Universidade Federal de Uberlândia
Faculdade de Matemática

Pedro Augusto Diniz Santos

Introdução as Bases de Gröbner

Uberlândia - MG

2020

Pedro Augusto Diniz Santos

Introdução as Bases de Gröbner

Monografia apresentada a Faculdade de Matemática, UFU, como requisito parcial para obtenção do título de Bacharel em Matemática, sob a orientação da Prof. Dr. Cicero Fernandes de Carvalho.

Uberlândia - MG

2020

Pedro Augusto Diniz Santos

Introdução as Bases de Gröbner

Monografia apresentada a Faculdade de Matemática, UFU, como requisito parcial para obtenção do título de Bacharel em Matemática, sob a orientação da Prof. Dr. Cicero Fernandes de Carvalho.

BANCA EXAMINADORA

_____

(Orientador)

_____

_____

Agradecimentos

Agradeço primeiramente ao meu pai José Francisco, a minha mãe Rosângela e a minha irmã Eduarda, pelo apoio incondicional durante toda a minha graduação, seja ele financeiro ou emocional.

Agradeço também à Universidade Federal de Uberlândia pela minha formação acadêmica de qualidade. Juntamente com os professores que me mostraram o quão bela a é matemática.

Agradeço muito ao meu orientador Cicero Fernandes de Carvalho, pela oportunidade e por entender minhas limitações. Por sempre me incentivar a buscar o meu melhor, por ser compreensivo quando tive que adiar as reuniões. Fica aqui o meu muito obrigado!

Eu não poderia deixar de agradecer aos meus amigos não posso falar todos, mas em especial ao Márcio Willian dos Reis Filho, Maryanny Martins de Rezende Oliveira, Matheus Deodato Arruda, Paulo César Andreucci, Paulo Vitor Bonifácio Moraes e Tiago Marques Luiz, por estarem ao lado meu todos os dias rindo comigo e me ajudarem nos momentos difíceis que passamos juntos.

Por fim, mas não menos importante quero agradecer à minha namorada Vitória Alves Martins, que surgiu em um momento muito conturbado e me ajudou a dar volta por cima. Muito obrigado meu amor, amo você!

Resumo

Neste trabalho, temos como enfoque o estudo das bases de Gröbner e algumas de suas propriedades. Primeiramente definindo o que é uma ordem monomial, logo em seguida apresentando um algoritmo da divisão para polinômios em várias variáveis com coeficientes sobre um corpo $\mathbb{K}$ buscando manter algumas propriedades do algoritmo da divisão de polinômios em uma variável. Depois estudamos ideais monomiais e uma demonstração do Teorema da Base de Hilbert, para que por fim, se definisse as bases de Gröbner. Ao fim deste trabalho, estudamos o algoritmo de Buchberger, que nos fornece um método efetivo para calcular as bases de Gröbner e algumas melhorias no algoritmo de Buchberger.

Palavras-Chave: Ordem Monomial, Algoritmo da Divisão para Polinômios em Varias Variáveis, Ideais Monomiais,Teorema da Base de Hilbert, Bases de Gröbner, Algoritmo de Buchberger, Melhorias no Algoritmo de Buchberger.

Abstract

In this work, we focus on the study of Gröbner's bases and some of their properties. Firstly defining what a monomial order is, then immediately presenting a division algorithm for polynomials in several variables with coefficients on a $\mathbb{K}$ body trying to maintain some properties of the polynomial division algorithm in a variable. Then we studied monomial ideals and a demonstration of Hilbert's Base Theorem, so that finally, Gröbner's bases could be defined. At the end of this work, we study the Buchberger algorithm, which provides us with an effective method to calculate Gröbner bases and some improvements in this algorithm.

Key-Words: Monomial Order, Division Algorithm for Polynomials in Several Variables, Monomial Ideals, Hilbert's Base Theorem, Gröbner's Bases, Buchberger's Algorithm, Buchberger's Algorithm Improvements.

Sumário

1 Introdução

O conceito de bases de Gröbner surgiu no ano de 1965 na tese de doutorado de Bruno Buchberger, ali chamado de bases padrão. Anos depois Buchberger as renomeia como bases de Gröbner em homenagem ao seu orientador Wolfgang Gröbner.

Inicialmente este resultado não teve grande impacto, somente nos anos 80 pesquisadores começaram uma investigação mais profunda nesta nova teoria, vendo sua aplicabilidade em diversas áreas tais como a Geometria Algébrica, Sistemas computacionais e na Álgebra Comutativa, e também generalizaram alguns resultados.

Neste trabalho, vamos estudar o conceito de ordem monomial e o processo de divisão polinomial em várias variáveis, que são essenciais para a definição e cálculo das bases de Gröbner, que também estudaremos.

Seja $\mathbb{K}$ um corpo, denotaremos por $\mathbb{K}[X]$ o anel de polinômios $\mathbb{K}[X_1, \ldots, X_n]$. O produto $X_1^{\alpha_1} \ldots X_n^{\alpha_n}$ é chamado de monômio, que também poderá ser denotado por X^α. Chamaremos de $\mathcal{M}$ o conjunto dos monômios de $\mathbb{K}[X]$. Seja $f \in \mathbb{K}[X]$, diremos que um monômio X^β aparece em f se o coeficiente de X^β em f é não nulo. Chamamos de termo o produto $aX_1^{\alpha_1} \ldots X_n^{\alpha_n}$, onde $a \in \mathbb{K}$ e $X_1^{\alpha_1} \ldots X_n^{\alpha_n} \in \mathcal{M}$.

Vamos estudar também o algoritmo de Buchberger para o cálculo de tais bases. Este algoritmo é usado em vários sistemas de álgebra computacional para estudar ideais polinomiais específicos. Neste trabalho, vamos nos concentrar em resolver dois problemas:

1. Todo ideal $I \subset \mathbb{K}[X]$ tem um conjunto gerador finito? Ou seja, podemos escrever $I = \langle f_1, \ldots, f_s \rangle$ com $f_i \in \mathbb{K}[X]$, para todo $i = 1, \ldots, s$?

2. Dado $f \in \mathbb{K}[X]$ um ideal $I = \langle f_1, \ldots, f_s \rangle$, como determinar se $f \in I$?

Finalizamos o trabalho apresentando algumas melhorias no algoritmo de Buchberger.

2 Ordenando monômios em várias variáveis

Nesta seção vamos definir o que é uma ordem monomial sobre o conjunto $\mathcal{M}$. A ordem monomial tem uma grande importância na construção do algoritmo da divisão de polinômios de várias variáveis.

Definição 2.1. *Seja $\mathbb{K}$ um corpo, uma ordem monomial é uma relação $>$ sobre o conjunto $\mathcal{M}$ de monômios de $\mathbb{K}[X_1 \dots X_n]$ satisfazendo:*

- *$>$ é uma ordem total sobre $\mathcal{M}$.*
- *Se $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3 \in \mathcal{M}$ e $\mathcal{M}_1 > \mathcal{M}_2$, então $\mathcal{M}_1\mathcal{M}_3 > \mathcal{M}_2\mathcal{M}_3$*
- *$>$ é uma boa ordem sobre $\mathcal{M}$ (ou seja, todo subconjunto não vazio de $\mathcal{M}$ tem um menor elemento).*

O lema a seguir nos ajudará entender o que significa o terceiro item da definição.

Lema 2.2. *Uma relação de ordem $>$ sobre $\mathcal{M}$ é uma boa ordenação se, e somente se, toda sequência estritamente decrescente em $\mathcal{M}$,*

$$\mathcal{M}_1 > \mathcal{M}_2 > \mathcal{M}_3 > \dots$$

eventualmente termina.

Demonstração. Provemos pela contrapositiva,
($\Rightarrow$) Dada uma sequência estritamente decrescente como no enunciado então $\{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3, \dots\}$ é um subconjunto não vazio de $\mathcal{M}$ com nenhum elemento mínimo, logo $>$ não é uma boa ordem.
($\Leftarrow$) Se $>$ não é uma boa ordem, então algum conjunto não vazio $\mathcal{S} \subset \mathcal{M}$ não tem um menor elemento. Seja $\mathcal{M}_i \in \mathcal{S}$, como $\mathcal{M}_i$ não é o elemento mínimo existe $\mathcal{M}_{i+1}$ tal que $\mathcal{M}_i > \mathcal{M}_{i+1}$ em $\mathcal{S}$. Continuando o raciocínio obteremos uma sequência estritamente decrescente que não termina. Assim concluímos a prova. □

Definição 2.3. *(Ordem Lexicográfica) Dados dois monômios $\prod_{i=1}^n X_i^{\alpha_i}$ e $\prod_{i=1}^n X_i^{\beta_i}$ dizemos que*

$$\prod_{i=1}^n X_i^{\alpha_i} >_{lex} \prod_{i=1}^n X_i^{\beta_i}$$

se existe $i \in 1, \ldots, n$ *tal que* $\alpha_i > \beta_i$ *e* $\alpha_j = \beta_j$*, para todo* $j < i$*.*

Proposição 2.4. *A Ordem Lexicográfica sobre* $\mathcal{M}$ *é uma ordem monomial.*

Demonstração. Mostraremos que a Ordem Lexicográfica satisfaz as condições de ordem monomial.

