Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

Lema de Seidenberg para Computar Geradores de um Radical

Dissertação de Mestrado

RENE BALTAZAR JUNIOR

Porto Alegre, 18 de março de 2011

Dissertação submetida por Rene Baltazar Júnior* **, como requisito parcial para a obtenção do grau de Mestre em Ciência Matemática, pelo Programa de Pós-Graduação em Matemática, do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.**

Professor Orientador:

Prof. Dra. Luisa Rodriguez Doering

Banca examinadora:

Prof. Dra. Luisa Rodriguez Doering (PPGMAT-UFRGS, Orientador)

Prof. Dr. Alveri Alves Sant'Ana (PPGMAT-UFRGS)

Prof. Dra. Ada Maria de Souza Doering (PPGMAT-UFRGS)

Prof. Dr. Ivan Edgardo Pan Perez (Universidad de la República-Uruguay)

*Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq)

Agradecimentos

Aos professores do Programa de Pós Graduação em Matemática da Universidade Federal do Rio Grande do Sul, pela oportunidade de estudar Matemática.

Para minha família, pelo apoio. Em especial à minha mãe, minha primeira professora; se não fosse ela, não teria aprendido a tabuada para poder ir à praia naquele verão. Ao meu pai, sendo um exemplo de pai, não poupando carinhos e atenção. Ao meu irmão, que tanto me orgulha.

À Danielle por ser uma pessoa incrível, pelos carinhos e momentos inesquecíveis ao seu lado.

Agradeço muito as professoras Ada Doering e Luisa Doering por todos os nossos seminários, horas de discussões e por me ensinarem a buscar entender sempre um pouco mais de Matemática.

Aos professores Alveri Santana, Ivan Pan e Yves Lequain, pela dedicação e interesse com a minha formação.

Aos amigos, sou muito agradecido por todos os momentos juntos, guardo um pouco de cada um comigo:

Adilson, Andre, Andréa, Carlos, Carolina, Daiana, Diego Chaves, Diego Lieban, Diego Marcon, Felipe Castro, Joao Helder, Josiane, Juliana, Juliane C., Laerte, Leandro, Lucas, Lucas Backes, Lucineia, Matheus, Miriam, Nicolau, Patrícia Guidolin, Patrícia K. K., Patropy, Pitágoras, Rafael, Raquel, Ricardo, Rodrigo, Saradia, Thaisa Muller, Thaisa Tamusiunas, Thiago Silva.

Resumo

O objetivo deste trabalho é computar, em alguns casos específicos, os geradores do radical de um ideal no anel de polinômios $K[x_1, ..., x_n]$. Para isso, utilizamos a teoria das bases de Groebner. Primeiramente, usamos o Lema de Seidenberg para computar os geradores do radical de um ideal zero-dimensional onde K é um corpo perfeito e depois utilizamos os resultados de R. Matsumoto para um corpo K de característica positiva e perfeito.

Abstract

The goal of this work is to compute in some specific cases the generators of the radical ideal in a polynomial ring $K[x_1, ..., x_n]$. For this, we use the theory of Groebner bases. First, we use Lemma Seidenberg to compute the generators of the radical of an zero-dimensional ideal, where K is a perfect field and then we used the results of R. Matsumoto for a field K of positive characteristic and perfect.

Índice

Introdução

O objetivo deste trabalho é estudar a seguinte questão:

Questão: *Dado os geradores $f_1, ..., f_s$ de um ideal I no anel de polinômios $K[x_1, ..., x_n]$, será que podemos encontrar os geradores do seu radical $\sqrt{I}$?*

Ao longo da história, para responder essa questão, o problema foi sendo separado de acordo com a estrutura do corpo K e, também, fazendo-se reduções a casos particulares de ideais. Da mesma forma, vamos estudar essa questão através de situações específicas. Antes disso, iniciamos apresentando um estudo de bases de Groebner e oferecemos algumas resultados dessas bases no primeiro capítulo. Nesse capítulo, responderemos ainda outras questões interessantes de Álgebra Computacional com a finalidade de estar familiarizando-se com as "boas"propriedades das bases de Groebner, conforme D. Cox em [3] e W. Adams em [1].

A primeira referência à resposta para essa questão foi oferecida por Seideinberg, mostrando o seguinte resultado:

(Lema de Seidenberg 2.1.13) Seja K um corpo perfeito e $I \subseteq K[x_1, ..., x_n]$ um ideal zero-dimensional. Suponhamos que, para todo $i \in \{1, ..., n\}$, existe um polinômio não nulo $g_i \in I \cap K[x_i]$ tal que $mdc(g_i, g_i') = 1$. Então $I = \sqrt{I}$.

Ao longo do capítulo 2, provaremos esse resultado e obteremos como con-

sequência um conjunto de geradores para o ideal radical de I; mais que isso, encontraremos um conjunto $\{g_1^\star, ..., g_n^\star\}$ com $g_i^\star \in K[x_i]$ tal que

$$\sqrt{I} = \langle I, g_1^\star, ..., g_n^\star \rangle.$$

Esse resultado de Seidenberg tem uma grande importância, pois impulsionou o estudo da possibilidade da construção de algoritmos e pode-se criar programas matemáticos implementáveis. Podemos citar Eisenbud, Huneke e Vasconcelos em [4] para computar a decomposição primária de um ideal, Matsumoto em [10] para computar radicais sobre corpos perfeitos de caraterística $p > 0$ e Kemper em [7] para computar radicais sobre corpos que são finitamente gerados por um corpo perfeito.

Para finalizar, o seguinte algoritmo de Matsumoto em [10] para computar o radical será discutido no capítulo 3.

(Algoritmo de Matsumoto 3.2.4) Seja K um corpo de característica $p > 0$ e um ideal $I \subseteq K[x_1, ..., x_n]$.

Entrada: Uma base de Groebner B para um ideal próprio I de $K[x_1, ..., x_n]$ com uma ordem monomial qualquer, e q um potência da característica p.

Saída: Uma base de Groebner para o radical $\sqrt{I}$.

Com a finalidade de apresentar o algoritmo, mostraremos que uma alternativa para computar o radical é transferir esse problema a uma questão de como determinar os geradores do núcleo de uma aplicação polinomial, que é resolvido com propriedades de bases de Groebner. Ou seja, o segredo será transferir o problema para um outro ambiente, resolvê-lo, para então voltar ao radical e determinar seus geradores.

Capítulo 1

Pré-requisitos

1.1 Ordem Monomial em $K[x_1, ..., x_n]$

O algoritmo da divisão no anel de polinômios em uma variável é construído conforme a ordenação natural dos monômios:

$$... > x^{m+1} > x^m > ... > x^2 > x > 1.$$

O que faremos nesta seção é apresentar e discutir um pouco as propriedades, através de exemplos, de uma ordem de monômios em $K[x_1, ..., x_n]$. Como veremos nas próximas seções, a escolha de uma ordem monomial é muito importante na construção de bases de Groebner de um ideal. Veremos também nas seções seguintes que em determinados momentos nossa ordem monomial poderá ser uma qualquer; mas em outros, nossa ordem deverá ser uma específica.

Iremos identificar um monômio em $K[x_1, ..., x_n]$ com a n-upla $\alpha = (\alpha_1, ..., \alpha_n) \in$

$\mathbb{N}^n$ escrevedo $x_1^{\alpha_1}...x_n^{\alpha_n} = x^\alpha$. Ou seja,

$$(\alpha_1, ..., \alpha_n) \longleftrightarrow x_1^{\alpha_1}...x_n^{\alpha_n}$$

Estabelecemos uma ordem em $\mathbb{N}^n$, para então passarmos para uma ordem de monômios em $K[x_1, ..., x_n]$ da seguinte forma:

$$\alpha > \beta \longrightarrow x^\alpha > x^\beta$$

Definimos agora, com as propriedades que nos interessam, uma ordem monomial em $K[x_1, ..., x_n]$, para, após, mostrar exemplos de algumas dessas ordens que serão utilizadas posteriormente.

Definição 1.1.1. *Uma ordem monomial em $K[x_1, ..., x_n]$ é uma relação $>$ em $\mathbb{N}^n$ satisfazendo:*
(i) $>$ é uma ordem total em $\mathbb{N}^n$;
(ii) Se $\alpha > \beta$ e $\gamma \in \mathbb{N}^n$, então $\alpha + \gamma > \beta + \gamma$;
(iii) $\mathbb{N}^n$ é um conjunto bem ordenado pela ordem $>$.

As seguintes definições são exemplos de ordens monomiais.

Definição 1.1.2. *Sejam α, β em $\mathbb{N}^n$ e $|\alpha| = \alpha_1 + ... + \alpha_n$, $|\beta| = \beta_1 + ... + \beta_n$.*
1. Ordem Lexicográfica: *$\alpha >_{lex} \beta$ se, e somente se, a entrada não nula mais a esquerda de $\alpha - \beta$ é positiva;*
2. Ordem Graduada Lexicográfica: *$\alpha >_{grlex} \beta$ se, e somente se, $|\alpha| > |\beta|$ ou ($|\alpha| = |\beta|$ e $\alpha >_{lex} \beta$));*
3. Ordem Graduada Lexicográfica Reversa: *$\alpha >_{grevlex} \beta$ se, e somente se, $|\alpha| > |\beta|$ ou ($|\alpha| = |\beta|$ e a entrada não nula mais a direita de $\alpha - \beta$ é negativa);*

Exemplo 1.1.3. *Sejam α e β em $\mathbb{N}^3$.*

- $(3,2,1) = \alpha >_{lex} \beta = (1,2,4)$, *pois* $\alpha - \beta = (2,0,-3)$.
  Então, $x^3y^2z >_{lex} xy^2z^4$;

- $(2,4,1) = \alpha >_{grlex} \beta = (1,6,0)$, *pois* $|\alpha| = |\beta| = 7$. *Como* $\alpha - \beta = (1,-2,1)$, *temos* $\alpha >_{grlex} \beta$. *Então,* $x^2y^4z >_{grlex} xy^6$;

- $(1,3,1) = \alpha >_{grevlex} \beta = (1,2,2)$, *pois* $|\alpha| = |\beta| = 5$. *Como* $\alpha - \beta = (0,1,-1)$, *temos* $\alpha >_{grevlex} \beta$. *Então,* $xy^3z >_{grlex} xy^2z^2$.

Definição 1.1.4. *Dados um polinômio não nulo* $f = \sum_\alpha a_\alpha x^\alpha \in K[x_1, ..., x_n]$ *e uma ordem* $>$ *monomial. Definimos:*

- *O grau de* f *como:* $grau(f) = max\{\alpha : a_\alpha \neq 0\}$.
- *O monômio líder de* f *como:* $LM(f) = x^{grau(f)}$.
- *O coeficiente líder de* f *como:* $LC(f) = a_{grau(f)}$.
- *O termo líder de* f *como:* $LT(f) = LC(f).LM(f)$.

1.2 Algoritmo de Divisão em $K[x_1, ..., x_n]$

Nesta seção queremos formular um algoritmo de divisão em $K[x_1, ..., x_n]$ para, então, estudar o problema da pertinência de polinômios de várias variáveis em um ideal I. Em outras palavras, dado um elemento $f \in K[x_1, ..., x_n]$ e $\{g_1, ..., g_s\}$ um conjunto finito de polinômios, queremos poder escrever

$$f = a_1g_1 + ... + a_sg_s + r$$

onde os $a_1, ...a_s$ são os quocientes na divisão pelos g_i's e r o resto da divisão em $K[x_1, ..., x_n]$. Veremos, também, que esse resto não é unicamente determinado, gerando uma dúvida sobre a pertinência de uma dado polinômio em um ideal.

A ideia básica do algoritmo é a mesma que no caso de uma variável: queremos cancelar o termo líder de f, com respeito a ordem de monômios fixada. Para ver isso, primeiro trabalharemos com alguns exemplos. Falaremos que um monômio x^α é divisível por outro x^β se existe um monômio x^ω tal que $x^\alpha = x^\beta x^\omega$.

