, \ldots, i_n) \quad \text{e} \quad r_i \in R.$$

Exemplos 2.1.

i) A álgebra de Weyl ou o anel de operadores diferenciais com coeficientes polinomiais:

$$A_n = K[y_1, y_2, \ldots, y_n][D_1, D_2, \ldots, D_n], \tag{2.1}$$

onde K é um corpo de caraterística 0.

ii) O anel de operadores diferenciais com coeficientes funções racionais:

$$B_n = K(y_1, y_2, \ldots, y_n)[D_1, D_2, \ldots, D_n], \tag{2.2}$$

iii) O anel de operadores diferenciais com coeficientes séries de potências formais:

$$D_n = K[[y_1, y_2, \ldots, y_n]][D_1, D_2, \ldots, D_n]. \tag{2.3}$$

Existe um outro exemplo importante para $R[D]$, este é o anel de operadores diferenciais com coeficientes em um anel local R, $A = R[D_1, D_2, \ldots, D_n]$, onde

$$R = K[y_1, y_2, \ldots, y_n]_M = \left\{ \frac{f}{g} \in K(y_1, y_2, \ldots, y_n) | f \in K[y_1, y_2, \ldots, y_n], g \in M \right\}$$

e M é um sistema multiplicativo de $K[y_1, y_2, \ldots, y_n] \backslash \{0\}$.

No anel de operadores diferenciais $R[D]$, o conjunto de monômios é $\{D^\alpha, \alpha \in \mathbb{N}^n\}$. **Note que neste caso os monômios não comutam com os coeficientes** $r \in R$.

Seja $\preceq$ uma ordem monomial em $\mathbb{N}^n$. Lembramos que para um operador diferencial $f = \sum_{i \in \mathbb{N}^n} r_i D^i$ com $f \neq 0$ definimos grau, coeficiente líder, monômio líder e termo líder como se segue:

$deg(f) = max_{\preceq}\{i | r_i \neq 0\} \in \mathbb{N}^n$,

$lc(f) = r_{deg(f)} \in R$,

$lm(f) = D^{deg(f)}$,

$lt(f) = lc(f)D^{deg(f)}$.

Para um subconjunto F de $R[D]$ definimos:

$deg(F) = \{deg(f)|f \in F, f \neq 0\}$,

$Lt(F) = \{lt(f)|f \in F, f \neq 0\}$.

Observação 2. *As seguintes afirmações em A são válidas para todo $\alpha \in \mathbb{N}^n$ e $f, g \in A$ tais que $fg \neq 0$*

1. *$deg(fg) = deg(f) + deg(g)$, em particular $deg(x^\alpha f) = \alpha + deg(f)$,*

2. *$lc(fg) = lc(f)lc(g)$, em particular $lc(x^\alpha f) = lc(f)$.*

É fácil verificar que estas propiedades valem para toda ordem monomial e todo anel de operadores diferenciais. Em um anel comutativo de polinômios ainda temos $lt(x^\alpha f) = x^\alpha lt(f)$, mas no anel de operadores diferenciais isto não é verdade em geral. Consideremos por exemplo o operador $D_1(y_1D_1) = (D_1y_1)D_1 = (y_1D_1+1)D_1 = y_1D_1^2+D_1$. Então,

$$lt(D_1(y_1D_1)) = y_1D_1^2 \neq D_1y_1D_1 = D_1lt(y_1D_1).$$

Vamos introduzir a seguinte notação. Se B é um subconjunto de R (resp: A) denotaremos por ${}_R(B)$ (resp:${}_R(A)$) o ideal (resp: ideal à esquerda) gerado por B em R (resp em A).

Teorema 2.2. *[Teorema de Divisão] Seja F um subconjunto finito de $A\backslash\{0\}$ e seja $g \in A$. Então existe $r \in A$ e uma família $(h_f)_{f\in F}$ em A tal que:*

(i) $g = \sum_{f\in F} h_f f + r$ (r é um resto de g depois da divisão por F),

(ii) para todo $f \in F$, $h_f = 0$ ou $deg(h_f f) \preceq deg(g)$,

(iii) $r = 0$ ou $lc(r) \notin {}_R(lc(f) : f \in F$ e $deg(r) \in deg(f) + \mathbb{N}^n)$.

Demonstração:

Para demostrar o teorema, é suficiente mostrar que o algoritmo que vamos apresentar em seguida termina em um número finito de passos. Ele vai nos permitir calcular os elementos $r \in A$ e $h_f \in A$ $(f \in F)$ dados no teorema.

Algoritmo 3.

Entrada: *$F \subset A\backslash\{0\}$ um subconjunto finito e $g \in A$.*

Saída: *$r \in A$ e $\{h_f\}_{f\in F}$ uma família em A tais que:*

- *$g = \sum_{f\in F} h_f f + r$,*
- *para todo $f \in F$, $h_f = 0$ ou $deg(h_f f) \preceq deg(g)$,*
- *$r = 0$ ou $lc(r) \notin {}_R(lc(f) : f \in F \text{ e } deg(r) \in deg(f) + \mathbb{N}^n)$.*

Inicialização *$h_f := 0$ para todo $f \in F$, $r := g$.*

Enquanto *$r \neq 0$ e $lc(r) \in {}_R(lc(f) : f \in F \text{ e } deg(r) \in deg(f) + \mathbb{N}^n)$* ***faça***

$F' := \{f \in F : deg(r) \in deg(f) + \mathbb{N}^n\}$.