- Que $>_{lex}$ é uma ordem total segue diretamente da definição, pois dados dois monômios é sempre possível comparar os expoentes deles.

- Seja $\prod_{i=1}^{n} X_i^{\alpha_i}$,$\prod_{i=1}^{n} X_i^{\beta_i}$ e$\prod_{i=1}^{n} X_i^{\gamma_i}$, com $\prod_{i=1}^{n} X_i^{\alpha_i} >_{lex} \prod_{i=1}^{n} X_i^{\beta_i}$. Vamos comparar $\prod_{i=1}^{n} X_i^{\alpha_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i}$ com $\prod_{i=1}^{n} X_i^{\beta_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i}$.
  Observe que $\prod_{i=1}^{n} X_i^{\alpha_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i} = \prod_{i=1}^{n} X_i^{\alpha_i+\gamma_i}$ e $\prod_{i=1}^{n} X_i^{\beta_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i} = \prod_{i=1}^{n} X_i^{\beta_i+\gamma_i}$.
  Agora, por hipótese $\prod_{i=1}^{n} X_i^{\alpha_i} >_{lex} \prod_{i=1}^{n} X_i^{\beta_i}$, ou seja $\alpha_l > \beta_l$ e $\alpha_j = \beta_j$ para todo $j < l$. Assim temos que $\alpha_l + \gamma_l > \beta_l + \gamma_l$ e $\alpha_j + \gamma_j = \beta_j + \gamma_j$ para todo $j < l$. Portanto $\prod_{i=1}^{n} X_i^{\alpha_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i} >_{lex} \prod_{i=1}^{n} X_i^{\beta_i} \cdot \prod_{i=1}^{n} X_i^{\gamma_i}$, como queríamos mostrar.

- Por fim, mostraremos que a ordem Lexicográfica é uma boa ordem, ou seja, todo subconjunto de $\mathcal{M}$ possui um menor elemento. Seja $S \subset \mathcal{M}$ um subconjunto não vazio de monômios, então existe $\prod_{i=1}^{n} X_i^{\beta} \in S$. Olhando para X_1, existe $X_1^{\alpha_1}$ tal que $X_1^{\alpha_1} \prod_{i=2}^{n} X_i^{\alpha_i} \in \mathcal{S}$ $X_1^{\alpha_1} \prod_{i=2}^{n} X_i^{\alpha_i} < X_1^{\beta_1} \prod_{i=2}^{n} X_i^{\beta_i}$ para todo $X_1^{\beta_1} \prod_{i=2}^{n} X_i^{\beta_i} \in \mathcal{S}$. Se o monômio $X_1^{\alpha_1} \prod_{i=2}^{n} X_i^{\alpha_i}$ seja o único que possui um termo $X_1^{\alpha_1}$, ele será o menor termo. Caso contrario, vamos repetir o mesmo processo para X_2. Logo, existe $X_1^{\alpha_1} X_2^{\alpha_2} \prod_{i=3} X_{i=3}^{n} X_i^{\alpha_i} \in \mathcal{S}$, tal que $X_1^{\alpha_1} X_2^{\alpha_2} \prod_{i=3}^{n} X_i^{\alpha_i} < X_1^{\beta_1} X_2^{\beta_2} \prod_{i=2}^{n} X_i^{\beta_i}$ para todo $X_1^{\beta_1} X_2^{\beta_2} \prod_{i=2}^{n} X_i^{\beta_i}$ Se $X_1^{\alpha_1} X_2^{\alpha_2} \prod_{i=3}^{n} X_i^{\alpha_i}$ for único, ele será o menor elemento. Caso contrário, repetiremos o processo para $X_3, X_4, \ldots, X_n$.E pela finitude das variáveis o resultado segue.
  Portanto, a ordem Lexicográfica como definimos é uma ordem monomial.

□

Definição 2.5. *Ordem Lexicográfica Graduada. Sejam* $\prod_{i=1}^{n} X_i^{\alpha_i}$ *e* $\prod_{i=1}^{n} X_i^{\beta_i} \in \mathcal{M}$*. Dizemos que* $\prod_{i=1}^{n} X_i^{\alpha_i} >_{grlex} \prod_{i=1}^{n} X_i^{\beta_i}$*, se*

$$|\alpha| := \textstyle\sum_{i=1}^{n} \alpha_i > |\beta| := \sum_{i=1}^{n} \beta_i, \text{ ou}$$
$$|\alpha| = |\beta| \text{ e } \textstyle\prod_{i=1}^{n} X_i^{\alpha_i} >_{lex} \prod_{i=1}^{n} X_i^{\beta_i}.$$

Definição 2.6. *Ordem Lexicográfica Graduada Reversa. Sejam* $\prod_{i=1}^{n} X_i^{\alpha_i}$ *e* $\prod_{i=1}^{n} X_i^{\beta_i} \in \mathcal{M}$.

Dizemos que $\prod_{i=1}^{n} X_i^{\alpha_i} >_{grevlex} \prod_{i=1}^{n} X_i^{\beta_i}$, *se*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ ou}$$
$$|\alpha| = |\beta| \text{ e existe } i \in 1, \ldots, n \text{ tal que } \alpha_i < \beta_i \text{ e } \alpha_j = \beta_j \text{ para todo } j > i.$$

Observação 2.7. *As Ordens Lexicográfica Graduada e Lexicográfica Graduada Reversa, são ordens monomiais e a demonstração de ambos os caso são análogas a demonstração da ordem Lexicográfica ser uma ordem monomial.*

A seguir faremos um exemplo para entender melhor como ordenaremos monômios.

Exemplo 2.8. *Considere os seguintes monômios* X^5YZ *e* X^4YZ^2. *Vamos ordenar estes monômios de acordo com as ordens que definimos anteriormente.*
Note que $X^5YZ >_{grlex} X^4YZ^2$, *pois ambos os monômios tem grau total 7 e* $X^5YZ >_{lex} X^4YZ^2$. *Neste caso, também temos que* $X^5YZ >_{grevlex} X^4YZ^2$, *pois o expoente da variável* Z *em* X^5YZ *é menor que o expoente da variável* Z *em* X^4YZ^2.

Definição 2.9. *Sejam* $f = \sum_{\alpha} a_\alpha X^\alpha$ *um polinômio não nulo em* $\mathbb{K}[X]$ *e* $>$ *uma ordem monomial.*

- *O monômio líder de* f *será denotado por* $LM(f) = X^\alpha$, *onde* $X^\alpha > X^\beta$ *com* X^α, X^β *que aparecem em* f.
- *O coeficiente líder de* f *será denotado por* $LC(f) = a_\alpha \in \mathbb{K}$.
- *O termo líder de* f *será denotado por* $LT(f) = LC(f) \cdot LM(f)$.

Definição 2.10. *Seja* $>$ *uma ordem monomial em* $\mathcal{M}$ *e sejam* α *e* β *duas n-uplas cujas entradas são inteiros não negativos. Escrevemos* $\alpha > \beta$ *se* $X^\alpha > X^\beta$.

Exemplo 2.11. *Seja* $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^3Z^2$ *e considere a ordem lexicográfica. Assim:*

$$LC(f) = 7,$$
$$LM(f) = X^3Z^2,$$
$$LT(f) = 7X^3Z^2.$$

Lema 2.12. *Sejam $f, g \in \mathbb{K}[X]$ polinômios não nulos e $>$ uma ordem monomial sobre $\mathcal{M}$. Então:*

1. $LM(f \cdot g) = LM(f) \cdot LM(g)$

2. *Se $f + g \neq 0$, então $LM(f + g) \leq \max(LM(f), LM(g))$. Se, além disso, $LM(f) \neq LM(g)$, então a igualdade ocorre.*

Demonstração. 1. Sejam $f = a_{\alpha_1} X^{\alpha_1} + \cdots + a_n X^{\alpha_n}$ e $g = b_{\beta_1} X^{\beta_1} + \cdots + b_m X^{\beta_m}$, com $LM(f) = X^{\alpha_1}$ e $LM(g) = X^{\beta_1}$. Logo $f \cdot g = a_{\alpha_1} b_{\beta_1} X^{\alpha_1+\beta_1} + \cdots + a_{\alpha_n} b_{\beta_m} X^{\alpha_n+\beta_m}$. Note que $X^{\alpha_1} > X^{\alpha_i}$ para todo $i = 2, \ldots, n$ e $X^{\beta_1} > X^{\beta_j}$ para todo $j = 2, \ldots, m$, então o produto $X^{\alpha_1+\beta_1} > X^{\alpha_i+\beta_j}$ para todo $(i, j) \neq (1, 1)$, $(i, 1)$ com $i = 2, \ldots, n$ e $(1, j)$ com $j = 2, \ldots, m$.
Assim, $LM(f \cdot g) = X^{\alpha_1+\beta_1} = X^{\alpha_1} \cdot X^{\beta_1} = LM(f) \cdot LM(g)$.