Exemplo 1.2.1. *Observe que, da mesma forma que em $K[x]$, dividiremos em $K[x, y]$:*

$$f = xy^2 + 1 \text{ por } f_1 = xy + 1 \text{ e } f_2 = y + 1$$

usando a ordem lex com $x > y$.

Os termos líderes $LT(f_1) = xy$ e $LT(f_2) = y$ ambos dividem o termo líder $LT(f) = xy^2$. Como listaremos f_1 primeiro, y é o polinômio, assim como em uma variável, que produzirá um cancelamento de termo líder. Escrevemos:

$$\begin{array}{rr|l} xy^2 & +1 & \underline{xy+1,\, y+1} \\ -xy^2 & -y & y \\ \hline -y & +1 & \end{array}$$

Agora repetimos o processo sobre $-y + 1$. Porém, devemos passar a usar o polinômio f_2, pois $LT(f_1) = xy$ não divide $LT(-y + 1) = -y$. Sendo assim, obtemos:

$$\begin{array}{rr|l} xy^2 & +1 & \underline{xy+1,\, y+1} \\ -xy^2 & -y & y, \quad -1 \\ \hline -y & +1 & \\ y & +1 & \\ \hline & 2 & \end{array}$$

Como $LT(f_1)$ e $LT(f_2)$ não dividem 2, o resto da divisão é $r = 2$ e a divisão está pronta. Portanto, podemos escrever $f = xy^2 + 1$ na seguinte forma:

$$xy^2 + 1 = y(xy + 1) + (-1)(y + 1) + 2$$

Exemplo 1.2.2. *Nesse exemplo mostraremos um fato interessante que não ocorre em uma variável. Vamos dividir $f = x^2y + xy^2 + y^2$ por $f_1 = xy - 1$ e $f_2 = y^2 - 1$. Como no exemplo anterior, usaremos a ordem monominal lex com $x > y$ e primeiro efetuamos a divisão por f_1. Assim sendo, obtemos:*

$$\begin{array}{rrr|l} x^2y & +xy^2 & +y^2 & \underline{|xy-1,\, y^2-1} \\ -x^2y & +x & & x+y \\ \hline xy^2 & +y^2 & +x & \\ -xy^2 & +y & & \\ \hline x & +y^2 & +y & \end{array}$$

Note que $LT(f_1)$ e $LT(f_2)$ não dividem $LT(x + y^2 + y) = x$, porém $x + y^2 + y$ não é o resto da divisão pois $LT(f_2)$ divide y^2. Assim, se movemos x para o resto podemos continuar a divisão. Então, guardando x para o resto, prosseguimos da seguinte forma:

$$\begin{array}{rrr|l} x^2y & +xy^2 & +y^2 & \underline{|xy-1,\, y^2-1} \\ -x^2y & +x & & x+y,\quad 1 \\ \hline xy^2 & +y^2 & +x & \\ -xy^2 & +y & & \\ \hline x & +y^2 & +y & \\ \hline & +y^2 & +y & \\ & -y^2 & +1 & \\ \hline & y & +1 & \end{array}$$

Da mesma forma que antes, levamos y e 1 para o resto. Obtendo:

$$\begin{array}{rrr|l} x^2y & +xy^2 & +1 & |\underline{xy-1,\, y^2-1} \\ -x^2y & +x & & x+y, \quad 1 \\ \hline xy^2 & +y^2 & +x & \\ -xy^2 & +y & & \\ \hline x & +y^2 & +y & \\ \hline & +y^2 & +y & \\ & -y^2 & +1 & \\ \hline & y & +1 & \end{array}$$

Portanto, o resto da divisão é $x+y+1$, e obtemos:

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

Note que o resto é uma soma de monômios que não são divisíveis pelos termos líderes $LT(f_1)$ e $LT(f_2)$.

Observação 1.2.3. Usando o mesmo método do exemplo anterior, porém trocando a ordem em que dividimos os polinômios f_1 e f_2. Encontramos uma nova escrita:

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

Se compararmos com o exemplo anterior, veremos que conseguimos dois restos distintos. Isso mostra que o resto e os quocientes não são unicamente determinado quando exigimos que seus termos não sejam divisíveis por $LT(f_1), ..., LT(f_s)$. Nossas próximas seções discutirão esse fato.

O exemplo acima é uma ilustração bastante completa de como a divisão funciona. Tendo ele em vista, enunciamos o teorema da divisão em $K[x_1, ..., x_n]$.

Teorema 1.2.4. Algoritmo da Divisão em $K[x_1, ..., x_n]$ *Fixada uma ordem monomial* $>$ *e* $F = (f_1, ..., f_s)$ *uma s-upla ordenada de polinômios em* $K[x_1, ..., x_n]$. *Então, todo* $f \in K[x_1, ..., x_n]$ *pode ser escrito na forma:*

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

onde $a_i, r \in K[x_1, ..., x_n]$, *e* $r = 0$ *ou* r *é uma combinação, com coeficientes em* K, *de monômios que não são divisíveis por qualquer* $LT(f_1), ..., LT(f_s)$. *Chamaremos* r *de um resto da divisão de* f *por* F. *Além disso, se* $a_i f_i \neq 0$, *então temos que*

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

1.3 Ideais Monomiais e Lema de Dickson

Nesta seção definiremos ideais monomiais e mostraremos o Lema de Dickson, que será útil nas seções seguintes.

Definição 1.3.1. *Um ideal* $I \subseteq K[x_1, ..., x_n]$ *é um ideal monomial se existe um subconjunto* $A \subset \mathbb{N}^n$ *tal que* I *consiste de todos os polinômios que são uma soma finita da forma* $\sum_{\alpha \in A} h_\alpha x^\alpha$, *onde* $h_\alpha \in K[x_1, ..., x_n]$. *Nesse caso, escrevemos* $I = \langle x^\alpha : \alpha \in A \rangle$.

Antes de apresentar o Lema de Dickson, caracterizaremos todos os monômios que pertencem a um ideal monomial.

Lema 1.3.2. *Seja* $I = \langle x^\alpha : \alpha \in A \rangle$ *um ideal monomial. Então um monômio* x^β *está em* I *se, e somente se,* x^β *é divisível por* x^α, *para algum* $\alpha \in A$.

Demonstração: Se x^β é um múltiplo de x^α para algum $\alpha \in A$, então $x^\beta \in I$ pela definição de ideal. Por outro lado, se $x^\beta \in I$, então $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, onde $h_i \in K[x_1, ..., x_n]$ e $\alpha(i) \in A$. Se expandirmos cada h_i como uma combinação de

monômios, percebemos que todo termo do lado direito da equação é divisível por algum $x^{\alpha(i)}$. Tomando $\alpha(j)$ o mínimo do conjunto $\{\alpha(1), ..., \alpha(s)\}$, temos que todo termo do lado direito da equação é divisível por $x^{\alpha(j)}$. Então, o lado esquerdo x^{β} deve ter a mesma propriedade, completando a prova. □

Vamos apresentar, com o próximo lema, um resultado que garante que um polinômio pertence a um ideal monomial quando todos seus monômios também pertencem.

Lema 1.3.3. *Seja I uma ideal monomial e $f \in K[x_1, ..., x_n]$. Então, são equivalentes:*

(i) $f \in I$.

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

Demonstração: A implicação $(ii) \Rightarrow (i)$ é direta. A prova de $(i) \Rightarrow (ii)$ é similar a feita no lema anterior, bastando substituir x^{β} por f. □

Uma consequência imediata da parte (ii) do lema anterior é que um ideal monomial é unicamente terminado por seus monômios. Então, segue o seguinte corolário.

Corolário 1.3.4. *Dois ideais monomiais são iguais se, e somente se, eles contêm os mesmos monômios.*

O principal resultado que queremos mostrar nesta seção é que todos ideais monomiais de $K[x_1, ..., x_n]$ são finitamente gerados por monômios. Afirmação essa que é conhecida como o Lema de Dickson.

Teorema 1.3.5. (Lema de Dickson) *Um ideal monomial $I = \langle x^{\alpha} : \alpha \in A \rangle \subset K[x_1, ..., x_n]$ pode ser escrito na forma $I = \langle x^{\alpha(1)}, ..., x^{\alpha(s)} \rangle$, onde $\alpha(1), ..., \alpha(s) \in A$. Em particular, I tem uma base finita.*

Demonstração: (por indução sobre n, o número de variáveis) Se $n = 1$, então I é gerado pelos monômios x_1^{α} onde $\alpha \in A \subset \mathbb{N}$. Seja β o menor elemento de A. Então,

$\beta \leq \alpha$ para todo $\alpha \in A$, logo x_1^β divide todos geradores x_1^α. Assim sendo, $I = \langle x_1^\beta \rangle$. O que mostra a afirmação.

Agora tomamos $n > 1$ e suponhamos que o teorema seja verdadeiro para $n-1$. Escreveremos as variáveis como $x_1, ..., x_{n-1}, y$, assim os monômios em $K[x_1, ..., x_{n-1}, y]$ podem ser escritos como $x^\alpha y^m$, onde $\alpha = (\alpha_1, ..., \alpha_{n-1}) \in \mathbb{N}^{n-1}$ e $m \in \mathbb{N}$.

Suponhamos que $I \subseteq K[x_1, ..., x_{n-1}, y]$ é um ideal monomial. Para encontrar os geradores para I, seja J o ideal em $K[x_1, ..., x_{n-1}]$ gerado pelos monômios x^α tal que $x^\alpha y^m \in I$ para algum $m \geq 0$. Como J é um ideal monomial em $K[x_1, ..., x_{n-1}]$, nossa hipótese de indução nos diz que $J = \langle x^{\alpha(1)}, ..., x^{\alpha(s)} \rangle$. O ideal J pode ser entendido como a projeção de I em $K[x_1, ..., x_{n-1}]$.

Para cada i entre 1 e s, a definição de J nos garante que $x^{\alpha(i)} y^{m_i} \in I$ para algum $m_i \geq 0$. Seja m o máximo dos m_i. Então, para cada k entre 0 e $m-1$, consideramos o ideal $J_k \subset K[x_1, ..., x_{n-1}]$ gerado pelos monômios x^β tal que $x^\beta y^k \in I$. Usando novamente nossa hipótese de indução, escrevemos $J_k = \langle x^{\alpha_k(1)} y^k, ..., x^{\alpha_k(s_k) y^k} \rangle$.

Afirmamos que I é gerado pelos monômios do seguinte conjunto:

$$\{x^{\alpha(1)} y^m, ..., x^{\alpha(s)} y^m, x^{\alpha_{m-1}(1)} y^{m-1}, ..., x^{\alpha_{m-1}(s_{m-1})} y^{m-1}, ..., x^{\alpha_0(1)} y^0, ..., x^{\alpha_0(s_0)} y^0\}$$

Primeiro note que todo monômio em I é divisível por algum monômio desse conjunto. Para ver isso, seja $x^\alpha y^p \in I$. Se $p \geq m$, então $x^\alpha y^p$ é divisível por algum $x^{\alpha(i)} y^m$ por construção de J. Por outro lado, se $p \leq m-1$, então $x^\alpha y^p$ é divisível por algum $x^{\alpha_p(j)} y^p$ por construção de J_p. Segue, do Lema 1.4.2, que os monômios da lista acima geram um ideal tendo os mesmos monômios que I. Pelo Corolário 1.4.4, isso força os ideais serem os mesmos, e nossa afirmação está provada.