Calcule $\{c_f\}_{f\in F'}$ em R tal que

$$\sum_{f\in F'} c_f lc(f) = lc(r).$$

$r := r - (\sum_{f\in F'} c_f D^{deg(r)-deg(f)} f)$

$h_f := h_f + c_f D^{deg(r)-deg(f)}$ para todo $f \in F'$.

Vamos provar que o algoritmo termina e calcula o que desejamos.

Note que, se $deg(g) \prec deg(f)$ para todo $f \in F$ então, pelo primeiro passo do algoritmo (inicialização), obtemos $r = g$ e $h_f = 0$ para todo $f \in F$.

Caso contrário, existe algum $F' \subset F$ não vazio tal que $deg(f) \preceq deg(g)$ para todo $f \in F'$. Assim, depois da inicialização do algoritmo temos que considerar: $r \neq 0$ e $lc(r) \in {}_R(lc(f) : f \in F \text{ e } deg(r) \in deg(f) + \mathbb{N}^n)$. Suponhamos que $r \neq 0$. Se $lc(r) \notin$

$(lc(f) : f \in F \text{ e } deg(r) \in deg(f) + \mathbb{N}^n)$ então temos $r = g$ e $h_f = 0$ para todo $f \in F$. Por outro lado, se $lc(r) \in {}_R(lc(f) : f \in F \text{ e } deg(r) \in deg(f) + \mathbb{N}^n)$ então entramos no loop e obtemos $r_1 = r - \sum_{f \in F_1'} c_f D^{deg(r)-deg(f)} f$ e $h_f := h_f + c_f D^{deg(r)-deg(f)}$ para todo $f \in F_1' = \{f \in F : deg(r) \in deg(f) + \mathbb{N}^n\}$. Agora, se $r_1 = 0$ temos, $r = r_1$ e $h_f = 0$ para todo $f \in F \backslash F_1'$ e portanto o teorema termina em um número finito de passos. Se $r_1 \neq 0$ e $lc(r_1) \notin (lc(f) : f \in F \text{ e } deg(r_1) \in deg(f) + \mathbb{N}^n)$ então temos $r = r_1$ e $h_f = 0$ para todo $f \in F \backslash F_1'$. Por outro lado, se $lc(r_1) \in {}_R(lc(f) : f \in F \text{ e } deg(r_1) \in deg(f) + \mathbb{N}^n)$ então entramos no loop pela segunda vez, e obtemos $r_2 = r_1 - \sum_{f \in F_2'} c_f D^{deg(r_1)-deg(f)} f$ e $h_f := h_f + c_f D^{deg(r_1)-deg(f)}$ para todo $f \in F_2' = \{f \in F : deg(r_1) \in deg(f) + \mathbb{N}^n\}$. Podemos proceder assim continuamente, e obtemos uma sequência de monômios líderes

$$lm(r) \succ lm(r_1) \succ lm(r_2) \succ \cdots \succ lm(r_t) \succ \cdots$$

Como $\succ$ é uma ordem admissível então temos que a cadeia para e portanto o algoritmo acaba num numero finito de passos com $r = r_t$ onde $lm(r_t)$ é o monômio líder minimal da cadeia. ❑

Exemplo 2.3. *Seja* $R := K[y_1, y_2]$ *e sejam* $f_1 := y_2D_1 + 1$, $f_2 := y_1D_2$ *e* $g := (y_1 + y_2)D_1D_2 + y_1y_2D_2$ *operadores diferenciais em* $A_2 = K[y_1, y_2][D_1, D_2]$ *(a segunda álgebra de Weyl). Então fazendo a divisão de* g *por* $\{f_1, f_2\}$ *obtemos:*

Passo 1

- $r := g$, $h_{f_1} := 0$, $h_{f_2} := 0$.
- $lc(r) = (y_1 + y_2)$ e $deg(r) = (1, 1)$
  $lc(f_1) = y_2$ e $deg(f_1) = (1, 0)$
  $lc(f_2) = y_1$ e $deg(f_2) = (0, 1)$.
- Assim,
$$lc(r) = c_{f_1} lc(f_1) + c_{f_2} lc(f_2)$$
ou seja,
$$y_1 + y_2 = c_{f_1} y_2 + c_{f_2} y_1$$
com, $c_{f_1} = 1$ e $c_{f_2} = 1$.

- $$\begin{aligned} r :=& (y_1+y_2)D_1D_2 + y_1y_2D_2 - 1D_2f_1 - 1D_1f_2 \\ =& (y_1+y_2)D_1D_2 + y_1y_2D_2 - D_2(y_2D_1) - D_2 - D_1(y_1D_2) \\ =& (y_1+y_2)D_1D_2 + y_1y_2D_2 - (y_2D_2+1)D_1 - D_2 - (y_1D_1+1)D_2 \\ =& (y_1y_1-2)D_2 - D_1. \end{aligned}$$

- $h_{f_1} := D_2$ e $h_{f_2} := D_1$.