2. Se $f+g \neq 0$ dado um monômio M de $f+g$ pela definição de soma de polinômios temos que esse monômio deve aparecer em f ou g, logo $M \leq LM(f)$ ou $M \leq LM(g)$ e portanto $M \leq \max(LM(f), LM(g))$, em particular $LM(f+g) \leq \max(LM(f), LM(g))$. Se $LM(f) \neq LM(g)$ então novamente da definição de soma de polinômios temos $LM(f + g) = \max(LM(f), LM(g))$.

□

3 O Algoritmo da divisão em várias variáveis

Nesta seção vamos descrever um algoritmo da divisão em $\mathbb{K}[X]$ que é de grande importância para a construção das bases de Gröbner.

Theorem 3.1 (Algoritmo da divisão em várias variáveis)**.** *Fixe uma ordem monomial $>$ em $\mathbb{K}[X]$, e seja $F = (f_1, \ldots, f_s)$ uma s-upla ordenada de polinômios em $\mathbb{K}[X]$. Então todo $f \in \mathbb{K}[X]$ pode ser escrito como:*

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

onde $a_1, \ldots, a_s, r \in \mathbb{K}[X]$, e ainda ou $r = 0$ ou r é uma combinação linear, com coeficientes em $\mathbb{K}$, de monômios, nos quais nenhum é divisível por qualquer $LT(f_1), \ldots, LT(f_s)$. Chamamos r de resto da divisão de f por F. Além disso se $a_i f_i \neq 0$ então

$$LT(f) \geq LT(a_i f_i).$$

Demonstração. Nós provaremos a existência de $a_1, \ldots, a_s$ e r construindo um algoritmo e mostrando que o mesmo funciona corretamente para todos os polinômios em $\mathbb{K}[X]$. Abaixo segue o algoritmo.

ENTRADA: $f_1, \ldots, f_s, f$

SAÍDA: $a_1, \ldots, a_s, r$

$a_1 := 0; \ldots; a_s := 0; r = 0$

$p := f$ ENQUANTO $p \neq 0$ FAÇA

$i := 1$

ocorredivisao:=falso

ENQUANTO $i \leq s$ E ocorredivisao=falso FAÇA

SE $LT(f_i)$ divide $LT(p)$ ENTÃO

$a_i := a_i + \frac{LT(p)}{LT(f_i)}$.

$p := p - \frac{LT(p)}{LT(f_i)} \cdot f_i$

ocorredivisao=verdade

OUTRO

$i := i + 1$

SE ocorredivisao=falso ENTÃO

$r := r + LT(p)$

$p := p - LT(p)$

Observe que a variável p representa um dividendo intermediário em cada estágio, a variável r representa o resto e $a_1, \ldots, a_s$ são os quocientes listados acima do radical.

Por fim, a variável booleana (que assume os valores de verdadeiro ou falso nesse algoritmo) ocorredivisao nos diz quando algum $LT(f_i)$ divide o termo líder do dividendo intermediário. Neste algoritmo temos que verificar duas coisas

1. (Etapa de Divisão) Se algum $LT(f_i)$ divide $LT(p)$, o algoritmo prossegue como no caso de uma variável.

2. (Etapa de Resto) Se nenhum $LT(f_i)$ dividir $LT(p)$, o algoritmo adiciona $LT(p)$ ao resto.

Para mostrar que o algoritmo funciona, primeiro mostraremos que pode ser escrito da seguinte forma

$$f = \sum_{i=1}^{s} a_i f_i + p + r \tag{1}$$

em todas as etapas do algoritmo. Isso é verdade para os valores iniciais de $a_1, \ldots, a_s, p$ e r.

Suponha que (1) seja válido em uma etapa do algoritmo. Se o próximo passo for uma Etapa de Divisão, então alguns $LT(f_i)$ dividem $LT(p)$ e a igualdade

$$a_i f_i + p = \left(a_i + \frac{LT(p)}{LT(f_i)}\right) \cdot f_i + \left(p - \left(\frac{LT(p)}{LT(f_i)}\right) \cdot f_i\right) \tag{2}$$

mostra que $a_i f_i + p$ permanece inalterado. Como todas as outras variáveis não são alteradas, (1) permanece verdade neste caso. Por outro lado, se o próximo passo for uma Etapa de Resto, então p e r serão alterados, mas a soma $p + r$ permanece inalterada

$$p + r = (p - LT(p)) + (r + LT(p)) .$$

Como antes, a igualdade (1) ainda é preservada.

Em seguida, observe que o algoritmo é interrompido quando $p = 0$ e nessa situação, (1) torna-se

$$f = \sum_{i=1}^{s} a_i f_i + r$$

Como adicionamos termos a r somente quando não são divisíveis por nenhum dos $LT(f_i)$, segue que $a_1, \ldots, a_s$ e r tem as propriedades desejadas quando chegamos ao fim do algoritmo.

Finalmente, precisamos mostrar que o algoritmo termina após um número finito de passos. A chave é notar que, toda vez que redefinimos a variável p há uma queda em seu monômio líder em relação ao seu termo anterior e pode ser que a variável p fique igual a 0. Para ver isso, primeiramente iremos supor que durante uma Etapa de Divisão p é redefinido para

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

Pelo Lema 2.12 da seção 2, temos que

$$LT\left(\frac{LT(p)}{LT(f_i)} \cdot f_i\right) = \frac{LT(p)}{LT(f_i)} \cdot LT(f_i) = LT(p), \tag{3}$$

de modo que p e $\frac{LT(p)}{LT(f_i)} \cdot f_i$ têm o mesmo termo líder. Portanto, a diferença deles p' deve ter multigrau estritamente menor quando $p \neq 0$. Em seguida, suponha que durante uma Etapa de Resto, p é redefinido para ser da forma

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

Então, pode-se notar que $LM(p') < LM(p)$ quando $p' \neq 0$. Portanto, em ambos os casos, o monômio líder deve ser menor. Se o algoritmo nunca terminasse, obteríamos um sequência decrescente infinita de monômios.

Agora pela boa ordenação de $>$ conforme foi enunciada no Lema 2.2, mostra que isso não pode ocorrer.

Assim, $p = 0$ deve ocorrer eventualmente, para que o algoritmo se encerre após um número finito de passos. Por fim, nos resta estudara relação entre $LM(f)$ e $LM(a_i f_i)$. Todo termo a_i é da forma $\frac{LT(p)}{LT(f_i)}$ para alguma valor da variável p. O algoritmo começa com $p = f$, e acabamos de provar que o $LM(p)$ diminui. Isso mostra que $LT(p) \leq LT(f)$ e como $LT(a_i f_i) = LT(p)$ por (3), segue o $LM(a_i f_i) \leq LM(f)$. Provando o teorema. □

No decorrer desta seção alguns exemplos serão feitos para compreender o funcionamento do algoritmo da divisão e a importância da ordem monomial escolhida.

Exemplo 3.2. *Considere* $f = X^2Y + XY^2 + Y^2$, $f_1 = XY - 1$ *e* $f_2 = Y^2 - 1$ *e dividiremos* f *por* f_1 *e* f_2 *usando a ordem lexicográfica com* $X > Y$. *Iremos utilizar o mesmo esquema*

feito pela divisão de polinômios em uma variável, tendo como uma única diferença a existência de mais divisores e quocientes. O termo líder de f é X^2Y, o termo líder de f_1 é XY e o termo líder de f_2 é Y^2, note que o termo líder de f_1 é o único termo líder que divide o termo líder de f, sabendo disso começaremos dividindo f por f_1. Observe que $LT(f) = X^2Y = LT(f_1)X$, então escrevemos $f = Xf_1 + (f - Xf_1) = Xf_1 + (XY^2 + X + Y^2)$. Agora aplicaremos o processo ao resto intermediário $r_1 = XY^2 + X + Y^2$ pelo algoritmo vamos dividir por f_1. Note que o termo líder desse o r_1 é XY^2 e é menor que o termo líder de f, além disso $LT(r_1)$ é múltiplo de $LT(f_1) = XY$. Como $XY^2 = LT(f_1)$ escrevemos $r_1 = Yf_1 + (r_1 - Yf_1) = Yf_1(X + Y^2 + Y)$ e portanto

$$f = Xf_1 + Yf_1 + (X + Y^2 + Y) = (X + Y)f_1 + (X + Y^2 + Y)$$

Note que o resto intermediário agora é $r_2 = X + Y^2 + Y$ cuja o termo líder é X que não é múltiplo nem de $LT(f_1)$ nem de $LT(f_2)$. Contudo r_2 não é nosso resto final pois o termo líder de f_2 divide Y^2. Deste modo, moveremos X para o resto final, escrevemos $f = (X + Y)f_1 + (Y^2 + Y) + X$ e assim vamos dividir $Y^2 + Y$ por f_1 e f_2. Veja que o termo líder de $Y^2 + Y$ é Y^2 e que $Y^2 = LT(f_2)$, então $Y^2 + Y = f_2 + (Y^2 + Y - f_2) = f_2 + (Y + 1)$. Agora o termo líder do resto intermediário é Y que não é múltiplo dos termos líderes nem de f_1 nem de f_2, então moveremos Y para o resto final e escrevemos $f = (X+Y)f_1+f_2+(1)+X+Y$, um raciocínio análogo é feito para o resto intermediário 1 que será movido para o resto final, e agora o resto intermediário é 0, e encerramos o algoritmo. Portanto,

$$f = (X + Y)f_1 + f_2 + X + Y + 1$$

Uma boa propriedade do algoritmo da divisão em $\mathbb{K}[X]$ é a maneira que ele resolve o problema de um polinômio pertencer ou não a um ideal. Conseguimos algo similar para mais variáveis? Um resultado direto do Teorema 3.1 simples de ver é o seguinte.