Para completar a prova do teorema, precisamos mostrar que o conjunto finito de geradores podem ser escolhidos a partir de um dado conjunto de geradores para o ideal. Se voltarmos a escrever as variáveis como $x_1, ..., x_n$, então o nosso ideal mono-

mial é $I = \langle x^\alpha : \alpha \in A \rangle \subset K[x_1, ..., x_n]$. Precisamos mostrar que I é gerado por finitos x^α's, onde $\alpha \in A$. Pelo parágrafo anterior, sabemos que $I = \langle x^{\beta(1)}, ..., x^{\beta(s)} \rangle$, para alguns monômios $x^{\beta(i)} \in I$. Como $x^{\beta(i)} \in I = \langle x^\alpha : \alpha \in A \rangle$, o Lema 1.4.2 nos diz que cada $x^{\beta(i)}$ é divisível por $x^{\alpha(i)}$, para algum $\alpha(i) \in A$. Assim, mostramo que $I = \langle x^{\alpha(1)}, ..., x^{\alpha(s)} \rangle$. E isso completa a prova do teorema.

Com o Lema de Dickson em mãos, estamos prontos para seguir e definir o que virá ser chamado de base de Groebner.

1.4 Bases de Groebner

Bases de Groebner em anéis de polinômios foram introduzidos por B.Buchberger na sua tese em 1965, e assim denominadas em homenagem ao seu orientador austríaco, W.Gröbner (1989-1980). A ideia desta seção é introduzir os conceitos de Bases de Groebner para, na seguinte, apresentar as propriedade interessantes que temos citado. Sabemos que, uma vez escolhido uma ordenação, cada polinômio $f \in K[x_1, ..., x_n]$ possui um único termo líder $LT(f)$. Então, para qualquer ideal I, podemos definir seu ideal de termos lideres da seguinte forma:

Definição 1.4.1. *Seja $I \subseteq K[x_1, ..., x_n]$ um ideal não nulo.*
(i) Escrevemos $LT(I)$ para o conjunto de termos líderes de elementos de I; Ou seja,

$$LT(I) = \{LT(f); f \in I\}.$$

(ii) Escrevemos $\langle LT(I) \rangle$ para o ideal gerado pelos elementos de $LT(I)$.

Vimos na seção anterior a importância da escolha de uma ordem, consequentemente um ideal de termos líderes, para o algoritmo da divisão. Se apresentamos um conjunto finito de geradores para I, digamos $I = \langle f_1, ..., f_s \rangle$, então $\langle LT(f_1), ..., LT(f_s) \rangle$

e $\langle LT(I)\rangle$ podem ser ideais distintos. Sabemos que $LT(f_i) \in LT(I) \subset \langle LT(I)\rangle$. Ou seja,

$$\langle LT(f_1), ..., LT(f_s)\rangle \subset \langle LT(I)\rangle.$$

Porém, $\langle LT(I)\rangle$ pode ser um ideal estritamente maior. Para mostrar isso, consideramos o seguinte exemplo.

Exemplo 1.4.2. *Seja $I = \langle f_1, f_2\rangle$, onde $f_1 = x^3 - 2xy$ e $f_2 = x^2y - 2y^2 + x$ e usando a ordem monomial grlex em $K[x, y]$. Então,*

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

Assim, $x^2 = LT(x^2) \in \langle LT(I)\rangle$. Porém, x^2 não é divisível por $LT(f_1) = x^3$ ou $LT(f_2) = x^2y$. Portanto, $x^2 \notin \langle LT(f_1), LT(f_2)\rangle$; ou seja, o ideal $\langle LT(I)\rangle$ é um ideal estritamente maior que $\langle LT(f_1), LT(f_2)\rangle$.

Proposição 1.4.3. *Seja $I \subseteq K[x_1, ..., x_n]$ um ideal.*
(i) $\langle LT(I)\rangle$ é um ideal monomial;
(ii) Existem $g_1, ..., g_t \in I$ tais que $\langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_t)\rangle$.

Demonstração: (i) o monômio líder $LM(g)$ de um elemento não nulo $g \in I$ gera o ideal monomial $\langle LM(g) : g \in I\rangle$. Como $LM(g)$ e $LT(g)$ diferem por uma constante e K é corpo, $\langle LM(g) : g \in I\rangle$=$\langle LT(g) : g \in I\rangle = \langle LT(I)\rangle$. Assim,$\langle LT(I)\rangle$ é um ideal monomial.

(ii)Como $\langle LT(I)\rangle$ é gerado pelos monômios $LM(g)$ tal que $g \in I - \{0\}$, pelo Lema de Dickson temos que $\langle LT(I)\rangle = \langle LM(g_1), ..., LM(g_t)\rangle$ para finitos $g_1, ..., g_t \in I$. Por $LM(g_i)$ e $LT(g_i)$ diferirem por uma constante, segue que:

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

Teorema 1.4.4. (Teorema da Base de Hilbert) *Todo ideal $I \subseteq K[x_1, ..., x_n]$ possui um conjunto finito de geradores. Isto é, $I = \langle g_1, ..., g_s\rangle$ para certos $g_1, ..., g_s \in I$.*

Demonstração: Se $I = \{0\}$, ele é gerado pelo conjunto $\{0\}$. Se I contêm um polinômio não nulo, observamos que pela proposição 1.4.3 existem $g_1, ..., g_s \in I$ tal que $\langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_s)\rangle$. Afirmamos que então $I = \langle g_1, ..., g_s\rangle$.

É claro que $\langle g_1, ..., g_s\rangle \subset I$, pois cada $g_i \in I$. Por outro lado, seja $f \in I$ um polinômio qualquer. Se aplicarmos o algoritmo da divisão visto na seção anterior para dividir f por $\langle g_1, ..., g_s\rangle$, obtemos uma expressão da forma:

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

onde todo termo em r não é divisível por nenhum dos $LT(g_1), ..., LT(g_s)$. Agora, escrevemos:

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

Se $r \neq 0$, então $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_s)\rangle$. Como $LT(r)$ é um monômio que está em um ideal monomial, $LT(r)$ deve ser divisível por algum $LT(g_i)$. Porém, isso contradiz o que acabamos de afirmar acima quando tomamos a divisão e obtemos r como resto. Portanto, $r = 0$. Mostrando assim que $I = \langle g_1, ..., g_s\rangle$. □

Na demonstração do Teorema da Base de Hilbert a base usada $\{g_1, ..., g_s\}$ foi muito especial por satisfazer a propriedade que $\langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_s)\rangle$. Como mostramos no primeiro exemplo dessa seção, nem todas as bases de um ideal satisfazem essa propriedade; consequentemente, daremos um nome para as bases que, como no Teorema de Hilbert, apresentam tal propriedade.

Definição 1.4.5. *Fixada uma ordem monomial. Um subconjunto finito $G = \{g_1, ..., g_s\}$ de um ideal I é dito ser uma* **base de Groebner** *de I se*

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

Corolário 1.4.6. *Fixada uma ordem monomial. Então todo ideal não nulo* $I \subseteq K[x_1, ..., x_n]$ *tem uma base de Groebner. Além disso, qualquer base de Groebner de um ideal* I *é uma base para* I*.*

Demonstração: Dado um ideal não nulo, o conjunto $G = \{g_1, ..., g_s\}$ construído na prova do teorema da Base de Hilbert é uma base de Groebner por definição. Para a segunda parte, note que se $\langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_s)\rangle$, então o mesmo argumento da demonstração do teorema nos afirma que $I = \langle g_1, ..., g_s\rangle$. Assim, G é uma base de I

1.5 Propriedades das Bases de Groebner

Mostramos na seção anterior que todo ideal não nulo $I \subseteq K[x_1, ..., x_n]$ tem uma base de Groebner. Nesta seção, iremos estudar algumas propriedades das bases de Groebner e conseguir decidir quando um conjunto dado é uma tal base. Iniciaremos resolvendo o problema da não unicidade do resto presente na divisão em $K[x_1, ..., x_n]$. Para isso, provaremos agora que o resto é unicamente determinado quando dividimos por uma base de Groebner.

Proposição 1.5.1. *Seja* $G = \{g_1, ..., g_s\}$ *uma base de Groebner para o ideal* $I \subseteq K[x_1, ..., x_n]$ *e* $f \in K[x_1, ..., x_n]$*. Então existe um único* $r \in K[x_1, ..., x_n]$ *com as seguintes propriedades:*
(i) *Nenhum termo de* r *é divisível por qualquer dos monômios* $LT(g_1), ..., LT(g_s)$*;*
(ii)*Existe* $g \in I$ *tal que* $f = g + r$*.*
Em particular, r *é o resto da divisão de* f *por* G *não importando como os elementos de* G *são listado quando usamos o algoritmo da divisão.*

Demonstração: O algoritmo da divisão nos oferece uma escrita da forma

$$f = a_1g_1 + ... + a_sg_s + r,$$

onde r satisfaz (i). Além disso, podemos tomar $g = a_1g_1 + ... + a_sg_s \in I$, o que nos diz que (ii) também é satisfeita. Resta então provar a unicidade de r.

Suponhamos que $f = g' + r_1 = g'' + r_2$ são duas escritas que satisfazem (i) e (ii). Então $r_2 - r_1 = g' - g'' \in I$. Logo, se $r_1 \neq r_2$, então $LT(r_2 - r_1) \in \langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_s)\rangle$. Observamos que por esse último ideal ser monomial, podemos garantir que $LT(r_2 - r_1)$ é divisível por algum $LT(g_i)$. Isto é impossível, pois nenhum termo de r_1 ou r_2 é divisível por qualquer dos termos $LT(g_1), ..., LT(g_s)$. Portanto, $r_2 - r_1$ deve ser zero, e a unicidade está provada.□

Observação 1.5.2. Embora a unicidade do resto, utilizando bases de Groebner, esteja provada, os quocientes a_i resultantes do algoritmo divisão podem mudar se listamos os geradores da base em uma ordem diferente. Como exemplo, usando o algoritmo de Buchberger, que veremos em seguida, pode se mostrar que $G = \{x + z, y - z\}$ é uma base de Groebner, e que o polinômio xy produz distintos quocientes com mesmo resto quando efetuamos a divisão por G; pois,

$$xy = y(x + z) - z(y - z) - z^2, \quad xy = z(x + z) + x(y - z) - z^2$$

são duas formas de escrever xy com distintos quocientes.

Como corolário, obtemos o seguinte critério de pertinência a um ideal.

Corolário 1.5.3. *Seja $G = \{g_1, ..., g_s\}$ uma base de Groebner para o ideal $I \subseteq K[x_1, ..., x_n]$ e $f \in K[x_1, ..., x_n]$. Então $f \in I$ se, e somente se, o resto da divisão de f por G é zero.*

De acordo com o último corolário, podemos determinar quando um polinômio está, ou não, em um determinado ideal. Para isso, devemos saber construir uma base de Groebner para o ideal. O que nos será apresentado como um teorema de Buchberger; em que, é classificado uma base de Groebner em função da divisão de certos polinômios por elementos da base.

Apresentamos na seção anterior os seguintes polinômios que são um exemplo de uma base que não é de Groebner: $f_1 = x^3 - 2xy$ e $f_2 = x^2y - 2y^2 + x$. Tomando a seguinte combinação:

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

temos que $x^2 = LT(x^2) \in \langle LT(I)\rangle$. Porém, $x^2 \notin \langle LT(f_1), LT(f_2)\rangle$;

Observamos que esse fato ocorreu pois efetuamos um cancelamento de termos líderes, resultando em um novo polinômio com termo líder não sendo combinação dos termos líderes dos polinômios f_i. Para estudar esses cancelamentos, apresentamos uma definição e, em seguida, mostraremos que qualquer cancelamento é dessa forma.

