Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

APLICAÇÕES DAS BASES DE GROEBNER

por

DANTON PEREIRA DA SILVA JUNIOR

Porto Alegre, agosto de 1999

Dissertação submetida por DANTON PEREIRA DA SILVA JUNIOR como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:
Drª. Luisa Rodriguez Doering

Banca Examinadora:
Drª. Ada Maria de Souza Doering
Dr. Alveri Alves Sant'Ana
Dr. Aron Simis

Data de Defesa: 05 de agosto de 1999

Agradecimentos

Agradeço a minha família, pelo apoio e pelas constantes demonstrações de carinho e orgulho pela minha pessoa.

Aos meus colegas do Grupo de Engenharia Biomédica do Hospital de Clínicas, pelo apoio e pelas animadas conversas.

Ao professor Claus Doering, pela revisão do trabalho. Além das correções e ótimas sugestões, é também o responsável por muitas das vírgulas presentes neste trabalho.

À minha orientadora Luisa Doering, pela paciência em orientar meu trabalho e por sempre acreditar no meu potencial. Sua competência e didática ao ministrar Álgebra Linear durante minha graduação em Engenharia Elétrica me induziram a este mestrado.

Aos professores do CPGMAT pela paciência e compreensão ao longo destes últimos anos.

RESUMO

Neste trabalho estudamos os homomorfismos entre anéis de polinômios do ponto de vista da teoria de bases de Groebner. Em particular, determinamos o núcleo de um tal homomorfismo e desenvolvemos um método para determinar quando este é sobrejetivo. Estes resultados são então generalizados para anéis quocientes.

O estudo de tais homomorfismos nos permite determinar os polinômos minimais de elementos em extensões de corpos, bem como encontrar soluções para um problema de programação inteira.

ABSTRACT

In this work we study the homomorphisms between polynomial rings as an application of the Groebner basis theory. In particular, we determine generators for the kernel of such a homomorphism and we give a method to determine whether it is onto. We then generalize these results to the case of quocient rings.

The study of these homomorphisms allows us to determine minimal polynomials of elements in field extensions, as well as to find solutions to an integer programming problem.

Índice

Introdução

A teoria de bases de Groebner é hoje uma área de grande interesse em Álgebra Computacional devido a sua utilidade na construção de ferramentas computacionais aplicáveis a uma grande variedade de problemas em Matemática, Engenharia e Ciência da Computação.

O objetivo do presente trabalho é o estudo das aplicações de bases de Groebner, apresentado no Capítulo 2. Para isto é de fundamental importância o estudo dos homomorfismos entre anéis de polinômios, feito na Seção 2.1. Em particular, utilizando o material desenvolvido em [3], determinamos explicitamente o núcleo de tais homomorfismos e desenvolvemos um método para determinar quando estes são sobrejetivos.

A partir da teoria desenvolvida na Seção 2.1, apresentamos duas aplicações de bases de Groebner, a saber: na Seção 2.2 determinamos polinômios minimais de elementos em extensões de corpos e na Seção 2.3, baseado em [4], encontramos soluções para um problema de programação inteira.

Uma introdução ao conceito de bases de Groebner é apresentada no Capítulo 1, tendo como referências básicas [1] e [2].

Embora bases de Groebner tenham importantes aplicações teóricas, elas são essencialmente ferramentas de uso computacional. Desta forma o uso de um sistema de Álgebra Computacional torna-se imprescindível para a solução dos problemas aqui apresentados. No Apêndice listamos os algoritmos implementados no CoCoA[1] para a solução de tais problemas bem como a solução dos exemplos numéricos apresentados ao longo do texto.

---

[1] A. Capani, G. Niesi, L.Robbiano,
CoCoA, a system for doing Computations in Commutative Algebra,
Available via anonymous ftp from: cocoa.dima.unige.it

1. Bases de Groebner

1.1 Preliminares

Seja k um corpo. Os polinômios em n variáveis com coeficientes em k serão denotados por $f(x_1,...,x_n)$. Tais polinômios são somas finitas de ***monômios***, ou seja, termos da forma $ax_1^{\beta_1}...x_n^{\beta_n}$, onde $a \in k$ e $\beta_i \in Z_{\geq 0}$, $i = 1,...,n$.

O conjunto $k[x_1,...,x_n]$ de todos os polinômios em n variáveis com coeficientes em k é um anel comutativo com as operações usuais de adição e multiplicação de polinômios.

Neste primeiro capítulo iremos apresentar uma breve introdução a teoria de bases de Groebner. O conceito de ordem de monômios, juntamente com a algoritmo de divisão em $k[x_1,...,x_n]$, nos permitirá mostrar que todo ideal de $k[x_1,...,x_n]$ é finitamente gerado (Teorema da base de Hilbert), e a prova de tal fato nos guiará de maneira natural a construção de bases com "boas" propriedades relativas ao algoritmo de divisão, as quais daremos o nome de bases de Groebner.

Por fim apresentamos o algoritmo de Buchberger para o cômputo de bases de Groebner de um ideal em $k[x_1,...,x_n]$.

1.2 Ordem de Monômios em $k[x_1,...,x_n]$.

Nesta seção discutiremos as propriedades de uma ordem de monômios em $k[x_1,...,x_n]$, e construiremos vários exemplos de modo a satisfazer tais propriedades. Como veremos nas próximas seções, a escolha de uma ordem de monômios será de fundamental importância na construção de bases de Groebner de um ideal.

Observe que podemos reconstruir o monômio $x^\alpha = x_1^{\alpha_1}...x_n^{\alpha_n}$ a partir da n-upla de expoentes $\alpha = (\alpha_1,...,\alpha_n) \in \mathcal{Z}_{\geq 0}^n$. Tal observação estabelece uma relação um a um entre monômios em $k[x_1,...,x_n]$ e $\mathcal{Z}_{\geq 0}^n$. Desta forma qualquer ordem em $\mathcal{Z}_{\geq 0}^n$ nos dará uma ordem de monômios: se de acordo com esta ordem tivermos $\alpha > \beta$ então $x^\alpha > x^\beta$.

Existem várias ordens em $\mathcal{Z}_{\geq 0}^n$; no entanto, para nossos propósitos tais ordens devem ser compatíveis com a estrutura algébrica dos anéis de polinômios.

Para começar, como polinômios são somas de monômios, gostaríamos de poder arranjar os termos de um dado polinômio de forma única em ordem descendente (ou ascendente). Para que isto possa ser feito devemos ser capazes de comparar todo par de monômios e estabelecer uma ordem entre eles. Isto significa que para todo par de monômios x^α e x^β, exatamente uma das três possibilidades deve ocorrer:

$$x^\alpha > x^\beta, \qquad x^\alpha = x^\beta, \qquad x^\beta > x^\alpha.$$

Ordens que satisfazem tal propriedade são ditas ***ordens lineares*** ou ***totais***.

A seguir devemos considerar o efeito das operações de soma e produto de polinômios. Quando adicionamos polinômios, após combinar os termos semelhantes, simplesmente rearranjamos os termos na ordem apropriada e desta forma a soma de polinômios não apresenta dificuldades. O produto no entanto é mais complicado. Uma vez que a multiplicação em um anel de polinômios é distributiva com relação a adição, é

suficiente considerar o que acontece quando multiplicamos um monômio por um polinômio. Se ao fazer isto tivermos uma troca na ordem relativa dos termos, teremos problemas em qualquer processo similar ao algoritmo da divisão em $k[x]$, onde é de fundamental importância estabelecer uma ordem entre os vários monômios de um dado polinômio $f \in k[x]$. Iremos portanto exigir que nossa ordem de monômios tenha uma propriedade adicional. Se $x^{\alpha} > x^{\beta}$ e x^{γ} é um monômio qualquer, então devemos ter que $x^{\alpha}x^{\gamma} > x^{\beta}x^{\gamma}$. Isto significa que se $\alpha > \beta$ em nossa ordem de $\mathcal{Z}_{\geq 0}^{n}$, então para todo $\gamma \in \mathcal{Z}_{\geq 0}^{n}$, $\alpha + \gamma > \beta + \gamma$. Temos então a seguinte definição:

Definição 1.2.1. Uma ordem de monômios em $k[x_1,\ldots,x_n]$ é qualquer relação $>$ em $\mathcal{Z}_{\geq 0}^{n}$, ou equivalentemente no conjunto de monômios x^{α}, $\alpha \in \mathcal{Z}_{\geq 0}^{n}$, satisfazendo:

(i) $>$ é uma ordem *total* (ou *linear*) em $\mathcal{Z}_{\geq 0}^{n}$.

(ii) Se $\alpha > \beta$ e $\gamma \in \mathcal{Z}_{\geq 0}^{n}$, então $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ é uma boa ordem em $\mathcal{Z}_{\geq 0}^{n}$.

O lema a seguir nos ajudará a entender o significado da boa ordem na condição (iii) da definição acima, i.e., todo conjunto não-vazio de $\mathcal{Z}_{\geq 0}^{n}$ tem um menor elemento (relativamente a $>$).

Lema 1.2.2. Uma relação de ordem em $\mathcal{Z}_{\geq 0}^{n}$ é uma boa ordem se e somente se toda sequência estritamente decrescente em $\mathcal{Z}_{\geq 0}^{n}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

é finita.

Prova:

Suponhamos por contradição que $>$ não é uma boa ordem, logo deve existir um subconjunto não-vazio $S \subseteq \mathcal{Z}_{\geq 0}^{n}$ o qual não possui elemento mínimo. Seja $\alpha(1) \in S$.

Como $\alpha(1)$ não é o menor elemento, podemos encontrar $\alpha(2)$ tal que $\alpha(1) > \alpha(2)$ em S. Prosseguindo da mesma maneira temos uma sequência infinita estritamente decrescente

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

Reciprocamente, dada uma sequência infinita como acima, $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ é um subconjunto não-vazio de $\mathcal{Z}_{\geq 0}^n$ que não possui elemento mínimo, e desta forma $>$ não é uma boa ordem.□

O lema acima será de grande importância no que segue pois será usado para mostrar que vários algoritmos devem terminar porque algum termo decresce estritamente a cada passo do algoritmo.

Nosso primeiro exemplo de ordem de monômios será a ordem lexicográfica (***lex***).

Definição 1.2.3 (Ordem Lexicográfica). Sejam $\alpha = (\alpha_1,\ldots,\alpha_n)$ e $\beta = (\beta_1,\ldots,\beta_n) \in \mathcal{Z}_{\geq 0}^n$. Dizemos que $\alpha >_{lex} \beta$ se, no vetor diferença $\alpha - \beta \in \mathcal{Z}_{\geq 0}^n$, a coordenada não-nula mais à esquerda é positiva. Escreveremos $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.

Exemplos

- $(2,0,0) >_{lex} (1,2,4)$, já que $\alpha - \beta = (1, -2, -4)$.
- $(1,2,3) >_{lex} (1,2,1)$, já que $\alpha - \beta = (0, 0, 2)$.
- As variáveis $x_1,\ldots,x_n$ são ordenadas da maneira usual pela ordem lexicográfica

  $(1,0,\ldots,0) >_{lex} (0,1,\ldots,0) >_{lex} \ldots >_{lex} (0,0,\ldots,1)$

  e portanto $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$.

Temos que mostrar ainda que a ordem lexicográfica satisfaz as três condições da Definição 1.2.1.

Proposição 1.2.4. A ordem lexicográfica é uma ordem de monômios.

Prova:

(i) $>_{lex}$ é uma ordem total pelo fato da ordem numérica usual em $\mathcal{Z}$ ser uma ordem total.

(ii) Se $\alpha >_{lex} \beta$, então a coordenada não-nula mais à esquerda em $\alpha - \beta$, digamos $\alpha_k - \beta_k$, é positiva. Mas $x^{\alpha}x^{\gamma} = x^{\alpha+\gamma}$ e $x^{\beta}x^{\gamma} = x^{\beta+\gamma}$. Então em $(\alpha+\gamma)-(\beta+\gamma) = (\alpha-\beta)$ a coordenada não-nula mais à esquerda é novamente $\alpha_k - \beta_k > 0$.

(iii) Suponhamos que $>_{lex}$ não seja uma boa ordem. Então pelo Lema 1.2.2, deve existir uma sequência infinita estritamente decrescente

$$\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \cdots$$

de elementos de $\mathcal{Z}^n_{\geq 0}$. Isto nos guiará a uma contradição.

Considere a primeira coordenada de cada um dos vetores $\alpha(i) \in \mathcal{Z}^n_{\geq 0}$. Pela definição de ordem lexicográfica estas formam uma sequência não crescente de numeros inteiros não-negativos e portanto devem estabilizar, isto é, existe um m tal que a primeira coordenada dos vetores $\alpha(i)$ com $i \geq m$ são iguais.

Começando em $\alpha(m)$, as segundas coordenadas são quem determinam a ordem lexicográfica. As segundas coordenadas de $\alpha(m),\alpha(m+1),\ldots$ formam uma sequência não crescente. Pela mesma razão anterior, as segundas coordenadas devem também estabilizar. Continuando da mesma maneira vemos que, para algum l, $\alpha(l),\alpha(l+1),\ldots$ são todos iguais. Isto contradiz o fato que $\alpha(l) > \alpha(l+1)$. □

É importante observar que existem muitas ordens lexicográficas de acordo com a forma em que as variáveis são ordenadas. Em geral no caso de n variáveis existem $n!$ diferentes ordens lexicográficas. Na ordem lexicográfica uma variável domina qualquer monômio envolvendo apenas variáveis menores, independente do grau total. Por exemplo, para a ordem lexicográfica com $x > y > z$, temos $x^5 >_{lex} y^5z^3$.

Podemos em algumas situações querer levar em conta o grau total de um monômio e ordenar monômios de graus maiores primeiro. Uma forma de fazer isto é usar a ordem lexicográfica graduada (***grlex***).

Definição 1.2.5 (Ordem Lexicográfica Graduada). Sejam $\alpha = (\alpha_1,...,\alpha_n)$ e $\beta = (\beta_1,...,\beta_n) \in \mathcal{Z}^n_{\geq 0}$. Dizemos que $\alpha >_{grlex} \beta$ se

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

A ordem lexicográfica graduada ordena inicialmente pelo grau total e, quando estes são iguais, pela ordem lexicográfica.

Exemplos:

- $(2,2,3) >_{grlex} (4,1,1)$, pois temos que $7 = |(2,2,3)| > |(4,1,1)| = 6$.
- $(2,1,3) >_{grlex} (0,1,5)$, já que $|(2,1,3)| = 6 = |(0,1,5)|$ e $(2,1,3) >_{lex} (0,1,5)$.

Assim como no caso anterior (ordem lexicográfica) temos que a ordem lexicográfica graduada satisfaz as três condições da Definição 1.2.1.

Uma outra ordem é dada pela ordem lexicográfica graduada reversa (***grevlex***), que é a mais eficiente das ordens em muitas das operações referentes a bases de Groebner.

Definição 1.2.6 (Ordem Lexicográfica Graduada Reversa). Sejam $\alpha = (\alpha_1,...,\alpha_n)$ e $\beta = (\beta_1,...,\beta_n) \in Z^n_{\geq 0}$. Dizemos que $\alpha >_{grevlex} \beta$ se

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i = |\beta|,$$

ou

$|\alpha| = |\beta|$ e em $\alpha - \beta \in Z^n$ a primeira coordenada não-nula, começando à direita, é negativa.

É fácil verificar que a ordem lexicográfica graduada satisfaz as três condições da Definição 1.2.1.

Exemplos:

- $(1,3,2) >_{grevlex} (4,0,1)$, já que $6 = |(1,3,2)| > |(4,0,1)| = 5$.
- $(3,4,1,2) >_{grevlex} (4,2,2,2)$, já que $|(3,4,1,2)| = 10 = |(4,2,2,2)|$ e $\alpha - \beta = (-1,2,-1,0)$.

Vale ressaltar que existem muitas outras ordens além das aqui citadas.

Abaixo temos algumas definições referentes a ordens de monômios.

Definição 1.2.7. Sejam $f = \sum_{\alpha} a_\alpha x^\alpha$ um polinômio não-nulo em $k[x_1,...,x_n]$ e $>$ uma ordem de monômios.

(i) O **grau** de f é

$$\text{multdeg}(f) = \max \{\alpha \in Z^n_{\geq 0} \mid a_\alpha \neq 0\},$$

onde o máximo é tomado com relação a $>$.

(ii) O **coeficiente líder** de f é

$$lc(f) = a_{\text{multdeg}(f)} \in k .$$

(iii) O **monômio líder** de f é

$$lm(f) = x^{\text{multdeg}(f)} .$$

(iv) O **termo líder** de f é

$$lt(f) = lc(f) \cdot lm(f) .$$

Lema 1.2.8. Sejam $f, g \in k[x_1,...,x_n]$ polinômios não-nulos. Então:

(i) multdeg $(f.g)$ = multdeg (f) + multdeg (g).

(ii) Se $f + g \neq 0$, então multdeg $(f + g) \leq$ max {multdeg (f), multdeg (g)}.

Ainda se multdeg $(f) \neq$ multdeg (g),então

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

Prova:

(i) Sejam $f = \sum_{i=1}^{N} a_i x^{\alpha(i)}$ e $g = \sum_{j=1}^{M} b_j x^{\beta(j)}$ polinômios em $k[x_1,...,x_n]$ com $a_i, b_j \in k$ e $\alpha(i), \beta(j) \in \mathbb{Z}^n_{\geq 0}$, para $1 \leq i \leq N$ e $1 \leq j \leq M$. Seja $>$ uma ordem de monômios qualquer, de forma que podemos sem perda de generalidade supor

$$\alpha(1) > \alpha(2) > \cdots > \alpha(N) \text{ e } \beta(1) > \beta(2) > \cdots > \beta(M) ,$$

e portanto temos que multdeg $(f) = \alpha(1)$ e multdeg $(g) = \beta(1)$.

Temos ainda que

$$f \cdot g = \left(\sum_{i=1}^{N} a_i x^{\alpha(i)}\right) \cdot \left(\sum_{j=1}^{M} b_j x^{\beta(j)}\right) = \sum_{i=1}^{N} \sum_{j=1}^{M} a_i b_j x^{\alpha(i)+\beta(j)} .$$

Queremos mostrar que $\alpha(1) + \beta(1)$ é o grau de $f \cdot g$, e portanto multdeg $(f \cdot g)$ = multdeg (f) + multdeg (g). Para isto observe que

$$\alpha(1) > \alpha(i) \ ; 2 \leq i \leq N,$$

e da definição de ordem de monômios temos

(1.2.1) $$\alpha(1) + \beta(j) > \alpha(i) + \beta(j) \ ; 2 \leq i \leq N \text{ e } 1 \leq j \leq M.$$

Da mesma forma temos que

$$\beta(1) > \beta(j) \ ; 2 \leq j \leq M,$$

e portanto

(1.2.2) $$\alpha(1) + \beta(1) > \alpha(1) + \beta(j) \ ; 2 \leq j \leq M.$$

Logo, substituindo (1.2.1) em (1.2.2), temos que

$$\alpha(1) + \beta(1) > \alpha(1) + \beta(j) > \alpha(i) + \beta(j) \ ; 2 \leq i \leq N \text{ e } 2 \leq j \leq M \ ,$$

e portanto $\alpha(1) + \beta(1)$ é o grau de $f \cdot g$.

(ii) Sejam f e g como no item (i) acima e tais que $f + g \neq 0$, de forma que multdeg $(f + g)$ está definido.

Suponhamos inicialmente que multdeg $(f) \neq$ multdeg (g). Temos então que $\alpha(1) > \alpha(i)$ para $2 \leq i \leq N$ e $\beta(1) > \beta(j)$ para $2 \leq j \leq M$; como $\alpha(1) \neq \beta(1)$, o multdeg $(f + g)$ será o maior entre os dois, ou seja

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

Se no entanto tivermos que multdeg $(f) =$ multdeg (g), então temos duas possibilidades:

(1) $lt(f) = - lt(g)$.

Neste caso os termo líderes se cancelam, deixando apenas termos menores que $x^{\alpha(1)} = x^{\beta(1)}$ e temos que multdeg $(f + g) < \alpha(1) = \beta(1)$ e portanto

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

(2) $lt(f) \neq - lt(g)$.

Neste caso não há cancelamento entre os termos líderes e temos que

$$lt(f + g) = (a_1 + b_1)x^{\alpha(1)} = (a_1 + b_1)x^{\beta(1)},$$

e portanto

$$\text{multdeg}\,(f + g) = \alpha(1) = \beta(1) = \max\{\text{multdeg}\,(f), \text{multdeg}\,(g)\}.\square$$

1.3 Algoritmo de Divisão

Nesta seção estudaremos um algoritmo de divisão em $k[x_1,...,x_n]$. A idéia básica é a mesma do caso de polinômios em uma variável: quando dividimos f por $f_1,...,f_s$ queremos cancelar os termos de f usando os termos líderes dos f_i, de forma que os termos introduzidos sejam sempre menores que os termos cancelados e continuamos este processo até que o mesmo não possa mais ser realizado.

Consideramos inicialmente o caso da divisão de f por g, onde $f, g \in k[x_1,...,x_n]$. Fixamos também uma ordem de monômios em $k[x_1,...,x_n]$.

Definição 1.3.1. Dados $f, g \in k[x_1,...,x_n]$, com $g \neq 0$, dizemos que f se reduz a h módulo g em um passo, e escrevemos

$$f \xrightarrow{g} h$$

se e somente se $lm(g)$ divide um termo não nulo X que aparece em f e

$$h = f - \frac{X}{lt(g)}g.$$

Exemplo 1.3.2. Sejam $f = x^2y + xy^2 + 2y + 1$ e $g = x^2 + 2xy$ polinômios em $\mathbb{Q}[x,y]$. Se a ordem lexicográfica com $x > y$ é a ordem escolhida, então $f \xrightarrow{g} h$, onde $h = -xy^2 + 2y + 1$, já que neste caso $X = x^2y$ é o termo de f que nós cancelamos usando $lt(g) = x^2$.

Podemos pensar em h como sendo o resto da divisão de f por g após um passo de divisão. Podemos continuar este processo e subtrair de f todos os termos divisíveis por $lt(g)$.

Exemplo 1.3.3. Sejam $f = x^2y^2 + 2xy^2 - xy$, $g = x + 2y + 1 \in Q[x,y]$ e *grlex* a ordem escolhida com $x > y$. Então

$$f \xrightarrow{g} -2xy^3 + xy^2 - xy \xrightarrow{g} 4y^4 + xy^2 + 2y^3 - xy \xrightarrow{g} 4y^4 - xy - y^2 \xrightarrow{g} 4y^4 + y^2 + y.$$

Notamos que no último polinômio obtido, $4y^4 + y^2 + y$, nenhum termo é divisível por $lt(g) = x$ e desta forma o procedimento termina.

No caso de várias variáveis podemos ainda dividir por mais de um polinômio de cada vez, e desta forma o processo de redução acima pode ser estendido para incluir o caso mais geral.