Corolário 3.3. *Seja $f \in \mathbb{K}[X]$ e $F = (f_1, \ldots, f_s) \in \mathbb{K}[X]$. Se é feita a divisão de f por $F = (f_1, \ldots, f_s)$ e obtido $r = 0$, então $f \in \langle f_1, \ldots, f_s \rangle$.*

Contudo, $r = 0$ não é uma condição necessária para f pertencer ao ideal. Veremos isso no exemplo abaixo:

Exemplo 3.4. *Seja* $f_1 = XY + 1$, $f_2 = Y^2 - 1 \in \mathbb{K}[X, Y]$ *com a ordem lexicográfica. Dividindo* $f = XY^2 - X$ *por* $F = (f_1, f_2)$ *o resultado é*

$$XY^2 - X = Y \cdot (XY + 1) + 0 \cdot (Y^2 - 1) + (-X - Y).$$

Com $F = (f_2, f_1)$, *entretanto, temos*

$$XY^2 - X = X \cdot (Y^2 - 1) + 0 \cdot (XY + 1) + 0.$$

A segunda divisão mostra que $f \in \langle f_1, \ldots, f_s \rangle$. *Então mesmo na primeira divisão o resto dando diferente de* 0, f *ainda assim pertence a* $\langle f_1, \ldots, f_s \rangle$.

4 Ideais monomiais e o Lema de Dickson

Nesta seção estudaremos ideais monomiais e responderemos uma das perguntas feitas no início deste trabalho: Todo ideal $I \subset \mathbb{K}[X]$ tem um conjunto gerador finito? Ou seja, podemos escrever $I = \langle f_1, \ldots, f_n \rangle$ para algum $f_i \in \mathbb{K}[X]$,$i = 1, \ldots, n$?
A resposta é sim e mostraremos isso nesta seção.

Definição 4.1. *Um ideal $I \subset \mathbb{K}[X]$ é um ideal monomial se existe um conjunto de monômios que gera I.*

Lema 4.2. *Seja $I = \langle X^\alpha : \alpha \in A \rangle$ um ideal monomial. Então um monômio X^β pertence a I se, e somente se, X^β é múltiplo de X^α para algum $\alpha \in A$.*

Demonstração. Começaremos supondo que X^β pertence a I. Logo se $X^\beta \in I$, então $X^\beta = \sum_{i=1}^{n} X^{\alpha_i} h_i$. Assim, X^β é um monômio tal que algum polinômio $X^{\alpha_i} h_i$ tem um monômio X^β, para algum $i = 1, \ldots, n$. Portanto X^β é múltiplo de X^{α_i} para algum $i = 1, \ldots, n$.
Reciprocamente, se X^β é um múltiplo de X^α para algum $\alpha \in A$, então $X^\beta \in I$ pela definição de ideal. □

Lema 4.3. *Seja I um ideal monomial e seja $f \in \mathbb{K}[X]$. Então as seguintes afirmações são equivalentes:*

1. *$f \in I$.*
2. *Todo termo de f pertence a I.*
3. *f é uma combinação linear de monômios de I.*

Demonstração. Observe que as implicações (3) ⇒ (2) ⇒ (1) são obvias. Logo para concluir que os três itens são equivalentes basta mostrar (1) ⇒ (3).
Considere $I = \langle m_1, \ldots, m_n \rangle$. Veja que $f \in I$ e $f = \sum_{i=1}^{n} m_i h_i$ e podemos expandir cada h_i como combinação linear de monômios com coeficientes em $\mathbb{K}$, aplicando a propriedade distributiva sobre os $m_i's$ o resultado segue. □

Corolário 4.4. *Dois ideais monomiais I e J são iguais se, e somente se, eles contém os mesmos monômios.*

Demonstração. Sejam I e J dois ideais monomiais iguais, então é claro que eles possuem os mesmos monômios.

Reciprocamente sabemos que, se os ideais contém os mesmos monômios, então pelo item (3) do Lema 4.3 que todo polinômio $f \in I$ é uma combinação linear de monômios de I com coeficientes em $\mathbb{K}$, mas esses monômios estão em J, então f é uma combinação linear de monômios de J com coeficientes em $\mathbb{K}$. Fazendo um raciocínio análogo, tomando qualquer polinômios $g \in J$ veja que $g \in I$. E isso mostra que $I \subseteq J$ e $J \subseteq I$, logo $I = J$. □

Lema 4.5 (Lema de Dickson)**.** *Seja I um ideal monomial de $\mathbb{K}[X]$, então existe um conjunto finito de monômios que geram I.*

Demonstração. Faremos a prova deste lema usando indução sobre o número de variáveis.Veja que para o caso de uma variável temos que a existência de um número finito de geradores é verdade, e isso vem do fato de I ser um ideal principal em $\mathbb{K}[X]$, ou seja, $I = \langle f \rangle$ para algum $f \in \mathbb{K}[X]$.Assim dado um monômio $m \in I$ temos que, $m = h \cdot f$ para algum $h \in \mathbb{K}[X]$. Pela igualdade de polinômios, segue que f e h devem ser um monômios.

Agora suponhamos que o lema é válido para ideais em anéis de polinômios com $n-1$ variáveis, com $n \geq 2$. Seja I um ideal monomial de $\mathbb{K}[X]$ e escolha um monômio $f_1 \in I$ tal que $f_1 = g_1 \cdot X_n^{\alpha_1}$ onde $g_1 \in \mathcal{M}_{n-1}$ e $X_n^{\alpha_1}$ é mínimo em I. Caso $I = \langle f_1 \rangle$, então o lema está provado. Caso contrario, escolha um monômio $f_2 = g_2 \cdot X_n^{\alpha_2} \in I \setminus \langle f_1 \rangle$, onde $g_2 \in \mathcal{M}_{n-1}$ e $X_n^{\alpha_2}$ mínimo possível. Se $I = \langle f_1, f_2 \rangle$, então provamos o lema. Caso contrário, continuamos o processo.

Vamos supor que este procedimento continua indefinidamente, ou seja, que possamos obter uma sequência infinita de monômios $f_1, f_2, \cdots \in I$ com $f_i = g_i \cdot X_n^{\alpha_i} \in I \setminus \langle f_1, \ldots, f_{i-1} \rangle$ com $g_i \in \mathcal{M}_{n-1}$ e $X_n^{\alpha_{i-1}}$ mínimo.

Por hipótese de indução, temos que o ideal $J \in \mathbb{K}[X_1, \ldots, X_n]$ dado por $J = \langle \{g_i | i = 1, \ldots \text{com} g_i \in \mathcal{M}_{n-1}\} \rangle$ é finitamente gerado, ou seja, existem $m_1, \ldots, m_s \in \mathcal{M}_{n-1}$ tais que $J = \langle m_1, \ldots, m_s \rangle$, ou seja, existe $p \in \mathcal{M}_{n-1}$ de modo que $g_i = p \cdot m_j$ para algum $j \in 1, \ldots, s$.

Por outro lado $m_j \in J$, então existe um monômio $q \in \mathcal{M}_{n-1}$ tal que $m_j = q \cdot g_k$ como descrito acima. Deste modo, temos que $g_i = p \cdot q \cdot g_k$. Se $i = k$, então $p \cdot q = 1$, ou seja, $p \in \mathbb{K} \setminus 0$ e $g_i = p \cdot m_j$. Como a sequência $g_1, g_2, \cdots \in \mathcal{M}_{n-1}$ é infinita não podemos ter esse caso indefinidamente, ou seja, existem índices $i \neq k$ tais que $g_k | g_i$, digamos $g_i = m \cdot g_k$

com $m \in \mathcal{M}_{n-1}$. Sem perda de generalidade, suponha $i > k$. Deste modo,

$$f_i = g_i \cdot X_n^{\alpha_i} = m \cdot g_k \cdot X_n^{\alpha_i - \alpha_k} \cdot X_n^{\alpha_k} = m \cdot X_n^{\alpha_i - \alpha_k} \cdot f_k$$

e $f_i \in \langle f_k \rangle \subset \langle f_1, \cdots, f_k \rangle$, contrariando a escolha de f_i.

Logo, existe um índice $t \in \mathbb{N}$ tal que $I = \langle f_1, \cdots, f_t \rangle$. Portanto, I é finitamente gerado por monômios. □

5 Teorema da Base de Hilbert e bases de Gröbner

Neste seção vamos mostrar que todo ideal $I \subset \mathbb{K}[X]$ possui um conjunto gerador finito. Veremos também que existem algumas bases com propriedades peculiares referentes ao algoritmo da divisão. Fixamos uma ordem monomial em $\mathcal{M}$.