Passo 2 $lc(r) = y_1y_2 - 2 \notin (y_1, y_2)$ e portanto o algoritmo termina.

Assim, $r = (y_1y_1 - 2)D_2 - D_1$, $h_{f_1} = D_2$ e $h_{f_2} = D_1$.

Observamos que, como no caso clássico (polinômios sobre um corpo), o resto da divisão não é único e pode depender até mesmo da ordem na lista dos divisores.

Definição 2.4. *Seja I um ideal à esquerda de A e seja G um subconjunto finito de $I\backslash\{0\}$. Dado $\alpha \in \mathbb{N}^n$, seja*

$$lc(\alpha, I) := {}_R(lc(f) : f \in I, deg(f) = \alpha).$$

Então G é uma base de Gröbner de I (com respeito a $\preceq$) se, e somente se, para todo $\alpha \in \mathbb{N}^n$ o ideal $lc(\alpha, I)$ é gerado por

$$\{lc(g) : g \in G, \alpha \in deg(g) + \mathbb{N}^n\}.$$

Proposição 2.5. *Se I é um ideal de A e G é uma base de Gröbner para I, então $(G) = I$.*

Demonstração:

Como $(G) \subset I$, devemos provar que $I \subset (G)$. Para isso vamos proceder por contradição, ou seja, suponhamos que $I\backslash(G)$ é não vazio. Como $\preceq$ é uma boa ordem temos que existe um $f \in I\backslash(G)$ tal que $lm(f)$ é minimal com respeito a $\preceq$. Como G é uma base de Gröbner para I, então $lc(f) \in {}_R(lc(g) : g \in G \text{ e } deg(f) \in deg(g) + \mathbb{N}^n)$. Assim, existe um $h \in (G)$ tal que $lm(h) = lm(f)$. Logo, $lm(h - f) \preceq lm(f)$ e pela minimalidade de $lm(f)$ temos que $h - f \in (G)$. Como $h \in (G)$ segue que $f = (f + h) - h \in (G)$ o que contradiz o fato que $f \in I\backslash(G)$. Portanto $(G) = I$.

❑

Exemplo 2.6. *Se R é um domínio e I é gerado por um operador diferencial f, então qualquer subconjunto finito de $I\backslash\{0\}$ que contém f é uma base de Gröbner de I. De fato, seja G subconjunto finito de $I\backslash\{0\}$ tal que, $f \in G$. Primeiro note que, dado qualquer $\alpha \in \mathbb{N}^n$ e dado $f' \in I$ com $deg(f') = \alpha$ temos que, $f' = hf$ para algum $h \in A$. Logo, $lc(f') = lc(h)lc(f)$ e assim, $lc(\alpha, I)$ é gerado por $\{lc(f)\}$. Portanto, $\{lc(g) : g \in G \text{ e } \alpha \in deg(g) + \mathbb{N}^n\}$ gera $lc(\alpha, I)$,o que implica que G é uma base de Gröbner para I.*

Como vimos no capítulo 1, se A é um anel comutativo, G é uma base de Gröbner de I se, e somente se, $Lt(G)$ gera em A o mesmo ideal que $Lt(I)$. Em geral isto não é verdade, como mostrará o exemplo a seguir.

Exemplo 2.7. *Seja $R \subseteq \mathbb{Q}(y_1, y_2)$ tal que y_1, y_2 não sejam invertíveis em R, por exemplo, $R = \mathbb{Q}[y_1, y_2]$ ou $R = \{\frac{f}{g} \in \mathbb{Q}[y_1, y_2], g(0,0) \neq 0\}$. Seja $\preceq$ um ordem monomial tal que $(1,0) \prec (0,1)$. Seja $F = \{y_1D_2, y_2D_1\}$ e $I = {}_A(y_1D_2, y_2D_1)$, note que F não é uma base de Gröbner para I, pois,*

$$(y_2D_1)(y_1D_2) - (y_1D_2)(y_2D_1) = y_2D_2 - y_1D_1 \in I$$

onde $deg(y_2D_2 - y_1D_1) = (0,1)$ e $lc(y_2D_2 - y_1D_1) = y_2$. Assim, $(y_2) \subseteq lc((0,1), I)$, o que implica que $lc((0,1), I)$ não é gerado por $y_1 = lc(y_1D_2)$.

Por enquanto não podemos dar exemplos interessantes de bases de Gröbner pois nos falta um algoritmo para calculá-las. Mas na próxima seção vamos apresentar uma generalização do algoritmo de Buchberger e assim poderemos calcular bases de Gröbner para qualquer conjunto finito de geradores de um ideal.

Proposição 2.8. *Seja I um ideal à esquerda em A. Seja G uma base de Gröbner de I e seja $f \in A$. Então $f \in I$ se, e somente se, o resto de f depois da divisão por G é zero.*

Demonstração:

($\Rightarrow$) Pelo teorema (2.2) tomando $F = G$ e $g = f$ temos que existem $r, h_g \in A$ tais que

$$f = \sum_{g \in G} h_g g + r.$$

Logo $r \in I$.