Definição 1.3.4. Sejam f e $f_1,\ldots,f_s$ polinômios em $k[x_1,\ldots,x_n]$, com $f_i \neq 0$, $(1 \leq i \leq s)$, e seja $F = \{f_1,\ldots,f_s\}$. Dizemos que f é reduzido a h módulo F, e denotamos

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

se e somente se existem uma seqüência de índices $i_1,i_2,\ldots,i_t \in \{1,\ldots,s\}$ e uma seqüência de polinômios $h_1,\ldots,h_{t-1} \in k[x_1,\ldots,x_n]$ tais que

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Exemplo 1.3.5. Sejam $f_1 = yx - y$, $f_2 = y^2 - x \in Q[x,y]$ e seja *lex* a ordem escolhida com $y > x$. Seja $F = \{f_1,f_2\}$, $f = y^2x$. Então

$$f \xrightarrow{F}_{+} x,$$

uma vez que

$$y^2x \xrightarrow{f_1} y^2 \xrightarrow{f_2} x.$$

Definição 1.3.6. Um polinômio r é dito ***reduzido*** com respeito a um conjunto de polinômios não-nulos $F = \{f_1,...,f_s\}$ se $r = 0$ ou nenhuma outra potência presente em r é divisível por um dos $lt(f_i)$, $i = 1,..,s$. Ou seja, r não pode ser reduzido módulo F.

Definição 1.3.7. Se $f \xrightarrow{F}_+ r$ e r é reduzido com respeito a F, então chamamos r um ***resto de f com respeito a F***.

O processo de redução nos permite então definir um algoritmo para a divisão em $k[x_1,...,x_n]$. Dados $f, f_1,...,f_s \in k[x_1,...,x_n]$ com $f_i \neq 0$ $(1 \leq i \leq s)$, este algoritmo nos retorna quocientes $a_1,...,a_s \in k[x_1,...,x_n]$ e um resto $r \in k[x_1,...,x_n]$, tais que

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

A existência de tal algoritmo é dada abaixo:

Algoritmo 1.3.8 (Algoritmo da Divisão em $k[x_1,...,x_n]$). Fixe uma ordem de monômios $>$ em $\mathbb{Z}^n_{\geq 0}$ e seja $F = \{f_1,...,f_s\}$ um conjunto de polinômios em $k[x_1,...,x_n]$. Todo $f \in k[x_1,...,x_n]$ pode ser escrito como $f = a_1 f_1 + \cdots + a_s f_s + r$, onde a_i, $r \in k[x_1,...,x_n]$ e $r = 0$ ou r é uma combinação linear com coeficientes em k de monômios, nenhum dos quais é divisível por $lt(f_i)$, $i = 1,2,...,s$. Temos ainda que, se $a_i f_i \neq 0$ então

$$\text{multdeg}(f) \geq \text{multdeg}(a_i f_i).$$

Prova:

Provamos a existência de $a_1,...,a_s, r$ dando um algoritmo e mostrando que ele opera corretamente para qualquer entrada dada. O algoritmo é:

INPUT: $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ com $f_i \neq 0$,$(1 \leq i \leq s)$.

OUTPUT: $a_1, \ldots, a_s, r$ tal que $f = a_1 f_1 + \cdots + a_s f_s + r$ e r é reduzido com respeito a $\{f_1, \ldots, f_s\}$.

INICIALIZAÇÃO: $a_1 = 0, \ldots, a_s = 0$, $r = 0$, $h = f$.

WHILE $h \neq 0$ **DO**

$i = 1$

divisão_ocorreu = FALSE

WHILE $i \leq s$ **AND** *divisão_ocorreu* = FALSE **DO**

IF $lt(f_i)$ divide $lt(h)$ **THEN**

$$a_i = a_i + \frac{lt(h)}{lt(f_i)}$$

$$h = h - \frac{lt(h)}{lt(f_i)} f_i$$

divisão_ocorreu = TRUE

ELSE

$i = i + 1$

IF *divisão_ocorreu* = FALSE **THEN**

$r = r + \mathrm{lt}(h)$

$h = h - \mathrm{lt}(h)$

Para provarmos que o algoritmo funciona mostraremos inicialmente que

(1.3.1) $$f = a_1 f_1 + \cdots + a_s f_s + h + r$$

vale a qualquer instante. Isto claramente é verdadeiro para os valores iniciais de $a_1, \ldots, a_s$, h e r. Suponhamos que vale também em algum momento do algoritmo. Se no próximo passo algum $lt(f_i)$ divide $lt(h)$, então a igualdade

$$a_i f_i + h = (a_i + lt(h) / lt(f_i)) f_i + (h - (lt(h) / lt(f_i)) f_i)$$

mostra que $a_i f_i + h$ não se altera, já que todas as outras variáveis não são alteradas e portanto (1.3.1) é verdadeiro neste caso. Por outro lado, se $lt(f_i)$ não divide $lt(h)$ para $i = 1,2,...,s$, então embora h e r se alterem, a soma $h + r$ se mantém inalterada já que

$$h + r = (h - lt(h)) + (r + lt(h)),$$

e portanto também neste caso (1.3.1) é verdadeiro.

Temos ainda que provar que o algoritmo termina, e isto acontece quando $h = 0$. Nesta situação temos de (1.3.1) que

$$f = a_1 f_1 + ... + a_s f_s + r,$$

uma vez que os termos são adicionados a r somente quando não são divisíveis por $lt(f_i)$, para $i = 1,2,...,s$. Segue que r tem as propriedades desejadas quando o algoritmo termina.

Para ver que o algoritmo termina, observe que toda vez que redefinimos a variável h seu grau diminui (ou torna-se nulo). Para ver isto, suponhamos inicialmente que h é redefinido por

$$h' = h - \frac{lt(h)}{lt(f_i)} f_i;$$

pelo Lema 1.2.8 temos então

$$lt\left(\frac{lt(h)}{lt(f_i)} f_i\right) = \frac{lt(h)}{lt(f_i)} lt(f_i) = lt(h),$$

e portanto h e $(lt(h)/lt(f_i))f_i$ têm o mesmo termo líder. Logo a sua diferença deve ter grau estritamente menor quando $h' \neq 0$.

Suponhamos agora que $lt(f_i)$ não divide $lt(h)$ para $i = 1,2,...,s$. Então h é redefinido por

$$h' = h - lt(h)$$

e neste caso claramente o grau de h diminui, como no caso anterior. Suponhamos que o algoritmo nunca termine; teremos então uma seqüência decrescente infinita formada

pelos sucessivos graus de h' mas, como > é uma boa ordem, isto não pode ocorrer. Portanto $h = 0$ e o algoritmo termina.□

Exemplo 1.3.9. Queremos dividir $f = x^3y^3 + 2y^2$ por $f_1 = 2xy^2 + 3x + 4y^2$ e $f_2 = y^2 - 2y - 2$ usando a ordem lexicográfica com $x > y$. Listamos os divisores f_1 e f_2 e os quocientes a_1 e a_2. Temos:

a_1:

a_2:

$f_1 = 2xy^2 + 3x + 4y^2$ $\qquad$ $x^3y^3 + 2y^2$

$f_2 = y^2 - 2y - 2$

Os termos líderes de $lt(f_1) = 2xy^2$ e $lt(f_2) = y^2$ dividem $lt(f) = x^3y^3$. Como f_1 está listado primeiro utilizamos $lt(f_1) = 2xy^2$ para iniciar o processo de divisão. Desta forma, dividindo x^3y^3 por $2xy^2$, obtemos $\frac{1}{2}x^2y$. Subtraímos $\frac{1}{2}x^2y \cdot f_1$ de $x^3y^3 + 2y^2$ e obtemos:

a_1: $\frac{1}{2}x^2y$

a_2:

$f_1 = 2xy^2 + 3x + 4y^2$ $\qquad$ $x^3y^3 + 2y^2$

$\qquad\qquad\qquad\qquad\quad$ $x^3y^3 + \frac{3}{2}x^3y + 2x^2y^3$

$f_2 = y^2 - 2y - 2$ $\qquad$ ———————————

$\qquad\qquad\qquad\qquad\quad$ $-\frac{3}{2}x^3y - 2x^2y^3 + 2y^2$

Repetimos o mesmo processo, agora utilizando $-\frac{3}{2}x^3y - 2x^2y^3 + 2y^2$. Note agora que $lt\left(-\frac{3}{2}x^3y - 2x^2y^3 + 2y^2\right) = -\frac{3}{2}x^3y$ não é divisível por $lt(f_1)$ nem por $lt(f_2)$. Todavia $-\frac{3}{2}x^3y - 2x^2y^3 + 2y^2$ não é o resto da divisão, já que um dos seus termos $(-2x^2y^3)$ é

divisível por $lt(f_1)$ (por $lt(f_2)$ também, no entanto utilizamos sempre o que está listado primeiro !). Portanto movendo $-\frac{3}{2}x^3y$ para o resto podemos continuar.

Para implementar esta idéia criamos uma coluna chamada resto (r) à direita. Ao polinômio da coluna do centro damos o nome de ***dividendo intermediário***. Desta forma continuamos com o processo até que o *dividendo intermediário* seja zero.

Abaixo temos o passo onde $-\frac{3}{2}x^3y$ é movido para o resto (como indicado pela seta).

a_1: $\frac{1}{2}x^2y$

a_2:

$f_1 = 2xy^2 + 3x + 4y^2$	$x^3y^3 + 2y^2$		
	$x^3y^3 + \frac{3}{2}x^3y + 2x^2y^3$		
$f_2 = y^2 - 2y - 2$	———————		
	$-\frac{3}{2}x^3y - 2x^2y^3 + 2y^2$		
	———————		
	$-2x^2y^3 + 2y^2$	$\rightarrow$	$-\frac{3}{2}x^3y$

Agora continuamos do mesmo modo; se pudermos dividir por algum $lt(f_i)$, procedemos como o usual, caso contrário movemos o termo líder do *dividendo intermediário* para a coluna do resto. Na próxima página continuamos a divisão.

a_1: $\frac{1}{2}x^2y - xy + 2y$

a_2: $-8y - 14$

$f_1 = 2xy^2 + 3x + 4y^2$

$f_2 = y^2 - 2y - 2$

$x^3y^3 + 2y^2$

$x^3y^3 + \frac{3}{2}x^3y + 2x^2y^3$

$-\frac{3}{2}x^3y - 2x^2y^3 + 2y^2$

$-2x^2y^3 + 2y^2 \quad \rightarrow \quad -\frac{3}{2}x^3y$

$-2x^2y^3 - 3x^2y - 4xy^3$

$3x^2y + 4xy^3 + 2y^2$

$4xy^3 + 2y^2 \quad \rightarrow \quad -\frac{3}{2}x^3y + 3x^2y$

$4xy^3 + 6xy + 8y^3$

$-6xy - 8y^3 + 2y^2$

$-8y^3 + 2y^2 \quad \rightarrow \quad -\frac{3}{2}x^3y + 3x^2y - 6xy$

$-8y^3 + 16y^2 + 16y$

$-14y^2 - 16y$

$-14y^2 + 28y + 28$

$-44y - 28$

$-28 \quad \rightarrow \quad -\frac{3}{2}x^3y + 3x^2y - 6xy - 44y$

$0 \quad \rightarrow \quad -\frac{3}{2}x^3y + 3x^2y - 6xy - 44y - 28$

Portanto o resto é $r = -\frac{3}{2}x^3y + 3x^2y - 6xy - 44y - 28$ e obtivemos

$$x^3y^3 + 2y^2 = (\frac{1}{2}x^2y - xy + 2y).(2xy^2 + 3x + 4y^2) + (-8y - 14).(y^2 - 2y - 2) + r.$$

Observe que o resto é uma soma de monômios, nenhum dos quais é divisível por $lt(f_1)$ ou $lt(f_2)$.

1.4 Ideais Monomiais e Lema de Dickson

Nesta seção iremos determinar quando um dado polinômio $f \in k[x_1,...,x_n]$ pertence a um ideal I, onde I é um ideal monomial. Para isto faremos um estudo detalhado das propriedades de tais ideais e, em particular, mostraremos que os mesmos são finitamente gerados. Para isto definimos inicialmente ideais monomiais em $k[x_1,...,x_n]$.

Definição 1.4.1. Um ideal $I \subset k[x_1,...,x_n]$ é dito um ***ideal monomial*** se admite um conjunto de geradores constituído de monômios. Neste caso escrevemos

$$I = \langle x^\alpha \mid \alpha \in A \rangle,$$

onde A é um subconjunto de $\mathcal{Z}^n_{\geq 0}$ (possivelmente infinito).

Exemplo 1.4.2.

$I = \langle x, x^6y, y^2 \rangle \subset k[x, y]$ é um ideal monomial.

Iremos inicialmente caracterizar todos os monômios pertencentes a um dado ideal monomial.

Lema 1.4.3. Seja $I = \langle x^\alpha \mid \alpha \in A \rangle$ um ideal monomial. Então um monômio x^β está em I se e somente se é divisível por x^α para algum $\alpha \in A$.

Prova:

Se x^β é múltiplo de x^α para algum $\alpha \in A$, então $x^\beta \in I$ por definição de ideal.

Reciprocamente, se $x^\beta \in I$ então

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}, \text{ onde } h_i \in k[x_1,...,x_n] \text{ e } \alpha(i) \in A.$$

Se expandirmos cada h_i como uma combinação linear de monômios, podemos ver que todo termo no lado direito da equação é divisível por algum $x^{\alpha(i)}$. Logo o lado esquerdo x^{β} deve ter a mesma propriedade.□

Note que x^{β} é divisível por x^{α} quando existe algum $\gamma \in \mathbb{Z}^n_{\geq 0}$ tal que $x^{\beta} = x^{\alpha}x^{\gamma}$. Isto é equivalente a $\beta = \alpha + \gamma$ em $\mathbb{Z}^n_{\geq 0}$.

Portanto

$$\alpha + \mathbb{Z}^n_{\geq 0} = \left\{\alpha + \gamma \mid \gamma \in \mathbb{Z}^n_{\geq 0}\right\}$$

é o conjunto dos expoentes de todos os monômios divisíveis por x^{α}.

O lema a seguir nos permite determinar quando um dado polinômio pertence a um ideal monomial.

Lema 1.4.4. Sejam $I = \langle x^{\alpha} \mid \alpha \in A \rangle$ um ideal monomial e $f \in k[x_1,...,x_n]$. Então as seguintes afirmações são equivalentes:

(i) $f \in I$.

(ii) Todo termo de f está em I.

(iii) f é uma combinação k-linear de monômios de I.

Prova:

As implicações (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) são triviais e basta mostrar (i) $\Rightarrow$ (iii). Se $f \in I$ então

$$f = \sum_{i=1}^{s} h_i x^{\alpha(i)}, \text{onde } h \in k[x_1,...,x_n] \text{ e } \alpha(i) \in A.$$

Se expandirmos cada h_i como uma combinação linear de monômios, então todo termo no lado direito da equação é divisível por algum $x^{\alpha(i)}$, e portanto pertence a I. Logo f deve ser uma combinação k-linear de monômios de I.□

A seguir mostraremos que todo ideal monomial de $k[x_1,...,x_n]$ é finitamente gerado.

Teorema 1.4.5 (Lema de Dickson). Se I é um ideal gerado por um conjunto A de monômios, então I é também gerado por um subconjunto finito de A.

Prova:

Por indução em n, o número de variáveis.

Para $n = 1$ temos que $I = \left\langle x_1^{\alpha} \mid \alpha \in A \subset \mathbb{Z}_{\geq 0} \right\rangle$. Seja β o menor elemento de $A \subset \mathbb{Z}_{\geq 0}$, ou seja, $x_1^{\beta} < x_1^{\alpha}$ para todo $\alpha \in A$, $\alpha \neq \beta$. Segue-se que x_1^{β} divide todos os outros geradores x_1^{α} e portanto $I = \left\langle x_1^{\beta} \right\rangle$.

Suponhamos o teorema válido para $n - 1$.

Para n escrevemos as variáveis como sendo $x_1,...,x_{n-1},y$, de forma que os monômios em $k[x_1,...,x_{n-1},y]$ podem ser escritos como $x^{\alpha}y^{m}$, onde $\alpha = (\alpha_1,...,\alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ e $m \in \mathbb{Z}_{\geq 0}$.

Suponhamos que $I \subset k[x_1,...,x_{n-1},y]$ é um ideal monomial.

Seja $J = \left\langle x^{\alpha} \mid x^{\alpha}y^{m} \in I \text{ para algum } m \geq 0 \right\rangle \subset k[x_1,...,x_{n-1}]$. Como J é um ideal monomial em $n - 1$ variáveis, nossa hipótese de indução implica que J é finitamente gerado por monômios, digamos $J = \left\langle x^{\alpha(1)},...,x^{\alpha(s)} \right\rangle$. Podemos ver J como a projeção de I sobre $k[x_1,...,x_{n-1}]$.

Por definição de J, temos que $x^{\alpha(i)}y^{m_i} \in I$, para algum $m_i \geq 0$ e $1 \leq i \leq s$. Seja m o maior entre os m_i. Então para cada l entre 0 e m, considere o ideal $J_l = \left\langle x^{\beta} \mid x^{\beta}y^{l} \in I \right\rangle \subset k[x_1,...,x_{n-1}]$. Podemos pensar em J_l como sendo uma "fatia" de I gerada por monômios contendo y na l-ésima potência. Usando nossa hipótese de indução, J_l é finitamente gerado por um conjunto de monômios, digamos $J_l = \left\langle x^{\alpha_l(1)},...,x^{\alpha_l(s_l)} \right\rangle$.

Afirmamos que I é gerado pelos monômios na lista abaixo:

$$\begin{aligned}
&\text{de } J\text{: } && x^{\alpha(1)}y^m,\ldots,x^{\alpha(s)}y^m \\
&\text{de } J_0\text{: } && x^{\alpha_0(1)},\ldots,x^{\alpha_0(s_0)} \\
&\text{de } J_1\text{: } && x^{\alpha_1(1)}y,\ldots,x^{\alpha_1(s_1)}y \\
&\qquad\vdots \\
&\text{de } J_{m-1}\text{: } && x^{\alpha_{m-1}(1)}y^{m-1},\ldots,x^{\alpha_{m-1}(s_{m-1})}y^{m-1}.
\end{aligned}$$

Para ver isto, seja $x^\alpha y^q \in I$. Temos então:

(i) $q \geq m$. Então $x^\alpha y^q$ é divisível por algum $x^{\alpha(i)}y^m$, pela construção de J.

(ii) $q \leq m-1$. Então $x^\alpha y^q$ é divisível por algum $x^{\alpha(i)}y^q$, pela construção de J_q.

Seja B o conjunto de todos os monômios da lista acima; como todo monômio de I é divisível por algum elemento de B, o ideal gerado por B contém todos os monômios de I.

Desta forma (pelo Lema 1.4.4) qualquer polinômio $f \in I$ está no ideal gerado pelos elementos de B (a reciproca é trivial, já que todo elemento de B está em I).

Para completar a prova, iremos mostrar que o conjunto finito de geradores pode ser escolhido dentro de um dado conjunto de geradores (possivelmente infinito) de um ideal. Para isto considere as variáveis como sendo $x_1,\ldots,x_n$ e o ideal monomial $I = \langle x^\alpha \mid \alpha \in A \rangle \subset k[x_1,\ldots,x_n]$.

Queremos mostrar que I é gerado por um número finito de monômios x^α, onde $\alpha \in A$.

Acima vimos que $I = \langle x^{\beta(1)},\ldots,x^{\beta(s)} \rangle$ para alguns $x^{\beta(i)} \in I$. Como $x^{\beta(i)} \in I$ temos, pelo Lema 1.4.3, que $x^{\beta(i)}$ é divisível por algum $x^{\alpha(i)}$, onde $\alpha(i) \in A$, e portanto

$$x^{\beta(i)} = h_i x^{\alpha(i)}, \text{ onde } h_i \in k[x_1,\ldots,x_n] \text{ para } i = 1,2,\ldots,s.$$

Dado $f \in I$, podemos escrever

$$f = \sum_{i=1}^{s} a_i x^{\beta(i)} = \sum_{i=1}^{s} (a_i h_i) x^{\alpha(i)} \text{ onde } a_i, h_i \in k[x_1,\ldots,x_n],$$

e portanto $f \in \langle x^{\alpha(1)},\ldots,x^{\alpha(s)} \rangle$. □

1.5 Teorema da base de Hilbert e Bases de Groebner

Nesta seção daremos a solução completa para o problema da descrição de um ideal, i.e., seremos capazes de identificar quando um dado polinômio $f \in k[x_1,...,x_n]$ pertence a um ideal I de $k[x_1,...,x_n]$. Nosso estudo nos guiará a bases de ideais com "boas" propriedades relativas ao algoritmo da divisão (bases de Groebner). A idéia chave é que uma vez escolhida uma ordem de monômios, todo $f \in k[x_1,...,x_n]$ terá um único termo líder $lt(f)$. Então para um ideal I podemos definir seu ideal de termos líderes como segue.

Definição 1.5.1. Seja $I \subset k[x_1,...,x_n]$ um ideal não nulo.

(i) Denotamos por $lt(I)$ o conjunto dos termos líderes de elementos de I. Desta forma

$$lt(I) = \left\{ cx^\alpha \mid lt(f) = cx^\alpha \text{ para algum } f \in I \right\}.$$

(ii) Denotamos por $\langle lt(I) \rangle$ o ideal gerado pelos elementos de $lt(I)$.

Dado um conjunto finito de geradores de um ideal I, digamos $I = \langle f_1,...,f_s \rangle$, observamos que $\langle lt(f_1),...,lt(f_s) \rangle$ e $\langle lt(I) \rangle$ podem ser ideais diferentes. Por definição temos $lt(f_i) \in lt(I) \subset \langle lt(I) \rangle$, portanto $\langle lt(f_1),...,lt(f_s) \rangle \subset \langle lt(I) \rangle$. Todavia $\langle lt(I) \rangle$ pode ser estritamente maior, como mostra o exemplo a seguir.

Exemplo 1.5.2. Seja $I = \langle f_1, f_2 \rangle$, onde $f_1 = x^2y^2 + 2xy + y$ e $f_2 = x^4y + 2xy + x$, e considere a ordem lexicográfica com $x > y$ em $k[x,y]$. Então, como

$$2x^3y + x^2y - 2xy^2 - xy = x^2(x^2y^2 + 2xy + y) - y\,(x^4y + 2xy + x)\,,$$

temos que $2x^3y + x^2y - 2xy^2 - xy \in I$. Desta forma $lt(2x^3y + x^2y - 2xy^2 - xy) = 2x^3y \in \langle lt(I) \rangle$. No entanto $2x^3y$ não é divisível por $lt(f_1) = x^2y^2$ nem por $lt(f_2) = x^4y$, e portanto de acordo com o Lema 1.4.3, $2x^3y \notin \langle lt(f_1), lt(f_2) \rangle$.

Mostraremos agora que $\langle lt(I) \rangle$ é um ideal monomial. Isto nos permitirá utilizar os resultados da seção anterior; em particular mostraremos que $\langle lt(I) \rangle$ será finitamente gerado por termos líderes de I.

Proposição 1.5.3. Seja $I \subset k[x_1,...,x_n]$ um ideal.

(i) $\langle lt(I) \rangle$ é um ideal monomial.