Definição 5.1. *Seja $I \subset \mathbb{K}[X]$ um ideal diferente de $\{0\}$.*

1. *Denotamos por $LT(I)$ o conjunto dos termos dos elementos de I. Então*

$$LT(I) = \{cx^\alpha : \exists f \in I \text{ tal que } LT(f) = cx^\alpha\}$$

2. *Denotamos por $\langle LT(I)\rangle$ o ideal gerado por elementos de $LT(I)$.*

Proposição 5.2. *Seja $I \subset \mathbb{K}[X]$ um ideal.*

1. *$\langle LT(I)\rangle$ é um ideal monomial.*

2. *Existem $g_1, \ldots, g_t \in I$ tais que $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.*

Demonstração. 1. $\langle LT(I)\rangle$ é um ideal gerado por termos lideres, e portanto é gerado pelos monômios que aparecem nesses termos líderes, e assim é um ideal monomial.

2. Como $\langle LT(I)\rangle$ é um ideal monomial por 1, o Lema 4.5 nos garante a existência de um conjunto finito de monômios $\{M_1, \ldots, M_t\}$ tais que $\langle LT(I)\rangle = \langle M_1, \ldots, M_t\rangle$. É claro que esses monômios aparecem em termos líderes de polinômios de I, digamos $g_1, \ldots, g_t$, e portanto $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.

□

Theorem 5.3 (Teorema da Base de Hilbert)**.** *Todo ideal $I \subset \mathbb{K}[X]$ tem um conjunto gerador finito. Isto é, $I = \langle g_1, \ldots, g_t\rangle$, com $g_1, \ldots, g_t \in I$.*

Demonstração. Se $I = \{0\}$, tomamos $\{0\}$ como o conjunto gerador, que claramente é finito.

Caso I contenha algum polinômio não nulo, então um conjunto de geradores pode ser construído. Fixamos uma ordem monomial em $\mathcal{M}$, o conjunto dos monômios de $\mathbb{K}[X]$.

Pela proposição anterior, existem $g_1, \ldots, g_t \in I$ tais que $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.

Mostremos que $I = \langle g_1, \ldots, g_t \rangle$.

Como $g_i \in I$, $i = 1, \ldots, t$, segue que $\langle g_1, \ldots, g_t \rangle \subset I$. Para concluir a demonstração, queremos mostrar que $I \subset \langle g_1, \ldots, g_t \rangle$.

Seja $f \in I$ aplicando o algoritmo da divisão em f por $g_1, \ldots, g_t$ segue

$$f = a_1 g_1 + \cdots + a_t g_t + r, \text{ com } a_1, \ldots, a_t, r \in \mathbb{K}[X],$$

onde se $r \neq 0$, então $LT(g_i) \nmid LT(r)$ para todo $i = 1, \ldots, t$.

Temos $r = f - (a_1 g_1 + \cdots + a_t g_t) \in I$. Suponha $r \neq 0$. Como $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$, pelo Lema anterior segue que exite um $g_i \in I$ tal que $LT(g_i)$ divide $LT(r)$. Contrariando o que vimos acima, logo $r = 0$ e portanto $I \subset \langle g_1, \ldots, g_t \rangle$. □

Definição 5.4. *Fixe uma ordem. Um subconjunto finito $G = \{g_1, \ldots, g_t\}$ de um ideal I é chamada de base Gröbner se*

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

Podemos definir de maneira mais informal, um conjunto $\{g_1, \ldots, g_t\} \subset I$ é dito uma base de Gröbner de I se, e somente se, o termo líder de qualquer elemento de I não nulo é divisível por um $LT(g_i)$ com $i \in \{1, \ldots, t\}$.

Corolário 5.5. *Fixe uma ordem monomial. Então todo ideal $I \subset \mathbb{K}[X]$ diferente de $\{0\}$ tem uma base Gröbner. Além disso, qualquer base de Gröbner para I é uma base para I.*

Demonstração. Considere um ideal não nulo I, e seja o conjunto $G = \{g_1, \ldots, g_t\}$ conforme construído na prova do Teorema 5.3, que por definição é uma base de Gröbner. Agora pela definição de base Gröbner, dado $f \in I$ qualquer $LT(f)$ é divisível por $LT(g_i)$ para algum $i = 1, \ldots, t.$,ou seja, $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Então pelo Teorema 5.3 temos $I = \langle g_1, \ldots, g_t \rangle$, logo G é uma base para I. □

Theorem 5.6 (Condição de cadeia Ascendente)**.** *Seja $I_1 \subset I_2 \subset \cdots$ uma cadeia ascendente de ideias em $\mathbb{K}[X]$. Então existe $N \geq 1$ tal que $I_N = I_{N+1} = \cdots$.*

Demonstração. Dada uma cadeia ascendente $I_1 \subset I_2 \subset \cdots$, considere o conjunto $I = \bigcup_{i=1}^{\infty} I_i$. Mostremos que I é um ideal em $\mathbb{K}[X]$. Sabemos que $0 \in I$, pois $0 \in I_i$, para todo $i \geq 0$. Agora dados $f, g \in I$, veja que $f \in I_i$ e $g \in I_j$ para determinados $i, j \in \{1, 2, \ldots\}$.

Como os ideais formam uma cadeia ascendente podemos supor $i \geq j$, logo $g \in I_i$ e $f + g \in I_i$. Portanto $f + g \in I$. Assim I é um ideal. Pelo Teorema 5.3, o ideal I deve ter uma base finita. Porém cada um dos geradores está contido em algum dos I_j, isto é $f_i \in I_{j_i}$ para algum j_i, $i = 1, \ldots, s$. Tome N o máximo do j_i. Então pela definição de cadeia ascendente $f_i \in I_N$ para todo i. Logo,

$$I = \langle f_1, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I.$$

Assim, $I_N = I_{N+i}$ para todo $i \geq 1$. □

6 Propriedades das Bases de Gröbner

No seção anterior, provamos que, fixando uma ordem monomial todo ideal não nulo $I \subset \mathbb{K}[X]$ possui uma base de Gröbner. Neste capítulo, estudaremos as propriedades destas bases e aprenderemos quando uma base de um ideal I é uma base de Gröbner.

Fixamos uma ordem monomial em $\mathcal{M}$. O resultado abaixo prova a unicidade do resto quando dividimos um polinômio $f \in \mathbb{K}[X]$ por uma base de Gröbner.

Proposição 6.1. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subset \mathbb{K}[X]$ e seja $f \in \mathbb{K}[X]$. Então existe um único $r \in \mathbb{K}[X]$ com as seguintes propriedades:*

1. *Nenhum termo de r é múltiplo de qualquer $LT(g_1), \ldots, LT(g_t)$.*
2. *Há um $g \in I$ tal que $f = g + r$.*

Em particular, r é o resto da divisão de f por G independente de como os elementos de G estão listados no algoritmo da divisão.

Demonstração. O algoritmo da divisão nos fornece que $f = \sum_{i=1}^{t} a_i g_i + r$, onde r satisfaz 1. Além disso, definindo $g = \sum_{i=1}^{t} a_i g_i$, temos $g \in I$ e $f = g + r$ satisfazendo 2. Provando assim a existência de r. Agora mostremos a unicidade para tal suponha que $f = g + r = g' + r'$. Então $r - r' = g' - g \in I$, tal que se $r \neq r'$, então $LT(r - r') \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Agora pelo lema 4.2, segue que $LT(r - r')$ é múltiplo de algum $LT(g_i)$, $i = 1, \ldots t$.
O que é impossível, pois nenhum termo de r e r' é múltiplo de algum $LT(g_i)$ com $i = 1, \ldots t$.
Assim $r = r'$ provando a unicidade. □

Corolário 6.2. *Seja $G = \{g_1, \ldots, g_t\}$ uma base de Gröbner para um ideal $I \subset \mathbb{K}[X]$ e seja $f \in \mathbb{K}[X]$. Então $f \in I$ se, e somente se, o resto da divisão de f por G é zero.*

Demonstração. ($\Rightarrow$) Seja $f \in I$ e seja $f = \sum_{i=1}^{t} h_i g_i + r$ a divisão de f por $(g_1, \ldots, g_t)$. Então $r = f - \sum_{i=1}^{t} h_i g_i \in I$ e assim pela proposição 6.1 segue que $r = 0$.
($\Leftarrow$) A volta é obvia. □

Definição 6.3. *Escrevemos $\overline{f}^F$ para o resto da divisão de f pela s-upla $F = (f_1, \ldots, f_s)$. Se F é uma base de Gröbner para $(f_1, \ldots, f_s)$, então podemos ver F como um conjunto (sem qualquer ordem particular) pela proposição 6.1.*

Exemplo 6.4. *Seja* $F = \left(X^2Y - Y^2, X^4Y^2 - Y^2\right) \subset \mathbb{K}[X,Y]$, *usando a ordem lexicográfica,temos:*

$$\overline{X^5Y}^F = XY^3.$$

Pois o algoritmo da divisão nos dá que:

$$X^5Y = \left(X^3 + XY\right) \cdot \left(X^2Y - Y^2\right) + 0 \cdot \left(X^4Y^2 - Y^2\right) + XY^3.$$

Definição 6.5. *Sejam* $f, g \in \mathbb{K}[X]$ *polinômios não nulos.*

1. *Se* $LM(f) = X^\alpha$ *e* $LM(g) = X^\beta$, *então definimos* $X^\gamma = (X_1^{\gamma_1}, \ldots, X_n^{\gamma_n})$, *onde* $X_i^{\gamma_i} = max\left(X_i^{\alpha_i}, X_i^{\beta_i}\right)$ *para cada* $i = 1, \ldots, n$.
   Chamamos X^γ *o mínimo múltiplo comum dos monômios líderes de* f *e* g *e escrevemos* $X^\gamma = LCM\left(LM(f), LM(g)\right)$.