Se $r \neq 0$, como $G \subset I\backslash\{0\}$ é uma base de Gröbner temos que $lc(r) \in lc(\alpha, I)$ com $\alpha = deg(r)$. Mas $lc(\alpha, I)$ é gerado por $\{lc(g) : g \in G \text{ e } deg(r) \in deg(g) + \mathbb{N}^n\}$ o que contradiz o teorema (2.2) item (iii). Portanto $r = 0$.

($\Leftarrow$) Como o resto de f depois da divisão por G é zero temos que

$$f = \sum_{g \in G} h_g g.$$

Como $G \subset I\backslash\{0\}$ segue que $f \in I$.

❑

Como no caso clássico, obtemos a unicidade do resto depois da divisão por uma base de Gröbner.

2.2 Algoritmo de Buchberger

Definição 2.9. *Seja E um subconjunto finito de $A\backslash\{0\}$. Definimos*

$$m(E) := \Big(\max_{e \in E}(deg(e)_1), \max_{e \in E}(deg(e)_2), \ldots, \max_{e \in E}(deg(e)_n)\Big) \in \mathbb{N}^n,$$

onde, $deg(e)_i$ é a i-ésima coordenada do vetor grau de $e \in E$.

Note que o monômio $D^{m(E)}$ desempenha um papel semelhante, no caso comutativo, ao mínimo múltiplo comum dos monômios líderes de E.

Definição 2.10. *Seja R um domínio de ideais principais e sejam $f, g \in A\backslash\{0\}$. Tome $c, d \in R$ tais que*

$$c \cdot lc(f) = d \cdot lc(g) = mmc(lc(f), lc(g)).$$

Então

$$S(f,g) := cD^{m(\{f,g\})-deg(f)}f - dD^{m(\{f,g\})-deg(g)}g.$$

Teorema 2.11 (Critério de Buchberger)**.** *Seja G um subconjunto finito de $A\backslash\{0\}$ e seja I o ideal à esquerda gerado por G. Para qualquer subconjunto não vazio $E \subset G$, seja S_E um conjunto finito de geradores do R-módulo de syzygies*

$$\left\{(c_e)_{e\in E} : \sum_{e\in E} c_e lc(e) = 0\right\} \subseteq_R (R^{|E|}).$$

Então as seguintes afirmações são equivalentes:

(*i*) *G é uma base de Gröbner de I.*

(*ii*) *Para todo $E \subseteq G$ e para todo $(c_e)_{e\in E} \in S_E$ o resto de*

$$Spoly(E, (c_e)_{e\in E}) := \sum_{e\in E} c_e D^{m(E)-deg(e)}\, e \quad \textit{(o S-polinômio generalizado)}$$

depois da divisão por G é zero.

Mais ainda, se R é um domínio de ideais principais, então (i) e (ii) são equivalentes a:

(*iii*) *para todo $f, g \in G$ o resto de $S(f,g)$ depois da divisão por G é zero.*

Demonstração:

$(i) \Rightarrow (ii)$ Segue da Proposição 2.8

$(ii) \Rightarrow (i)$ Seja $h \in I$. Temos que mostrar que

$$lc(h) \in {}_R(lc(g) : g \in G, deg(h) \in deg(g) + \mathbb{N}^n).$$

Note que, como $h \in I$ então $lc(h) \in lc(\alpha, I)$ com $deg(h) = \alpha$. Definamos, para uma família $(f_g)_{g\in G}$ em A,

$$\delta((f_g)_{g\in G}) := \max_{\prec}\{deg(f_g g) : g \in G)\}.$$

Como $h \in I$, existe uma família $(h_g)_{g\in G}$ em A tal que $h = \sum_{g\in G} h_g g$. Podemos escolher $(h_g)_{g\in G}$ tal que $\delta := \delta((h_g)_{g\in G})$ seja minimal (i.e. se $(h'_g)_{g\in G}$ é tal que $h = \sum_{g\in G} h'_g g$, então $\delta((h'_g)_{g\in G}) \succeq \delta$). Seja $E := \{g \in G : deg(h_g g) = \delta\} \subset G$.

Caso 1: $deg(h) = \delta$.

Então

$$lm(h) = \sum_{g\in E} lm(h_g g) \quad \text{e} \quad lc(h) = \sum_{g\in E} lc(h_g)lc(g) \in {}_R(lc(g) : g \in E').$$

Note que pela observação (2) sobre A temos que $lc(h_g g) = lc(h_g)lc(g)$, para todo $g \in G$. Assim se $g \in E$, então $deg(h) = \delta = deg(h_g g) = deg(h_g) + deg(g)$. Logo, $deg(h) \in deg(g) + \mathbb{N}^n$. Portanto $lc(h) \in {}_R(lc(g) : g \in G, deg(h) \in deg(g) + \mathbb{N}^n)$ o que implica que G é uma base de Gröbner.

Caso 2: $deg(h) \prec \delta$.