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

Prova:

(i) Os monômios líderes $lm(g)$ de elementos de $g \in I - \{0\}$ geram o ideal monomial $\langle lm(g) \mid g \in I - \{0\} \rangle$. Como $lm(g)$ e $lt(g)$ diferem por uma constante não nula, temos $\langle lm(g) \mid g \in I - \{0\} \rangle = \langle lt(g) \mid g \in I - \{0\} \rangle = \langle lt(I) \rangle$. Portanto $\langle lt(I) \rangle$ é um ideal monomial.

(ii) Como $\langle lt(I) \rangle$ é gerado por monômios $lm(g)$ para $g \in I - \{0\}$, o Lema de Dickson nos diz que $\langle lt(I) \rangle = \langle lm(g_1),..., lm(g_s) \rangle$ para um número finito de $g_1,...,g_s \in I$. Mais uma vez, como $lm(g_i)$ difere de $lt(g_i)$ por uma constante não nula, temos

$$\langle lt(I) \rangle = \langle lt(g_1) ,..., lt(g_s) \rangle. \square$$

Com o uso da proposição anterior e do algoritmo da divisão podemos provar a existência de um conjunto finito de geradores para todo ideal polinomial.

Seja $I \subset k[x_1,...,x_n]$ um ideal e $\langle lt(I) \rangle$ o ideal gerado pelos termos líderes de elementos de I. Selecionamos também uma ordem de monômios para uso no algoritmo da divisão e para computar os termos líderes.

Teorema 1.5.4 (Teorema da base de Hilbert). Todo ideal $I \subset k[x_1,...,x_n]$ tem um conjunto finito de geradores, isto é, $I = \langle g_1,...,g_s \rangle$ para certos $g_1,...,g_s \in I$.

Prova:

Se $I = \{0\}$ então tomamos $\{0\}$ como conjunto gerador, o qual é finito.

Se I contém algum polinômio não nulo então podemos construir um conjunto de geradores $g_1,...,g_s$ como segue. Pela Proposição 1.5.3 existem $g_1,...,g_s \in I$ tais que $\langle lt(I) \rangle = \langle lt(g_1),..., lt(g_s) \rangle$. Afirmamos que $I = \langle g_1,...,g_s \rangle$. É óbvio que $\langle g_1,...,g_s \rangle \subset I$, já que cada $g_i \in I$, $i = 1,2,...,s$.

Reciprocamente, seja $f \in I$ um polinômio qualquer. Dividindo f por $g_1,...,g_s$ obtemos uma expressão da forma

$$f = a_1 g_1 + ... + a_s g_s + r,$$

onde nenhum termo de r é divisível por $lt(g_1),..., lt(g_s)$. Afirmamos que $r = 0$. Para isto note que

$$r = f - a_1 g_1 - \cdots - a_s g_s \in I.$$

Se $r \neq 0$ então $\langle lt(r) \rangle \in \langle lt(I) \rangle = \langle lt(g_1),..., lt(g_s) \rangle$ e pelo Lema 1.4.3, $lt(r)$ deve ser divisível por algum $lt(g_i)$. Isto contradiz o fato de r ser o resto da divisão de f por $g_1,...,g_s$ e portanto r deve ser zero. Desta forma

$$f = a_1 g_1 + \cdots + a_s g_s \in \langle g_1,...,g_s \rangle,$$

o que mostra que $I \subset \langle g_1,...,g_s \rangle$.□

Na prova do Teorema 1.5.4 a base $\{g_1,...,g_s\}$ do ideal I possui uma propriedade especial, a saber

$$\langle lt(I)\rangle = \langle lt(g_1),...,lt(g_s)\rangle.$$

Como foi visto no exemplo 1.5.2, nem todas as bases de um ideal possuem tal propriedade. A estas bases especiais que satisfazem tal propriedade damos o seguinte nome:

Definição 1.5.5. Fixe uma ordem de monômios. Um subconjunto finito $G = \{g_1,...,g_s\}$ de um ideal I é dito uma ***base de Groebner*** de I se

$$\langle lt(I)\rangle = \langle lt(g_1),..., lt(g_s)\rangle.$$

Do Lema 1.4.3 temos que um conjunto $\{g_1,...,g_s\} \subset I$ é uma base de Groebner se e somente se o termo líder de qualquer elemento de I é divisível por um dos $lt(g_i)$.

Corolário 1.5.6. Fixe uma ordem de monômios. Então todo ideal $I \subset k[x_1,...,x_n]$ tem uma base de Groebner. Temos ainda que qualquer base de Groebner de I é uma base de I.

Prova:

Dado um ideal não nulo, o conjunto $G = \{g_1,...,g_s\}$ construído na prova do Teorema 1.5.4 é uma base de Groebner por definição.

Para a segunda afirmativa, note que se $\langle lt(I)\rangle = \langle lt(g_1),..., lt(g_s)\rangle$ então o argumento dado no Teorema 1.5.4 mostra que $I = \langle g_1,...,g_s\rangle$ e portanto G é uma base de Groebner de I.□

Bases de Groebner de ideais em anéis de polinômios foram introduzidos em 1965 por B.Buchberger e assim denominadas por ele em homenagem ao orientador da sua tese, W.Gröbner (1899-1980).

Abaixo temos uma aplicação para o Teorema da base de Hilbert.

Teorema 1.5.7 (Condição da Cadeia Ascendente). Se $I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq I_n \subseteq ...$ é uma cadeia ascendente de ideais de $k[x_1,...,x_n]$, então existe N tal que $I_N = I_{N+1} = I_{N+2} = ...$

Prova:

Seja $I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq I_n \subseteq ...$ uma cadeia ascendente de ideais de $k[x_1,...,x_n]$ e seja $I = \bigcup_{n=1}^{\infty} I_n$. Afirmamos que I é um ideal.

(1) $0 \in I_n$, $\forall n = 1,2,...,$ logo $0 \in I$.

(2) Sejam $a,b \in I$, logo existem $l,k \in \mathbb{N}$ tais que $a \in I_k$ e $b \in I_l$. Como os ideais formam uma cadeia ascendente podemos, sem perda de generalidade, supor $I_k \subseteq I_l$ e portanto $a,b \in I_l$; portanto por definição de ideal temos $a + b \in I_l \subset I$.

(3) Sejam $a \in I$ e $h \in k[x_1,...,x_n]$. Existe portanto $l \in \mathbb{N}$ tal que $a \in I_l$ e, como I_l é ideal de $k[x_1,...,x_n]$, temos que $ha \in I_l \subseteq I$.

Temos então do Teorema da base de Hilbert que existem $f_1,..,f_s \in k[x_1,...,x_n]$ tais que $I = \langle f_1,...,f_s \rangle$. Como $f_i \in I$, existe N_i tal $f_i \in I_{N_i}$. Seja $N = \max\{N_i \mid i = 1,2,...,s\}$, então $f_i \in I_N$, para todo $i = 1,2,...,s$, e portanto $I \subseteq I_N$. □

A condição da cadeia ascendente (ACC) é equivalente ao Teorema da base de Hilbert. De fato mostramos acima que o Teorema da base de Hilbert implica a condição da cadeia ascendente. Por outro lado suponhamos que exista I um ideal de $k[x_1,...,x_n]$ o qual não é finitamente gerado e seja $f_1 \in I$. Como I não é finitamente gerado, deve existir

$f_2 \in I$ tal que $f_2 \notin \langle f_1 \rangle$ e desta forma $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle$. Continuando desta maneira temos uma cadeia estritamente ascendente de ideais de $k[x_1,\ldots,x_n]$, contradizendo a condição da cadeia ascendente.

1.6 Propriedades das Bases de Groebner

Como visto anteriormente todo ideal em $k[x_1,...,x_n]$ possui uma base de Groebner. Nesta seção estudaremos as propriedades das bases de Groebner e como identificar quando uma dada base de um ideal é base de Groebner. Para começar mostraremos que o resto obtido no algoritmo da divisão é único quando dividimos por uma base de Groebner.

Proposição 1.6.1. Seja $G = \{g_1,...,g_s\}$ uma base de Groebner de um ideal $I \subset k[x_1,...,x_n]$ e seja $f \in k[x_1,...,x_n]$. Então existe um único $r \in k[x_1,...,x_n]$ com as seguintes propriedades:

(i) Nenhum termo de r é divisível por $lt(g_1)$,... ou $lt(g_s)$.

(ii) Existe $g \in I$ tal que $f = g + r$.

Em particular, r é o resto da divisão de f por G, não importando a maneira como os elementos de G são listados no algoritmo da divisão.

Prova:

O algoritmo da divisão nos dá $f = a_1g_1 + \cdots + a_sg_s + r$, onde r satisfaz (i). Podemos também satisfazer (ii) simplesmente fazendo $g = a_1g_1 + \cdots + a_sg_s \in I$. Isto prova a existência de r.

Para provar a unicidade suponhamos que $f = g_1 + r_1 = g_2 + r_2$ satisfaça (i) e (ii). Então $r_2 - r_1 = g_1 - g_2 \in I$ e portanto, se $r_2 \neq r_1$, então $lt(r_2 - r_1) \in \langle lt(I) \rangle = \langle lt(g_1),..., lt(g_s) \rangle$. Pelo Lema 1.4.3, temos que $lt(r_2 - r_1)$ é divisível por algum $lt(g_i)$. Isto é impossível uma vez que nenhum termo de r_1, r_2 é divisível por $lt(g_1)$,... ou $lt(g_s)$. Logo $r_1 - r_2$ deve ser zero e portanto $r_1 = r_2$. A afirmação final da proprosição segue da unicidade de r. □

Embora o resto r seja único, mesmo para bases de Groebner os "quocientes" a_i produzidos pelo algoritmo de divisão em $f = a_1 g_1 + \cdots + a_s g_s + r$ podem mudar se listarmos os geradores em uma ordem diferente.

Como corolário, temos o seguinte critério para determinar quando um polinômio está em um ideal.

Corolário 1.6.2. Seja $G = \{g_1,\ldots,g_s\}$ uma base de Groebner de um ideal $I \subset k[x_1,\ldots,x_n]$ e seja $f \in k[x_1,\ldots,x_n]$. Então $f \in I$ se e somente se o resto da divisão de f por G é zero.

Prova:

Se o resto é zero então $f = a_1 g_1 + \cdots + a_s g_s \in I$.

Reciprocamente, dado $f \in I$ então $f = f + 0$ satisfaz as duas condições da proposição anterior. Segue portanto que 0 é o resto da divisão de f por G.□

Usando o Corolário 1.6.2 obtemos um algoritmo que nos permite identificar quando um polinômio $f \in k[x_1,\ldots,x_n]$ pertence a um dado ideal $I \subset k[x_1,\ldots,x_n]$: supondo conhecida uma base de Groebner G do ideal I, basta computar o resto de f com respeito a divisão por G.

A seguir discutimos quando um dado conjunto de geradores de um ideal é uma base de Groebner. Um conjunto $\{f_1,\ldots,f_s\}$ só não será base de Groebner se ocorrerem combinações dos f_i's tais que os termos líderes destas combinações não estejam no ideal gerado por $lt(f_i)$.

Uma forma em que isto pode ocorrer é os termos líderes em uma combinação da forma

$$ax^{\alpha} f_i - bx^{\beta} f_j$$

cancelarem-se, deixando apenas termos menores (com relação à ordem adotada). Por outro lado $ax^{\alpha}f_i - bx^{\beta}f_j \in I$, logo seu termo líder está em $lt(I)$. Para estudar este fenômeno de cancelamento introduzimos tipos especiais de combinações.

Definição 1.6.3. Sejam $f, g \in k[x_1,...,x_n]$ polinômios não nulos.

(i) Se multdeg $(f) = \alpha$ e multdeg $(g) = \beta$, tomamos $\gamma = (\gamma_1,...,\gamma_n)$, onde $\gamma_i = \max(\alpha_i,\beta_i)$ para cada $i = 1,2,...,n$. Chamamos x^{γ} o ***mínimo múltiplo comum*** de $lm(f)$ e $lm(g)$, e escrevemos $x^{\gamma} = \mathbf{LCM}(lm(f), lm(g))$.

(ii) O S-polinômio de f e g é a combinação

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

Exemplo 1.6.4. Sejam $f = x^2y^2 + x^3 + xy^2 + 2x$, $g = x^4y^2 + x^5 + 2xy \in k[x,y]$, e considere a ordem lexicográfica graduada com $x > y$. Então $\gamma = (4,2)$ e

$$S(f,g) = \frac{x^4y^2}{x^2y^2}(x^2y^2 + x^3 + xy^2 + 2x) - \frac{x^4y^2}{x^4y^2}(x^4y^2 + x^5 + 2xy)$$

$$= x^2(x^2y^2 + x^3 + xy^2 + 2x) - (x^4y^2 + x^5 + 2xy)$$

$$= x^3y^2 + 2x^3 - 2xy.$$

Um S-polinômio $S(f, g)$ é definido de modo a produzir cancelamento de termos líderes. O seguinte lema mostra que todo cancelamento de termos líderes entre polinômios de mesmo grau resulta deste tipo de cancelamento.

Lema 1.6.5. Considere uma soma $\sum_{i=1}^{s} c_i f_i$, onde $c_i \in k$ e multdeg $(f_i) = \delta \in Z_{\geq 0}^n$ para todo $i = 1,2,...,s$. Se multdeg $\left(\sum_{i=1}^{s} c_i f_i\right) < \delta$, então $\sum_{i=1}^{s} c_i f_i$ é uma combinação linear com

coeficientes em k dos S-polinômios $S(f_j, f_k)$, para $1 \leq j, k \leq s$. Além disto, cada $S(f_j, f_k)$ tem grau $< \delta$.

Prova :

Seja $d_i = lc(f_i)$, de forma que $c_i d_i$ é o coeficiente líder de $c_i f_i$. Como $c_i f_i$ tem multdeg $(c_i f_i) = \delta$ e a soma tem grau estritamente menor, segue que $\sum_{i=1}^{s} c_i d_i = 0$.

Definimos $p_i = \frac{f_i}{d_i}$, e observamos que p_i tem coeficiente líder igual a 1. Consideramos a soma telescópica

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

Por construção, $lt(f_i) = d_i x^\delta$, logo $\mathbf{LCM}(lm(f_j), lm(f_k)) = x^\delta$ e portanto

$$S(f_j, f_k) = \frac{x^\delta}{lt(f_j)} f_j - \frac{x^\delta}{lt(f_k)} f_k = \frac{x^\delta}{d_j x^\delta} f_j - \frac{x^\delta}{d_k x^\delta} f_k = p_j - p_k . \tag{1.6.1}$$

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

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

a qual é uma soma da forma desejada. Como p_j e p_k têm grau igual a δ e coeficiente líder 1, $p_j - p_k$ tem grau $< \delta$. Pela equação (1.6.1), o mesmo vale para $S(f_j, f_k)$, e o lema está provado.□

Usando S-polinômios e o Lema 1.6.5, provamos o seguinte critério de Buchberger para determinar quando uma base de um ideal é uma base de Groebner.

Teorema 1.6.6. Seja I um ideal polinomial. Então a base $G = \{g_1, \ldots, g_s\}$ de I é uma base de Groebner de I se e somente se o resto da divisão de $S(g_i, g_j)$ por G (listados em alguma ordem) é zero, para todos pares $i \neq j$.

Prova:

Se G é uma base de Groebner de I, então como $S(g_i,g_j) \in I$, temos pelo Corolário 1.6.2 que o resto da divisão de $S(g_i,g_j)$ por G é igual a zero.

Reciprocamente, seja $f \in I$, $f \neq 0$. Queremos mostrar que se todos os S-polinômios têm resto zero na divisão por G, então $lt(f) \in \langle lt(g_1),...,lt(g_s)\rangle$, ou seja, G é uma base de Groebner de I.

Dado $f \in I = \langle g_1,...,g_s\rangle$, existem polinômios $h_i \in k[x_1,...,x_n]$ tais que

$$f = \sum_{i=1}^{s} h_i g_i \tag{1.6.1}$$

e, pelo Lema 1.2.8, temos

$$\text{multdeg}(f) \leq \max_{1 \leq i \leq s} \{\text{multdeg}(h_i g_i)\}. \tag{1.6.2}$$

Se a igualdade não ocorre, então deve ocorrer um cancelamento dos termos líderes. Pelo Lema 1.6.5 podemos escrever isto em termos de S-polinômios. Desta forma nossa hipótese de que os S-polinômios têm resto zero irá nos permitir uma expressão para f com menos cancelamentos. Prosseguindo obteremos eventualmente uma expressão para f tal que

$$\text{multdeg}(f) = \text{multdeg}(h_i g_i)$$

para algum i, e segue que $lt(f)$ é divisível por $lt(g_i)$. Isto irá mostrar portanto que $lt(f) \in \langle lt(g_1),...,lt(g_s)\rangle$, e nossa prova estará completa.

Sejam $f = \sum_{i=1}^{s} h_i g_i$ e $m_i = \text{multdeg}\,(h_i g_i)$. Definindo $\delta = \max\{m_1,...,m_s\}$, temos

$$\text{multdeg}(f) \leq \delta.$$

Considere agora todos os possíveis modos de escrever f como em (1.6.1). Para cada maneira temos possivelmente um δ diferente, mas como a nossa ordem de monômios é uma boa ordem, podemos escolher uma expressão para f tal que δ é mínimo. Basta

mostrar que para este δ mínimo escolhido, temos multdeg $(f) = \delta$, pois então vale a igualdade em (1.6.2) e em consequência temos que $lt(f) \in \langle lt(g_1),...,lt(g_s)\rangle$.

Provaremos agora, por contradição, que multdeg $(f) = \delta$. Para isto supomos que multdeg $(f) < \delta$ e escrevemos f como

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i$$

$$= \sum_{m(i)=\delta} lt(h_i) g_i + \sum_{m(i)=\delta} (h_i - lt(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i . \qquad (1.6.3)$$

A segunda e a terceira parcela tem grau menor que δ. Como multdeg$(f) < \delta$, decorre que multdeg$\left(\sum_{m(i)=\delta} lt(h_i) g_i\right) < \delta$.

Seja $lt(h_i) = c_i x^{\alpha(i)}$; então $\sum_{m(i)=\delta} lt(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ tem a forma descrita no Lema 1.6.5, onde $f_i = x^{\alpha(i)} g_i$, e portanto este cancelamento pode ser escrito como uma combinação linear de S-polinômios. Temos também que

$$S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) = \frac{x^{\delta}}{x^{\alpha(j)} lt(g_j)} x^{\alpha(j)} g_j - \frac{x^{\delta}}{x^{\alpha(k)} lt(g_k)} x^{\alpha(k)} g_k$$

$$= x^{\delta - \gamma_{jk}} S(g_j, g_k),$$

onde $x^{\gamma_{jk}} = \mathbf{LCM}(lm(g_j), lm(g_k))$.

Portanto existem constantes $c_{jk} \in k$ tais que

$$\sum_{m(i)=\delta} lt(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k). \qquad (1.6.4)$$

O próximo passo é usar nossa hipótese que o resto de $S(g_j, g_k)$ na divisão por $g_1,...,g_s$ é zero. Utilizando o algoritmo da divisão (Algoritmo 1.3.8), isto significa que cada polinômio $S(g_j, g_k)$ pode ser escrito na forma

$$S(g_j, g_k) = \sum_{i=1}^{s} a_{ijk} g_i, \text{ onde } a_{ijk} \in k[x_1,..,x_n].$$

O algoritmo da divisão nos diz ainda que

$$\text{multdeg}\,(a_{ijk} g_i) \leq \text{multdeg}\,(S(g_j, g_k)), \text{ para todo } i,j,k.$$

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

$$x^{\delta-\gamma_{jk}}S(g_j,g_k) = \sum_{i=1}^{s} b_{ijk}g_i, \text{ onde } b_{ijk} = x^{\delta-\gamma_{jk}}a_{ijk},$$

e pelo Lema 1.6.5 temos

(1.6.5) $$\text{multdeg}\,(b_{ijk}g_i) \leq \text{multdeg}\,(x^{\delta-\gamma_{jk}}S(g_j,g_k)) < \delta.$$

Substitundo esta expressão em (1.6.4) obtemos

$$\sum_{m(i)=\delta} lt(h_i)g_i = \sum_{j,k} c_{jk}x^{\delta-\gamma_{jk}}S(g_j,g_k) = \sum_{j,k} c_{jk}\left(\sum_{i=1}^{s} b_{ijk}g_i\right)$$

$$= \sum_{i=1}^{s} \tilde{h}_i g_i$$

e, de acordo com (1.6.5), temos que multdeg $(\tilde{h}_i g_i) < \delta$.

Finalmente substituimos $\sum_{m(i)=\delta} lt(h_i)g_i = \sum_{i=1}^{s} \tilde{h}_i g_i$ em (1.6.3) para obter uma expressão para f como combinação de polinômios g_i, todos com grau menor que δ, contradizendo a minimalidade de δ. □

O Teorema 1.6.6 é um dos resultados chave na teoria de bases de Groebner e com ele é fácil identificar quando uma dada base é base de Groebner. Como será visto na próxima seção, ele nos guiará de maneira natural à construção de um algoritmo para computar a base de Groebner de um ideal $I \subset k[x_1,\ldots,x_n]$.

1.7 Algoritmo de Buchberger

No Corolário 1.5.6 mostramos que todo ideal não nulo em $k[x_1,...,x_n]$ possui base de Groebner. Nesta seção apresentamos um algoritmo para computar uma base de Groebner de um ideal $I \subset k[x_1,...,x_n]$.

A idéia chave é tentar expandir o conjunto original de geradores a uma base de Groebner, adicionando mais polinômios em I. Que geradores devemos adicionar?

De acordo com o Teorema 1.6.6, parece natural estender o conjunto original de geradores adicionando os restos não nulos de $S(f_i, f_j)$ na divisão por F, onde F é o conjunto de geradores (possívelmente já estendido) em um determinado instante.

Temos desta forma o seguinte algoritmo para computar bases de Groebner de um ideal polinomial.

Algoritmo 1.7.1. Seja $I = \langle f_1,...,f_s \rangle \neq \{0\}$ um ideal polinomial. Então uma base de Groebner de I pode ser construída em um número finito de passos através do seguinte algoritmo.

INPUT: $F =: \{f_1,...,f_s\}$

OUTPUT: Uma base de Groebner $G = \{g_1,...,g_t\}$ de I com $F \subseteq G$.

$G := F$

REPEAT

$G' := G$

Para cada par {p,q}, $p \neq q$, em G' DO

$S :=$ resto da divisão de $S(p,q)$ por G'

IF $S \neq 0$ THEN $G =: G \cup \{S\}$

UNTIL $G = G'$

Prova:

Se $G = \{g_1,...,g_t\}$, então $\langle G \rangle$ e $\langle lt(G) \rangle$ irão denotar os seguintes ideais:

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

$$\langle lt(G) \rangle = \langle lt(g_1),...,lt(g_t) \rangle.$$

Vamos primeiramente mostrar que $G \subset I$ em qualquer estágio do algoritmo. Para os valores iniciais a afirmativa é óbvia, e toda vez que aumentamos G fazemos isto adicionando o resto de $S(p,q)$ na divisão por G', onde $p, q \in G$. Desta forma, se $G \subset I$ então p, q e portanto $S(p,q)$ estão em I , e como estamos dividindo por $G' \subset I$, temos que $G \cup \{S\} \subset I$. Note também que G contém a base F dada e portanto G é uma base de I.