2. *O S-polinômio de* f *e* g *é a combinação*

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

Abaixo temos um exemplo que nos mostra como calcular o S-polinômio de dois polinômios em $\mathbb{R}[X,Y]$.

Exemplo 6.6. *Sejam* $f = X^3Y^2 - X^2Y^3 + X$ *e* $g = 3X^4Y + Y^2 \in \mathbb{R}[X,Y]$ *com a ordem lexicográfica graduada.*
Então $X^\gamma = X^4Y^2$ *e*

$$\begin{aligned} S(f,g) &= \frac{X^4Y^2}{X^3Y^2} \cdot f - \frac{X^4Y^2}{3X^4Y} \cdot g \\ &= X \cdot f - \frac{1}{3}Y \cdot g \\ &= X^4Y^2 - X^3Y^3 + X^2 - \frac{3X^4Y^2}{3} - Y^3 \\ &= -Y^3X^3 - \frac{Y^3}{3} + X^2 \end{aligned}$$

Lema 6.7. *Suponha que temos um somatório* $\sum_{i=1}^{t} c_i f_i$ *com* $c_i \in K$ *e* $LM(f_i) = X^\delta$ *para todo* $i = 1, \ldots, t$.
Se $LM\left(\sum_{i=1}^{t} c_i f_i\right) < X^\delta$, *então* $\sum_{i=1}^{t} c_i f_i$ *é uma combinação linear com coeficientes em* $\mathbb{K}$, *de s-polinômios* $S(f_j, f_k)$ *para* $1 \leq j, k \leq t$. *Além disso, cada* $S(f_i, f_k)$ *tem monômio líder menor que* X^δ.

Demonstração. Para todo $i \in 1, \ldots, s$ chamamos d_i o coeficiente líder de f_i, de modo que $c_i d_i$ é o coeficiente líder de $c_i f_i$. Como todos os termos da forma $c_i f_i$ tem monômio líder X^δ e a soma $\sum_{i=1}^{t} c_i f_i$ tem monômio líder menor que X^δ, é fácil observar que $\sum_{i=1}^{t} c_i d_i = 0$. Defina $p_i = \frac{f_i}{d_i}$ e observe que o coeficiente líder de p_i é 1 com $i \in 1, \ldots, t$. Considere a soma telescópica

$$\sum_{i=1}^{t} c_i f_i = \sum_{i=1}^{t} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + (c_1 d_1 + \cdots + c_{t-1} d_{t-1})(p_{t-1} - p_t) + (c_1 d_1 + \cdots + c_t d_t) p_t.$$

Pela hipótese, o termo líder de f_i é $d_i X^\delta$, para todo $i \in 1, \ldots, t$ o que implica que o mínimo múltiplo comum do termo líder de f_j e do termo líder de f_m é X^δ, onde $j, m \in 1, \ldots, t$, assim segue

$$S(f_j, f_m) = \frac{X^\delta}{LT(f_j)} f_j - \frac{X^\delta}{LT(f_m)} f_m = \frac{X^\delta}{d_j X^\delta} f_j - \frac{X^\delta}{d_m X^\delta} f_m = p_j - p_m. \tag{4}$$

Usando a equação 6.1 e $\sum_{i=1}^{t} c_i d_i = 0$, a soma telescópica acima se torna

$$\sum_{i=1}^{t} c_i f_i = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots + (c_1 d_1 + \cdots + c_{t-1} d_{t-1}) S(f_{t-1}, f_t), \tag{5}$$

que é a soma da forma desejada. E veja que para todo $j = 1, \ldots, m$ distintos, p_j e p_m tem monômio líder X^δ e coeficiente líder 1 e a diferença $p_j - p_m$ tem monômio líder menor que X^δ. Da equação (4), o mesmo é válido para o $S(f_j, f_m)$, o que prova o lema. □

A partir do S-polinômio e o Lema 6.7, podemos provar o critério de Buchberger que nos diz quando uma base de um ideal é uma base de Gröbner.

Theorem 6.8 (Critério de Buchberger)**.** *Seja* I *um ideal polinomial. Então uma base* $G = (g_1, \ldots, g_t)$ *para* I *é uma base de Gröbner para* I *se, e somente se, para todos os*

pares $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por G (independente da ordem que forem listados) é zero.

Demonstração. ($\Rightarrow$) Se G é uma base de Gröbner, então como $S(g_i, g_j) \in I$, temos do Corolário 6.2, que o resto da divisão de $S(g_i, g_j)$ por G é zero.
($\Leftarrow$) Seja $f \in I$ um polinômio não nulo. Devemos mostrar que se todos os s-polinômios tem resto zero na divisão por G, então $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$. Dado $f \in I = (g_1, \ldots, g_t)$, existem polinômios $h_i \in \mathbb{K}[X], i = 1, \ldots, t$ tais que

$$f = \sum_{i=1}^{t} h_i g_i \tag{6}$$

Assim, pelo Lema 2.12 segue

$$LM(f) \leq max\left\{LM(h_i g_i) | i = 1, \ldots, t\right\} \tag{7}$$

Se a igualdade não ocorre, então algum cancelamento ocorre sobre os termos líderes de (6). Dada uma expressão (6) para f, seja $X^{m(i)} = LM(h_i g_i)$, onde $i = 1, \ldots, t$ e defina $X^{\delta} = max\left\{X^{m(i)} | i = 1, \ldots, t\right\}$. Então a desigualdade 7 se torna

$$LM(f) \leq X^{\delta}.$$

Agora considere toda as maneiras possíveis que f pode ser escrita na forma (6) Para cada expressão, pegamos um δ diferente. Com uma ordem monomial é uma boa ordenação, podemos escolher uma expressão da forma (6) tal que X^{δ} é mínimo. Mostremos que uma vez escolhido o X^{δ}, temos $LM(f) = X^{\delta}$. Então igualdade ocorre em (7), assim $LM(f) = LM(h_i g_i)$, para algum i e seguirá que o termo líder de f é divisível pelo termo líder de g_i. Logo $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$, assim concluímos o que queríamos provar. Provemos $LM(f) = X^{\delta}$, por contradição. Para isolar os termos do *multigrau* igual a δ , vamos escrever f da seguinte forma.

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} \left(h_i - LT(i)\right) g_i + \sum_{m(i)<\delta} h_i g_i. \tag{8}$$

Note que $\sum_{m(i)=\delta} \left(h_i - LT(i)\right) g_i$ e $\sum_{m(i)<\delta} h_i g_i$ tem monômio líder menor que X^{δ}.
Então como supomos que o $LM(f) < X^{\delta}$, temos $LM\left(\sum_{m(i)=\delta} h_i g_i\right) < X^{\delta}$. Seja o termo líder de h_i igual a $c_i X^{\alpha(i)}$. Então a primeira soma $\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)=\delta} c_i X^{\alpha_i} g_i$ é

descrita conforme o Lema 6.7 com $f_i = X^{\alpha(i)} g_i$. Logo por consequência do Lema 6.7 esta soma é combinação linear de S-polinômios $S\left(X^{\alpha(j)} g_j, X^{\alpha(k)} g_k\right)$ Contudo,

$$S\left(X^{\alpha(j)} g_j, X^{\alpha(k)} g_k\right) = \frac{X^{\delta}}{X^{\alpha(j)} LT(g_j)} X^{\alpha(j)} g_j - \frac{X^{\delta}}{X^{\alpha(k)} LT(g_k)} X^{\alpha(k)} g_k = X^{\delta - \alpha_{jk}} S\left(g_j, g_k\right).$$

em que $X^{\alpha_{jk}} = LCM\left(LM(g_j), LM(g_k)\right)$. Então existem constantes $c_{jk} \in K$ tais que

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{j,k} c_{jk} X^{\delta - \alpha_{jk}} S\left(g_j, g_k\right). \tag{9}$$

Agora por hipótese resto da divisão de $S\left(g_j, g_k\right)$ por $g_1, \ldots, g_t$ é zero. Usando o algoritmo da divisão segue que cada S-polinômio pode ser escrito da forma

$$S\left(g_j, g_k\right) = \sum_{i=1}^{t} a_{ijk} g_i, \tag{10}$$

onde $a_{ijk} \in \mathbb{K}[X]$. E o algoritmo da divisão nos diz que

$$LM\left(a_{ijk} g_i\right) \leq LM\left(S\left(g_j, g_k\right)\right), \tag{11}$$

para todo i, j e k. Intuitivamente, isto nos diz que quando o resto é zero, podemos encontrar a expressão para $S\left(g_j, g_k\right)$ em termos de G onde nem todos os termos líderes se cancelam. Para explorar esse fato, multiplicamos a expressão (10) por $X^{\delta - \alpha_{jk}}$ para obter

$$X^{\delta - \alpha_{jk}} S\left(g_j, g_k\right) = \sum_{i=1}^{t} b_{ijk} g_i,$$

onde $b_{ijk} = X^{\delta - \alpha_{jk}} a_{ik}$. Então pela expressão (11) e o Lema 6.7 temos que

$$LM\left(b_{ijk} g_i\right) \leq LM\left(X^{\delta - \alpha_{jk}} S\left(g_j, g_k\right)\right) < X^{\delta}. \tag{12}$$