Então $\sum_{g\in E} lc(h_g)lc(g) = 0$. Assim,

$$(lc(h_g))_{g\in E} \in S_E = \{(c_g)_{g\in E} : \sum_{g\in E} c_g lc(g) = 0\}.$$

Logo, existem $r_c \in R$ tais que $(lc(h_g))_{g\in E} = \sum_{c\in S_E} r_c c$, i.e.,

$$lc(h_g) = \sum_{c\in S_E} r_c c_g, \quad \text{para todo} \quad g \in E.$$

Agora,

$$h = \sum_{g\in G} h_g g = \sum_{g\in E} h_g g + \sum_{g\in G\setminus E} h_g g.$$

Se somamos e subtraímos $\sum_{g\in E}\sum_{c\in S_E} r_c c_g X^{deg(h_g)}g$, obtemos

$$h = \sum_{g\in E}(h_g - \sum_{c\in S_E} r_c c_g X^{deg(h_g)})g + \sum_{g\in E}\sum_{c\in S_E} r_c c_g X^{deg(h_g)}g + \sum_{g\in G\setminus E} h_g g.$$

Lembremos que, para todo $g \in E$ temos $deg(h_g) + deg(g) = deg(h_g g) = \delta$. Assim, existe um elemento $u \in \mathbb{N}^n$ tal que $\delta = m(E) + u$. Se sumamos e subtraímo de novo,

$$\sum_{g\in E}\sum_{c\in S_E} r_c c_g X^{deg(h_g)}g = \sum_{c\in S_E} r_c X^u (\underbrace{\sum_{g\in E} c_g X^{m(E)-deg(g)}g}_{\star})$$
$$+ \sum_{c\in S_E} r_c (\sum_{g\in E} c_g X^{deg(h_g)} - X^u c_g X^{m(E)-deg(g)}g).$$

Pelo algoritmo da divisão, dado $c \in S_E$, existe uma família $(h_g(c))_{g\in G}$ em A tal que

$$\star = \sum_{g\in E} c_g X^{m(E)-deg(g)}g = \sum_{g\in G} h_g(c)g$$

e $deg(h_g(c)g) \prec \delta - u$, pois como $\sum_{g\in E} c_g lc(g) = 0$, temos que $deg(\star) \prec m(E) - deg(g) + deg(g) = m(E)$ e $m(E) = \delta - u$, para todo $g \in G$. Portanto, pelo algoritmo de divisão de novo, existe uma família $(h''_g)_{g\in G}$ tal que $\delta((h''_g)_{g\in G}) \prec \delta$ e

$$\sum_{c\in S_E} r_c X^u (\sum_{g\in E} c_g X^{m(E)-deg(g)}g) = \sum_{g\in G} h''_g g.$$

Finalmente, se $g \in E$, definimos

$$h'_g := (h_g - \sum_{c\in S_E} r_c c_g X^{deg(h_g)}) + h''_g + \sum_{c\in S_E} r_c (c_g X^{deg(h_g)} - X^u c_g X^{m(E)-deg(g)}),$$

e se $g \in G\backslash E$, definimos $h'_g := h_g + h''_g$. Então

$$\begin{aligned}\sum_{g\in G} h'_g g =& \sum_{g\in E} h'_g g + \sum_{g\in G\backslash E} h'_g g \\ =& \sum_{g\in E}\left((h_g - \sum_{c\in S_E} r_c c_g X^{deg(h_g)}) + h''_g + \sum_{c\in S_E} r_c(c_g X^{deg(h_g)} - X^u c_g X^{m(E)-deg(g)})\right) g \\ &+ \sum_{g\in G\backslash E}(h_g + h''_g)g.\end{aligned}$$

Assim,

$$\begin{aligned}\sum_{g\in G} h'_g g =& \sum_{g\in E}(h_g - \sum_{c\in S_E} r_c c_g X^{deg(h_g)})g + \sum_{g\in E} h''_g g \\ &+ \sum_{g\in E}\sum_{c\in S_E} r_c(c_g X^{deg(h_g)} - X^u c_g X^{m(E)-deg(g)})g \\ &+ \sum_{g\in G\backslash E} h_g g + \sum_{g\in G\backslash E} h''_g g. \\ &\sum_{g\in E} h_g g - \sum_{g\in E}\sum_{c\in S_E} r_c c_g X^{deg(h_g)} g + \sum_{g\in E} h''_g g \\ &+ \sum_{g\in E}\sum_{c\in S_E} r_c c_g X^{deg(h_g)} g - \sum_{g\in E}\sum_{c\in S_E} r_c X^u c_g X^{m(E)-deg(g)} g \\ &+ \sum_{g\in G\backslash E} h_g g + \sum_{g\in G\backslash E} h''_g g \\ =& \sum_{g\in E} h_g g + \sum_{g\in E} h''_g g - \sum_{g\in E}\sum_{c\in S_E} r_c X^u c_g X^{m(E)-deg(g)} g \\ &+ \sum_{g\in G\backslash E} h_g g + \sum_{g\in G\backslash E} h''_g g \\ =& \sum_{g\in G} h_g g + \sum_{g\in G} h''_g g - \sum_{g\in G} h''_g g \\ =& \sum_{g\in G} h_g g \\ =& h.\end{aligned}$$

Ou seja, $h = \sum_{g\in G} h'_g g$ e $\delta(h'_g)_{g\in G} \prec \delta$, o que contradiz a minimalidade de δ.