O algoritmo termina quando $G = G'$, o que significa que $S(p,q) \xrightarrow{G}_+ 0$ para qualquer $p, q \in G$. Logo pelo Teorema 1.6.6, G é uma base de Groebner de $\langle G \rangle = I$.

Temos que provar ainda que o algoritmo termina. Para isto consideramos o que acontece após a passagem pelo *loop* principal. O conjunto G consiste de G' (o velho G) juntamente com os restos não nulos dos S-polinômios de elementos de G'. Então

$$\langle lt(G') \rangle \subset \langle lt(G) \rangle, \tag{1.7.1}$$

já que $G' \subset G$. Ainda, se $G' \neq G$ afirmamos que $\langle lt(G') \rangle$ é estritamente menor que $\langle lt(G) \rangle$. Para ver isto suponha que um resto $r \neq 0$ de um S-polinômio tenha sido adicionado a G. Já que r é o resto da divisão por G', $lt(r)$ não é divisível por nenhum dos termos líderes de elementos de G', e desta forma $lt(r) \notin \langle lt(G') \rangle$. Mas $lt(r) \in \langle lt(G) \rangle$, o que prova a nossa afirmativa.

Por (1.7.1) os ideais $\langle lt(G') \rangle$ das sucessivas iterações do *loop* formam uma cadeia ascendente de ideais em $k[x_1,...,x_n]$. Desta forma a ***condição da cadeia ascendente***

implica que ao final de um número finito de iterações a cadeia estabiliza, de forma que $\langle lt(G') \rangle = \langle lt(G) \rangle$. Isto implica que $G' = G$, e portanto o algoritmo termina.□

O Algoritmo 1.7.1 é apenas uma versão rudimentar do algoritmo de Buchberger e não é prático do ponto de visto computacional. Note, por exemplo, que uma vez que o resto de $S(p, q)$ na divisão por G' é zero, ele permanecerá zero mesmo se adicionarmos mais elementos a G'. Desta forma não há razão para computá-lo novamente através do *loop* principal.

Bases de Groebner computadas através do Algoritmo 1.7.1 são, em geral, maiores que o necessário. De fato podemos eliminar alguns geradores não necessários utilizando o lema a seguir.

Lema 1.7.2. Seja G uma base de Groebner do ideal I. Seja $p \in G$ um polinômio tal que $lt(p) \in \langle lt(G - \{p\}) \rangle$. Então $G - \{p\}$ é também base de Groebner de I.

Prova:

Por definição de base de Groebner, temos que $\langle lt(G) \rangle = \langle lt(I) \rangle$. Se $lt(p) \in \langle lt(G - \{p\}) \rangle$, então $lt(G - \{p\}) = lt(G)$. Por definição, segue que $G - \{p\}$ é também uma base de Groebner de I. □

Ajustando constantes de modo a tornar todos os coeficientes líderes iguais a 1 e removendo de G qualquer p tal que $lt(p) \in \langle lt(G - \{p\}) \rangle$, obtemos o que denominamos uma base de Groebner mínima.

Definição 1.7.3. Uma ***base de Groebner mínima*** de um ideal polinomial I é uma base de Groebner G de I tal que:

(i) $lc(p) = 1$ para todo $p \in G$.

(ii) Para todo $p \in G$, $lt(p) \notin \langle lt(G - \{p\}) \rangle$.

Lema 1.7.4. Fixe uma ordem de monômios, e sejam G e $\tilde{G}$ duas bases de Groebner mínimas de um ideal I. Então

$$lt(G) = lt(\tilde{G}).$$

Prova:

Seja $g \in G$. Como G e $\tilde{G}$ são bases de Groebner mínimas de I temos que $g \xrightarrow{\tilde{G}}_+ 0$, e portanto existe $\tilde{g} \in \tilde{G}$ tal que $lt(\tilde{g})$ divide $lt(g)$, pois caso contrário $lt(g)$ estaria no resto da divisão de g por $\tilde{G}$.

Da mesma forma temos que $\tilde{g} \xrightarrow{G}_+ 0$ e portanto existe $g' \in G$ tal que $lt(g')$ divide $lt(\tilde{g})$. Temos então que $lt(g')$ divide $lt(g)$, onde $g, g' \in G$. Como G é uma base de Groebner mínima devemos ter $g = g'$. Logo $lt(\tilde{g})$ divide $lt(g)$ e $lt(g)$ divide $lt(\tilde{g})$, o que implica $lt(g) = lt(\tilde{g})$.

Desta forma, para todo elemento $g \in G$ existe um elemento $\tilde{g} \in \tilde{G}$ tal que $lt(g) = lt(\tilde{g})$, e vice-versa. Portanto $lt(G) = lt(\tilde{G})$ e o lema está provado.□

Um dado ideal pode ter muitas bases de Groebner mínimas (de fato infinitas). No entanto podemos sempre encontrar uma "melhor" do que todas as outras. A esta damos um nome especial, conforme a definição a seguir.

Definição 1.7.5. Uma ***base de Groebner reduzida*** de um ideal polinomial I é uma base de Groebner G de I tal que:

(i) $lc(p) = 1$ para todo $p \in G$.

(ii) Para todo $p \in G$, nenhum monômio de p está em $\langle lt(G - \{p\}) \rangle$.

Se $g \in G$ satifaz (ii) da definição acima, dizemos que g é ***reduzido*** para G. (De fato, de acordo com a Definição 1.3.6, g é reduzido com respeito a $G - \{g\}$).

Bases de Groebner reduzidas possuem uma propriedade especial que as tornam únicas para um dado ideal (e uma dada ordem de monômios).

Proposição 1.7.6. Seja $I \neq \{0\}$ um ideal polinomial. Então, para uma dada ordem de monômios, I tem uma única base de Groebner reduzida.

Prova:

Seja G uma base de Groebner mínima para I. Nosso objetivo é modificar G até que todos os elementos sejam reduzidos para G.

Observe que se g é reduzido para G, então também é reduzido para qualquer outra base de Groebner mínima que contenha g e o mesmo conjunto de termos líderes. Isto ocorre porque a definição de polinômio reduzido para G envolve apenas os termos líderes.

A seguir sejam $g \in G$ e g' o resto da divisão de g por $G - \{g\}$, isto é $g \xrightarrow{G-\{g\}}_{+} g'$.

Afirmamos que $G' = \{G - \{g\}\} \cup \{g'\}$ é uma base de Groebner mínima de I.

Para ver isto, note que ao dividirmos g por $G - \{g\}$, $lt(g)$ vai para o resto uma vez que não é divisível por nenhum elemento de $lt(G - \{g\})$. Portanto $lt(g') = lt(g)$, e temos que $\langle lt(G') \rangle = \langle lt(G) \rangle$. Como $G' \subset I$, temos que G' é uma base de Groebner mínima e por construção todo elemento é reduzido para G'.

Aplicamos o mesmo processo acima aos elementos de G até que todos sejam reduzidos. A base de Groebner pode mudar em cada passo do processo, mas pela observação feita acima uma vez que um elemento é reduzido ele assim permanece. Obtemos desta forma uma base de Groebner reduzida.

Para provarmos a unicidade, sejam G e $\tilde{G}$ bases de Groebner reduzidas. Então, em particular, G e $\tilde{G}$ são bases de Groebner mínimas e temos pelo Lema 1.7.4 que

$$lt(G) = lt(\tilde{G}).$$

Desta forma dado $g \in G$, existe $\tilde{g} \in \tilde{G}$ tal que $lt(g) = lt(\tilde{g})$. Se mostrarmos que $g = \tilde{g}$, então $G = \tilde{G}$ e a unicidade está provada.

Considere $g - \tilde{g} \in I$ e, como G é base de Groebner de I, temos que

(1.7.2) $$g - \tilde{g} \xrightarrow{G}_{+} 0.$$

Sabemos também que $lt(g) = lt(\tilde{g})$, e como estes termos se cancelam em $g - \tilde{g}$ e os termos restantes não são divisíveis por nenhum dos elementos de $lt(G) = lt(\tilde{G})$, já que G e $\tilde{G}$ são reduzidas, temos que

$$g - \tilde{g} \xrightarrow{G}_{+} g - \tilde{g}$$

e portanto por (1.7.2) temos que $g - \tilde{g} = 0$. □

Como consequência da unicidade na Proposição 1.7.6 temos um algoritmo para identificar quando dois conjuntos de polinômios $\{f_1,\ldots,f_s\}$ e $\{g_1,\ldots,g_t\}$ geram o mesmo ideal. Basta fixar uma ordem de monômios e computar a base de Groebner reduzida para $\langle f_1,\ldots,f_s\rangle$ e $\langle g_1,\ldots,g_t\rangle$. Os ideais serão iguais se e somente se as bases obtidas forem iguais.

1.8 Ordens de Eliminação

Na seção anterior mostramos um algoritmo para encontrar uma base de Groebner de um ideal polinomial. Mostraremos agora que a escolha apropriada da ordem de monômios nos guiará a bases de Groebner com propriedades particulares.

Considere dois conjuntos de variáveis $\{x_1,..,x_n\}$ e $\{y_1,...,y_m\}$. Supomos que os monômios nas variáveis x e os monômios nas variáveis y são ordenados por $>_x$ e $>_y$, respectivamente. Definimos uma ordem de monômios nas variáveis x e y como segue.

Definição 1.8.1. Dizemos que $>$ é uma ordem de eliminação com as variáveis x maiores que as variáveis y se valer

$$X_1Y_1 > X_2Y_2 \Leftrightarrow \begin{cases} X_1 >_x X_2 \text{ ou} \\ X_1 = X_2 \text{ e } Y_1 >_y Y_2 \end{cases}$$

para quaisquer monômios X_1,X_2 nas variáveis x e Y_1,Y_2 nas variáveis y.

As propriedades fundamentais das ordens de eliminação são enunciadas no lema a seguir, de demonstração imediata.

Lema 1.8.2. Uma ordem de eliminação $>$ com as variáveis x maiores que as variáveis y é uma ordem de monômios. Ainda, se Y é um monômio nas variáveis y e Z é um monômio nas variáveis x,y tal que um dos x_i aparece como uma potência positiva em Z então, $Z > Y$.

Definição 1.8.3. Dado $I = \langle f_1,...,f_s \rangle \subset k[x_1,...,x_n]$, o l-ésimo ***ideal de eliminação*** I_l é o ideal de $k[x_{l+1},...,x_n]$ definido por

$$I_l = I \cap k[x_{l+1},\ldots,x_n]$$

Bases de Groebner calculadas com relação a ordens de eliminação possuem uma propriedade importante conforme mostra o teorema a seguir.

Teorema 1.8.4. Seja I um ideal não nulo de $k[y_1,\ldots,y_m,x_1,\ldots,x_n]$ e $>$ uma ordem de eliminação com as variáveis x maiores que as variáveis y. Seja G uma base de Groebner de I. Então $G \cap k[y_1,\ldots,y_m]$ é uma base de Groebner para o ideal $I \cap k[y_1,\ldots,y_m]$.

Prova:

Claramente $G \cap k[y_1,\ldots,y_m] \subset I \cap k[y_1,\ldots,y_m]$.

Seja $0 \neq f(y_1,\ldots,y_m) \in I \cap k[y_1,\ldots,y_m]$. Como $f \in I$ e G é uma base de Groebner de I, existe $g_i \in G$ tal que $lm(g_i)$ divide $lm(f)$. Como f envolve apenas as variáveis y então, pela escolha da ordem $>$, também g_i deve envolver apenas as variáveis y. Logo, para todo $f \in I \cap k[y_1,\ldots,y_m]$ existe $g_i \in G \cap k[y_1,\ldots,y_m]$ tal que $lm(g_i)$ divide $lm(f)$, e portanto $G \cap k[y_1,\ldots,y_m]$ é uma base de Groebner para $I \cap k[y_1,\ldots,y_m]$.□

Corolário 1.8.5. A ordem lexicográfica com $x_1 > \cdots > x_n > y_1 \cdots > y_m$ é uma ordem de eliminação com as variáveis x maiores que as variáveis y.

Prova: Imediata.□

2. Aplicações

2.1 Aplicações Polinomiais

Nesta seção estudaremos os homomorfismos de k-álgebras entre os anéis de polinômios $k[y_1,...,y_m]$ e $k[x_1,...,x_n]$. O estudo de tais homomorfismos será de fundamental importância nas duas aplicações que seguem esta seção.

Relembramos que tais homomorfismos são homomorfismos de anéis

$$\phi: k[y_1,...,y_m] \to k[x_1,...,x_n]$$

e também transformações lineares de k-espaços vetoriais. Uma tal aplicação é unicamente determinada por

(2.1.1) $$\phi: y_i \to f_i ,$$

onde $f_i \in k[x_1,...,x_n]$, $1 \le i \le m$. Isto é, se $h \in k[y_1,...,y_m]$, digamos $h = \sum_{\nu} c_\nu y_1^{\nu_1}...y_m^{\nu_m}$, onde $c_\nu \in k$, $\nu = (\nu_1,...,\nu_m) \in \mathbb{Z}^m_{\ge 0}$, e apenas um número finito de c_ν's são não-nulos, temos

(2.1.2) $$\phi(h) = \sum_{\nu} c_\nu f_1^{\nu_1}...f_m^{\nu_m} = h(f_1,...,f_m) \in k[x_1,...,x_n].$$

Da mesma forma, dada uma expressão (2.1.1) qualquer, temos um homomorfismo de k-álgebras a partir de (2.1.2).

Relembramos que o núcleo de ϕ é o ideal

$$\ker(\phi) = \left\{ h \in k[y_1,...,y_m] \mid \phi(h) = 0 \right\}$$

e a imagem de ϕ é a k-subalgebra de $k[x_1,...,x_n]$,

$$\mathrm{im}(\phi) = \left\{ f \in k[x_1,...,x_n] \mid \exists\, h \in k[y_1,...,y_m] \text{ com } f = \phi(h) \right\},$$

que denotamos por $k[f_1,...,f_m]$. Da teoria de grupos abelianos temos

$$k[y_1,...,y_m] / \ker(\phi) \cong k[f_1,...,f_m]$$

como grupos abelianos através da aplicação

$$k[y_1,\ldots,y_m] / \ker(\phi) \rightarrow k[f_1,\ldots,f_m]$$

definida por

$$g + \ker(\phi) \rightarrow \phi(g) .$$

Podemos ver que esta aplicação é um homomorfismo de k-álgebras e portanto um isomorfismo de k-álgebras. Outra maneira de pensarmos no ker(ϕ) é a seguinte: $h \in \ker(\phi)$ se e somente se $h(f_1,\ldots,f_m) = 0$ e por esta razão ker (ϕ) é frequentemente chamado ***ideal de relações*** dos polinômios $f_1,\ldots,f_m$.

Nosso objetivo nesta seção será determinar o seguinte:

(i) O núcleo de ϕ ou mais precisamente, uma base de Groebner do núcleo de ϕ.

(ii) A imagem de ϕ ou mais precisamente, um algoritmo para determinar quando um polinômio f está na imagem de ϕ e um algoritmo para identificar quando ϕ é sobrejetora.

Antes de caracterizarmos o núcleo de ϕ precisamos de um lema técnico.

Lema 2.1.1. Sejam $a_1,a_2,\ldots,a_n$, $b_1,b_2,\ldots,b_n$ elementos de um anel comutativo R. Então o elemento $a_1a_2\ldots a_n - b_1b_2\ldots b_n$ está no ideal $\langle a_1 - b_1, a_2 - b_2,\ldots,a_n - b_n\rangle$.

Prova:

A prova é feita por indução em n.

Para $n = 1$ temos $a_1 - b_1 \in \langle a_1 - b_1\rangle$.

Supondo válido para n-1, isto é, $a_1a_2\ldots a_{n-1} - b_1b_2\ldots b_{n-1} \in \langle a_1 - b_1,\ldots,a_{n-1} - b_{n-1}\rangle$,

temos que mostrar que vale para n. Temos

$$a_1a_2...a_n - b_1b_2...b_n = a_n(a_1a_2...a_{n-1} - b_1b_2...b_{n-1}) + b_1b_2...b_{n-1}(a_n - b_n).$$

No entanto da nossa hipótese de indução temos que

$$a_n(a_1a_2...a_{n-1} - b_1b_2...b_{n-1}) \in \langle a_1 - b_1,...,a_{n-1} - b_{n-1} \rangle$$

e portanto, como

$$b_1b_2...b_{n-1}(a_n - b_n) \in \langle a_1 - b_1,...,a_n - b_n \rangle,$$

temos que

$$a_1a_2...a_n - b_1b_2...b_n \in \langle a_1 - b_1,...,a_n - b_n \rangle. \square$$

Teorema 2.1.2. Seja $K = \langle y_1 - f_1,...,y_m - f_m \rangle \subseteq k[y_1,...,y_m,x_1,...,x_n]$. Então temos

$$\ker(\phi) = K \cap k[y_1,...,y_m].$$

Prova:

Seja $g \in K \cap k[y_1,...,y_m]$. Então

$$g(y_1,...,y_m) = \sum_{i=1}^{m} (y_i - f_i(x_1,...,x_n))h_i(y_1,...,y_m, x_1,..., x_n),$$

onde $h_i \in k[y_1,...,y_m, x_1,..., x_n]$. No entanto g é zero quando aplicado em $(y_1,...,y_m) = (f_1,...,f_m)$ e portanto $g \in \ker(\phi)$.

Por outro lado, seja $g \in \ker(\phi)$. Podemos escrever

$$g = \sum_{\nu} c_\nu y_1^{\nu_1}...y_m^{\nu_m},$$

onde $c_\nu \in k$, $\nu = (\nu_1,...,\nu_m) \in Z_{\geq 0}^m$, e apenas um número finito de c_ν's são não-nulos. Como $g(f_1,...,f_m) = 0$ temos

$$g = g - g(f_1,...,f_m) = \sum_{\nu} c_\nu(y_1^{\nu_1}...y_m^{\nu_m} - f_1^{\nu_1}...f_m^{\nu_m}).$$

No entanto, pelo Lema 2.1.1, temos que $y_1^{v_1}...y_m^{v_m} - f_1^{v_1}...f_m^{v_m}$ está no ideal $K = \langle y_1 - f_1,...,y_m - f_m \rangle \subseteq k[y_1,...,y_m,x_1,...,x_n]$, e portanto $g \in K \cap k[y_1,...,y_m]$. □

Temos agora um algoritmo para computar uma base de Groebner do núcleo de ϕ. Primeiramente computamos uma base de Groebner G do ideal $K = \langle y_1 - f_1,...,y_m - f_m \rangle$ em $k[y_1,...,y_m,x_1,...,x_n]$ com relação a uma ordem de eliminação na qual as variáveis x são maiores que as variáveis y. Os polinômios sem nenhuma variável x formam uma base de Groebner do núcleo de ϕ.

Exemplo 2.1.3. Seja ϕ: $Q[u,v] \to Q[x]$ definida por

$$u \to x^2$$

$$v \to x^3$$

Primeiramente computamos uma base de Groebner do ideal $K = \langle u - x^2, v - x^3 \rangle$ com respeito à ordem lexicográfica, com $x > u > v$. Temos então

$$G = \{x^2 - u,\ xu - v,\ xv - u^2, u^3 - v^2\}.$$

Desta forma uma base de Groebner de ker (ϕ) é dada por

$$G \cap Q[u,v] = \{u^3 - v^2\}.$$

Nosso objetivo agora será encontrar um algoritmo para determinar quando um elemento $f \in k[x_1,...,x_n]$ está na imagem de uma aplicação ϕ e determinar quando ϕ é sobrejetora.

Teorema 2.1.4. Sejam $K = \langle y_1 - f_1,\ldots,y_m - f_m\rangle \subseteq k[y_1,\ldots,y_m,x_1,\ldots,x_n]$ e G uma base de Groebner de K com respeito a uma ordem de eliminação com as variáveis x maiores que as variáveis y. Então $f \in k[x_1,\ldots,x_n]$ está na imagem de ϕ se e somente se existe $h \in k[y_1,\ldots,y_m]$ tal que $f \xrightarrow{G}_+ h$. Neste caso, $f = \phi(h) = h(f_1,\ldots,f_m)$.

Prova:

Consideremos $f \in k[x_1,\ldots,x_n]$ na imagem de ϕ. Então $f = \phi(g) = g(f_1,\ldots,f_m)$ para algum $g \in k[y_1,\ldots,y_m]$. Considere o polinômio

$$f(x_1,\ldots,x_n) - g(y_1,\ldots,y_m) \in k[\, y_1,\ldots,y_m,x_1,\ldots,x_n]$$

e observe que

$$f(x_1,\ldots,x_n) - g(y_1,\ldots,y_m) = g(f_1,\ldots,f_m) - g(y_1,\ldots,y_m).$$

Seja $g = \sum_{v} c_v y_1^{v_1}\ldots y_m^{v_m}$; então

$$g(f_1,\ldots,f_m) - g(y_1,\ldots,y_m) = -\sum_{v} c_v(y_1^{v_1}\ldots y_m^{v_m} - f_1^{v_1}\ldots f_m^{v_m})$$

e portanto pelo Lema 2.1.1 $f(x_1,\ldots,x_n) - g(y_1,\ldots,y_m) \in K$. Temos então que $f - g \xrightarrow{G}_+ 0$ e portanto $g \xrightarrow{G}_+ h$, e $f \xrightarrow{G}_+ h$, onde h é reduzido com respeito a G. Mas como $g \in k[y_1,\ldots y_m]$, g só pode ser reduzido por polinômios em G que têm *termos líderes* apenas nas variáveis y. Pela nossa escolha de ordem, como as variáveis x são maiores que as variáveis y, os polinômios usados para reduzir g estão em $k[y_1,\ldots y_m]$. Desta forma temos que $h \in k[y_1,\ldots y_m]$.

Reciprocamente, seja $f \xrightarrow{G}_+ h$, onde $h \in k[y_1,\ldots y_m]$. Então $f - h \xrightarrow{G}_+ 0$ se e somente se $f - h \in K$, e portanto

$$f(x_1,\ldots,x_n) - h(y_1,\ldots,y_m) = \sum_{i=1}^{m} g_i(y_1,\ldots,y_m,x_1,\ldots,x_n)(y_i - f_i(x_1,\ldots,x_n)) \ .$$

Substituindo y_i por f_i vemos que $f(x_1,\ldots,x_n) = h(f_1,\ldots,f_m) = \phi(h)$, e f está na imagem de ϕ. □

Exemplo 2.1.5. Seja ϕ o homomorfismo dado por :

$$\phi: \mathbb{Q}[u,v,w] \to \mathbb{Q}[x,y]$$

$$u \to x^2$$
$$v \to x + y$$
$$w \to x^2 + 2xy$$

Queremos saber se $3x^2 + 2xy + y^2$ está na imagem de de ϕ.