Definição 1.5.4. *Sejam $f, g \in K[x_1, ..., x_n]$ polinômios não nulos e $\alpha = (\alpha_1, ..., \alpha_n)$, $\beta = (\beta_1, ..., \beta_n)$ n-uplas;*
(i) Se $grau(f) = \alpha$, $grau(g) = \beta$ e $\gamma = (\gamma_1, ..., \gamma_n)$, onde $\gamma_i = max(\alpha_i, \beta_i)$ para cada i. Dizemos que x^γ é o mínimo múltiplo comum de $LM(f)$ e $LM(g)$, escrevemos:

$$x^\gamma = MMC(LM(f), LM(g)).$$

(ii) O **S-polinômio** *de f e g, denotado por $S(f, g)$ é definido como a combinação:*

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

Por exemplo, $f = x^3y^2 - x^2y^3 + x$ e $g = 3x^4y + y^2$ em $\mathbb{R}[x, y]$ com a ordem monomial grlex. Então $\gamma = (4, 2)$ e

$$S(f, g) = \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g = xf - (1/3)yg = -x^3y^3 + x^2 - (1/3)y^3.$$

O S-polinômio $S(f, g)$ é concebido para produzir um cancelamento de termos líderes. O seguinte lema mostrará que qualquer cancelamento de termos líderes de mesmo grau é o resultado de um cancelamento desses S-polinômios.

Lema 1.5.5. *Suponhamos que temos uma soma* $\sum_{i=1}^{s} c_i f_i$*, onde* $c_i \in K$ *e* $grau(f_i) = \delta \in \mathbb{N}^n$ *para todo* i*. Se* $grau(\sum_{i=1}^{s} c_i f_i) < \delta$*, então* $\sum_{i=1}^{s} c_i f_i$ *é uma combinação linear, com coeficientes em* K*, de S-polinômios* $S(f_j, f_k)$ *para* $1 \leq j, k \leq s$*. Além disso, cada* $S(f_j, f_k)$ *tem grau* $< \delta$*.*

Demonstração: Seja $d_i = LC(f_i)$, assim $c_i d_i$ é o coeficiente líder de $c_i f_i$. Como $c_i f_i$ tem grau δ e sua soma tem grau estritamente menor, segue que $\sum_{i=1}^{s} c_i d_i = 0$

Definimos $p_i = f_i/d_i$, que tem coeficiente líder 1. Considere a soma telescópica:

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + ...+$$

$$+(c_1 d_1 + ... + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + ... + c_s d_s) p_s.$$

Sabemos que $LT(f_i) = d_i x^\delta$, o que implica que o mínimo múltiplo comum de $LM(f_j)$ e $LM(f_k)$ é x^δ. Logo,

$$S(f_j, f_k) = \frac{x^\delta}{LT(f_j)} f_j - \frac{x^\delta}{LT(f_k)} f_k = \frac{x^\delta}{x^\delta d_j} f_j - \frac{x^\delta}{x^\delta d_k} f_k = p_j - p_k. \tag{1.1}$$

Usando a equação $\sum_{i=1}^{s} c_i d_i = 0$, a soma telescópica transforma-se em:

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

Que é uma soma na forma desejada. Como p_j e p_k tem grau δ e coeficiente líder 1, a diferença $p_j - p_k$ tem grau $< \delta$. Pela equação 1.1 o mesmo vale para $S(f_j, f_k)$, e o lema está provado. □

Usando S-polinômios e o lema anterior, podemos provar o seguinte critério de Buchberger para determinar quando uma base de um ideal é uma base de Groebner.

Teorema 1.5.6. *Seja um ideal* $I \subseteq K[x_1, ..., x_n]$*. Então uma base* $G = \{g_1, ..., g_s\}$ *é uma base de Groebner para* I *se, e somente se, para todo par* $i \neq j$*, o resto da divisão de* $S(g_i, g_j)$ *por* G *é zero.*

Demonstração: Se G é uma base de Groebner, então como $S(g_i, g_j) \in I$, o resto da divisão por G é zero pela unicidade do resto.

Por outro lado, dado $f \in I$ um polinômio não nulo. Devemos mostrar que se todos S-polinômios tem resto zero na divisão por G, então $LT(f) \in \langle LT(g_1), ..., LT(g_s)\rangle$. Antes de apresentar os detalhes, vamos delinear a estratégia da prova.

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

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

Observamos que,

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

Se a igualdade não ocorrer, então alguns cancelamentos devem ocorrer entre os termos líderes de 1.2. O lema anterior permitirá reescrever 1.2 em termo dos S-polinômios. Então nossa hipótese que os S-polinômios tem resto zero no permitirá trocar os S-polinômios por expressões que envolvem menos cancelamentos. Assim, obtermos uma expressão para f que envolve menos cancelamento de termos líderes. Continuando dessa maneira, iremos encontrar uma expressão do tipo 1.2 para f onde a igualdade ocorre em 1.3. Então, $grau(f) = grau(h_i g_i)$ para algum i, e seguirá que $LT(f)$ é divisível por $LT(g_i)$. E, assim, será mostrado que $LT(f) \in \langle LT(g_1), ..., LT(g_s)\rangle$, que é exatamente o que queremos provar.

Agora oferecemos os detalhes dessa prova. Dada uma expressão como em 1.2 para f, seja $m(i) = grau(h_i g_i)$, e definimos $\delta = max(m(1), ..., m(s))$. Assim, a expressão 1.3 transforma-se:

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

Consideramos, também, todas as possibilidades de escrever f como em 1.2. Para cada tal expressão, obtemos um possível δ diferente. Como a ordem monomial é bem ordenada, escolhemos uma escrita para 1.2 tal que δ é mínimo.

Iremos mostrar que tomando esse δ mínimo, $grau(f)$ será δ. Então a igualdade em 1.3 ocorre. Como observamos após 1.1.4, isso resulta que $LT(f) \in \langle LT(g_1), ..., LT(g_s)\rangle$ e o teorema estará provado.

Vamos provar que $grau(f) = \delta$. Suponhamos que $grau(f) < \delta$. Isolando os termos de que tem grau δ, escrevemos f da seguinte forma:

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

Separando os termos líderes da primeira soma, obtemos:

$$f = \sum_{m(i)=\delta} LT(h_i)g_i + \sum_{m(i)=\delta} (h_i - LT(h_i))g_i + \sum_{m(i)<\delta} h_i g_i. \tag{1.4}$$

Os monômios aparecendo na segunda e na terceira soma tem grau menor que δ. Assim, como estamos supondo que $grau(f) < \delta$, a primeira soma tem grau $< \delta$ ou é nula.

Seja $LT(h_i) = c_i x^{\alpha(i)}$. Então, a soma $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ está exatamente nas condições do lema 1.5.5 com $f_i = x^{\alpha(i)} g_i$. Logo, essa soma é combinação linear dos S-polinômios $S(x^{\alpha(j)}g_j, x^{\alpha(k)}g_k)$. Porém,

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

Tomando $x^{\gamma_{jk}} = MMC(LM(g_j), LM(g_k))$, a igualdade acima transforma-se:

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

Assim, pelo lema 1.1.5, existem constantes $c_{jk} \in K$ tal que:

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k). \tag{1.5}$$

O próximo passo será usar nossa hipótese que o resto da divisão de $S(g_j, g_k)$ por $\{g_1, ..., g_s\}$ é zero. Usando o algoritmo da divisão, isso quer dizer que cada

S-polinômio pode ser escrito na forma:

$$S(g_j, g_k) = \sum_{i=1}^{s} a_{ijk} g_i, \tag{1.6}$$

onde $a_{ijk} \in K[x_1, ..., x_n]$. O algoritmo da divisão também nos diz que:

$$grau(a_{ijk} g_i) \leq grau(S(g_j, g_k)) \tag{1.7}$$

Multiplicando a expressão 1.6 por $x^{\delta - \gamma_{jk}}$ obtemos:

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

onde $b_{ijk} = x^{\delta - \gamma_{jk}} a_{ijk}$. Então, por 1.7 e o lema 1.1.5, temos que:

$$grau(b_{ijk} g_i) \leq grau(x^{\delta - \gamma_{jk}} S(g_j, g_k)) < \delta \tag{1.8}$$

Voltando para a expressão 1.5, obtemos uma nova equação:

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{j,k} c_{jk} \Big(\sum_{i} b_{ijk} g_i \Big) = \sum_{i} \widetilde{h}_i g_i$$

que por 1.8 tem a propriedade que para todo i,

$$grau(\widetilde{h}_i g_i) < \delta.$$

Para finalizar, substituímos $\sum_{m(i)=\delta} LT(h_i) g_i = \sum_i \widetilde{h}_i g_i$ na equação 1.4 e obtemos uma expressão para f através de uma combinação polinomial em que todos os termos tem grau $< \delta$. O que contradiz a minimalidade de δ e completa a prova do teorema. $\square$

Na seção anterior mostramos que todo ideal não nulo $I \subseteq K[x_1, ..., x_n]$ tem uma bases de Groebner; porém, nossa prova não foi construtiva no sentido de que não produzimos uma tal base. Assim, uma pergunta aparece: Como podemos construir de fato uma base de Groebner para I? O seguinte resultado é chamado de algoritmo de Buchberger e responderá essa questão através de sucessivas adições de S-polinômios à base de I.

Teorema 1.5.7. (Algoritmo de Buchberger) *Seja $I = \langle f_1, ..., f_s \rangle \neq 0$ um ideal em $K[x_1, ..., x_n]$. Então uma base de Groebner para I pode ser construída em um número finito de passos da seguinte forma:*

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

Saída: *uma base de Groebner $G = \{g_1, ..., g_t\}$ para I, com $F \subseteq G$*

Repetir:

para cada par $\{f_i, f_j\}$, $i \neq j$ em F, tomar

$S := \overline{S(f_i, f_j)}^F$, *definido como o resto da divisão de $S(p, q)$ por F.*

Se $S \neq 0$, então definimos $\widetilde{G} := F \cup S$

Repetimos esse processo como todos os pares de polinômios de F, o resultado de adicionar todos esses restos não nulos nos produzirá G, uma base de Groebner.

Demonstração:

O algoritmo termina quando $\overline{S(f_i, f_j)}^F = 0$ para todos $f_i, f_j \in F$. Então G, como foi construído, é uma base de Groebner de I, pelo teorema anterior.

Agora, para finalizar, vamos provar que o algoritmo termina. O conjunto G consiste de $\widetilde{G}$ (o velho G) junto com o resto não nulo da divisão de um S-polinômio por $\widetilde{G}$. Então,

$$\langle LT(\widetilde{G}) \rangle \subset \langle LT(G) \rangle \tag{1.9}$$

Se $\widetilde{G} \neq G$, temos que $\langle LT(\widetilde{G}) \rangle$ é estritamente maior que $\langle LT(G) \rangle$. Para ver isso, suponhamos que um resto r não nulo de um S-polinômio por $\widetilde{G}$ foi adicionado em G. Como r é um resto da divisão por $\widetilde{G}$, $LT(r)$ não é divisível pelos termos líderes de elementos de $\widetilde{G}$, assim $LT(r)$ não pertence ao ideal $\langle LT(\widetilde{G}) \rangle$. E, como $LT(r) \in \langle LT(G) \rangle$, provamos a inclusão estrita.

Por 1.9, os ideais $\langle LT(\widetilde{G}) \rangle$ de uma sequência de sucessivas iterações formam uma cadeia ascendente de ideais em $K[x_1, ..., x_n]$. Como $K[x_1, ..., x_n]$ é um anel Noetheriano, essa cadeia deve estabilizar e, então, deve ocorre que em algum mo-

mento $\langle LT(\widetilde{G})\rangle = \langle LT(G)\rangle$. Pelo parágrafo anterior, isso implica que $\widetilde{G} = G$, assim o algoritmo deve terminar em um número finito de passos. $\square$

1.6 Aplicações das Bases de Groebner

Neste seção, exibimos alguns tópicos de álgebra comutativa para motivar o estudo sobre a possibilidade de computar os geradores do radical de um ideal no anel de polinômios. Também falaremos um pouco da teoria da eliminação, que será seguidamente citada. Assim apresentados, mostraremos as principais propriedades dessas bases e suas consequências quanto ao poder de computar interseções, ideais quocientes e decidir se um certo polinômio pertence a um dado radical.