Portanto o caso 2 não pode ocorrer.

$(ii) \Leftrightarrow (iii)$: Suponhamos que R é um domínio de ideais principais. Seja $E \subset G$ um conjunto finito e $f, g \in E$. Sejam $c, d \in R$ tais que c$lc(f)$ =d$lc(g) = mmc(lc(f), lc(g))$. Considere a $|E|$-tupla:

$$s^e_{f,g} := \begin{cases} -d & \text{se} \quad e = f \\ c & \text{se} \quad e = g \\ 0 & \text{se} \quad e \neq f,\ e \neq g. \end{cases}$$

Vamos assumir, sem demonstração, o fato que, como R é um domínio de ideais principais, o módulo de syzygies é gerado por essas relações, isto é, $S_E = {}_R(\{(s^e_{f,g})_{e\in E} | f, g \in E\})$. Agora basta observar que, para cada um desses geradores,

$$Spoly(\{f, g\}, (c_e)_{e\in\{f,g\}}) = S(f, g).$$

❑

Como mostramos a seguir, o teorema (2.11) anterior nos fornece um algoritmo para calcular bases de Gröbner de modo análogo ao caso do anel de polinômios comutativos com coeficientes em um corpo.

Proposição 2.12 (Algoritmo de Buchberger)**.** *Seja I um ideal à esquerda em A. Dado um conjunto finito F de geradores de I, podemos calcular, em um número finito de passos, uma base de Gröbner para I.*

Demonstração:

Para demostrar o teorema, vamos mostrar que o algoritmo a seguir termina em um número finito de passos e de fato calcula uma base de Gröbner para I.

Algoritmo 4.

Entrada: *F um conjunto finito de geradores de I.*

Saída: *Uma base de Gröbner G de I.*

Inicialização: *G:=F.*

Enquanto *exista* $E \subset F$, $E \neq \emptyset$ ***faça***.

Tome uma família $(c_e) \in S_E$.

Considere o resto r *de*

$$Spoly(E, (c_e)_{e\in E}) = \sum_{e\in E} c_g D^{m(E)-deg(e)} e$$

depois da divisão por G.

Se $r \neq 0$ ***então***

$$G := G \cup \{r\}.$$

Agora mostraremos que o algoritmo termina e calcula uma base de Gröbner para I.

Note que, para cada $E \subset G$ o algoritmo produz um novo conjunto de geradores de I sempre que o resto depois da divisão de $Spoly(E, (c_e)_{e\in E})$ por G seja não nulo. Assim, suponhamos que $G_0 = G$ e que G_j é o conjunto de geradores resultante ao final do j-ésimo passo. Então, $G_{j+1} = G_j \cup \{r_{j+1}\}$; onde r_{j+1} é o resto da divisão de algum $Spoly(E, (c_e)_{e\in E})$ por G_j. Logo, temos

$$G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_j \subseteq \cdots$$

o que produz, para cada $\alpha \in \mathbb{N}^n$, uma cadeia ascendente de ideais

$$lc(\alpha, (G_0)) \subseteq lc(\alpha, G_1) \subseteq \cdots \subseteq lc(\alpha, G_j) \subseteq \cdots$$

Como R é um anel noetheriano temos que essa cadeia é estacionária. Portanto, para cada $\alpha \in \mathbb{N}^n$, existe um $k_\alpha \in \mathbb{N}$ tal que $lc(\alpha, G_{k_\alpha}) = lc(\alpha, G_t)$ para todo $t \geq k_\alpha$. Logo $lc(r_t) \in lc(\alpha, G_{k_\alpha})$ e pelo teorema (2.2), $r_t = 0$ para todo $t \geq k_\alpha$. Assim encontramos um k_α tal que o resto de $Spoly(E, (c_e)_{e\in E})$ é zero. Agora o algoritmo termina quando percorremos todos os $E \subseteq F$.

O fato que o algoritmo calcula uma base de Gröbner segue do Teorema (2.11).

❑

2.3 Calculando Bases de Gröbner

Nesta seção vamos apresentar alguns exemplos de como calcular bases de Gröbner usando o algoritmo (4).

Exemplo 2.13. *Seja* $R = \left\{ \frac{f}{g} \in K[y] | f, g \in K[y], g(0) \neq 0 \right\}$. *Observe que* R *é um domínio de ideais principais, pois é uma localização de um domínio de ideais principais. Além disso vamos assumir que podemos resolver equações lineares sobre* R. *Seja* I *o ideal à esquerda gerado por* $f_1 := 2yD^2$ *e* $f_2 := D^3 + y^2D - y$. *Então*

$$\frac{S(f_1, f_2)}{2} = \frac{1}{2}Df_1 - yf_2 = D^2 - y^3D + y^2 =: f_3.$$

Note que não podemos reduzir f_3 *módulo* $\{f_1, f_2\}$, *mas como*

$$f_2 = (D - y^3)f_3 + y^2(y^4 + 3)D - y(y^4 + 3)$$

e como $y^4 + 3$ *é inversível em* R *podemos substituir* f_2 *por* $y^2D - y$. *Agora,* $G = \{f_1, f_2 = y^2D - y, f_3\}$.