Assim, substituindo a expressão acima em (10), obtemos a seguinte expressão

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{j,k} c_{jk} X^{\delta - \alpha_{jk}} S\left(g_j, g_k\right) = \sum_{j,k} c_{jk} \left(\sum_{i} b_{ijk} g_i\right) = \sum_{i} h_i' g_i, \tag{13}$$

que pela expressão (12), segue que para i temos

$$LM\left(h_i' g_i\right) < X^{\delta}.$$

Veja que substituindo $\sum_{m(i)=\delta} LT(h_i) g_i = \sum_i h_i' g_i$ na equação (8), podemos escrever f como uma combinação de polinômios $g_i' s$ onde todos os termos tem o monômio líder menor que X^{δ}. O que contradiz a minimalidade de X^{δ} e o resultado segue. □

Exemplo 6.9. *Neste exemplo mostraremos uma aplicação imediata do Teorema provado acima, para tal, seja* $I = \langle Y - X^2, Z - X^3 \rangle \subset \mathbb{R}[X, Y, Z]$. *Afirmamos que* $G = \{Y - X^2, Z - X^3\}$ *é uma base de Gröbner usando a ordem lexicográfica com* $Y > Z > X$. *Para mostrarmos isto, calcularemos o S-polinômio*

$$S\left(Y - X^2, Z - X^3\right) = \frac{YZ}{Y}\left(Y - X^2\right) - \frac{YZ}{Z}\left(Z - X^3\right) = -ZX^2 + YX^3.$$

Usando o algoritmo da divisão, temos

$$-ZX^2 + YX^3 = X^3 \cdot \left(Y - X^2\right) + \left(-X^2\right) \cdot \left(Z - X^3\right) + 0,$$

observe que $\overline{S\left(Y - X^2, Z - X^3\right)} = 0$. *Logo, pelo Teorema 6.8,* G *é uma base de Gröbner para* I.

7 O Algoritmo de Buchberger

No corolário 5.5, vimos que todo ideal em $\mathbb{K}[X]$ diferente do ideal trivial nulo possui uma base de Gröbner. Contudo, a demostração deste corolário não nos dá um método para construir está base. Então neste capítulo vamos deduzir um método para a construção de tal base.

O teorema a seguir nos dá um algoritmo para construção da base de Gröbner para um ideal $0 \neq I \in \mathbb{K}[X]$.

Theorem 7.1 (Algoritmo de Buchberger)**.** *Seja $I = \langle f_1, \ldots, f_s \rangle \neq 0$ um ideal polinomial. Então uma base de Gröbner para I pode ser construída em um número finito de passos seguindo o seguinte algoritmo.*

ENTRADA: $F = (f_1, \ldots, f_s)$

SAÍDA: Uma base de Gröbner $G = (g_1, \ldots, g_t)$ para I, com $F \subset G$

$G := F$

REPETIR

$G' := G$

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

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

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

ATÉ $G = G'$

Demonstração. Se $G = \{g_1, \ldots, g_t\}$ então $\langle G \rangle$ e $\langle LT(G) \rangle$ denotará os seguintes ideais:

$$\langle G \rangle = \langle g_1, \ldots, g_t \rangle$$

$$\langle LT(G) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$$

Primeiramente, mostraremos que $G \subset I$ em todos os estágios do algoritmo. Inicialmente isto é verdade mesmo se aumentarmos G, faremos isso adicionando o resto $S = \overline{S(p,q)}^{G'}$ com $p, q \in G$ e $p \neq q$. Portanto, se $G \subset I$ então p, q e consequentemente $S(p,q)$ estão em I e como estamos dividindo por $G' \subset I$ temos $G \cup \{S\} \subset I$. Note que G contém a base dada F de I de modo que agora G é uma base de I.

O algoritmo termina quando $G = G'$, isso significa que $S = \overline{S(p,q)}^{G'} = 0$, para todo $p, q \in G$. Então G é uma base de Gröbner de $\langle G \rangle = I$ pelo Teorema 6.8.

Nos resta provar que o algoritmo termina. Para isso precisamos observar o que acontece após cada passo do algoritmo através do laço principal. O conjunto G consiste do conjunto G' unido com os restos não nulos dos S-polinômios de elementos de G'. Então

$$\left\langle LT(G') \right\rangle \subset \langle LT(G) \rangle , \tag{14}$$

já que $G' \subset G$. Além disso, $G' \neq G$, afirmamos que $\langle LT(G') \rangle \subsetneqq \langle LT(G) \rangle$. Para mostrar isto, suponha que um resto não nulo r de um S-polinômio foi adicionado a G. Como r é o resto da divisão por G', $LT(r)$ não é divisível pelo termos líderes de elementos de G' e então $LT(r) \notin \langle LT(G) \rangle$ o que mostra nossa afirmação.

Pela expressão (14), os ideais $\langle LT(G') \rangle$ das sucessivas interações formam uma cadeia ascendente de ideais. Logo, pelo Teorema 5.6 segue que depois de um número finito de iterações a cadeia se estaciona e assim $\langle LT(G) \rangle = \langle LT(G') \rangle$.

E por consequência $G = G'$, o que mostra a finitude do algoritmo como queríamos provar. □

Lema 7.2. *Seja G uma base de Gröbner para o ideal polinomial I. Seja $p \in G$ um polinômio tal que $LT(p) \in \langle LT(G - \{p\}) \rangle$. Então $G - \{p\}$ é uma base de Gröbner para I.*

Demonstração. Sabemos que $\langle LT(G) \rangle = \langle LT(I) \rangle$. Se $LT(p) \in \langle LT(G - \{p\}) \rangle$, então temos $\langle LT(G - \{p\}) \rangle = \langle LT(G) \rangle$. Assim, segue da definição que $G - \{p\}$ é uma base de Gröbner. □

Definição 7.3. *Uma base de Gröbner minimal para um ideal polinomial I é uma base de Gröbner para I tal que*

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

O exemplo abaixo ilustra como construímos uma base de Gröbner minimal para um ideal não nulo. Para tal, aplicaremos o algoritmo de Buchberger e em seguida usaremos o Lema 7.2 para eliminar os geradores desnecessários que possam ter sido incluídos.

Exemplo 7.4. *Considere o ideal I gerado pela seguinte base de Gröbner:*

$$f_1 = X^2 - 2XY,$$

$$f_2 = X^2Y - 2Y^2 + X,$$

$$f_3 = -X^2,$$

$$f_4 = -2XY,$$

$$f_5 = -2Y^2 + X.$$

Observe que como temos alguns coeficientes líderes diferentes de 1, o primeiro passo é multiplicar os geradores por constantes adequadas de modo a satisfazer o item 1 da definição de base de Gröbner minimal. Em seguida, note que $LT(f_1) = X^3 = -X \cdot LT(f_3)$ e $LT(f_2) = X^2Y = -\frac{1}{2}X \cdot LT(f_4)$, segue do Lema 7.2 que podemos exluir f_1 e f_2. Como não há mais casos onde o termo líder de um gerador divide o termo líder de um outro gerador, concluímos que

$$\widetilde{f_3} = X^2,$$

$$\widetilde{f_4} = XY,$$

$$\widetilde{f_5} = Y^2 - \frac{1}{2}X$$

formam uma base de Gröbner minimal para I.

Infelizmente, um ideal polinomial pode ter mais de uma base de Gröbner minimal. No exemplo anterior, podemos ver que outra base de Gröbner minimal pode ser dada por

$$f_3' = X^2 + aXY,$$

$$\widetilde{f_4} = XY,$$

$$\widetilde{f_5} = Y^2 - \frac{1}{2}X,$$

onde $a \in \mathbb{K}$ é uma constante qualquer. Então, podemos produzir infinitas bases de Gröbner minimais. Por outro lado, felizmente podemos destacar uma base de Gröbner minimal que é melhor que as demais.

Definição 7.5. *Uma base de Gröbner reduzida para um ideal polinomial I é uma base de Gröbner para I tal que*

1. $LC(p) = 1$ *para todo* $p \in G$.

2. *Para todo* $p \in G$, *nenhum monômio de* p *pertence a* $\langle LT(G - \{p\})\rangle$.

Proposição 7.6. *Seja* $I \neq 0$ *um ideal polinomial. Então para uma ordem monomial dada,* I *tem uma única base de Gröbner reduzida.*

Demonstração. Seja G uma base de Gröbner minimal para I. Dizemos que $g \in G$ é reduzido para G desde que nenhum monômio de G esteja em $\langle LT(G - g)\rangle$. Temos como objetivo modificar G até que todos os seus elementos estejam reduzidos. Observe que, se g é reduzido para G, então g é reduzido para qualquer base de Gröbner minimal de I que contenha g e tem o mesmo conjunto de termos líders. Isto segue porque a definição de base reduzida só envolve os termos líderes.