Definição 1.6.1. *Dado um subconjunto $S \subseteq K[x_1, ..., x_n]$, definimos a variedade, ou conjunto de zeros de S, em K^n por*

$$V_K(S) = \{(a_1, ..., a_n) \in K^n / f(a_1, ..., a_n) = 0, \quad \forall f \in S\}$$

(sendo claro no contexto, omitiremos o índice K na notação da variedade)

Tomando $I = \langle f_1, ..., f_s\rangle \subseteq K[x_1, ..., x_n]$, se $f_i(a_1, ..., a_n) = 0\ \forall i = 1, ..., s$ e ainda $f \in I$; isto é, $f = g_1 f_1 + ... + g_s f_s$ com g_i em $K[x_1, ..., x_n]$, então

$$f(a_1, ..., a_n) = g_1(a_1, ..., a_n) f_1(a_1, ..., a_n) + ... + g_s(a_1, ..., a_n) f_s(a_1, ..., a_n) = 0$$

Por outro lado, se $f(a_1, ..., a_n) = 0, \quad \forall f \in I$, em particular $f_i(a_1, ..., a_n) = 0$ $\forall i = 1, ..., s$. Portanto, $V_K(I) = V_K(f_1, ..., f_n)$.

Definimos, também, um ideal de $K[x_1, ..., x_n]$ associado ao conjunto de zeros, $V \subseteq K^n$:

$$I(V) = \{f \in K[x_1, ..., x_n] / f(a_1, ..., a_n) = 0, \quad \forall (a_1, ..., a_n) \in V\}$$

Na seção anterior mostramos um algoritmo para computar bases de Groebner, que é realizado adicionando certos polinômios ao conjunto de geradores até construir uma tal base; porém, nesse processo podemos adicionar muitos polinômios que não seriam necessários ao conjunto gerador. Ou seja, certos polinômios podem ser retirados da base e, mesmo assim, ela continuará sendo uma base de Groebner. Esse processo de eliminar polinômios desnecessários à base é o conceito de base de Groebner reduzida. Antes disso, precisaremos de um lema.

Lema 1.6.2. *Sejam G uma base de Groebner para o ideal I e $p \in G$ um polinômio tal que $LT(p) \in \langle LT(G - \{p\})\rangle$. Então, $G - \{p\}$ também é uma base de Groebner para I.*

Demonstração: Sabemos 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 é uma base de Groebner para I. □

Ajustando as constantes de maneira que todos os coeficientes líderes sejam 1 e removendo todos os polinômios p tal que $LT(p) \in \langle LT(G-\{p\})\rangle$, vamos obter uma base que chamaremos de base de Groebner minimal.

Exemplo 1.6.3. *Usando o algoritmo de Buchberger e o lema anterior, podemos verificar que*

$$f_1 = x^2, \quad f_2 = xy, \quad f_3 = y^2 - (1/2)x$$

é uma base de Groebner minimal. Porém, um ideal qualquer pode ter muitas bases de Groebner mínimas. Por exemplo, no ideal gerado pelos polinômios acima, é fácil mostrar que

$$f_1' = x^2 + axy, \quad f_2 = xy, \quad f_3 = y^2 - (1/2)x$$

é também uma base de Groebner minimal, onde $a \in K$ é uma constante qualquer. Sendo K um corpo infinito, acabamos de mostrar que podem existir infinitas bases

mínimas. Apesar disso, podemos destacar uma base minimal que é melhor, no sentido de ser única, que todas as outras mínimas.

Definição 1.6.4. *Uma base de Groebner reduzida para um ideal I é uma base de Groebner G tal que:*
(i) $LC(p) = 1$ *para todo* $p \in G$.
(ii) Para todo $p \in G$, *nenhum monômio de* p *está no ideal* $\langle LT(G - \{p\})\rangle$.

Note que no exemplo 1.6.3, tomando $a = 0$ obtemos uma base de Groebner reduzida. A seguinte propriedade é interessante pois garante a unicidade das bases reduzidas.

Proposição 1.6.5. *Seja* $I \neq 0$ *um ideal em* $K[x_1, ..., x_n]$. *Então, dada uma ordem monomial, I possui uma única base de Groebner reduzida.*

Demonstração: Ver proposição 2.7.6 em [3].

O teorema seguinte, chamado de Teorema dos Zeros de Hilbert Fraco, tem grande importância no decorrer desta seção, sua prova está presente em diversos livros de álgebra comutativa. Após enunciarmos o teorema, apresentaremos uma observação visando olhá-lo sobre um contexto das bases de Groebner. Para, então, provar o Teorema dos Zeros de Hilbert, onde sua demostração nos será útil em um teorema seguinte.

Teorema 1.6.6 (Teorema dos Zeros de Hilbert Fraco)**.** *Seja um ideal* $I \subseteq K[x_1, ..., x_n]$ *e K um corpo algebricamente fechado. Se* $V(I) = \emptyset$, *então* $I = K[x_1, ..., x_n]$.

Observação 1.6.7. Vamos ver nesta observação que o Nullstellensatz Fraco, junto com bases de Groebner, nos permite resolver o problema de consistência de um sistema de equações polinomiais. Isto é, nos garante condições para que um sistema de equações polinomiais tenha solução comum em $\mathbb{C}^n$.

Consideremos um ideal $I = \langle f_1, ..., f_s \rangle$ de $K[x_1, ..., x_n]$ e $G = \{g_1, ..., g_t\}$ uma base de Groebner reduzida para I com respeito a alguma ordem monomial. Então, $V(I) = \emptyset$ se, e somente se, $G = \{1\}$. Verificamos isso: Nullstellensatz Fraco nos diz que $V(I) = \emptyset$ se, e somente se, $I = K[x_1, ..., x_n]$; porém, $I = K[x_1, ..., x_n]$ se, e somente se, $1 \in I$. Também, lembramos que G é uma base de Groebner reduzida para I, pela definição $\langle LT(I) \rangle = \langle LT(g_1), ..., LT(g_t) \rangle$. No entanto, sabemos que $1 \in I$; ou seja, $1 \in \langle LT(I) \rangle = \langle LT(g_1), ..., LT(g_t) \rangle$, como o termo da direita da igualdade anterior é um ideal monomial e 1 pertece a esse ideal, acontece que $LT(g_i) = 1$ para algum $i = 1, ..., t$. Portanto, como G é base de Groebner reduzida e $LT(g_i) = 1$, e em uma base reduzida não aparece um termo líder que é múltiplo de algum outro termo líder que já apareceu em G, concluímos que $G = \{1\}$.

Portanto, temos o seguinte algoritmo de consistência: dados $f_1, ...f_s \in \mathbb{C}[x_1, ..., x_n]$, computamos uma base de Groebner reduzida do ideal gerado pelos polinômios com respeito a qualquer ordem monomial. Se a base é $\{1\}$, os polinômios não tem zero comum em $\mathbb{C}^n$; se a base não é $\{1\}$, então eles possuem um zero em comum.

Teorema 1.6.8 (Teorema dos Zeros de Hilbert)**.** *Seja K um corpo algebricamente fechado. Se $f, f_1, ..., f_s \in K[x_1, ..., x_n]$ são tais que $f \in I(V(f_1, ..., f_s))$, então existe um inteiro $m \geq 1$ tal que,*

$$f^m \in \langle f_1, ..., f_s \rangle.$$

Demonstração: Devemos mostrar que existe um inteiro $m \geq 1$ e polinômios $A_1, ...A_s$ tal que,

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

Considere o ideal,

$$\widetilde{I} = \langle f_1, ..., f_s, 1 - yf \rangle \subset K[x_1, ..., x_n, y],$$

onde $f, f_1, ..., f_s$ são como acima. Afirmamos que

$$V(\widetilde{I}) = \emptyset.$$

Para ver isso, seja $(a_1, ..., a_n, a_{n+1}) \in K^{n+1}$. Então:

- $(a_1, ..., a_n)$ é um zero comum de $f_1, ..., f_s$, ou
- $(a_1, ..., a_n)$ não é um zero comum de $f_1, ..., f_s$.

No primeiro caso $f(a_1, ..., a_n) = 0$, pois f é anulado em qualquer zero comum de $f_1, ..., f_s$. Assim, o polinômio $1 - yf$ assume o valor $1 - a_{n+1}f(a_1, ..., a_n) = 1 \neq 0$ no ponto $(a_1, ..., a_n, a_{n+1})$. Em particular, $(a_1, ..., a_n, a_{n+1})$ não pertence a $V(\widetilde{I})$. No segundo caso, para algum i, $1 \leq i \leq s$, devemos ter que $f_i(a_1, ..., a_n) \neq 0$. Pensando f_i como uma função de $n+1$ variáveis que não depende da última variável, concluímos que $f_i(a_1, ..., a_n, a_{n+1}) \neq 0$. Em particular, percebemos novamente que $(a_1, ..., a_n, a_{n+1})$ não pertence a $V(\widetilde{I})$. Como $(a_1, ..., a_n, a_{n+1}) \in K^{n+1}$ foi arbitrário, concluímos que $V(\widetilde{I}) = \emptyset$, como afirmamos.

Agora, aplicando o teorema de Nullstellensatz Fraco, vemos que $1 \in \widetilde{I}$. Isto é,

$$1 = \sum_{i=1}^{s} p_i(x_1, ..., x_n, y) f_i + q(x_1, ..., x_n, y)(1 - yf) \tag{1.10}$$

para certos polinômios $p_i, q \in K[x_1, ..., x_n, y]$. Tomamos $y = 1/f(x_1, ...x_n)$. Então a relação 1.10 acima implica que

$$1 = \sum_{i=1}^{s} p_i(x_1, ..., x_n, 1/f) f_i \tag{1.11}$$

Multiplicando ambos os lados da igualdade por f^m, onde m é escolhido suficientemente grande para eliminar todos os denominadores. Isso produz,

$$f^m = \sum_{i=1}^{s} A_i f_i, \tag{1.12}$$

para certos polinômios $A_i \in K[x_1, ..., x_n]$, que é o queríamos mostrar. □

Observação 1.6.9. A hipótese do corpo ser algebricamente é necessária e essa hipótese implica que o corpo é perfeito. No capítulo seguinte, corpos perfeitos serão apresentados; como exemplo, os algebricamente fechados são perfeitos.

Após esse teorema, percebemos a importância de uma potência de um polinômio pertencer ao ideal I. Assim sendo, naturalmente definimos o radical de um ideal como segue.

Definição 1.6.10. *Seja $I \subseteq K[x_1, ..., x_n]$ um ideal, definimos o radical de I, denotemos por $\sqrt{I}$,*

$$\sqrt{I} = \{f \in K[x_1, ..., x_n]; \quad existe \quad e \in \mathbb{N} \quad tal \quad que \quad f^e \in I\}$$

Teorema 1.6.11 (Teorema dos Zeros de Hilbert Forte)**.** *K um corpo algebricamente fechado, então $I(V(I)) = \sqrt{I}$ para todo ideal I de $K[x_1, ..., x_n]$*

Demonstração: Certamente $\sqrt{I} \subset I(V(I))$, pois $f \in \sqrt{I}$ implica que $f^m \in I$ para algum m. Então, f^m se anula sobre $V(I)$, o que garante que f se anula sobre $V(I)$. Assim, $f \in I(V(I))$.