Agora $f_3 = -yf_2 + D^2$ *e assim substituímos* f_3 *por* D^2 *e eliminamos* f_1 *(*$f_1 = 2yf_3$*). Logo,*

$$S(f_2, f_3) = Df_2 - y^2f_3 = y^2D^2 + 2yD - 1 - y^2D^2 = yD - 1 =: f_4$$

então podemos eliminar f_2 *(*$f_2 = yf_4$*). Como* $S(f_3, f_4) = 0$, $\{f_3, f_4\} = \{D^2, yD - 1\}$ *é uma base de Gröbner de* (f_1, f_2).

Exemplo 2.14. *Seja* $R = K(y)$ *e seja* $I := (f_1, f_2)$, *onde,* $f_1 := yD^2 + yD + 1$ *e* $f_2 = D^3 + y^2D^2 + D$.

$$S(f_1, f_2) = Df_1 - yf_2 = (1 + y - y^3)D^2 + (2 - y)D =: f_3$$

$$S(f_1, f_3) = (1 + y - y^3)f_1 - yf_3 = (-y + 2y^2 - y^4)D + (1 + y - y^3) =: f_4$$

$$S(f_1, f_4) = (-y^4 + 5y^3 + 2y^2 - 6y)D + (-y^3 + 3y^2 + 2y - 2) =: f_5$$

$$S(f_4, f_5) = -2y^6 + y^5 + y^4 + 6y^3 + 2y^2 - 8y =: f_6,$$

o qual é invertível em R. Assim, $\{1\}$ *é uma base de Gröbner de* (f_1, f_2).

Exemplo 2.15. *Seja* $R \subseteq \mathbb{Q}(y_1, y_2)$ *tal que* y_1, y_2 *não sejam invertíveis em R, por exemplo,* $R = \mathbb{Q}[y_1, y_2]$, $I = {}_A(y_1D_2, y_2D_1)$ *e* $A = R[D_1, D_2]$. *Sejam* $f_1 := y_1D_2$ *e* $f_2 := y_2D_1$, *então* $I = {}_A(f_1, f_2)$. *Seja* $\preceq$ *a ordem lexicográfica graduada com* $(0,1) \succ (1,0)$. *Seja* $G = \{f_1, f_2\}$, *note que* $deg(f_1) = (0,1)$, $lc(f_1) = y_1$, $deg(f_2) = (1,0)$ *e* $lc(f_2) = y_2$

- $E = \{f_1, f_2\} = G$. *Temos que,* $m(E) = (1,1)$, $S_E = \{(y_2, -y_1)\}$

$$\begin{aligned} Spoly(E, (y_2, -y_1)) =& y_2D_1f_1 - y_1D_2f_2 \\ =& y_2(y_1D_2D_1 + D_2) - y_1(y_2D_2D_1 + D_1) \\ =& y_2D_2 - y_1D_1 =: f_3. \end{aligned}$$

  Temos que $deg(f_3) = (0,1)$ *e* $lc(f_3) = y_2$. *Como* $lc(f_3) \notin lc((0,1), I) = (y_1)$ *então* $f_3 \xrightarrow{G}_+ f_3$. *Assim,* $G := G \cup \{f_3\} = \{f_1, f_2, f_3\} = \{y_1D_2, y_2D_1, y_2D_2 - y_1D_1\}$.

- $E = \{f_1, f_3\}$. *Temos que,* $m(E) = (0,1)$, $S_E = \{(y_2, -y_1)\}$

$$\begin{aligned} Spoly(E, (y_2, -y_1)) =& y_2f_1 - y_1f_3 \\ =& y_2y_1D_2 - y_1(y_2D_2 - y_1D_1) \\ =& y_1^2D_1 =: f_4. \end{aligned}$$

  Temos que $deg(f_4) = (1,0)$ *e* $lc(f_4) = y_1^2$. *Como* $lc(f_4) \notin lc((1,0), I) = (y_2)$ *então* $f_4 \xrightarrow{G}_+ f_4$. *Assim,* $G := G \cup \{f_4\} = \{f_1, f_2, f_3, f_4\} = \{y_1D_2, y_2D_1, y_2D_2 - y_1D_1, y_1^2D_1\}$.