Computamos a base de Groebner reduzida do ideal $K = \langle u - x^2, v - x - y, w - x^2 - 2xy \rangle \subset \mathbb{Q}[x,y,u,v,w]$ com relação à ordem lexicográfica com $x > y > u > v > w$. Obtemos então

$$G = \left\{ x + y - v,\ y^2 - v^2 + w,\ yv + \tfrac{1}{2}u - v^2 + \tfrac{1}{2}w,\ yu + yw + uv - vw,\ u^2 - 4uv^2 + 2uw + w^2 \right\}.$$

Reduzindo $3x^2 + 2xy + y^2$ com relação a G temos $3x^2 + 2xy + y^2 \xrightarrow{G}_{+} 2u + v^2$, e portanto $3x^2 + 2xy + y^2 \in \text{im}(\phi)$. Temos ainda que $3x^2 + 2xy + y^2 = \phi(2u + v^2)$.

Agora que temos um algoritmo para determinar quando um polinômio f está na imagem de ϕ, podemos determinar quando ϕ é sobrejetora. Basta verificar quando $x_1,\ldots,x_n \in \text{im}(\phi)$. A seguir mostraremos que isto pode ser feito apenas inspecionando a base de Groebner.

Teorema 2.1.6. Sejam $K = \langle y_1 - f_1,\ldots,y_m - f_m \rangle \subseteq k[y_1,\ldots,y_m,x_1,\ldots,x_n]$ e G a base de Groebner reduzida de K com respeito a uma ordem de eliminação com as variáveis x maiores que as variáveis y. Então ϕ é sobrejetora se e somente se para cada $i = 1,\ldots,n$, existe $g_i \in G$ tal que $g_i = x_i - h_i$, onde $h_i \in k[y_1,\ldots,y_m]$. Ainda, neste caso temos $x_i = h_i(f_1,\ldots,f_m)$.

Prova:

Suponhamos que ϕ é sobrejetora. Podemos também sem perda de generalidade assumir que a nossa ordem é tal que $x_1 < x_2 < \ldots < x_n$. Então pelo Teorema 2.1.4, uma vez que x_1 está na imagem de ϕ, existe $h_1' \in k[y_1,\ldots,y_m]$ tal que $x_1 \xrightarrow{G}_+ h_1'$. Desta forma $x_1 - h_1' \in K$ e portanto existe $g_1 \in G$ tal que $lt(g_1)$ divide $lt(x_1 - h_1') = x_1$. Portanto como os únicos termos menores que x_1 são termos apenas nas variáveis y, vemos que $g_1 = x_1 - h_1$ para algum $h_1 \in k[y_1,\ldots,y_m]$. Da mesma forma, como x_2 está na imagem de ϕ, existe $h_2' \in k[y_1,\ldots,y_m]$ tal que $x_2 \xrightarrow{G}_+ h_2'$, e portanto existe $g_2 \in G$ tal que $lt(g_2)$ divide $lt(x_2 - h_2') = x_2$. Como os únicos termos menores que x_2 são os termos envolvendo x_1 e termos apenas nas variáveis y, e como G é uma base de Groebner reduzida e qualquer termo envolvendo x_1 poderia ser reduzido utilizando $g_1 = x_1 - h_1$, devemos ter $g_2 = x_2 - h_2$ para algum $h_2 \in k[y_1,\ldots,y_m]$. Procedemos da mesma maneira para as outras variáveis x_i's.

Para mostrar a recíproca notamos primeiramente que ϕ é sobrejetora se e somente se $x_i \in \text{im}(\phi)$ para $1 \le i \le n$. Como $x_i - h_i \in G$, temos $x_i \xrightarrow{G}_+ h_i$. Como h_i é um polinômio apenas nas variáveis y, temos que x_i está na imagem de ϕ pelo Teorema 2.1.4, e portanto ϕ é sobrejetora.□

O resultado acima nos fornece um algoritmo para determinar quando a aplicação ϕ é sobrejetora. Primeiro computamos a base de Groebner reduzida do ideal K, e por inspeção, verificamos a existência de $g_i = x_i - h_i \in G$ para cada $i = 1,\ldots,n$, com $h_i \in k[y_1,\ldots,y_m]$.

Exemplo 2.1.7. Considere a aplicação

$$\phi: \mathbb{Q}[u,v,w] \to \mathbb{Q}[x,y]$$

$$u \to -x^2 + x$$
$$v \to y$$
$$w \to x - y$$

Queremos determinar se ϕ é sobrejetora.

Primeiro computamos a base de Groebner reduzida do ideal

$$K = \left\langle u + x^2 - x,\ v - y,\ w - x + y \right\rangle \subseteq \mathbb{Q}[u,v,w,x,y]$$

com respeito à ordem lexicográfica com $x > y > u > v > w$ e obtemos

$$G = \left\{ u + v^2 + 2vw - v + w^2 - w,\ x - v - w,\ y - v \right\}.$$

Como $x - v - w,\ y - v \in G$, a aplicação ϕ é sobrejetora.

Estenderemos agora os resultados anteriores a anéis quocientes de anéis polinomiais.

Definição 2.1.8. Uma k-álgebra é dita ***k-álgebra afim*** se é isomorfa como k-álgebra a $k[x_1,.....,x_n]/I$ para algum ideal I de $k[x_1,.....,x_n]$.

Obviamente $k[x_1,.....,x_n]$ é uma k-álgebra afim. Ainda, se $f_1,...,f_m \in k[x_1,....,x_n]$, então a imagem $k[f_1,...,f_m]$ da aplicação

$$\phi: k[y_1,...,y_m] \to k[x_1,...,x_n]$$

que leva y_i em f_i é uma k-álgebra afim, isomorfa a $k[y_1,...,y_m] / \ker(\phi)$, como visto no começo da seção.

Estudaremos agora os homomorfismos entre k-álgebras afins.

Sejam J um ideal de $k[y_1,...,y_m]$ e I um ideal de $k[x_1,...,x_n]$. Considere o homomorfismo de k-álgebras

$$\phi: k[y_1,...,y_m]/J \to k[x_1,...,x_n]/I$$

definido por

$$\phi: y_i + J \to f_i + I$$

Observamos que a aplicação está bem definida se e somente se a seguinte condição é satisfeita:

Se $J = \langle g_1,...,g_t \rangle$ então, para $i = 1,...,t$, temos que $g_i(f_1,...,f_m) \in I$.

Para ver isto, sejam $a, b \in k[y_1,...,y_m]$, $a \neq b$ tais que $\bar{a} \equiv \bar{b} \pmod{J}$, onde $\bar{a} = a + J$ e $\bar{b} = b + J$.

Temos que $\phi(\bar{a} - \bar{b}) = \phi(a - b + J) = \phi(J) = \bar{0} \pmod{I}$, e portanto $\phi(\bar{a}) = \phi(\bar{b}) \pmod{I}$.

Suponhamos agora $\phi(\bar{a}) = \phi(\bar{b})$. Temos então $\phi(\bar{a}) - \phi(\bar{b}) = \phi(a - b + J) = \phi(J) = \bar{0} \pmod{I}$ e portanto $\phi(J) \subset I$ o que implica que $g_i(f_1,...,f_m) \in I$ para $i = 1,...,t$.

Generalizando o Teorema 2.1.2 temos

Teorema 2.1.9. Seja K o ideal de $k[y_1,...,y_m,x_1,...,x_n]$ cujos geradores são aqueles de I juntamente com os polinômios $y_i - f_i$, $1 \leq i \leq m$, isto é, $K = \langle I, y_1 - f_1,....,y_m - f_m \rangle$. Então $\ker(\phi) = K \cap k[y_1,....,y_m] \pmod{J}$, ou seja, se $K \cap k[y_1,....,y_m] = \langle f_1',...,f_p' \rangle$ então $\ker(\phi) = \langle f_1' + J,...,f_p' + J \rangle$.

Prova:

Seja $f' \in K \cap k[y_1,...,y_m]$. Podemos escrever

$$f'(y_1,...,y_m) = \sum_{i=1}^{m} (y_i - f_i(x_1,...,x_n))h_i(y_1,...,y_m,x_1,...,x_n) + w(y_1,...,y_m,x_1,...,x_n),$$

onde

$$w(y_1,\ldots,y_m,x_1,\ldots,x_n) = \sum_{\nu} u_\nu(y_1,\ldots,y_m,x_1,\ldots,x_n)p_\nu(x_1,\ldots,x_n)\,,$$

com $p_\nu \in I$, e $h_i, u_\nu \in k[y_1,\ldots,y_m,x_1,\ldots,x_n]$. Então

$$\phi(f' + J) = f'(f_1,\ldots,f_m) + I = w(f_1,\ldots,f_m,x_1,\ldots,x_n) + I = 0\,,$$

já que $w(f_1,\ldots,f_m,x_1,\ldots,x_n) = \sum_{\nu} u_\nu(f_1,\ldots,f_m,x_1,\ldots,x_n)p_\nu(x_1,\ldots,x_n) \in I$, pois cada $p_\nu \in I$.

Por outro lado, seja $f' \in k[y_1,\ldots,y_m]$ com $\phi(f' + J) = 0$. Então $f'(f_1,\ldots,f_m) \in I$. Seja $f'(f_1,\ldots,f_m) = \sum_{\nu} c_\nu y_1^{\nu_1},\ldots,y_m^{\nu_m}$, onde $\nu = (\nu_1,\ldots,\nu_m) \in Z_{\geq 0}^m$, $c_\nu \in k$ e apenas um número finito de c_ν's são não-nulos. Então

$$\begin{aligned} f'(y_1,\ldots,y_m) &= (f'(y_1,\ldots,y_m) - f'(f_1,\ldots,f_m)) + f'(f_1,\ldots,f_m) \\ &= \sum_{\nu} c_\nu(y_1^{\nu_1},\ldots,y_m^{\nu_m} - f_1^{\nu_1},\ldots,f_m^{\nu_m}) + f'(f_1,\ldots,f_m))\,. \end{aligned}$$

Pelo Lema 2.1.1,

$$\sum_{\nu} c_\nu(y_1^{\nu_1},\ldots,y_m^{\nu_m} - f_1^{\nu_1},\ldots,f_m^{\nu_m})$$

está no ideal $\langle y_1 - f_1,\ldots,y_m - f_m\rangle$ e portanto

$$f'(y_1,\ldots,y_m) \in \langle I, y_1 - f_1,\ldots,y_m - f_m\rangle = K\,,$$

já que $f'(f_1,\ldots,f_m) \in I$. Assim $f'(y_1,\ldots,y_m) \in K \cap k[y_1,\ldots,y_m]$.□

Provaremos agora o análogo do Teorema 2.1.4

Teorema 2.1.10. Sejam $K = \langle I, y_1 - f_1,\ldots,y_m - f_m\rangle$ e G uma base de Groebner de K com respeito a uma ordem de eliminação com as variáveis x maiores que as variáveis y. Então $f + I \in k[x_1,\ldots,x_n] / I$ está na imagem de ϕ se e somente se existe $h \in k[y_1,\ldots,y_m]$ tal que $f \xrightarrow{G}_+ h$. Neste caso, $f + I = \phi(h + J) = h(f_1,\ldots,f_m) + I$.

Prova:

Seja $f + I \in im(\phi)$. Então existe $g \in k[y_1,...,y_m]$ tal que $f - g(f_1,...,f_m) \in I$. Consideramos o polinômio $f(x_1,...,x_n) - g(y_1,...,y_m) \in k[y_1,...,y_m,x_1,...,x_n]$.

Como $f(x_1,...,x_n) - g(y_1,...,y_m) = g(f_1,...,f_m) - g(y_1,...,y_m) + (f(x_1,...,x_n) - g(f_1,...,f_m))$, o Lema 2.1.1 garante que $f(x_1,...,x_n) - g(y_1,...,y_m) \in K$ e o resto do argumento segue exatamente como no desenvolvimento da prova do Teorema 2.1.4.

Por outro lado, seja $f \in k[x_1,...,x_n]$ tal que $f \xrightarrow{G}_+ h$ com $h \in k[y_1,...,y_m]$. Então $f - h \in K$, e desta forma

$$f(x_1,...,x_n) - h(y_1,...,y_m) = \sum_{i=1}^{m} g_i(y_1,...,y_m,x_1,...,x_n)(y_i - f_i(x_1,...,x_n)) + w(y_1,...,y_m,x_1,...,x_n),$$

onde

$$w(y_1,...,y_m,x_1,...,x_n) = \sum_{v} u_v(y_1,...,y_m,x_1,...,x_n)p_v(x_1,...,x_n)$$

com $p_v \in I$ e onde g_i, $u_v \in I\,k[y_1,...,y_m,x_1,...,x_n]$. Substituindo y_i por f_i, vemos que $f - h(f_1,...,f_m) \in I$, e portanto $f + I = \phi(h + J)$.□

Teorema 2.1.11. Sejam $K = \langle I, y_1 - f_1,....,y_m - f_m \rangle$ e G a base de Groebner reduzida de K com respeito a uma ordem de eliminação com as variáveis x maiores que as variáveis y. Então ϕ é sobrejetora se e somente se para cada $i = 1,...,n$, existe um polinômio $g_i = x_i - h_i \in G$, onde $h_i \in k[y_1,...,y_m]$.

Prova:

A demonstração é analoga à prova do Teorema 2.1.6.□

Exemplo 2.1.12. Seja a aplicação

$$\phi: \mathbb{Q}[u,v,w]/J \to \mathbb{Q}[x,y]/I$$

$$u + J \to x^2 + y + I$$
$$v + J \to x + y + I$$
$$w + J \to x^3 - xy^2 + I$$

onde $J = \langle uv - w \rangle \subset \mathbb{Q}[u,v,w]$ e $I = \langle xy + y \rangle \subset \mathbb{Q}[x,y]$.

Note que aplicação está bem definida, uma vez que

$$\phi(uv - w + J) = (x^2 + y)(x + y) - (x^3 - xy^2) + I$$

$$= x^2y + xy^2 + xy + y^2 + I$$

$$= (x + y)(xy + y) + I = 0 + I .$$

Computamos agora o núcleo de ϕ como no Teorema 2.1.9. Portanto seja

$$K = \langle xy + y,\ u - x^2 - y,\ v - x - y,\ w - x^3 + xy^2 \rangle \subset \mathbb{Q}[u,v,w,x,y].$$

Computamos a base de Groebner reduzida de K com respeito à ordem lexicográfica com $x > y > u > v > w$ e obtemos

$$G = \{uv - w,\ uw + v^4 + 2v^3 - v^2w - vw - 2w,\ v^5 + 2v^4 - v^3w - v^2w - 2vw + w^2,$$

$$yw - 8y + 4u - v^3 - 4v^2 + w,\ x + y - v,\ y^2 - 3y + u - v^2,$$

$$yv - 2y + u - v^2, yu - 4y + u - v^2,\ u^2 - 2u + v^3 + 2v^2 - vw - w\}.$$

Então pelo Teorema 2.1.9 temos

$$\ker(\phi) = \{uv - w,\ uw + v^4 + 2v^3 - v^2w - vw - 2w,\ v^5 + 2v^4 - v^3w - v^2w - 2vw + w^2,$$
$$u^2 - 2u + v^3 + 2v^2 - vw - w\} \bmod (J)$$

Também pelo Teorema 2.1.11 temos que ϕ não é sobrejetora. Note, por exemplo, que $y \notin \text{im}(\phi)$ uma vez que y não é divisível pelo termo líder de nenhum elemento de G.

Definição 2.1.13. Seja k um corpo. Uma ***função racional*** em $t_1,\ldots,t_m$ com coeficientes em k é um quociente f / g de dois polinômios $f, g \in k[t_1,\ldots,t_m]$, onde g é um polinômio não nulo. Ao conjunto de todas as funções racionais em $t_1,\ldots,t_m$ com coeficientes em k denotamos $k(t_1,\ldots,t_m)$.

Queremos agora determinar quando $k(f_1,\ldots,f_m) = k(x_1,\ldots,x_n)$; para isto considere o homomorfismo

(2.1.3)
$$\gamma\colon k[x_1,\ldots,x_n,y_1,\ldots,y_m] \to k[x_1,\ldots,x_n]$$
$$f(x_1,\ldots,x_n,y_1,\ldots,y_m) \to f(x_1,\ldots,x_n,f_1,\ldots,f_m)$$

e o ideal $K = \langle y_1 - f_1,\ldots,\ y_m - f_m \rangle \subset k[x_1,\ldots,x_n,y_1,\ldots,y_m]$.

Lema 2.1.14. Temos que $\ker(\gamma) = K$.

Prova:

Seja $g \in K$. Então

$$g(x_1,\ldots,x_n,y_1,\ldots,y_m) = \sum_{i=1}^{m} (y_i - f_i(x_1,\ldots,x_n))h_i(x_1,\ldots,x_n,y_1,\ldots,y_m)\ ,$$

onde $h_i \in k[x_1,\ldots,x_n,y_1,\ldots,y_m]$, e portanto

$$\gamma\Big(g(x_1,\ldots,x_n,y_1,\ldots,y_m\Big) = \gamma\left(\sum_{i=1}^{m} (y_i - f_i(x_1,\ldots,x_n))h_i(x_1,\ldots,x_n,y_1,\ldots,y_m)\right)$$
$$= \sum_{i=1}^{m} (f_i - f_i(x_1,\ldots,x_n))h_i(x_1,\ldots,x_n,y_1,\ldots,y_m) = 0\ ,$$

de modo que $g \in \ker(\gamma)$.

Reciprocamente, seja $g \in \ker(\gamma)$. Podemos escrever

$$g = \sum_{\nu} c_\nu x_1^{\nu_1}\ldots x_n^{\nu_n} y_1^{\nu_{n+1}}\ldots y_m^{\nu_{n+m}}\ ,$$

onde $c_\nu \in k$, $\nu = (\nu_1,...,\nu_n,\nu_{n+1},...,\nu_{n+m}) \in Z_{\geq 0}^{n+m}$, e apenas um número finito de c_ν's são não-nulos. Como $g(x_1,...,x_n,f_1,...,f_m) = 0$ temos

$$g = g - g(x_1,...,x_n,f_1,...,f_m) = \sum_\nu c_\nu x_1^{\nu_1}...x_n^{\nu_n}(y_1^{\nu_{n+1}}...y_m^{\nu_{n+m}} - f_1^{\nu_{n+1}}...f_m^{\nu_{n+m}}).$$

De acordo com o desenvolvimento na prova do Lema 2.1.1 temos que

$$y_1^{\nu_{n+1}}...y_m^{\nu_{n+m}} - f_1^{\nu_{n+1}}...f_m^{\nu_{n+m}} \in K = \langle y_1 - f_1,...,y_m - f_m \rangle \subseteq k[y_1,...,y_m,x_1,...,x_n]$$

e portanto $g \in K$.□

Se G é uma base de Groebner de K, definimos os subconjuntos

$$G_T = G \cap k[y_1,...,y_m]$$

e

$$G_M = \{g \in G \mid lm(g) \text{ não é divisível pelo termo líder de qualquer elemento de } G_T\}.$$

Teorema 2.1.15. Sejam γ um homomorfismo como em (2.1.3) e $>$ uma ordem monomial tal que cada x_i é maior que o produto de x_{i+1} por qualquer monômio em $k[y_1,...,y_m]$, ou seja,

(2.1.4) $$x_i > k[y_1,...,y_m] \cdot x_{i+1} \text{ , para } i = 1, 2,..., n-1.$$

Então $k(f_1,...,f_m) = k(x_1,...,x_n)$ se e somente se G_M contém um subconjunto $\{g_1,...,g_n\}$, onde $g_i = \delta_i x_i - \varphi_i$ com $\varphi_i \in k[x_{i+1},...,x_n,y_1,...,y_m]$ e $\delta_i \in k[y_1,...,y_m]$.

Prova:

Se G_M contém o subconjunto indicado então $g_n = \delta_n x_n - \varphi_n \in K = \ker(\gamma)$ e portanto

$$\gamma(g_n) = \gamma(\delta_n x_n - \varphi_n) = \delta_n(f_1,...,f_n)x_n - \varphi_n(f_1,...,f_n) = 0,$$

de modo que $\delta_n(f_1,...,f_n)x_n = \varphi_n(f_1,...,f_n)$.

Se $\delta_n(f_1,\ldots,f_n) = 0$ então $\delta_n \in K$ e portanto $\delta_n \xrightarrow{G_T} 0$, o que contradiz o fato de que os monômios líderes de elementos de G_M não são divisíveis por monômios líderes de elementos de G_T. Assim $\delta_n(f_1,\ldots,f_n) \neq 0$ e $x_n = \dfrac{\varphi_n(f_1,\ldots,f_n)}{\delta_n(f_1,\ldots,f_n)}$.

Da mesma forma, para g_{n-1} temos

$$\gamma(g_{n-1}) = \gamma(\delta_{n-1}x_{n-1} - \varphi_{n-1}) = \delta_{n-1}(f_1,\ldots,f_n)x_{n-1} - \varphi_{n-1}(x_n,f_1,\ldots,f_n) = 0 .$$

No entanto provamos acima que $x_n \in k(f_1,\ldots,f_m)$ e portanto $\varphi_{n-1}(x_n,f_1,\ldots,f_n) \in k(f_1,\ldots,f_n)$. Desta forma $\delta_{n-1}(f_1,\ldots,f_n)x_{n-1} = \theta(f_1,\ldots,f_n)$, onde $\theta(f_1,\ldots,f_n) = \varphi_{n-1}(x_n,f_1,\ldots,f_n)$ e, assim como no caso anterior, temos que $\delta_{n-1}(f_1,\ldots,f_n) \neq 0$ e portanto $x_{n-1} = \dfrac{\varphi_{n-1}(f_1,\ldots,f_n)}{\delta_{n-1}(f_1,\ldots,f_n)}$.

A prova segue como no caso acima para g_i, com $i = 1,2,\ldots,n-2$.

Reciprocamente, vamos assumir que $k(f_1,\ldots,f_m) = k(x_1,\ldots,x_n)$ e portanto para $i = 1,2,\ldots,n-1$ devem existir polinômios $\alpha_i, \beta_i \in k[y_1,\ldots,y_m]$ tais que

$$\alpha_i(f_1,\ldots,f_m)x_i = \beta_i(f_1,\ldots,f_m) \neq 0.$$

Entre todos os pares de polinômios α_i, β_i pegue o par onde o monômio líder de α_i é o menor possível (existe devido à boa ordenação de >). Definimos então $P_i = \alpha_i x_i - \beta_i$ e desta forma temos $P_i \in \ker(\gamma)$, pois

(2.1.5) $$\gamma(P_i) = \alpha_i(f_1,\ldots,f_m)x_i - \beta_i(f_1,\ldots,f_m) = 0.$$

Seja $\eta_i x_i$ o monomio líder de P_i, onde $\eta_i = lm(\alpha_i)$. Como $P_i \in \ker(\gamma)$, temos que $P_i \xrightarrow{G} 0$ e portanto $\eta_i x_i$ deve ser dividido pelo monômio líder de um elemento de G. Suponhamos (por contradição) que $\eta_i x_i$ seja divisível pelo monômio líder de um elemento de G_T, o qual deve ser um monômio envolvendo apenas $y_1,\ldots,y_m$. Então pela nossa escolha da ordem tal monômio deve dividir η_i e portanto α_i é reduzido por G_T.