Por outro lado, suponhamos que $f \in I(V(I))$. Logo, por definição, f é anulado sobre $V(I)$. Pelo Teorema dos Zeros de Hilbert, existe um inteiro $m \geq 1$ tal que $f^m \in I$, o que garante que $f \in \sqrt{I}$. Como f é arbitrário, $I(V(I)) \subset \sqrt{I}$. Completando a prova. □

Esse teorema estabelece uma ligação entre álgebra e geometria; sendo que, identificamos um conjunto de zeros a um ideal radical. O que afirma que qualquer questão sobre conjuntos de zeros pode ser passada a uma nova questão sobre ideais radicais (e reciprocamente). Os ideais radicais tem sua importância garantida pelo Nullstellensatz, assim é natural estabelecer questões sobre esses ideais. Sendo $I = \langle f_1, ..., f_s \rangle$, vejamos algumas questões:

- (Geradores do Radical) Existe um algoritmo que produz um conjunto $g_1, ..., g_m$ de polinômios de modo que $\sqrt{I} = \langle g_1, ..., g_m \rangle$?
- (Pertinência ao Radical) Dado $f \in K[x_1, ..., x_n]$, existe um algoritmo que determina se $f \in \sqrt{I}$?

A primeira questão nos interessou bastante e será discutida no próximo capítulo quando apresentarmos um resultado de Seidenberg em [11], que nos garantirá esse algoritmo no caso de ideais zero-dimensionais. Faremos um exposição sobre ideais zero-dimensionais, pois todos algoritmos modernos, de cálculo dos geradores do radical, baseiam-se na passagem a esse caso para, então, concluir os geradores do ideal.

Por agora, iremos responder a segunda questão que, utilizando as bases de Groebner, é totalmente respondida. O que faremos, na seguinte proposição, é uma adaptação da prova do Teorema dos Zeros de Hilbert e a visão das bases de Groebner para oferecer um algoritmo que determina se $f \in \sqrt{\langle f_1, ..., f_s \rangle}$.

Proposição 1.6.12. (Pertinência ao Radical) *Seja K um corpo qualquer e um ideal $I = \langle f_1, ..., f_s \rangle \subset K[x_1, ..., x_n]$. Então, $f \in \sqrt{I}$ se, e somente se, o polinômio constante 1 pertence ao ideal $\widetilde{I} = \langle f_1, ..., f_s, 1 - yf \rangle \subset K[x_1, ..., x_n, y]$.*

Demonstração: Das equações 1.10, 1.11 e 1.12 da prova do Teorema dos Zeros de Hilbert, obtemos que $I \subset \widetilde{I}$ implica $f^m \in I$ para algum m; ou seja, $f \in \sqrt{I}$. Por outro lado, suponhamos que $f \in \sqrt{I}$. Então $f^m \in I \subset \widetilde{I}$ para algum m. Sabemos que $1 - yf \in \widetilde{I}$, resultando:

$$1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + ... + y^{m-1} f^{m-1}) \in \widetilde{I},$$

o que mostra a implicação. □

A proposição anterior junto com a observação 1.6.3 produzem o algoritmo de pertinência ao radical. Para decidir se $f \in \sqrt{\langle f_1, ..., f_s \rangle}$, computamos uma base de Groebner reduzida para o ideal $\widetilde{I} = \langle f_1, ..., f_s, 1-yf \rangle \subset K[x_1, ..., x_n, y]$ com respeito a alguma ordem monomial. Se o resultado dessa base for $\{1\}$, então $f \in \sqrt{I}$. Caso contrário, $f \notin \sqrt{I}$.

Exemplo 1.6.13. *Considere o ideal $I = \langle xy^2+2y^2, x^4-2x^2+1 \rangle$ em $K[x, y]$. Vamos testar se $f = y - x^2 + 1 \in \sqrt{I}$. Usando a ordem lex sobre $K[x, y, z]$, podemos ver,*

utilizando o algoritmo de Buchberber e as propriedade de base de Groebner reduzida, que o ideal

$$\widetilde{I} = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1)\rangle \subset K[x, y, z]$$

tem um base de Groebner reduzida $\{1\}$*, de onde segue que* $f = y - x^2 + 1 \in \sqrt{I}$*.*

Para seguir, definiremos o ideal de eliminação da seguinte forma.

Definição 1.6.14. *Dado* $I = \langle f_1, ..., f_s\rangle \subset K[x_1, ..., x_n]$*, o l-ésimo ideal de eliminação é o ideal de* $K[x_{l+1}, ..., x_n]$ *definido por*

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

Esse ideal de eliminação é produzido para analisar o ideal I em cada variável, o teorema seguinte mostrará isso e também que esse ideal de eliminação comporta-se bem quando passamos a bases de Groebner com uma fixada ordem monomial.

Teorema 1.6.15. (Teorema da Eliminação) *Seja* $I \subset K[x_1, ..., x_n]$ *um ideal e* G *uma base de Groebner de* I *com a ordem lex onde* $x_1 > x_2 > ... > x_n$*. Então, para todo* $0 \leq l \leq n$*, o conjunto*

$$G_l = G \cap K[x_{l+1}, ..., x_n]$$

é uma base de Groebner para o ideal de eliminação I_l*.*

Demonstração: Fixado l entre 0 e n. Como $G_l \subset I_l$ por construção, é suficiente provar que

$$\langle LT(I_l)\rangle = \langle LT(G_l)\rangle.$$

Vamos provar a inclusão $\langle LT(I_l)\rangle \subset \langle LT(G_l)\rangle$, pois a outra é direta. Vamos mostrar, então, que o termo líder de qualquer polinômio $f \in I_l$ é divisível por $LT(g)$ para algum $g \in G_l$.

Note que esse f acima também está em I, ou seja $LT(f)$ é divisível por $LT(g)$ para algum $g \in G$, pois G é uma base de Groebner para I. Como $f \in I_l$, isso quer dizer que $LT(g)$ envolve somente as variáveis $x_{l+1}, ..., x_n$. O ponto importante é que estamos usando a ordem lex com $x_1 > x_2 > ... > x_n$; sendo assim, qualquer monômio envolvendo $x_1, ..., x_l$ é maior que todos os monômios em $K[x_{l+1}, ..., x_n]$, logo $LT(g) \in K[x_{l+1}, ..., x_n]$, o que implica que $g \in K[x_{l+1}, ..., x_n]$. Portanto, mostramos que $g \in G_l$, e o teorema está provado. □

Como primeira aplicação do teorema anterior vamos apresentar um método para encontrar os geradores da interseção de dois ideais.

Proposição 1.6.16. *Sejam I e J ideais em $K[x_1, ..., x_n]$ e w uma nova variável. Considere o ideal $\langle wI, (1-w)J\rangle$ em $K[x_1, ..., x_n, w]$. Então,*

$$I \cap J = \langle wI, (1-w)J\rangle \cap K[x_1, ..., x_n].$$

Demonstração: Observe que se $I = \langle f_1, ..., f_s\rangle$ e $J = \langle g_1, ..., g_t\rangle$, então um conjunto de geradores para o ideal $\langle wI, (1-w)J\rangle$ é $\{wf_1, ..., wf_s, (1-w)g_1, ..., (1-w)g_t\}$.

Seja $f \in I \cap J$, escrevendo

$$f = wf + (1-w)f,$$

obtemos que $f \in \langle wI, (1-w)J\rangle \cap K[x_1, ..., x_n]$. Por outro lado, suponhamos que $f \in \langle wI, (1-w)J\rangle \cap K[x_1, ..., x_n]$. Dessa forma, sabemos que $f \in \langle wI, (1-w)J\rangle \subset K[x_1, ..., x_n, w]$ e podemos expressar f na seguinte forma:

$$f(x_1, ..., x_n) = \sum_{i=1}^{s} wf_i(x_1, ..., x_n)h_i + \sum_{j=1}^{t}(1-w)g_j(x_1, ..., x_n)h'_j$$

onde h_i e h'_j são polinômios em $K[x_1, ..., x_n, w]$. Agora, observamos que w não deve aparecer em f, assim podemos tomar $w = 1$ e obter que $f \in I$, e também $w = 0$ e obter que $f \in J$, o que demonstra a proposição. □

Como consequência da proposição anterior, obtemos um interessante método para computar os geradores para o ideal $I \cap J$. Primeiro computamos uma base de Groebner G para o ideal $\langle wI, (1-w)J\rangle \subset K[x_1, ..., x_n, w]$ usando a ordem monomial lex onde $x_1 > x_2 > ... > x_n > w$. Então, obtemos uma base de Groebner para $I \cap J$ computando $G \cap K[x_1, ..., x_n]$, que é feito simplesmente por inspeção.

Exemplo 1.6.17. *Considere os seguintes ideais em* $\mathbb{Q}[x, y]$*:*

$$I = \langle x^2 + y^3 - 1, x - yx + 3\rangle,$$

$$J = \langle x^2y - 1\rangle.$$

Queremos calcular os geradores do ideal $I \cap J$*. Calculamos uma base de Groebner* G *para o ideal*

$$\langle w(x^2 + y^3 - 1), w(x - yx + 3), (1 - w)(x^2y - 1)\rangle \subset \mathbb{Q}[x, y, w]$$

usando a ordem deglex nas variáveis x *e* y *com* $x > y$ *e uma ordem sobre* w *que o faça ser maior que x,y. Com essas condições pode-se obter* $G = \{x^3y^2 - x^3y - 3x^2y - xy + x + 3, x^2y^4 + x^4y - x^2y - y^3 - x^2 + 1, 12853w + 118x^4y + 9x^2y^3 - 357x^3y - 972x^2y^2 + 2152x^2y - 118x^2 - 9y^2 + 357x + 972y - 2152, x^5y + 3x^2y^3 + 3x^2y^2 - x^3 + 3x^2y - 3y^2 - 3y - 3\}$.

Assim, uma base de Groebner para o ideal $I \cap J$ *é*

$$\{x^3y^2 - x^3y - 3x^2y - xy + x + 3, x^2y^4 + x^4y - x^2y - y^3 - x^2 + 1,$$

$$x^5y + 3x^2y^3 + 3x^2y^2 - x^3 + 3x^2y - 3y^2 - 3y - 3\}.$$

Capítulo 2

Ideais Zero-Dimensionais

Neste capítulo, veremos dois resultados sobre ideais que serão chamados de zero-dimensionais. O primeiro deles trata de resolver um sistema de equações polinomiais, que já apareceu anteriormente na teoria da eliminação; pórem, agora apresentaremos o caso em ideais zero-dimensionais. Falamos em resolver um sistema no sentido de que é suficiente ter um algoritmo para encontrar raízes de polinômios em uma variável. Essas técnicas de determinar raízes de polinômios em uma variável não fazem parte da teoria das bases de Groebner.

O outro resultado é computar, sob certas condições para I, os geradores do radical de um ideal $I \subseteq K[x_1, ..., x_n]$ sabendo os geradores do ideal I. Começaremos com o caso de ideais principais em $K[x_1, ..., x_n]$ e após passaremos aos zero-dimensionais. Neste momento, apresentaremos um resultado de Seidenberg em [11] para calcular os geradores do radical de um ideal zero-dimensional $I \subseteq K[x_1, ..., x_n]$. A grande importância desse artigo de Seidenberg está no fato de que, entre os recentes resultados para calcular os geradores do radical de um ideal, o problema é solucionado reduzindo para o caso zero dimensional. Dentre estes, podemos citar [5], [4] e [9]

para o caso geral, [11] para o caso zero-dimensional e [10] para os ideais sobre corpos de característica positiva.

2.1 Lema de Seidenberg

Exemplo 2.1.1. *Sejam* $f_1(x,y) = (x-1)^2+y^2-1$ *e* $f_2(x,y) = 4(x-1)^2+y^2+xy-2$ *polinômios em* $\mathbb{Q}[x,y]$. *Consideremos a interseção do círculo* $f_1 = (x-1)^2+y^2-1 = 0$ *e a elípse* $f_2 = 4(x-1)^2 + y^2 + xy - 2 = 0$ *sobre os racionais. Usando a ordem mononial* $x > y$ *podemos ver que uma base de Groebner para o ideal* $\langle f_1, f_2\rangle$ *é* $\{g_1, g_2\}$, *onde* $g_1 = 5y^4-3y^3-6y^2+2y+2$ *e* $g_2 = x-5\ y^3+3y^2+3y-2$. *Claramente, sabemos que* $g_1 = 0$ *tem no máximo quatro soluções e para cada solução de* $g_1 = 0$ *obtemos precisamente uma solução de* $g_2 = 0$*; isto é primeiro resolvemos a equação em uma variável* $g_1 = 0$ *e para cada solução* α *de* $g_1 = 0$, *resolvemos a equação* $g_2(x, \alpha)$.