- $E = \{f_2, f_3\}$. *Temos que,* $m(E) = (1,1)$, $S_E = \{(1, -1)\}$

$$\begin{aligned} Spoly(E, (1, -1)) =& D_2f_2 - D_1f_3 \\ =& D_2(y_2D_1) - D_1(y_2D_2 - y_1D_1) \\ =& y_1D_1^2 + 2D_1 =: f_5. \end{aligned}$$

Temos que $deg(f_5) = (2,0)$ *e* $lc(f_5) = y_1$. *Como* $lc(f_5) \notin lc((2,0), I) = (y_2.y_1^2)$ *então* $f_5 \xrightarrow{G}_+ f_5$. *Assim,* $G := G \cup \{f_5\} = \{f_1, f_2, f_3, f_4, f_5\} = \{y_1D_2, y_2D_1, y_2D_2 - y_1D_1, y_1^2D_1, y_1D_1^2 + 2D_1\}$.

- $E = \{f_1, f_2, f_3\}$. *Temos que,* $m(E) = (1,1)$, $S_E = \{(y_2, -y_1, 0), (0,1,-1)\}$

$$Spoly(E, (y_2, -y_1, 0)) = y_2D_1f_1 - y_1D_2f_2 =: f_6.$$

Note que, $f_6 = f_3$ *portanto* $f_6 \xrightarrow{G}_+ 0$.

$$Spoly(E, (0,1,-1)) = D_2f_2 - D_1f_3 =: f_7.$$

Note que, $f_7 = f_5$ *portanto* $f_7 \xrightarrow{G}_+ 0$.

- $E = \{f_1, f_4\}$. *Temos que,* $m(E) = (1,1)$, $S_E = \{(y_1, -1)\}$

$$Spoly(E, (y_1, -1)) = y_1D_1f_1 - D_2f_4 =: f_8.$$

Note que, $f_8 = f_1$ *portanto* $f_8 \xrightarrow{G}_+ 0$.

- $E = \{f_2, f_4\}$. *Temos que,* $m(E) = (1,0)$, $S_E = \{(y_1^2, -y_2)\}$

$$\begin{aligned} Spoly(E, (y_1^2, -y_2)) &= y_1^2f_2 - y_2f_4 \\ &= 0. \end{aligned}$$

- $E = \{f_3, f_4\}$. *Temos que,* $m(E) = (1,1)$, $S_E = \{(y_1^2, -y_2)\}$

$$Spoly(E, (y_1^2, -y_2)) = y_1^2D_1f_3 - -y_2D_2f_4 =: f_9.$$

Note que, $f_9 = -x_1f_5 - 2f_4$ *portanto* $f_9 \xrightarrow{G}_+ 0$.

Repetindo o processo até esgotar todos os subconjuntos finitos E de G, obtemos que $G = \{f_1, f_2, f_3, f_4, f_5\}$ *é uma base de Gröbner de* (f_1, f_2).

Referências Bibliográficas

[1] W. W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*, volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, 1994.

[2] J. Björk. *Rings of Diferential Operators*, volume 21. North Holland Publishing Company Amsterdam, New York, Oxford, 1979.

[3] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, Innsbruck-Austria, 1965.

[4] B. Buchberger. Ein algorithmiches Kriterium für die Löbsbarkeit eines algebraischen Gleichungssystems. *Aequation Math*, 4:374–383, 1970.

[5] B. Buchberger. A critical pair/completion algorithm for finitely generated ideals in rings. In E. Börger, editor, *Logic and Machines: Decision Problems and Complexity*, volume 171 of *Lecture Note in Computer Science*, pages 137–155. Springer, 1984.

[6] F. Castro. Calculs effectifs pour les ideaux d'opérateurs differentiels. In J. Aroca, editor, *Géometrie Algébrique et Applications*, volume III, pages 1–20. Hermmam, Paris, 1987.

[7] S. Coutinho. *Polinômios e Computação Algébrica*. Coleção Matemática e Aplicações. Instituto Nacional de Matemática Pura e Aplicada - IMPA, 2012.

[8] F. Galligo. Some algorithmic questions on ideals of diferential operators. *Springer Notes in Computer Science*, 204:413–421, 1985.

[9] M. Insa and F. Pauer. Gröbner bases in rings of differential operators. In B. Buchberger and F. winkler, editors, *Gröbner Bases and Applications*, volume 251 of *London Math. Soc. Lecture Note*, pages 367–380. Cambridge Univ. Press, 1998.

[10] A. Kandri-Rody and D. Kapur. Computing a Gröbner bases of a polynomial ideal over a Euclideam domain. *Journal of Symbolic Computation*, 26:37–58, 1988.

[11] H. Möller. On the constrution of Gröbner bases using syzygies. *Journal of Symbolic Computation*, 6:345–359, 1988.

[12] L. Pan. On the D-bases of polynomials ideal over principal ideal domains. *Journal of Simbolic Computation*, 7:55–69, 1988.

[13] F. Pauer. On lucky ideals for Gröbner bases computation. *Journal of Simbolic Computation*, 14:471–482, 1992.

[14] F. Pauer. Gröbner bases with coeficients in rings. *Journal of Symbolic Computation*, 42:1003–1011, 2007.

[15] F. Pauer and M. Pfeifhofer. The theory of Gröbner bases. *L'Enseignement Mathematique*, 34:215–232, 1988.

[16] W. Trinks. Über B. Buchberger verfahren systeme algebraischer Gleichugen zu lösen. *Journal of Number Theory*, 10:475–488, 1992.

Índice Remissivo