Seja $\alpha_i' \in k[y_1,\ldots,y_m]$ tal que $\alpha_i \xrightarrow{G_T} \alpha_i'$. Desta forma temos que $\alpha_i - \alpha_i' \in K$ e portanto

$$\alpha_i(f_1,\ldots,f_m) = \gamma(\alpha_i) = \gamma(\alpha_i) = \alpha_i'(f_1,\ldots,f_m) \neq 0.$$

Podemos então substituir α_i por α_i' na equação (2.1.5); no entanto, note que $lm(\alpha_i) > lm(\alpha_i')$, o que contradiz a minimalidade de α_i. Logo $lm(P_i) = \eta_i x_i$ é divisível pelo monômio líder de um elemento de $g_i \in G \setminus G_T$. Este elemento g_i deve ter um monomio líder da forma $\tau_i x_i$ onde τ_i é um monômio em $y_1,\ldots,y_m$ e que divide η_i.

Seja ζ um monômio interno de g_i, isto é, um monômio com coeficiente não nulo e que não é um monômio líder. Queremos mostrar que ζ é da forma

$$\pi x_i \text{ com } \pi \in k[y_1,\ldots,y_m]$$

ou

$$\zeta \in k[x_{i+1},\ldots,x_n,y_1,\ldots,y_m].$$

Se x_i divide ζ então $\frac{\zeta}{x_i} < \frac{\eta_i x_i}{x_i} = \eta_i \in k[y_1,\ldots,y_m]$ e portanto $\frac{\zeta}{x_i} \in k[y_1,\ldots,y_m]$ e ζ é da forma πx_i com $\pi \in k[y_1,\ldots,y_m]$.

Vamos supor agora que x_j divide ζ com $j < i$, de modo que $\zeta \geq x_j$. Observe no entanto que pela escolha da ordem temos que $x_j \geq x_{i-1} > \tau_i x_i$ o que contradiz o fato de que ζ é um monômio interno de g_i. Logo x_j não divide ζ e temos que ζ é da segunda forma. □

- Note que a ordem lexicográfica pura com $x_1 > \cdots > x_n > y_1 > \cdots > y_m$ satisfaz (2.1.4).

2.2 Polinômios Minimais de Elementos em Extensões de Corpos

Nesta seção utilizaremos os resultados da Seção 2.1 para encontrar o polinômio minimal de um elemento algébrico sobre um corpo k.

Seja $k \subseteq K$ uma extensão do corpo k. Relembramos que se $\alpha \in K$ é algébrico sobre k, então o polinômio minimal de α sobre k é definido como sendo o polinômio mônico p em uma variável, com coeficientes em k, de menor grau tal que $p(\alpha) = 0$.

Seja $k(\alpha)$ o conjunto de todos os elementos da forma $\frac{f(\alpha)}{g(\alpha)}$, onde $f, g \in k[x]$, e considere o homomorfismo de k-álgebras

$$\phi: k[x] \to k(\alpha)$$

$$x \to \alpha$$

Lema 2.2.1. Se p é o polinômio minimal de α sobre k então $\ker(\phi) = \langle p \rangle$.

Prova:

Se $f \in \langle p \rangle$, existe $h \in k[x]$ tal que $f = hp$. Temos então que

$$\phi(f) = \phi(hp) = \phi(h)\phi(p) = h(\alpha)p(\alpha) = h(\alpha).0 = 0$$

e portanto $f \in \ker(\phi)$.

Reciprocamente, seja $f \in \ker(\phi)$. Pelo algoritmo da divisão em $k[x]$ podemos escrever

$$f = qp + r \text{ , para } q, r \in k[x] \text{ e tais que } r = 0 \text{ ou } grau(r) < grau(p).$$

Supondo que $r \neq 0$, temos

$$0 = \phi(f) = \phi(qp + r) = \phi(q)\phi(p) + \phi(r) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha) .$$

Seja r' o polinômio mônico obtido dividindo r pelo coeficiente do seu termo de maior grau. Então r' é mônico e $r'(\alpha) = 0$, o que contradiz a hipótese de p ser o polinômio minimal de α, já que $grau(r') < grau(p)$. Isto mostra que $r = 0$ e portanto $f = qp \in \langle p \rangle$.□

Lema 2.2.2. Sejam k um corpo e $\alpha \in K$ algébrico sobre k com polinômio minimal p. Qualquer elemento de $k(\alpha)$ tem uma expressão única da forma $q(\alpha)$, onde $q \in k[x]$ e $grau\ (q) < grau(p)$.

Prova:

Seja $h \in k(\alpha)$, digamos $h(\alpha) = \dfrac{f(\alpha)}{g(\alpha)}$ com $f, g \in k[x]$ e $g(\alpha) \neq 0$.

Como $g(\alpha) \neq 0$, temos que p não divide g e, como p é irredutível, temos que p e g são primos entre si. Existem portanto $a, b \in k[x]$ tais que $ag + bp = 1$ e assim

$$1 = a(\alpha)g(\alpha) + b(\alpha)p(\alpha) = a(\alpha)g(\alpha).$$

Desta forma

$$h(\alpha) = \frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)}{g(\alpha)} \cdot \frac{a(\alpha)}{a(\alpha)} = f(\alpha)a(\alpha) = q(\alpha) \text{ para o polinômio } q = f \cdot a \in k[x].$$

Pelo algoritmo de Euclides existem $u, r \in k[x]$ tais que

$$q = up + r \text{ , com } grau(r) < grau(p) \text{ .}$$

Mas $q(\alpha) = r(\alpha)$, logo $grau(q) < grau(p)$, o que prova a existência. Para provar a unicidade, sejam $q, q^* \in k[x]$ tais que $q(\alpha) = q^*(\alpha)$ e $grau(q), grau(q^*) < grau(p)$. Tomando $q(x) - q^*(x) = a(x) \in k[x]$ obtemos $grau(a) < grau(q)$. Como $a(\alpha) = q(\alpha) - q^*(\alpha) = 0$, a minimalidade de p garante que $a = 0$ e portanto $q = q^*$.□

Pelo Lema 2.2.1 temos que $\ker(\phi) = \langle p \rangle$ e pelo Lema 2.2.2 ϕ é sobre, de modo que

(2.2.1) $$k[x] / \langle p \rangle \cong k(\alpha)$$

pela aplicação definida por $x + \langle p \rangle \to \alpha$.

Consideraremos inicialmente o caso $K = k(\alpha)$, com α algébrico sobre k, e nosso objetivo é computar o polinômio minimal de qualquer $\beta \in K$. Notamos que para computar em $k(\alpha)$ é suficiente, de acordo com (2.2.1), computar na k-álgebra afim $k[x] / \langle p \rangle$. Supomos conhecido o polinômio minimal p de α.

Teorema 2.2.3. Sejam $k \subseteq K$ uma extensão do corpo k, $\alpha \in K$ algébrico sobre k e $p \in k[x]$ o polinômio minimal de α sobre k. Seja $0 \neq \beta \in k(\alpha)$ um elemento qualquer, digamos

$$\beta = \frac{a_0 + a_1\alpha + \ldots + a_n\alpha^n}{b_0 + b_1\alpha + \ldots + b_m\alpha^m} = \frac{f(\alpha)}{g(\alpha)},$$

onde $a_i, b_j \in k$ para $0 \leq i \leq n$ e $0 \leq j \leq m$. Sejam $f(x) = a_0 + a_1x + \ldots + a_nx^n$ e $g(x) = b_0 + b_1x + \ldots + b_mx^m$ os polinômios correspondentes em $k[x]$ e considere o ideal $J = \langle p, gy - f \rangle$ de $k[x,y]$. Então o polinômio minimal de β sobre k é o polinômio mônico que gera o ideal $J \cap k[y]$.

Note que $J \cap k[y]$ é gerado por um único polinômio, uma vez que isto é válido para todo ideal em $k[y]$, já que $k[y]$ é um domínio de ideais principais.

Prova :

Note que como $k[x] / \langle p \rangle$ é um corpo e $g(\alpha) \neq 0$ (g é o denominador de β), existe um polinômio $l \in k[x]$ tal que

(2.2.2) $gl \equiv 1 \pmod{\langle p \rangle}$, ou seja, $gl - 1 \in \langle p \rangle$.

Escrevendo $h = fl$ temos $h(\alpha) = \dfrac{f(\alpha)l(\alpha)}{g(\alpha)l(\alpha)} = \dfrac{f(\alpha)}{g(\alpha)} = \beta$. Considere agora a composição ϕ dos homomorfismos de k-álgebras afins dada por

$$\phi: k[y] \to k[x] / \langle p \rangle \to k(\alpha)$$

$$y \to h + \langle p \rangle \to \beta$$

Note que $q \in \ker(\phi)$ se e somente se $q(\beta) = 0$. Para ver isto, seja $q \in \ker(\phi) \subseteq k[y]$, digamos $q = \sum_{finita} c_i y^{\sigma_i}$. Temos então que

$$\phi(q) = \phi\left(\sum_{finita} c_i y^{\sigma_i}\right) = \sum_{finita} c_i \beta^{\sigma_i} = q(\beta)$$

e, como $q \in \ker(\phi)$, temos que $\phi(q) = 0 = q(\beta)$; a recíproca é imediata.

Desta forma, para encontrar o polinômio minimal de β, procuramos pelo gerador mônico do $\ker(\phi)$. Pelo Teorema 2.1.9, $\ker(\phi) = \langle p, y - h \rangle \cap k[y]$. Desta forma é suficiente mostrar que $\langle p, y - h \rangle = \langle p, gy - f \rangle$. Temos que $y - h = y - fl = l(gy - f) + (-y)(gl - 1)$ e de (2.2.2) temos que $gl - 1 \in \langle p \rangle$. Desta forma $y - h \in \langle p, gy - f \rangle$.

Reciprocamente, temos que $gy - f = f(gl - 1) + g(y - fl)$ e de (2.2.2) temos que $gl - 1 \in \langle p \rangle$. Desta forma $gy - f \in \langle p, y - fl \rangle$.□

O resultado anterior nos dá um algoritmo para encontrar o polinômio minimal de um elemento β em $k(\alpha)$:

Dados α e β como no Teorema 2.2.3, computamos a base de Groebner reduzida G para o ideal $\langle p, gy - f \rangle$ de $k[x,y]$ com respeito a *lex* (ou outra ordem de eliminação) com $x > y$. O polinômio em G na variável y sozinha é o polinômio minimal de β.

Exemplo 2.2.4. Considere a extensão de corpo $\mathbb{Q}(\alpha)$ de $\mathbb{Q}$, onde α é uma raiz do polinômio irredutível $x^2 - 5$. Considere agora o elemento $\beta = \frac{-\alpha^2 + 2\alpha + 1}{\alpha}$, e o ideal $J = \langle x^2 - 5, xy + x^2 - 2x - 1 \rangle \subset \mathbb{Q}[x,y]$. Computamos a base de Groebner reduzida para o ideal J com respeito à ordem lexicográfica com $x > y$ e obtemos

$$G = \left\{ x + \frac{5}{4}y - \frac{5}{2},\ y^2 - 4y + \frac{4}{5} \right\}.$$

Desta forma o polinômio minimal de β é $y^2 - 4y + \frac{4}{5}$.

Esta técnica pode ser estendida para o caso mais geral de extensões de corpos da forma $K = k(\alpha_1,...,\alpha_n)$. Para isto necessitamos da seguinte notação :

Para $i = 2,...,n$ e $p \in k(\alpha_1,...,\alpha_{i-1})[x_i]$, seja $\bar{p}$ qualquer polinômio em $k[x_1,...,x_i]$ tal que $\bar{p}(\alpha_1,...,\alpha_{i-1},x_i) = p$. Note que $\bar{p}$ não é unicamente definido, mas qualquer uso que fizermos de $\bar{p}$ não irá depender desta escolha particular.

Iremos agora determinar o polinômio minimal de qualquer elemento β de $k(\alpha_1,...,\alpha_n)$ usando o seguinte resultado, que é similar ao Teorema 2.2.3.

Teorema 2.2.5. Seja $K = k(\alpha_1,...,\alpha_n)$ uma extensão algébrica de k. Para $i = 1,...,n$, seja $p_i \in k(\alpha_1,...,\alpha_{i-1})[x_i]$ o polinômio minimal de α_i sobre $k(\alpha_1,...,\alpha_{i-1})$. Seja $\beta \in k(\alpha_1,...,\alpha_n)$, digamos

$$\beta = \frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)},$$

onde $f, g \in k[x_1,...,x_n]$. Considere o ideal $J = \langle \bar{p}_1,...,\bar{p}_n, gy - f \rangle$ contido em $k[x_1,...,x_n,y]$. Então o polinômio minimal de β sobre k é o polinômio mônico que gera o ideal $J \cap k[y]$.

Prova:

Basta mostrar que $k[x_1,...,x_n] / \langle \bar{p}_1,...,\bar{p}_n \rangle \cong k(\alpha_1,...,\alpha_n)$, pois o resto da demonstração segue da mesma forma que na demonstração do Teorema 2.2.3. Para tal consideramos a aplicação

$$\phi_n: k[x_1,...,x_n] \to k(\alpha_1,...,\alpha_n)$$

$$x_i \to \alpha_i$$

Como ϕ_n é sobrejetiva, resta mostrar que ker $(\phi_n) = \langle \bar{p}_1,...,\bar{p}_n \rangle$.

Temos que $\bar{p}_1,...,\bar{p}_n \in$ ker (ϕ_n), já que $\phi_n(\bar{p}_i) = \bar{p}_i(\alpha_1,...,\alpha_i) = p_i(\alpha_1,...,\alpha_i) = 0$ por definição de $\bar{p}_i$. A reciproca será feita por indução no número de variáveis n.

O caso $n = 1$ é dado pelo Lema 2.2.1. Considere agora $f \in k[x_1,...,x_n]$ tal que $f(\alpha_1,...,\alpha_n) = 0$ e seja $h(x_n) = f(\alpha_1,...,\alpha_{n-1},x_n) \in k(\alpha_1,...,\alpha_{n-1})[x_n]$. Note que $h(\alpha_n) = f(\alpha_1,...,\alpha_{n-1},\alpha_n) = 0$ e portanto p_n divide h por definição de p_n. Existe portanto $l_n \in k(\alpha_1,...,\alpha_{n-1})[x_n]$ tal que $h = p_n l_n$. Considere

$$f - \bar{p}_n \bar{l}_n = \sum g_\nu(x_1,...,x_{n-1}) x_n^\nu \in k[x_1,...,x_n] .$$

Como

$$f - \bar{p}_n \bar{l}_n(\alpha_1,...,\alpha_{n-1},x_n) = h - p_n l_n = 0,$$

temos que $g_\nu(\alpha_1,...,\alpha_{n-1}) = 0$ para todo ν. Desta forma $g_\nu(x_1,...,x_{n-1}) \in$ ker (ϕ_{n-1}), onde

$$\phi_{n-1}: k[x_1,...,x_{n-1}] \to k(\alpha_1,...,\alpha_{n-1})$$

e portanto da nossa hipótese de indução, $g_\nu(x_1,...,x_{n-1}) \in \langle \bar{p}_1,...,\bar{p}_{n-1} \rangle$. Desta forma temos que $f - \bar{p}_n \bar{l}_n \in \langle \bar{p}_1,...,\bar{p}_{n-1} \rangle$ e portanto $f \in \langle \bar{p}_1,...,\bar{p}_n \rangle$, como queríamos demonstrar. □

Exemplo 2.2.6. Considere a extensão de corpo $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3},\sqrt{5})$. O polinômio minimal de $\sqrt{3}$ sobre $\mathbb{Q}$ é $p_1 = x_1^2 - 3 \in \mathbb{Q}[x_1]$ e o polinômio minimal de $\sqrt{5}$ sobre $\mathbb{Q}(\sqrt{3})$ é $p_2 = x_2^2 - 5 \in \mathbb{Q}(\sqrt{3})\,[x_2]$. Queremos determinar o polinômio minimal de $\sqrt{3} - \sqrt{5}$. Para isto computamos a base de Groebner reduzida para o ideal

$$J = \left\langle \bar{p}_1, \bar{p}_2, y - (x_1 - x_2) \right\rangle = \left\langle x_1^2 - 3,\ x_2^2 - 5,\ y - x_1 + x_2) \right\rangle \subseteq \mathbb{Q}[x_1,x_2,y]$$

com respeito à ordem lexicográfica com $x_1 > x_2 > y$ e obtemos

$$G = \left\{ x_2 - \frac{1}{4}y^3 - \frac{9}{2}y,\ x_1 - \frac{1}{4}y^3 + \frac{7}{2}y,\ y^4 - 16y^2 + 4 \right\}.$$

Desta forma o polinômio minimal de $\sqrt{3} - \sqrt{5}$ sobre $\mathbb{Q}$ é $y^4 - 16y^2 + 4$. Vemos também que $\sqrt{3} - \sqrt{5}$ tem grau 4 sobre $\mathbb{Q}$, e portanto $\mathbb{Q}(\sqrt{3} - \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Exemplo 2.2.7. O polinômio minimal de $\sqrt[4]{3}$ sobre $\mathbb{Q}$ é $p_1 = x_1^4 - 3 \in \mathbb{Q}[x_1]$. As raízes deste polinômio geram a extensão $\mathbb{Q}(\sqrt[4]{3},i)$. Seja o elemento $\beta = \dfrac{\sqrt[4]{3} + i}{\sqrt[4]{3}}$, i.e., $\beta = \dfrac{f(\sqrt[4]{3},i)}{g(\sqrt[4]{3},i)}$, onde $f = x_1 + x_2$, $g = x_1 \in k[x_1,x_2]$. Queremos encontar o polinômio minimal de β sobre $\mathbb{Q}$. O polinômio minimal de i sobre $\mathbb{Q}(\sqrt[4]{3})$ é $p_2 = x_2^2 + 1$, desta forma temos $p_1 = \overline{p_1}$ e $p_2 = \overline{p_2}$. Seja o ideal $J = \left\langle x_1^4 - 3,\ x_2^2 + 1,\ x_1 y - (x_1 + x_2) \right\rangle \subset \mathbb{Q}[x_1,x_2,y]$. A base de Groebner reduzida de J com respeito à ordem lexicográfica com $x_1 > x_2 > y$ é dada por:

$$G = \left\{ x_2^2 + 1,\ x_1 - 3x_2y^3 + 9x_2y^2 - 9x_2y + 3x_2,\ y^4 - 4y^3 + 6y^2 - 4y + \frac{2}{3} \right\}.$$

Desta forma temos que o polinômio minimal de β sobre $\mathbb{Q}$ é $y^4 - 4y^3 + 6y^2 - 4y + \frac{2}{3}$.

Alternativamente $\mathbb{Q}(\sqrt[4]{3},i) = \mathbb{Q}(\sqrt[4]{3}, i\sqrt[4]{3})$. O polinômio minimal de $i\sqrt[4]{3}$ sobre $\mathbb{Q}(\sqrt[4]{3})$ é $p_2 = x_2^2 + \sqrt{3}$. Desta forma $\overline{p_2} = x_2^2 + x_1^2$. Queremos determinar o polinômio minimal de $\beta = \dfrac{\sqrt[4]{3} + i}{\sqrt[4]{3}}$.

Temos que $\beta = \dfrac{f(\sqrt[4]{3}, i\sqrt[4]{3})}{g(\sqrt[4]{3}, i\sqrt[4]{3})}$, onde $f = x_1^2 + x_2$, $g = x_1^2 \in k[x_1,x_2]$. O ideal J é dado agora por $J = \left\langle x_1^4 - 3,\ x_2^2 + x_1^2,\ x_1^2 y - (x_1^2 + x_2) \right\rangle \subset \mathbb{Q}[x_1,x_2,y]$ e sua base de Groebner reduzida para a ordem lexicográfica com $x_1 > x_2 > y$ é

$$G = \left\{ x_2 + 3y^3 - 9y^2 + 9y - 3,\ x_1^2 + 3y^2 - 6y + 3,\ y^4 - 4y^3 + 6y^2 - 4y + \frac{2}{3} \right\}.$$

Obtemos desta forma o mesmo resultado acima. Como o grau de β sobre $\mathbb{Q}$ é 4 vemos que $\mathbb{Q}(\beta)$ é um subcorpo de $\mathbb{Q}(\sqrt[4]{3},i)$.

Nos dois exemplos anteriores, usamos o grau para decidir quando $k(\beta)$ é igual a $k(\alpha_1,\ldots,\alpha_n)$. A seguir apresentamos um outro método para determinar isto com a vantagem de expressar os α_i's em termos de β. Este algoritmo é consequência do seguinte teorema:

Teorema 2.2.8. Seja $K = k(\alpha_1,\ldots,\alpha_n)$ uma extensão algébrica de k. Para $i = 1,\ldots,n$, seja $p_i \in k(\alpha_1,\ldots,\alpha_{i-1})[x_i]$ o polinômio minimal de α_i sobre $k(\alpha_1,\ldots,\alpha_{i-1})$. Seja $\beta \in k(\alpha_1,\ldots,\alpha_n)$, digamos

$$\beta = \frac{f(\alpha_1,\ldots,\alpha_n)}{g(\alpha_1,\ldots,\alpha_n)},$$

onde $f, g \in k[x_1,\ldots,x_n]$. Considere o ideal $J = \left\langle \overline{p_1},\ldots,\ \overline{p_n},\ gy - f \right\rangle$ contido em $k[x_1,\ldots,x_n,y]$ e seja G a base de Groebner reduzida de J com as variáveis x maiores que a variável y. Então

$k(\alpha_1,...,\alpha_n) = k(\beta)$ se e somente se para cada $i = 1,2,...,n$ existe um polinômio $g_i \in G$ tal que $g_i = x_i - h_i$ para algum $h_i \in k[y]$. Neste caso, $\alpha_i = h_i(\beta)$.

Prova:

Sejam $I = \langle \bar{p}_1,...,\bar{p}_n \rangle$ e $l \in k[x_1,...,x_n]$ tais que $gl - 1 \in I$. Escrevendo $h = fl$ temos

$$h(\alpha_1,...,\alpha_n) = \frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)} \cdot \frac{l(\alpha_1,...,\alpha_n)}{l(\alpha_1,...,\alpha_n)} = \beta .$$

Considere a aplicação

$$k[y] \xrightarrow{\phi} k[x_1,...,x_n] / I \xrightarrow{\equiv} k(\alpha_1,...,\alpha_n)$$

$$y \to h + I \to \beta$$

Então $k(\alpha_1,...,\alpha_n) = k(\beta)$ se e somente se ϕ é sobrejetora. Seguindo o mesmo argumento utilizado na demonstração do Teorema 2.2.3 podemos mostrar que $J = \langle \bar{p}_1,...,\bar{p}_m, gy - f \rangle = \langle I, y - h \rangle$.

Desta forma, pelo Teorema 2.1.11, temos que ϕ é sobrejetora se e somente se existe um polinômio $g_i \in G$ tal que $g_i = x_i - h_i$ para algum $h_i \in k[y]$. Neste caso, $\alpha_i = h_i(\beta)$.□

Exemplo 2.2.9. No Exemplo 2.2.7, note que não existe em

$$G = \left\{ x_2^2 + 1,\ x_1 - 3x_2y^3 + 9x_2y^2 - 9x_2y + 3x_2,\ y^4 - 4y^3 + 6y^2 - 4y + \frac{2}{3} \right\}$$

nenhum polinômio da forma $x_1 - h_1$, com $h_1 \in \mathbb{Q}[y]$, e desta forma temos que $\mathbb{Q}(\beta) \neq \mathbb{Q}(\sqrt[4]{3}, i)$.