Agora, dado $g \in G$, seja $g' = \overline{g}^{G-g}$ e defina $G' = (G - g) \cup g'$. Afirmamos, G' é uma base de Gröbner minimal pra I. Para ver isto, primeiramente note que $LT(g') = LTLT(g)$, pois quando dividimos g por $G - g$, $LT(g)$ vai para o resto pois não é possível dividir por qualquer elemento de $LT(G - g)$. Isto mostra que $\langle LT(G')\rangle = \langle LT(G)\rangle$. Como G' claramente contido em I, vemos que G' é uma base de Gröbner e a minimalidade segue. E por fim, note que g' é reduzido para G' por construção.

Tome os elementos de G e aplique o processo acima até que todos esses elementos estejam reduzidos. A base de Gröbner talvez mude a cada processo que fizermos, já observamos que uma vez que um elemento é reduzido para G, ele continua reduzido para qualquer outra base de Gröbner minimal de I que contenha G, uma vez que nunca mudamos o termos líderes. Assim, terminamos com uma base de Gröbner reduzida.

Finalmente, para mostrar a unicidade, suponha que G e $\widetilde{G}$ são bases de Gröbner reduzidas, e por definição de base de Gröbner $\langle LT(G)\rangle = \langle LT(I)\rangle = \left\langle LT(\widetilde{G})\right\rangle$. Tome m, termo líder de qualquer de G, ele pode ser escrito com

$$m = a_1\widetilde{m_1} + \cdots + a_n\widetilde{m_n},$$

onde $\widetilde{m_i} \in LT(\widetilde{G})$ com $i \in \{1, \ldots, n\}$. Por definição de base de Gröbner minimal, o coeficiente líder de m é 1 e os coeficientes líderes de cada $\widetilde{m_i}$, com $i \in \{1, \ldots, n\}$ são 1, assim é fácil ver que $m = \widetilde{m_i}$, para algum $\widetilde{m_i}$. Portanto $LT(G) \subset LT(\widetilde{G})$.

A implicação $LT(\widetilde{G}) \subset LT(G)$ é mostrada de maneira análoga ao raciocínio usado anteriormente.

Então, dado $g \in G$, existe $\widetilde{g} \in \widetilde{G}$ tal que $LT(g) = LT(\widetilde{g})$. Se mostrarmos que $g = \widetilde{g}$, seguirá que $G = \widetilde{G}$, e a unicidade estará provada.

Para mostrar que $g = \widetilde{g}$, vamos olhar para a diferença entre g e $\widetilde{g}$. Esta diferença está em I e como G é uma base de Gröbner, segue que $\overline{g - \widetilde{g}}^{G} = 0$. Mas também sabemos que o termo líder de g é igual ao termo líder de $\widetilde{g}$. Então, estes termos se cancelam na diferença entre g e $\widetilde{g}$ e o restante dos termos não são divisíveis por nenhum dos termos líderes de G pois G é base de Gröbner reduzida. Isto mostra que $\overline{g - \widetilde{g}}^{G} = g - \widetilde{g}$, e então $g - \widetilde{g} = 0$.

□

8 Melhorias no Algoritmo de Buchberger

Definição 8.1. *Fixando uma ordem monomial, seja* $G = \{g_1, \ldots, g_s\} \subset \mathbb{K}[X]$. *Dado* $f \in \mathbb{K}[X]$, *dizemos que* f *reduz a zero módulo* G, *e escrevemos*

$$f \to_G 0,$$

caso f *possa ser escrito da forma*

$$f = a_1 g_1 + \cdots + a_s g_s$$

sempre que $a_i g_i \neq 0$ *com* $i = 1, \ldots, s$, *temos*

$$LM(f) \geq LM(a_i g_i).$$

Lema 8.2. *Seja* $G = (g_1, \ldots, g_s)$ *um conjunto ordenado de elementos e fixe* $f \in \mathbb{K}[X]$. *Se* $\overline{f}^G = 0$, *então* $f \to_G 0$.

Demonstração. Como $\overline{f}^G = 0$, então o algoritmo da divisão nos fornece que f pode ser escrito como

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

com $a_1, \ldots, a_s \in \mathbb{K}[X]$ e que também o $LM(f) \leq LM(a_i g_i)$ sempre que $a_i g_i \neq 0$. E isso é a definição de $\overline{f}^G = 0$. O que conclui a demonstração do Lema. □

A recíproca deste lema não é verdadeira. O exemplo abaixo mostra isso.

Exemplo 8.3. *Vamos considerar o exemplo 3.5. Se dividirmos* $f = XY^2 - X$ *por* $G\left(XY + 1, Y^2 - 1\right)$ *o algoritmo da divisão nos fornece*

$$XY^2 - X = Y \cdot (XY + 1) + 0 \cdot \left(Y^2 - 1\right) + (-X - Y).$$

Contudo, $\overline{f}^G = -X - Y \neq 0$.

No entanto, também podemos escrever

$$XY^2 - X = 0 \cdot (XY + 1) + X \cdot \left(Y^2 - 1\right),$$

com

$$LM\left(XY^2 - X\right) \geq LM\left(X \cdot \left(Y^2 - 1\right)\right).$$

Neste caso ocorrendo a igualdade, segue-se que $f \to_G 0$.

Theorem 8.4. *A base $G = \{g_1, \ldots, g_t\}$ para um ideal I é uma base de Gröbner se, e somente se, $S(g_i, g_j) \to_G 0$ para todo $i \neq j$.*

Demonstração. Pelo Teorema (6.8), já provamos este resultado sob as hipóteses de que $\overline{S(g_i, g_j)}^G = 0$ para todo $i \neq j$.

Ao analisarmos a prova do Teorema, podemos ver que usamos fortemente o fato de que

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

com que $LM(S(g_j, g_k)) \geq LM(a_{ijk} g_i)$ (Veja em (10) e (11)).

Isto é exatamente o que $S(g_i, g_j) \to_G 0$ significa e concluímos a demonstração. □

Proposição 8.5. *Dado um conjunto finito $G \subset \mathbb{K}[X]$ suponha que temos $f, g \in \mathbb{K}[X]$ tais que*

$$LCM\left(LM(f), LM(g)\right) = LM(f) \cdot LM(g).$$

Em outras palavras, os monômios líderes são relativamente primos. Então $S(f, g) \to_G 0$.

Demonstração. Por simplicidade, vamos assumir que f, g, foram multiplicados por constantes apropriadas tais que $LC(f) = LC(g) = 1$. Escrevemos $f = LM(f) + p$, $g = LM(g) + q$. Por hipótese temos $LCM\left(LM(f), LM(g)\right) = LM(f) \cdot LM(g)$, assim segue que

$$\begin{aligned} S(f, g) &= LM(g) \cdot f - LM(f) \cdot g \\ &= (g - q) \cdot f - (f - p) \cdot q \\ &= f \cdot g - f \cdot q - g \cdot f + g \cdot p \\ &= -f \cdot q + g \cdot p. \end{aligned} \tag{15}$$

Afirmamos,

$$LM\left(S\left(f, g\right)\right) = max\left(LM\left(p \cdot g\right), LM\left(f \cdot q\right)\right). \tag{16}$$

Note que (16) e (15) implicam que $S(f, g) \to_G 0$, pois $f, g \in G$.

Para provarmos a afirmação, observe que os monômios lideres $f \cdot q$ e $p \cdot g$ não podem se cancelar. Caso os monômios líderes fossem os mesmos teríamos

$$LM(p) \cdot LM(g) = LM(q) \cdot LM(f).$$

Assim $LM(g)$ dividiria $LM(q)$, pois f e g são relativamente primos. O que é um absurdo, pois o monômio líder de g é maior que o monômio líder de q. □

Para mostrar como a proposição acima funciona daremos um exemplo.

Exemplo 8.6. *Seja* $G = \left(YZ + Y, X^3 + Y, Z^4\right)$ *e use a ordem grlex em* $\mathbb{K}[X, Y, Z]$. *Então*

$$S\left(X^3 + Y, Z^4\right) \to_G 0,$$

pela Proposição (8.5). No entanto, usando o algoritmo de divisão, segue que

$$S\left(X^3 + Y, Z^4\right) = YZ^4 = \left(Z^3 - Z^2 + Z - 1\right)(YZ + Y) + Y$$

onde,

$$\overline{S\left(X^3 + Y, Z^4\right)}^G = Y \neq 0.$$

Mostrando mais uma vez que a recíproca do Lema 8.2 não é verdadeira.
Pelo Teorema 6.8 G não é base de Gröbner, podemos notar também que pelo Teorema 8.4 deve existir um par de polinômio em G tal que o S-polinômio não se reduz a zero módulo G.
E pelas contas acima podemos extrair a seguinte base de Gröbner $G' = \left(X^3 + Y, Z^4\right)$.

Referências

[1] Cox, D.;Little, J. and O'Shea, D.- Ideals, Varieties, and Algorithms, Springer- Verlag, 2010 (3a. ed.)