Percebemos nesse último exemplo que a forma da base de Groebner foi particularmente conveniente para determinar os pontos no conjunto de zeros. No caso, o primeiro polinômio tem somente a variável y e o termo líder do segundo é uma potência de x. Em seguida, mostraremos que, no caso do conjunto de zeros ser finito (como no exemplo anterior), esse tipo de estrutura na base de Groebner é sempre presente quando a ordem monomial $x_1 < x_2 < ... < x_n$ é usada.

Teorema 2.1.2. *Sendo* K *um corpo algebricamente fechado,* $I \subseteq K[x_1, ..., x_n]$ *um ideal e* $G = \{g_1, ..., g_t\}$ *um base de Groebner para* I. *As seguintes afirmações são equivalentes:*

(i) O conjunto de zeros $V(I)$ *é finita;*

(ii) Para cada $i = 1, ..., n$, *existe* $j \in \{1, ..., t\}$ *tal que* $LT(g_j) = x_i^{\nu}$ *para algum* $\nu \in \mathbb{N}$*;*

(iii) A dimensão de $K[x_1, ..., x_n]/I$ é finita como K-espaço vetorial.

Demonstração: $(i) \Rightarrow (ii)$. Suponhamos que $V(I)$ é finita. Se $V(I)$ é vazia, então pelo Teorema dos Zeros de Hilbert Fraco, $I = K[x_1, ..., x_n]$ e então $G = \{1\}$ e (ii) é satisfeita. Assim, assumimos que $V(I)$ não é vazia. Fixamos $i \in \{1, ..., n\}$. Seja $a_{ij}, j = 1, ..., l$ as distintas i-ésimas coordenada dos pontos em $V(I)$. Para cada $j, 1 \leq j \leq l$, seja $0 \neq f_j \in K[x_i]$ tal que $f_j(a_{ij}) = 0$. Tomamos $f = f_1 f_2 ... f_l \in K[x_i] \subseteq K[x_1, ..., x_n]$. Então, percebemos que $f \in I(V(I))$, e assim, pelo Teorema de Nullstellensatz, existe e tal que $f^e \in I$. Como $LM(f^e) = x_i^{em}$ para algum número natural m, e como todo monômio líder de um elemento de I é divisível por um monômio líder de algum elemento de G, existe um polinômio em G cujo monômio líder é apenas com a variável x_i. E isso é verdade para $i = 1, ..., n$.

$(ii) \Rightarrow (iii)$. Mostraremos que uma base para o K-espaço vetorial $K[x_1, ..., x_n]/I$ consiste no conjunto de classes de todos monômios X tal que $LT(g_i)$ não divide X para todo $i = 1, 2, ..., t$.. Por exemplo, uma base de Groebner para um ideal I com respeito a ordem grlex $x < y$ é $G = \{x^2y - y + x, -y^2 + xy + x^2, x^3 + y - 2x\}$. Assim, pelo o que iremos mostrar, uma base para $K[x, y]/I$ consiste em $1, x, y, x^2, xy$. Portanto, $dim_k K[x, y]/I = 5$.

Sabemos que uma propriedade boa das bases de Groebner é a unicidade do resto; ou seja, dado $f \in K[x_1, ..., x_n]$ existe um único elemento $r \in K[x_1, ..., x_n]$ que é chamado o resto da divisão de f por G. Observamos que dois elementos são equivalentes em $K[x_1, ..., x_n]/I$ se, e somente se, seus restos na divisão por G são iguais. Assim, dado $f \in K[x_1, ..., x_n]$ e r seu resto por G, $f + I = r + I$ em $K[x_1, ..., x_n]/I$. Logo, pela definição de resto, ele é uma combinação K-linear de monômios líderes X tal que $LT(g_i)$ não divide X para todo $i = 1, 2, ..., t$.Finalmente, é linearmente independente pela unicidade do resto.

Para finalizar a implicação, observamos que (ii) nos diz que cada variável x_i, em alguma potência, irá aparece como termo líder de algum polinômio da base de Groebner. Portanto, pelo que apresentamos acima, dimensão de $K[x_1, ..., x_n]/I$ é finita.

$(iii) \Rightarrow (i)$. Mostraremos que para qualquer $i = 1, ..., n$, existe somente finitos possíveis valores distintos para a i-ésima coordenada dos pontos de $V(I)$. Fixamos $i \in 1, ..., n$. Como estamos supondo que a dimensão de $K[x_1, ..., x_n]/I$ é finita como K-espaço vetorial, as potências $1, x_i, x_i^2, ...$ de x_i são linearmente dependente módulo I. Logo, existe um inteiro m e constantes $c_j \in K, 0 \leq j \leq m$, não todas nulas, tal que

$$\sum_{j=0}^{m} c_j x_i^j \in I.$$

Como o polinômio acima tem somente finitas raizes em K, existe somente finitos valores para a i-ésima coordenada dos pontos de $V(I)$; ou seja, $V(I)$ é finita. □

Um ideal $I \neq K[x_1, ..., x_n]$ que satisfaz qualquer umas das afirmações equivalentes do teorema anterior é chamado de zero-dimensional.

Exemplo 2.1.3. *Uma Base de Groebner para o ideal* $I = \langle x^2y - y + x, xy^2 - x \rangle$ *em* $\mathbb{Q}[x, y]$ *com respeito a ordem deglex usando* $x < y$ *é*

$$G = \{x^2y - y + x, -y^2 + xy + x^2, x^3 + y - 2x\}.$$

Percebemos que x^3 *e* y^2 *aparecem como monômios líderes de G, assim* $V(I)$ *é finito. Na verdade, é fácil de resolver as equações e obter*

$$V(I) = \{(0, 0), (\alpha, -1), (-\alpha, 1), (\alpha', -1), (-\alpha', 1)\},$$

onde α *e* α' *são raizes da equação* $z^2 - z - 1 = 0$.

Lembramos do exemplo 2.1.1. A base de Groebner obtida permitiu computar a interseção reduzindo o problema ao caso de polinômios em uma variável. O próximo corolário mostra que isso sempre pode ser feito. Mais precisamente, se I é zero-dimensional, podemos escolher uma ordenação "boa"para chegar em uma tal base conveniente. E, assim sendo, podemos computar o conjunto de zeros do ideal.

Corolário 2.1.4. *Seja I um ideal zero-dimensional e G uma base de Groebner reduzida de I com a ordem lex tal que $x_1 < x_2 < ... < x_n$. Então podemos ordenar $g_1, ..., g_t$ tal que g_1 possui somente a variável x_1, g_2 possui somente as variáveis x_1 e x_2 com $LT(g_2)$ uma potência de x_2, g_3 possui somente as variáveis x_1,x_2 e x_3 com $LT(g_3)$ uma potência de x_3, e assim até g_n.*

Demonstração: Segue imediatamente da parte (ii) do teorema anterior, que trocando, se necessário, a ordem de $\{g_1, ..., g_s\}$, obtemos $LT(g_i) = x^{\nu_i}$. Segue daí que $g_1 \in K[x_1]$, $g_2 \in K[x_1, x_2]$ e assim sucessivamente. □

Portanto, uma base de Groebner para um ideal zero-dimensional I pode ser pensada como uma forma "triangular"(tal qual o escalonamento no caso linear). Finalmente, para resolver um sistema de equações polinomiais determinada por um ideal zero-dimensional I, é suficiente ter um algoritmo para encontrar raizes de polinômios em uma variável. Isto é, primeiro resolvemos a equação em uma variável $g_1 = 0$. Para cada solução α de $g_1 = 0$, resolvemos a equação $g_2(\alpha, x_2) = 0$. Continuamos assim até $g_n = 0$. As soluções obtidas dessa maneira são as únicas possíveis soluções, porém ainda precisamos testar nas equações $g_{n+1} = 0, ..., g_t = 0$(caso $t > n$). Obtemos assim o conjunto de todas as soluções do sistema. Agora vamos apresentar um exemplo disso, e lembrar da possibilidade de computarmos uma base de Groebner de qualquer ideal usando um programa computacional, mesmo sabendo que isso possa demorar muito ou que o resultado seja um conjunto grande.

Exemplo 2.1.5. *Considere o ideal* $I = \langle z^2y + z^2, x^3y + x + y + 1, z + x^2 + y^3 \rangle$

em $\mathbb{Q}[x, y, z]$. *Computando uma base de Groebner reduzida* G *para* I *com respeito a ordem lex e* $x > y > z$. *Obtemos* $G = \{z^4 - z^3, y^{11} + 3y^8z - 2y^7 - 4y^4z + y^3 + y^2 + 2y + z^3 - z^2 + z + 1, x^2 + y^3 + z, yz^2 + z^2, xy + x + y^7 + 2y^4z - y^3 - z^2 - z, xz + y^{10} - y^9 + y^8 + 3y^7z - y^7 - 2y^6z - y^6 + 2y^5z + y^5 - 2y^4z - y^4 - 2y^3z + y^3 + y^2z - yz + y - z^3 + 5z^2 + z + 1\}$. *Usando a notação do corolário anterior, temos* $g_1 = z^4 - z^3$ *é um polinômio na variável* z. *Da mesma forma,* $g_2 = y^{11} + 3y^8z - 2y^7 - 4y^4z + y^3 + y^2 + 2y + z^3 - z^2 + z + 1$ *é um polinômio em* z *cujo* $LT(g_2) = y^{11}$. *Finalmente,* $g_3 = x^2 + y^3 + z$ *é um polinômio em x,y,z cujo* $LT(g_3) = x^2$. *Assim, para encontrar as soluções primeiro devemos notar que* $z = 0$ *ou* $z = 1$, *após encontrar as soluções de* $g_2(y, 0) = 0$ *e* $g_2(y, 1) = 0$. *Continuando assim, como exposto acima.*

Definição 2.1.6. *Um corpo* K *é chamado um corpo perfeito se sua característica é* 0 *ou tem característica* $p > 0$ *e temos* $K = K^p$; *isto é, todo elemento em* K *tem uma raiz p-ésima em* K.

Exemplo 2.1.7. *Sendo p primo, é fácil mostrar que corpos com p elementos e os de característica* 0 *são perfeitos. Porém, existem exemplos de corpos que não são dessa forma: seja* x *uma indeterminada,* $p > 0$ *a característica de* K *e* $L = K(x)$ *o corpo de frações de* $K[x]$. *Então, usando a fatoração de* $K[x]$, *podemos ver que* x *não tem uma p-raiz em* L. *Logo, o corpo* L *não é perfeito.*

Uma definição que será importante é a de polinômio livre de quadrados. Dado $f \in K[x_1, ..., x_n]$, escrevendo f como produto de distintos polinômios irredutíveis f_i, $f = f_1^{\alpha_1}...f_t^{\alpha_t}$, definimos o polinômio livre de "quadrados de f"como sendo o polinômio $f_1...f_t$ e o denotamos por $sqfree(f)$.

Por exemplo, sendo $f = (x + y^2)^3(x - y)$, então $sqfree(f) = (x + y^2)(x - y)$. Um polinômio f é dito livre de quadrados se $f = sqfree(f)$.

Voltamos a questão que é o centro desse capítulo, existe um método efetivo para computar o radical de um ideal zero-dimensional? O radical de um ideal

zero-dimensional $I = \langle f \rangle$ em $K[x]$ é fácil de ser descrito. Ele é o ideal principal gerado por $sqfree(f)$. Assim, primeiro vamos mostrar algumas propriedades dos polinômios livres de quadrados.