No Exemplo 2.2.4, note que temos $\mathbb{Q}(\alpha) = \mathbb{Q}(\frac{-\alpha^2 + 2\alpha + 1}{\alpha})$ e

$$\alpha = \frac{5}{4}\beta - \frac{5}{2}, \text{ onde } \beta = \frac{-\alpha^2 + 2\alpha + 1}{\alpha} .$$

2.3 Programação Inteira

Nesta seção utilizamos a teoria desenvolvida na Seção 2.1 para encontrar soluções para um problema de programação inteira.

O problema da programação inteira tem a seguinte forma: Sejam $a_{ij} \in Z$, $b_i \in Z$, e $c_j \in R$, para $i = 1,...,n$ e $j = 1,...,m$; desejamos encontrar uma solução $(\delta_1,\delta_2,...,\delta_m)$ em $Z^m_{\geq 0}$ do sistema

$$\text{(2.3.1)} \qquad \begin{cases} a_{11}\delta_1 + a_{12}\delta_2 + \cdots + a_{1m}\delta_m = b_1 \\ a_{21}\delta_1 + a_{22}\delta_2 + \cdots + a_{2m}\delta_m = b_2 \\ \vdots \\ a_{n1}\delta_1 + a_{n2}\delta_2 + \cdots + a_{nm}\delta_m = b_n \end{cases}$$

que minimize a "função custo"

$$\text{(2.3.2)} \qquad c(\delta_1,\delta_2,...,\delta_m) = \sum_{j=1}^{m} c_j\delta_j$$

Nosso objetivo aqui é aplicar os resultados de 2.1 para indicar um método de solução para este problema. Nossa estratégia é:

(1) Transpor o problema de programação inteira para um problema sobre polinômios.

(2) Usar bases de Groebner para resolver o problema polinomial.

(3) Transpor a solução do problema polinomial de volta para a solução do problema de programação inteira.

Primeiramente iremos resolver o caso particular em que todos os a_{ij}'s e b_i's são inteiros não negativos. Iremos nos concentrar primeiramente na resolução do sistema (2.3.1) sem levar em conta a condição da função custo (Equação 2.3.2).

Introduzimos uma variável para cada equação linear em (2.3.1), digamos $x_1,x_2,...,x_n$, e uma variável para cada incógnita δ_j , digamos $y_1,y_2,...,y_m$. Representamos então as equações em (2.3.1) como

$$x_i^{a_{i1}\delta_1+\cdots+a_{im}\delta_m}=x_i^{b_i}$$

para $i = 1,...,n$. O sistema (2.3.1) pode então ser representado como um monômio

$$x_1^{a_{11}\delta_1+a_{12}\delta_2+\cdots+a_{1m}\delta_m}\cdots x_n^{a_{n1}\delta_1+a_{n2}\delta_2+\cdots+a_{nm}\delta_m}=x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n},$$

ou equivalentemente,

$$(2.3.3)\qquad \left(x_1^{a_{11}}x_2^{a_{21}}\cdots x_n^{a_{n1}}\right)^{\delta_1}\cdots\left(x_1^{a_{1m}}x_2^{a_{2m}}\cdots x_n^{a_{nm}}\right)^{\delta_m}=x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}.$$

Notamos que o lado esquerdo do monômio em (2.3.3) pode ser visto como a imagem do monômio $y_1^{\delta_1}y_2^{\delta_2}\cdots y_m^{\delta_m}$ pela aplicação polinomial

$$\phi: k[y_1,...,y_m]\to k[x_1,...,x_n]$$

$$y_j\to x_1^{a_{1j}}x_2^{a_{2j}}\cdots x_n^{a_{nj}}$$

O seguinte lema então é claro, supondo que todos a_{ij}'s e b_i's são não-negativos..

Lema 2.3.1. Existe uma solução $(\delta_1,\delta_2,...,\delta_m)\in\mathcal{Z}_{\geq 0}^m$ do sistema (2.3.1) se e somente se o monômio $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ é a imagem por ϕ de um monômio em $k[y_1,...,y_m]$. Ainda se $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}=\phi(y_1^{\delta_1}y_2^{\delta_2}\cdots y_m^{\delta_m})$ então $(\delta_1,\delta_2,...,\delta_m)\in\mathcal{Z}_{\geq 0}^m$ é uma solução do sistema (2.3.1).

Na Seção 2.1 apresentamos um algoritmo para determinar quando um dado elemento de $k[x_1,...,x_n]$ está na imagem de uma aplicação como ϕ. Todavia, de acordo com o lema acima, é necessário que o monômio $x_1^{b_1}x_2^{b_2}\cdots x_n^{b_n}$ seja a imagem de um monômio. Mas como a aplicação ϕ leva as variáveis y_j em monômios de $k[x_1,...,x_n]$, temos o lema a seguir, no qual utilizamos a notação acima e supomos que todos os a_{ij}'s e b_i's são inteiros não-negativos.

Lema 2.3.2. Se $x_1^{b_1}x_2^{b_2}...x_n^{b_n}$ está na imagem de ϕ, então $x_1^{b_1}x_2^{b_2}...x_n^{b_n}$ é a imagem de um monômio $y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m} \in k[y_1,...,y_m]$.

Prova:

Sejam $K = \left\langle y_j - x_1^{a_{1j}}x_2^{a_{2j}}...x_n^{a_{nj}} \mid j = 1,...,m \right\rangle$ o ideal considerado no Teorema 2.1.4 e G uma base de Groebner de K com respeito a uma ordem de eliminação com as variáveis x maiores que as variáveis y. Então pelo Teorema 2.1.4 temos

$$x_1^{b_1}x_2^{b_2}...x_n^{b_n} \in \text{im}(\phi) \Leftrightarrow x_1^{b_1}x_2^{b_2}...x_n^{b_n} \xrightarrow{G}_+ h \text{ com } h \in k[y_1,...y_m].$$

Temos ainda, se $x_1^{b_1}x_2^{b_2}...x_n^{b_n} \xrightarrow{G}_+ h$ com $h \in k[y_1,...y_m]$ então $x_1^{b_1}x_2^{b_2}...x_n^{b_n} = \phi(h)$.

Basta portanto mostrar que $h \in k[y_1,...y_m]$ é um monômio.

Observamos primeiramente que os polinômios que geram o ideal K são todos diferenças de dois monômios. De acordo com o Algoritmo de Buchberger para computar uma base de Groebner G devemos adicionar o resto dos S-polinômios $S(f_i,f_j)$ pela divisão por $F = \{f_1,...,f_s\}$, onde F é um conjunto de geradores de K (e contendo os geradores iniciais de K) em um determinado instante do algoritmo. Como os S-polinômios cancelam os termos líderes dos polinômios em questão, temos que $S(f_i,f_j)$ é uma diferença de dois monômios para qualquer $f_i,f_j \in F$. Da mesma forma ao reduzirmos em um passo uma diferença de dois monômios por outro polinômio da mesma forma obtemos novamente uma diferença de dois monômios. Temos então que todos os polinômios em G são diferenças de dois monômios (veja Exemplo 2.3.3). Logo se $x_1^{b_1}x_2^{b_2}...x_n^{b_n}$ está na imagem de ϕ então $x_1^{b_1}x_2^{b_2}...x_n^{b_n}$ se reduz a um polinômio $h \in k[y_1,...y_m]$. Mas a redução em um passo de um monômio por uma diferença de dois monômios é um monômio. Logo como a redução é feita passo a passo, h é um monômio e o lema está provado.□

A prova do Lema 2.3.2 nos fornece um método para determinar quando (2.3.1) tem solução, bem como encontrar uma solução:

(1) Computar uma base de Groebner G de $K = \left\langle y_j - x_1^{a_{1j}} x_2^{a_{2j}} \ldots x_n^{a_{nj}} \mid j = 1,\ldots,m \right\rangle$ com respeito a uma ordem de eliminação com as variáveis x maiores que as variáveis y;

(2) Encontrar o resto h da divisão do monômio $x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$ por G;

(3) Se $h \notin k[y_1,\ldots,y_m]$, então o sistema (2.3.1) não tem soluções inteiras não-negativas. Se $h = y_1^{\delta_1} y_2^{\delta_2} \ldots y_m^{\delta_m}$, então $\left(\delta_1,\delta_2,\ldots,\delta_m\right)$ é uma solução do sistema (2.3.1).

Exemplo 2.3.3. Considere o sistema

$$\begin{cases} 2\delta_1 + \delta_2 + 2\delta_3 = 8 \\ 2\delta_2 + \delta_3 = 6 \end{cases}$$

Adicionamos uma variável x para cada equação: x_1 e x_2.

Adicionamos uma variável y para cada incógnita: y_1, y_2 e y_3.

De acordo com teoria desenvolvida acima a aplicação polinomial correspondente é dada por:

$$k[y_1,y_2,y_3] \to k[x_1,x_2]$$

$$\begin{aligned} y_1 &\to x_1^2 \\ y_2 &\to x_1 x_2^2 \\ y_3 &\to x_1^2 x_2 \end{aligned}$$

e desta forma $K = \left\langle y_1 - x_1^2,\ y_2 - x_1 x_2^2,\ y_3 - x_1^2 x_2 \right\rangle \subset k[x_1,x_2,y_1,y_2,y_3]$. Computamos a base de Groebner reduzida G para K com respeito à ordem lexicográfica com $x_1 > x_2 > y_1 > y_2 > y_3$, obtendo $G = \left\{ f_1,\ldots,f_{10} \right\}$, onde $f_1 = x_1^2 - y_1$, $f_2 = x_1 x_2^2 - y_2$, $f_3 = x_2 y_1 - y_3$, $f_4 = x_1 x_2 y_3 - y_1 y_2$, $f_5 = x_1 y_3^2 - y_1^2 y_2$, $f_6 = x_2 y_3^2 - y_1^2 y_2^2$, $f_7 = x_2^2 y_3^2 - y_1 y_2^2$, $f_8 = x_1 y_2 - x_2 y_3$, $f_9 = x_2^3 y_3 - y_2^2$, $f_{10} = y_1^3 y_2^2 - y_3^4$.

Temos então

$$x_1^8 x_2^6 \to_+ y_1 y_2^2 y_3^2 = h \text{ , onde } h \text{ é reduzido com respeito a } G.$$

Usando os expoentes de h temos que (1,2,2) é uma solução do sistema dado.

Voltamos nossa atenção agora para o caso mais geral onde os a_{ij}'s e b_i's em (2.3.1) são inteiros não necessariamente não-negativos. Uma vez mais estaremos interessados em determinar quando o sistema (2.3.1) tem soluções e em encontrar tais soluções ignorando a condição da "função custo". Procederemos como no caso anterior exceto que neste caso teremos expoentes negativos nas variáveis x. É obvio desta forma que isto não pode ser feito no anel de polinômios $k[x_1,...x_n]$. Adicionamos então uma nova variável w e trabalhamos no anel afim $k[x_1,...x_n,w] / I$ onde $I = \langle x_1 x_2 ... x_n w - 1 \rangle$. Podemos escolher inteiros não-negativos a'_{ij} e α_j para cada $j = 1,...,m$ e $i = 1,...,n$ tal que para cada $j = 1,...,m$ temos

$$(a_{1j},a_{2j},...,a_{nj}) = (a'_{1j},a'_{2j},...,a'_{nj}) + \alpha_j(-1,-1,...,-1) .$$

Por exemplo, $(-3,2,-5) = (2,7,0) + 5(-1,-1,-1)$. Então no anel afim $k[x_1,...x_n,w] / I$ podemos dar significado à classe $x_1^{a_{1j}} x_2^{a_{2j}} ... x_n^{a_{nj}} + I$ definindo

$$x_1^{a_{1j}} x_2^{a_{2j}} ... x_n^{a_{nj}} + I = x_1^{a'_{1j}} x_2^{a'_{2j}} ... x_n^{a'_{nj}} w^{\alpha_j} + I ,$$

pois

$$x_1^{a'_{1j}} x_2^{a'_{2j}} ... x_n^{a'_{nj}} w^{\alpha_j} - x_1^{a_{1j}} x_2^{a_{2j}} ... x_n^{a_{nj}} = x_1^{a_{1j}} x_2^{a_{2j}} ... x_n^{a_{nj}} (x_1^{a'_{1j} - a_{1j}} x_2^{a'_{2j} - a_{2j}} ... x_n^{a'_{nj} - a_{nj}} w^{\alpha_j} - 1)$$

$$= x_1^{a_{1j}} x_2^{a_{2j}} ... x_n^{a_{nj}} (x_1^{\alpha_j} x_2^{\alpha_j} ... x_n^{\alpha_j} w^{\alpha_j} - 1)$$

$$= x_1^{a_{1j}} x_2^{a_{2j}} ... x_n^{a_{nj}} ((x_1 x_2 ... x_n w)^{\alpha_j} - 1)$$

e, como

$$((x_1 x_2 ... x_n w)^{\alpha_j} - 1) = [(x_1 x_2 ... x_n w - 1)((x_1 x_2 ... x_n w)^{\alpha_j - 1} + (x_1 x_2 ... x_n w)^{\alpha_j - 2} + ... + (x_1 x_2 ... x_n w) + 1)] ,$$

temos que

$((x_1x_2...x_nw)^{\alpha_j} - 1) \in I = \langle x_1x_2...x_nw - 1 \rangle$, e portanto $x_1^{a'_{1j}}x_2^{a'_{2j}}...x_n^{a'_{nj}}w^{\alpha_j} - x_1^{a_{1j}}x_2^{a_{2j}}...x_n^{a_{nj}} \in I$.

Da mesma forma, $(b_1,b_2,...,b_n) = (b'_1,b'_2,...,b'_n) + \beta(-1,-1,...,-1)$, onde b_i e β são inteiros não-negativos para $i = 1,...,n$ e definimos

$$x_1^{b_1}x_2^{b_2}...x_n^{b_n} + I = x_1^{b'_1}x_2^{b'_2}...x_n^{b'_n}w^{\beta} + I .$$

Temos desta forma a seguinte equação, que corresponde à Equação (2.3.3):

$$(2.3.4) \qquad \left(x_1^{a'_{11}}...x_n^{a'_{n1}}w^{\alpha_1}\right)^{\delta_1}...\left(x_1^{a'_{1m}}...x_n^{a'_{nm}}w^{\alpha_m}\right)^{\delta_m} + I = x_1^{b'_1}...x_n^{b'_n}w^{\beta} + I .$$

Procedendo como no caso anterior podemos ver que o lado esquerdo desta equação pode ser visto como a imagem do monômio $y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m}$ pelo homomorfismo de k-álgebras

$$k[y_1,...,y_m] \to k[x_1,...,x_n,w] / I$$

$$y_j \to x_1^{a'_{1j}}x_2^{a'_{2j}}...x_n^{a'_{nj}}w^{\alpha_j} + I$$

Como no caso anterior, e usando o conjunto de notações acima, temos:

Lema 2.3.4. Existe uma solução $(\delta_1,\delta_2,...,\delta_m) \in \mathcal{Z}_{\geq 0}^m$ do sistema (2.3.1) se e somente se $x_1^{b'_1}...x_n^{b'_n}w^{\beta} + I$ é a imagem por ϕ de um monômio em $k[y_1,...,y_m]$. Ainda, se $x_1^{b'_1}...x_n^{b'_n}w^{\beta} + I = \phi(y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m})$, então $(\delta_1,\delta_2,...,\delta_m)$ é uma solução do sistema (2.3.1).

Na Seção 2.1 apresentamos um algoritmo para determinar quando um elemento de $[x_1,...,x_n,w] / I$ está na imagem de um homomorfismo de álgebras afins tais como ϕ (veja Teorema 2.1.4). Como no primeiro caso considerado, o lema acima exige que $x_1^{b'_1}...x_n^{b'_n}w^{\beta} + I$ seja a imagem de um monômio e não de um polinômio qualquer. De modo análogo temos:

Lema 2.3.5. Se $x_1^{b_1'}...x_n^{b_n'}w^{\beta} + I$ está na imagem de ϕ, então $x_1^{b_1'}...x_n^{b_n'}w^{\beta} + I$ é a imagem de um monômio $y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m} \in k[y_1,...y_m]$.

Prova:

Sejam $\left\langle x_1x_2...x_nw - 1,\ y_j - x_1^{a_{1j}'}...x_n^{a_{nj}'}w^{\alpha_j} \mid j = 1,2,...,m \right\rangle \subset k[x_1,...,x_n,w,y_1,...,y_m]$ e G uma base de Groebner de K com respeito a uma ordem de eliminação com as variáveis x e w maiores que as variáveis y. Então pelo Teorema 2.1.10 temos:

$$x_1^{b_1'}...x_n^{b_n'}w^{\beta} + I \in \text{im}(\phi) \Leftrightarrow x_1^{b_1'}...x_n^{b_n'}w^{\beta} \xrightarrow{G} h \in k[y_1,...,y_m].$$

Temos ainda que se $x_1^{b_1'}...x_n^{b_n'}w^{\beta} \xrightarrow{G} h$ com $h \in k[y_1,...,y_m]$, então $x_1^{b_1'}...x_n^{b_n'}w^{\beta} + I = \phi(h)$.

Assim como no Lema 2.3.1, os polinômios que geram K são todos diferenças de dois monômios, e portanto podemos novamente utilizar os argumentos do Lema 2.3.2. □

Exemplo 2.3.6. Considere o seguinte sistema

$$\begin{cases} 3\delta_1 - 2\delta_2 + 2\delta_3 - 2\delta_4 = 4 \\ 4\delta_1 + \ \delta_2 - 2\delta_3 \qquad = 2 \end{cases}$$

Temos duas variáveis, x_1 e x_2, uma para cada equação. Temos também 4 variáveis, y_1, y_2, y_3, y_4, uma para cada incógnita. Seja o ideal $I = \langle x_1x_2w - 1 \rangle$ e considere o homomorfismo de álgebras

$$\mathbb{Q}[y_1,y_2,y_3,y_4] \to \mathbb{Q}[x_1,x_2,w] / I$$

$$\begin{aligned} y_1 &\to x_1^3x_2^4 + I \\ y_2 &\to x_2^3w^2 + I \\ y_3 &\to x_1^4w^2 + I \\ y_4 &\to x_2^2w^2 + I \end{aligned}$$

Desta forma $K = \left\langle y_1 - x_1^3x_2^4,\ y_2 - x_2^3w^2,\ y_3 - x_1^4w^2,\ y_4 - x_2^2w^2,\ x_1x_2w - 1 \right\rangle$. Considere a ordem lexicográfica com $x_1 > x_2 > w > y_1 > y_2 > y_3 > y_4$. Computando a base de Groebner reduzida do ideal K com a ordem acima obtemos

$G = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9\}$, onde $f_1 = y_1^2 y_3^4 y_4^7 - 1$, $f_2 = w - y_1 y_2 y_3^3 y_4^4$, $f_3 = y_1^2 y_3^2 y_4^9 - y_2^4$, $f_4 = y_1^2 y_3 y_4^{10} - y_2^6$, $f_5 = y_1^2 y_4^{11} - y_2^8$, $f_6 = y_1^2 y_3^3 y_4^8 - y_2^2$, $f_7 = y_2^2 y_3 - y_4$, $f_8 = x_1 - y_1 y_3^2 y_4^3$ e $f_9 = x_2 - y_1^2 y_2 y_3^4 y_4^6$. Reduzimos agora o monômio $x_1^4 x_2^2$ por G. Temos então

$$x_1^4 x_2^2 \xrightarrow{f_1 f_8 f_9} y_1^4 y_2^2 y_3^8 y_4^{10}$$
$$\xrightarrow{f_1} y_1^2 y_2^2 y_3^4 y_4^3$$
$$\xrightarrow{f_7} y_1^2 y_3^3 y_4^4$$

e $y_1^2 y_3^3 y_4^4$ é reduzido com respeito a G. Observando o expoente dos diferentes monômios obtidos durante a redução temos as seguintes soluções para o sistema :

(4,2,8,10), (2,2,4,3) e (2,0,3,4).

Iremos voltar nossa atenção agora ao nosso problema original, i.e., encontrar soluções do sistema (2.3.1) que minimizem a função custo $c(\delta_1,\delta_2,\ldots,\delta_m) = \sum_{j=1}^{m} c_j \delta_j$ (Equação (2.3.2)). Podemos observar que a única exigência que fizemos em relação à ordem de monômios no processo de encontrar soluções para o sistema (2.3.1) foi de que esta ordem fosse uma ordem de eliminação entre as variáveis x_i, w e y, onde x_i e w eram maiores que y. Nossa estratégia para minimizar a função custo será utilizar os c_j's para definir uma ordem de termos.

Definição 2.3.7. Uma ordem de termos $<_c$ nas variáveis y é dita compatível com a função custo c e a aplicação ϕ se

$$\left.\begin{array}{l} \phi\left(y_1^{\delta_1} y_2^{\delta_2} \ldots y_m^{\delta_m}\right) = \phi\left(y_1^{\delta_1'} y_2^{\delta_2'} \ldots y_m^{\delta_m'}\right) \\ e \\ c(\delta_1,\ldots,\delta_m) < c(\delta_1',\ldots,\delta_m') \end{array}\right\} \Rightarrow y_1^{\delta_1} y_2^{\delta_2} \ldots y_m^{\delta_m} <_c y_1^{\delta_1'} y_2^{\delta_2'} \ldots y_m^{\delta_m'}$$

As ordens de termos nas variáveis y compatíveis com c e ϕ são exatamente as ordenações de termos que nos fornecerão as soluções de (2.3.1) com menor custo, conforme mostra a proposição abaixo, na qual utilizamos a notação introduzida acima.

Proposição 2.3.8. Seja G uma base de Groebner de K com respeito a uma ordem de eliminação com as variáveis x e w maiores que as variáveis y, e uma ordem $<_c$ nas variáveis y a qual é compatível com a função custo c e a aplicação ϕ. Se $x_1^{b_1'}x_2^{b_2'}...x_n^{b_n'}w^{\beta} \xrightarrow{G}_{+} y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m}$, onde $y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m}$ é reduzido com respeito a G, então $(\delta_1,...,\delta_m)$ é uma solução do sistema (2.3.1) que minimiza a função custo c.

Prova:

Seja $x_1^{b_1'}x_2^{b_2'}...x_n^{b_n'}w^{\beta} \rightarrow_{+} y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m}$ com $y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m}$ reduzido com respeito a G. Então pelo Lema 2.3.4 temos que $(\delta_1,..., \delta_m)$ é uma solução do sistema 2.3.1. Suponhamos agora que exista uma outra solução $(\delta_1',..., \delta_m')$ do sistema 2.3.1 a qual possua "menor" custo com relação a c, i.e., $\sum_{j=1}^{m} c_j\delta_j' < \sum_{j=1}^{m} c_j\delta_j$. Como $(\delta_1',..., \delta_m')$ é uma solução do sistema 2.3.1 temos que

$$\phi(y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m}) = \phi(y_1^{\delta_1'}y_2^{\delta_2'}...y_m^{\delta_m'}) = x_1^{b_1'}x_2^{b_2'}...x_n^{b_n'}w^{\beta} + I,$$

e logo temos que $y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m} - y_1^{\delta_1'}y_2^{\delta_2'}...y_m^{\delta_m'} \in \ker(\phi)$. Pelo Teorema 2.1.2, $\ker(\phi) \subseteq K$, e portanto $y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m} - y_1^{\delta_1'}y_2^{\delta_2'}...y_m^{\delta_m'} \in K$. Temos então que $y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m} - y_1^{\delta_1'}y_2^{\delta_2'}...y_m^{\delta_m'} \xrightarrow{G}_{+} 0$. Como $<_c$ é uma ordem nas variáveis y a qual é compatível com a função custo c e a aplicação ϕ, temos que $y_1^{\delta_1'}y_2^{\delta_2'}...y_m^{\delta_m'} <_c y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m}$, e portanto $lt(y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m} - y_1^{\delta_1'}y_2^{\delta_2'}...y_m^{\delta_m'}) = y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m}$. No entanto $y_1^{\delta_1}y_2^{\delta_2}...y_m^{\delta_m}$ é reduzido com respeito a G e portanto não pode ser reduzido a 0 por G. Logo tal solução deve ter um custo maior com relação à função custo c.□

Podemos obter uma solução minimal diferente se usarmos uma ordem diferente, desde que tenhamos uma ordem de eliminação com as variáveis x e w maiores que as variáveis y, e uma ordem nas variáveis y compatível com a função custo c e a aplicação ϕ.

Consideremos o caso particular em que a função custo c envolva apenas coeficientes positivos, isto é, $c_j > 0$, $j = 1,2,...,m$. A seguinte ordem é então compatível com a função custo e a aplicação ϕ: Primeiro ordene os monômios usando a função custo, e caso sejam iguais, por uma outra ordem qualquer. O exemplo abaixo ilustra esta idéia.

Exemplo 2.3.9. Considere o sistema do exemplo 2.3.6

$$\begin{cases} 3\delta_1 - 2\delta_2 + 2\delta_3 - 2\delta_4 = 4 \\ 4\delta_1 + \delta_2 - 2\delta_3 = 2 \end{cases}$$

com a função custo

$$c(\delta_1, \delta_2, \delta_3, \delta_4) = \delta_1 + 10\delta_2 + 100\delta_3 + 1000\delta_4 .$$

Utilizamos *lex* nas variáveis x e w com $x_1 > x_2 > w$. Os monômios em y são ordenados primeiramente usando a função custo e, caso estes sejam iguais, com *lex* onde $y_1 > y_2 > y_3 > y_4$. Isto é, $y_1^{\delta_1} y_2^{\delta_2} y_3^{\delta_3} y_4^{\delta_4} < y_1^{\delta_1'} y_2^{\delta_2'} y_3^{\delta_3'} y_4^{\delta_4'}$ se e somente se

$$\delta_1 + 10\delta_2 + 100\delta_3 + 1000\delta_4 < \delta_1' + 10\delta_2' + 100\delta_3' + 1000\delta_4'$$

ou

$$\delta_1 + 10\delta_2 + 100\delta_3 + 1000\delta_4 = \delta_1' + 10\delta_2' + 100\delta_3' + 1000\delta_4' \quad \text{e} \quad y_1^{\delta_1} y_2^{\delta_2} y_3^{\delta_3} y_4^{\delta_4} <_{lex} y_1^{\delta_1'} y_2^{\delta_2'} y_3^{\delta_3'} y_4^{\delta_4'}.$$

Finalmente usamos uma ordem de eliminação com w e as variáveis x maiores que as variáveis y. A base de Groebner reduzida de K é $G = \{g_1,...,g_5\}$, onde $g_1 = w - y_1 y_2^9 y_3^7$, $g_2 = y_1^2 y_2^{14} y_3^{11} - 1$, $g_3 = y_4 - y_2^4 y_3$, $g_4 = x_1 - y_1 y_2^6 y_3^5$ e $g_5 = x_2 - y_1^2 y_2^{13} y_3^{10}$.

Temos que $x_1^4 x_2^2 \xrightarrow{G}_+ y_1^2 y_2^8 y_3^7$, e portanto (2,8,7,0) é uma solução de custo mínimo.

3. Apêndice

CoCoA[1]

CoCoA é um software para manipulação de expressões em Álgebra Comutativa e capaz de realizar operações sofisticadas em anéis de polinômios em n variáveis e em vários dados relacionados com eles (ideais, módulos, matrizes, funções racionais). O sistema é capaz de realizar operações tais como:

- Somas, produtos, potências, derivadas, mmc e mdc de polinômios.
- Somas, produtos, potências, derivadas de funções racionais.
- Somas, produtos, potências de ideais.
- Somas de módulos.
- Somas, produtos, potências, determinantes, adjuntas de matrizes.
- Bases de Groebner de ideais e módulos.
- Syzygies de ideais e módulos.

CoCoA inclui uma linguagem de programação semelhante a Pascal, que permite o usuário personalizar o sistema e criar novas *bibliotecas*. Referências são obtidas em [5]. É importante ressaltar que o príncipio fundamental em todas as operações realizadas no **CoCoA** é a implementação do algoritmo de Buchberger para o cômputo das bases de Groebner de um ideal e/ou módulo.

Nesta seção listamos os diversos algoritmos implementados no **CoCoA** e a resolução dos exemplos numéricos apresentados ao longo do texto. Vale ressaltar que os algoritmos implementados são os mesmos apresentados anteriormente e não tivemos em momento nenhum a preocupação com a eficiência computacional dos mesmos. Desta forma o cálculo de bases de Groebner através do algoritmo de Buchberger pode, em alguns casos, se tornar extremamente demorado e portanto, nas aplicações referentes às Seções 2.1, 2.2 e 2.3, utilizamos bases de Groebner calculadas através dos algoritmos implementados no próprio **CoCoA** .

---

[1] A. Capani, G. Niesi, L. Robiano,
CoCoA, a system for doing Computations in Commutative Algebra,
Available via anonymous ftp from: cocoa.dima.unige.it

- **Algumas rotinas no software CoCoA.**

Exemplo 1.3.2

```
<<'reducao.coc';                -- carrega algoritmo divisão.
Use R::=Q[xy],Lex;              -- define anel e ordem.
F:=x^2y+xy^2+2y+1;              -- polinômio a ser dividido.
G:=[x^2+2xy];                   -- Lista de divisores.
Reducao(F,G);                   -- Executa divisão/redução.
-----------------------------------------------------------------
--Resposta:
        reduzido por G(1) a  -xy^2 + 2y + 1
        Resto=-xy^2 + 2y + 1
        A(1)=y
```

Exemplo 1.3.3

```
<<'reducao.coc';                -- carrega algoritmo divisão.
Use R::=Q[xy],DegLex;           -- define anel e ordem.
F:=x^2y^2+2xy^2-xy;             -- polinômio a ser dividido.
G:=[x+2y+1];                    -- Lista de divisores.
Reducao(F,G);                   -- Executa divisão/redução.
-----------------------------------------------------------------
--Resposta:
        reduzido por G(1) a  -2xy^3 + xy^2 - xy
        reduzido por G(1) a  4y^4 + xy^2 + 2y^3 - xy
        reduzido por G(1) a  4y^4 - xy - y^2
        reduzido por G(1) a  4y^4 + y^2 + y
        Resto=4y^4 + y^2 + y
        A(1)=xy^2 - 2y^3 + y^2 - y
```

Exemplo 1.3.5

```
<<'reducao.coc';                -- carrega algoritmo divisão.
Use R::=Q[yx],Lex;              -- define anel e ordem.
F:=y^2x;                        -- polinômio a ser dividido.
G:=[yx-y,y^2-x];                -- Lista de divisores.
Reducao(F,G);                   -- Executa divisão/redução.
-----------------------------------------------------------------
--Resposta:
        reduzido por G(1) a  y^2
        reduzido por G(2) a  x
        Resto=x
        A(1)=y
        A(2)=1
```

Exemplo 1.3.9

```
<<'reducao.coc';                -- carrega algoritmo divisão.
Use R::=Q[xy],Lex;              -- define anel e ordem.
F:=x^3y^3+2y^2;                 -- polinômio a ser dividido.
G:=[2xy^2+3x+4y^2,y^2-2y-2];    -- Lista de divisores.
Reducao(F,G);                   -- Executa divisão/redução.
-----------------------------------------------------------------
--Resposta:
        reduzido por G(1) a  -3/2x^3y - 2x^2y^3 + 2y^2
        reduzido por G(1) a  -3/2x^3y + 3x^2y + 4xy^3 + 2y^2
        reduzido por G(1) a  -3/2x^3y + 3x^2y - 6xy - 8y^3 + 2y^2
        reduzido por G(2) a  -3/2x^3y + 3x^2y - 6xy - 14y^2 - 16y
        reduzido por G(2) a  -3/2x^3y + 3x^2y - 6xy - 44y - 28
        Resto=-3/2x^3y + 3x^2y - 6xy - 44y - 28
        A(1)=1/2x^2y - xy + 2y
        A(2)=-8y - 14
```

Exemplo 1.6.4

```
<<'spol.coc';                          -- carrega S_Polinômios.
Use R::=Q[xy],DegLex;                  -- define anel e ordem.
F:=x^2y^2+x^3+xy^2+2x;                 -- polinômio f.
G:=x^4y^2+x^5+2xy;                     -- polinômio g.
Print S_Polinomio(F,G);                -- calcula o S-polinômio de f e g.
-------------------------------------------------------------------------
--Resposta:
        S(F,G)= x^3y^2 + 2x^3 - 2xy
```

Exemplo 2.1.3

```
Use R::=Q[xuv],Lex;
K:=Ideal(u-x^2,v-x^3);
G:=ReducedGBasis(K);
Set Indentation;
PrintLn "Base de Groebner reduzida G= ",G;
-------------------------------------------------------------------------
--Resposta
                Base de Groebner reduzida G= [
                                              x^2 - u,
                                              xu - v,
                                              xv - u^2,
                                              u^3 - v^2]
```

Exemplo 2.1.5

```
Use R::=Q[x,y,u,v,w],Lex;
K:=Ideal(u-x^2,v-x-y,w-x^2-2xy);
G:=ReducedGBasis(K);                   -- Calcula base Groebner reduzida.
R:=NF(3x^2+2xy+y^2,G);                 -- Reduz polinômio em relação a G.
Set Indentation;
PrintLn "Base de Groebner reduzida G= ",G;
PrintLn "R= ",R,"  ;onde R e reduzido com respeito a G";
-------------------------------------------------------------------------
-- Resposta
             Base de Groebner reduzida G= [
                                            x + y - v,
                                            y^2 - v^2 + w,
                                            yv + 1/2u - v^2 + 1/2w,
                                            yu + yw + uv - vw,
                                            u^2 - 4uv^2 + 2uw + w^2]

              R= 2u + v^2  ;onde R e reduzido com respeito a G
```

Exemplo 2.1.7

```
Use R::=Q[x,y,u,v,w],Lex;
K:=Ideal(u+x^2-x,v-y,w-x+y);
G:=ReducedGBasis(K);                   -- Calcula base de Groebner reduzida.
Set Indentation;
PrintLn "Base de Groebner reduzida G= ",G;
-------------------------------------------------------------------------
-- Resposta
          Base de Groebner reduzida G= [
                                         y - v,
                                         x - v - w,
                                         u + v^2 + 2vw - v + w^2 - w]
```

Exemplo 2.1.12

```
Use R::=Q[x,y,u,v,w],Lex;
K:=Ideal(xy+y,u-x^2-y,v-x-y,w-x^3+xy^2);
G:=ReducedGBasis(K);                    -- Calcula base Groebner reduzida.
I:=Ideal(xy+y);
F:=(x^2+y)*(x+y)-(x^3-xy^2);
Set Indentation;
If IsIn(F,I) Then
                    -- Se estiver bem definida calcula Groebner
                    PrintLn "Base de Groebner reduzida G= ",G;
               Else
                    PrintLn "Aplicacao nao esta  bem definida";
End;

-------------------------------------------------------------------
-- Resposta
   Base de Groebner reduzida G= [
                                 uv - w,
                                 uw + v^4 + 2v^3 - v^2w - vw - 2w,
                                 v^5 + 2v^4 - v^3w - v^2w - 2vw + w^2,
                                 yw - 8y + 4u - v^3 - 4v^2 + w,
                                 x + y - v,
                                 y^2 - 3y + u - v^2,
                                 yv - 2y + u - v^2,
                                 yu - 4y + u - v^2,
                                 u^2 - 2u + v^3 + 2v^2 - vw - w]
```

Exemplo 2.2.4

```
Use R::=Q[xy],Lex;
J:=Ideal(x^2-5,xy+x^2-2x-1);
G:=ReducedGBasis(J);
Set Indentation;
PrintLn "Base de Groebner reduzida G=",G;
-------------------------------------------------------------------
-- Resposta
                Base de Groebner reduzida G=[
                                                x + 5/4y - 5/2,
                                                y^2 - 4y + 4/5]
```

Exemplo 2.2.6

```
Use R::=Q[x[1..2]y],Lex;
J:=Ideal(x[1]^2-3,x[2]^2-5,y-x[1]+x[2]);
G:=ReducedGBasis(J);
Set Indentation;
PrintLn "Base de Groebner reduzida G=",G;
-------------------------------------------------------------------
-- Resposta
                Base de Groebner reduzida G=[
                                                x[2] - 1/4y^3 + 9/2y,
                                                y^4 - 16y^2 + 4,
                                                x[1] - 1/4y^3 + 7/2y]
```

Exemplo 2.2.7

```
Use R::=Q[x[1..2]y],Lex;
J:=Ideal(x[1]^4-3,x[2]^2+1,x[1]y-(x[1]+x[2]));
G:=ReducedGBasis(J);
Set Indentation;
PrintLn "Base de Groebner reduzida G=",G;

Jlinha:=Ideal(x[1]^4-3,x[2]^2+x[1]^2,x[1]^2y-(x[1]^2+x[2]));
Glinha:=ReducedGBasis(Jlinha);
PrintLn "Base de Groebner reduzida Glinha=",Glinha;
-------------------------------------------------------------------------
-- Resposta
      Base de Groebner reduzida
                  G=[   x[2]^2 + 1,
                        y^4 - 4y^3 + 6y^2 - 4y + 2/3,
                        x[1] - 3x[2]y^3 + 9x[2]y^2 - 9x[2]y + 3x[2]]
      Base de Groebner reduzida Glinha=[
                                        x[2] + 3y^3 - 9y^2 + 9y - 3,
                                        y^4 - 4y^3 + 6y^2 - 4y + 2/3,
                                        x[1]^2 + 3y^2 - 6y + 3]
```

Exemplo 2.3.3

```
Use R::=Q[x[1..2]y[1..3]],Lex;
K:=Ideal(y[1]-x[1]^2,y[2]-x[1]x[2]^2,y[3]-x[1]^2x[2]);
G:=ReducedGBasis(K);                  -- Calcula base Groebner reduzida.
R:=NF(x[1]^8x[2]^6,G);                -- Redução por G.
Set Indentation;
PrintLn "Base de Groebner reduzida G= ",G;
PrintLn "R= ",R,"  ;onde R e reduzido com respeito a G)";
-------------------------------------------------------------------------
-- Resposta
        Base de Groebner reduzida G= [
                                        x[1]^2 - y[1],
                                        x[1]x[2]^2 - y[2],
                                        x[2]y[1] - y[3],
                                        x[1]x[2]y[3] - y[1]y[2],
                                        x[1]y[3]^2 - y[1]^2y[2],
                                        x[2]y[3]^3 - y[1]^2y[2]^2,
                                        x[2]^2y[3]^2 - y[1]y[2]^2,
                                        x[1]y[2] - x[2]y[3],
                                        x[2]^3y[3] - y[2]^2,
                                        y[1]^3y[2]^2 - y[3]^4]

        R= y[1]y[2]^2y[3]^2  ;onde R e reduzido com respeito a G)
```

Exemplo 2.3.6

```
Use R::=Q[x[1..2]wy[1..4]],Lex;
<<'reducao.coc';
K:=Ideal(y[1]-x[1]^3x[2]^4,y[2]-x[2]^3w^2,y[3]-x[1]^4w^2,y[4]-
x[2]^2w^2,x[1]x[2]w-1);
G:=ReducedGBasis(K);                    -- Calcula base Groebner reduzida.
Set Indentation;
PrintLn "Base de Groebner reduzida G= ",G;
Reducao(x[1]^4x[2]^2,G);
-------------------------------------------------------------------------
-- Resposta
        Base de Groebner reduzida G= [
                                        y[1]^2y[3]^4y[4]^7 - 1,
                                        w - y[1]y[2]y[3]^3y[4]^4,
                                        y[1]^2y[3]^2y[4]^9 - y[2]^4,
                                        y[1]^2y[3]y[4]^10 - y[2]^6,
                                        y[1]^2y[4]^11 - y[2]^8,
                                        y[1]^2y[3]^3y[4]^8 - y[2]^2,
                                        y[2]^2y[3] - y[4],
                                        x[1] - y[1]y[3]^2y[4]^3,
                                        x[2] - y[1]^2y[2]y[3]^4y[4]^6]

        reduzido por G(8) a  x[1]^3x[2]^2y[1]y[3]^2y[4]^3
        reduzido por G(8) a  x[1]^2x[2]^2y[1]^2y[3]^4y[4]^6
        reduzido por G(8) a  x[1]x[2]^2y[1]^3y[3]^6y[4]^9
        reduzido por G(1) a  x[1]x[2]^2y[1]y[3]^2y[4]^2
        reduzido por G(8) a  x[2]^2y[1]^2y[3]^4y[4]^5
        reduzido por G(9) a  x[2]y[1]^4y[2]y[3]^8y[4]^11
        reduzido por G(1) a  x[2]y[1]^2y[2]y[3]^4y[4]^4
        reduzido por G(9) a  y[1]^4y[2]^2y[3]^8y[4]^10
        reduzido por G(1) a  y[1]^2y[2]^2y[3]^4y[4]^3
        reduzido por G(7) a  y[1]^2y[3]^3y[4]^4

        Resto = y[1]^2y[3]^3y[4]^4

A(1)= x[1]x[2]^2y[1]y[3]^2y[4]^2 + x[2]y[1]^2y[2]y[3]^4y[4]^4 +
      y[1]^2y[2]^2y[3]^4y[4]^3
A(2)=0
A(3)=0
A(4)=0
A(5)=0
A(6)=0
A(7)=y[1]^2y[3]^3y[4]^3
A(8)=x[1]^3x[2]^2 + x[1]^2x[2]^2y[1]y[3]^2y[4]^3 +
     x[1]x[2]^2y[1]^2y[3]^4y[4]^6 + x[2]^2y[1]y[3]^2y[4]^2
A(9)=x[2]y[1]^2y[3]^4y[4]^5 + y[1]^2y[2]y[3]^4y[4]^4
```

Exemplo 2.3.9

```
Ordem:=Mat[[1,0,0,0,0,0,0],[0,1,0,0,0,0,0],[0,0,1,0,0,0,0],[0,0,0,1,10
,100,1000],[0,0,0,1,0,0,0],[0,0,0,0,1,0,0],[0,0,0,0,0,1,0]];
Use R::=Q[x[1..2]wy[1..4]],Ord(Ordem);
K:=Ideal(y[1]-x[1]^3x[2]^4,y[2]-x[2]^3w^2,y[3]-x[1]^4w^2,y[4]-
x[2]^2w^2,x[1]x[2]w-1);
G:=ReducedGBasis(K);                    -- Calcula base Groebner reduzida
Set Indentation;
R:=NF(x[1]^4x[2]^2,G);
PrintLn " Base de Groebner reduzida G= ",G;
PrintLn " Solucao de custo minimo, dada por =",R;
```

Exemplo 2.3.9 (continuação)

```
--Resposta
            Base de Groebner reduzida G=[  w - y[1]y[2]^9y[3]^7,
                                           y[1]^2y[2]^14y[3]^11 - 1,
                                           y[4] - y[2]^2y[3],
                                           x[1] - y[1]y[2]^6y[3]^5,
                                           x[2] - y[1]^2y[2]^13y[3]^10]

            Solucao de custo minimo, dada por y[1]^2y[2]^8y[3]^7.
```

Algoritmo Divisão/Redução

```
Define Reducao(F,G)

        A:=G;                    --dimensiona para o mesmo tamanho de G.

        For C:=1 To Len(G) Do
                A[C]:=0;
        End;
        R:=0;
        H:=F;
        S:=Len(G);

      While H<>0 Do;
                I:=1;
                Division:=FALSE;
                While (I<=S AND Division=FALSE) Do
                        If (LT(H) IsIn Ideal(LT(G[I]))) Then

A[I]:=A[I]+((LC(H)*LT(H))/(LC(G[I])*LT(G[I])));
                                        H:=H-
((LC(H)*LT(H))/(LC(G[I])*LT(G[I]))*(G[I]));
                                        Division:=TRUE;
                                        PrintLn "reduzido por G(", I,") a
",H+R;
                        Else
                                        I:=I+1;
                        End;
                End;

                If Division=FALSE Then
                        R:=R+LC(H)*LT(H);
                        H:=H-LC(H)*LT(H);
                End;


        End;
        Print NewLine,'Resto=',R;
        For C:=1 To Len(G) Do
              Print NewLine, 'A(',C,')=',A[C];
        End;
End;
```

Calcula S-polinômios

```
Define S_Polinomio(F,G);
    Mmc:=LCM(LT(F),LT(G));
    Spol:=Mmc*F/(LC(F)*LT(F))-Mmc*G/(LC(G)*LT(G));
    Return Spol;
 End;
```

Algoritmo de Buchberger

```
Define Base_Groebner(F);
        <<'spol.coc';
        G:=F;
        Glinha:=[];                              -- Inicializa com nulo.
        While G<>Glinha Do;
          Glinha:=G;
          For Cont:=1 To Len(Glinha) Do;
              For Cont0:=Cont To Len(Glinha) Do;

S:=NF((S_Polinomio(Glinha[Cont],Glinha[Cont0])),Glinha);
                        If S<>0 Then (Append(G,S));End;
              End;
          End;

        End;
        Set Indentation;                        -- Para melhor vizualizacao
        PrintLn "Groeber: G =" ,G;
End;
```

Exemplo

```
<<'buch.coc';
Use R::=Q[xy],DegLex;
L:=x^3-2xy;
M:=x^2y-2y^2+x;
F:=[L,M];
Base_Groebner(F);
```

BIBLIOGRAFIA

[1] W. Adams e P. Loustaunau (1994), *An Introduction to Gröebner Bases*, Graduate Studies in Mathematics 3, MAS, Providence.

[2] D. Cox, J. Little e D. O'Shea (1997), *Ideals, Varieties and Algorithms*, Springer Verlag, New York – Berlin – Heidelberg.

[3] D. Shannon e M. Sweedler, *Using Gröbner bases do determine algebra membership, split surjective algebra homomorphisms determine birational equivalence*, J.Symb. Comp. 6 (1988), 267-273.

[4] P. Conti e C. Traverso, *Buchberger algorithm and integer programming*, Lectures Notes in Comput. Sci., vol 539, Springer Verlag, Berlin and New York, 1991, 130-139.

[5] I. Stewart, *Galois Theory*, Chapman and Hall, London, 1973.

[6] A. Capani e G. Niesi, *CoCoA User's Manual*, Department of Mathematics, University of Genova.