Proposição 2.1.8. *Sejam K um corpo, $f \in K[x]$ um polinômio não constante e f' sua derivada usual:*

a) Se $mdc(f, f') = 1$, então f é livre de quadrados.

b) Assumimos que uma das seguintes condições acontece.

1) Temos $Car(K) = 0$.

2) Temos $Car(K) = p > 0$ e $f = cf_1^{\alpha_1}...f_t^{\alpha_t}$, onde $c \in K \setminus \{0\}$, e $\alpha_1, ..., \alpha_t > 0$ satisfazem que $p \nmid \alpha_i$ para $i = 1, ..., t$, e onde $f_1, ..., f_t$ são distintos polinômios mônicos irredutíveis.

Então $sqfree(f) = f/mdc(f, f')$.

c) Seja K um corpo perfeito de característica $p > 0$. Então, temos que $f' = 0$ se, e somente se, f é da forma $f = g^p$ para algum polinômio $g \in K[x]$.

d) Seja K um corpo perfeito. Então a recíproca de a) acontece; isto é, se f é livre de quadrados, vale que $mdc(f, f') = 1$.

Demonstração: Para provar a), suponhamos que f não é livre de quadrados. Então podemos escrever f na forma $f = f_1^2 f_2$ com $f_1, f_2 \in K[x]$ e f_1 não constante. Assim, $f' = 2f_1 f_1' f_2 + f_1^2 f_2'$. E, dessa forma, $f_1 | mdc(f, f')$, o que é uma contradição.

Para provar b), escrevemos a fatoração $f = cf_1^{\alpha_1}...f_t^{\alpha_t}$ como em 2. E, assim, notamos que $mdc(f, f') = f_1^{\alpha_1 - 1}...f_t^{\alpha_t - 1}$. Logo, $f/mdc(f, f') = cf_1...f_t = sqfree(f)$.

Para provar c), observamos que se $f = g^p$, então $f' = pg'g^{p-1} = 0$. Por outro lado, se $f' = 0$ então escrevemos $f = \sum_{i \geq 0} a_i x^i$ com $a_i \in K$, e dessa forma $f' = \sum_{i \geq 1} i a_i x^{i-1} = 0$ nos diz que $a_i = 0$ para todo $i \geq 0$ tal que $p \nmid i$. Então, o polinômio f é da forma $f = \sum_{i \geq 0} a_{pi} x^{pi}$. Como o corpo K é perfeito, existe um elemento $b_i \in K$ tal que $a_{pi} = b_i^p$ para todo $i \geq 0$. Logo, $f = \sum_{i \geq 0} (b_i x^i)^p = g^p$ para

$g = \sum_{i \geq 0} b_i x^i$.

Finalmente, para provar d), escrevemos f como produto de fatores irredutíveis, $f = f_1 ... f_t$, e observamos que $f' = \sum_{i=1}^{t} f_1 ... f_{i-1} f_i' f_{i+1} ... f_t$. Agora afirmamos que cada polinômio f_i satisfaz $f_i' \neq 0$. Se $Car(K) = 0$, então a afirmação é clara. Se $Car(K) = p > 0$, o resultado segue de c; pois assim, $mdc(f_i, f_i') = 1$ o que implica que $mdc(f_i, f') = mdc(f_i, f_i') = 1$. Logo, $mdc(f, f') = 1$. $\square$

Para chegar em nosso objetivo, precisaremos de uma definição nova. Quando definimos corpos perfeitos de característica $p > 0$, falamos que todo elemento tem uma raiz p-ésima, mas não necessariamente sabemos calculá-las. Um passo importante será supor que possuímos essa habilidade de computar a raiz p-ésima.

Definição 2.1.9. *Seja K um corpo perfeito de característica $p > 0$. Dizemos que K tem efetivamente p-raízes se existe um algoritmo que computa a raiz p-ésima de qualquer elemento de K.*

Observação 2.1.10. Seja K um corpo perfeito de característica $p > 0$ que tem efetivamente p-raízes. Suponhamos que $f \in K[x]$ é um polinômio não constante tal que $f' = 0$. Então podemos efetivamente calcular o único polinômio $g \in K[x]$ tal que $f = g^p$. Para mostrar isso, vimos na proposição anterior que

$$f = \sum_{i \geq 0} a_{pi} x^{pi}.$$

Por hipótese, sabemos que para todo $i \geq 0$ tal que $a_{pi} \neq 0$, podemos computar o elemento $b_i \in K$ tal que $b_i^p = a_{pi}$. Logo, $g = \sum_{i \geq 0} b_i x^i$ é o polinômio desejado.

Agora apresentamos um algoritmo para computar o $sqfree(f)$ sobre corpos de característica p tendo efetivamente p-raízes e, em seguida, um exemplo para deixar claro cada passo apresentado no algoritmo.

Algoritmo 2.1.11. *Sejam K um corpo perfeito de característica $p > 0$ que tem efetivamente p-raízes e $f \in K[x]$ um polinômio não constante. Os seguintes passos computam o $sqfree$ do polinômio f:*

(1) *Calcule $s_1 = mdc(f, f')$. Se $s_1 = 1$, então retorne ao f.*

(2) *Calcule s_1'. Se $s_1' = 0$, então $s_1 = g^p$ para um polinômio $g \in K[x]$ unicamente determinado pela observação anterior. Calcule g, troque f por $\frac{fg}{s_1} = \frac{f}{g^{p-1}}$, e continue com o primeiro passo.*

(3) *Calcule $s_{i+1} = mdc(s_i, s_i')$ para $i = 1, 2, ...$ até que $s_{i+1}' = 0$; ou seja, $s_{i+1} = g^p$ para algum $g \in K[x]$. Então calcule g, troque f por $\frac{fg}{s_{i+1}}$ e continue com o primeiro passo.*

Demonstração: Ver em [8].

Exemplo 2.1.12. *Sejam $K = \mathbb{Z}/(5)$ e $f = x^{31} - 2x^{30} - x^6 + 2x^5 \in K[x]$. Aplicamos o algoritmo anterior para computar o $sqfree$ do polinômio f.*

(1) *Como $f' = x^{30} - x^5$, obtemos que $s_1 = mdc(f, f') = x^{30} - x^5 \neq 1$.*

(2) *Como $s_1' = 0$, podemos escrever $s_1 = g^5$, onde $g = x^6 - x$. Assim, trocamos f por $f = fg/s_1 = x^7 - 2x^6 - x^2 + 2x$ e iniciamos novamente.*

(1) *Como $f' = 2x^6 - 2x^5 - 2x + 2$, obtemos $s_1 = mdc(f, f') = x^5 - 1 \neq 1$.*

(2) *Como $s_1' = 0$, podemos escrever $s_1 = g^5$, onde $g = x - 1$. Assim, trocamos f por $f = fg/s_1 = x^3 + 2x^2 + 2x$ e iniciamos novamente.*

(1) *Como $f' = -2x^2 - x + 2$, obtemos $s_1 = mdc(f, f') = 1$. Nesse ponto o algoritmo para e retorna o polinômio $sqfree(f) = x^3 + 2x^2 + 2x$.*

Usando um algoritmo de fatoração, poderíamos verificar que $f = x^{31} - 2x^{30} - x^6 + 2x^5 = x^5(x-1)^{25}(x-2)$ e, assim, $sqfree(f) = x^3 + 2x^2 + 2x = x(x-1)(x-2)$.

Lema 2.1.13. (Lema de Seidenberg) *Seja K um corpo perfeito e $I \subseteq K[x_1, ..., x_n]$ um ideal zero-dimensional. Suponhamos que, para todo $i \in \{1, ..., n\}$, existe um polinômio não nulo $g_i \in I \cap K[x_i]$ tal que $mdc(g_i, g_i') = 1$. Então $I = \sqrt{I}$.*

Demonstração: Pela proposição anterior, os polinômios $g_1, ..., g_n$ sao livres de quadrados. Iremos fazer a prova do lema por indução sobre n. Para $n = 1$, o ideal principal $I \subset K[x_1]$ contém um polinômio livre de quadrados. Logo, o ideal é gerado por um polinômio livre de quadrados; ou seja, é um ideal radical.

Seja $n > 1$. Escrevemos $g_1 = h_1...h_t$ como produto de polinômios irredutíveis $h_i \in K[x_1]$. Afirmamos que podemos decompor o ideal I da seguinte forma:

$$I = \bigcap_{i=i}^{t} (I + (h_i)).$$

Que $I \subseteq \bigcap_{i=i}^{t}(I + (h_i))$ é imediato. Para ver a outra inclusão, tomamos $f \in \cap_{i=i}^{t}(I + (h_i))$; ou seja, para todo $i = 1, ..., t$ existem $r_i \in I$ e $q_i \in K[x_1, ..., x_n]$ tal que $f = r_i + q_i h_i$. É claro de ver que $f.\prod_{i\neq j} h_j \in I$ para $i = 1, ..., t$, e também como $mdc(\prod_{j\neq 1} h_j, ..., \prod_{j\neq j} h_j) = 1$, resulta que podemos encontrar $l_1, ..., l_t \in K[x_1]$ tal que $l_1 \prod_{j\neq 1} h_j + ... + l_t \prod_{j\neq j} h_j = 1$. Portanto, $f = \sum_{i=1}^{t} l_i f \prod_{i\neq j} h_j \in I$ o que prova a afirmação.

Juntando essa afirmação e o fato que uma interseção finita de ideais radicais é também radical, é suficiente provar que $I + (h_i)$ é radical para $i = 1, ..., t$. Ou seja, podemos supor que g_1 é um polinômio irredutível, como precisamos mostrar que cada componente da decomposição de I é um ideal radical, notamos g_1 por h_1. Então corpo $L = K[x_1]/(g_1)$ é um K-espaço vetorial de dimensão finita, e o homomorfismo sobrejetor canônico $\varphi : K[x_1, ..., x_n] \to L[x_2, ..., x_n]$ é tal que $ker(\varphi) = (g_1) \subseteq (I + (h_1))$. O ideal $J = \varphi(I + (h_1))$ é zero-dimensional, pois $L[x_2, ..., x_n]/J$ é isomorfo a $K[x_1, ..., x_n]/(I + (h_1))$. E, percebemos que $\varphi(g_i) = g_i \in L[x_2, ..., x_n]$ satisfazem que $mdc(g_i', g_i) = 1$ para $i = 2, ..., n$. O ideal J é radical por hipótese de indução; isto é, não temos nilpotentes não nulos em $L[x_2, ..., x_n]/J$. E o isomorfismo acima garante que em $K[x_1, ..., x_n]/(I + (h_1))$ também não temos nilpotentes não nulos, então $(I + (h_1))$ é um ideal radical. Provando o lema.

Teorema 2.1.14. *Sejam K é um corpo perfeito, I um ideal zero-dimensional, $p > 0$*

característica de K, K tendo efetivamente p-raízes , g_i como no lema e $g_i^\star$ seu polinômio square-free calculado pelo algoritmo (2.1.12). Então, sabemos escrever os geradores do ideal $\sqrt{I}$ da seguinte forma:

$$\sqrt{I} = \langle I, g_1^\star, ..., g_n^\star \rangle.$$

Demonstração: consequência direta do lema anterior.

Exemplo 2.1.15. *Seja $I = \langle y + z, z^2 \rangle \subset \mathbb{Q}[y, z]$, $z^2 \in I$ e, também, $y^2 = (y - z)(y + z) + z^2 \in I$. Então pelo resultado anterior,*

$$\sqrt{I} = \langle y + z, z^2, y, z \rangle = \langle y, z \rangle.$$

Observação 2.1.16. Se o corpo K não é perfeito o resultado de Seidenberg não funciona. Por exemplo, considere $I = \langle x^p - t, y^p - t \rangle \subset \mathbb{Z}_p(t)[x, y]$. Sabemos que $x^p - t$ e $y^p - t$ são ambos square-free, mas $x^p - y^p \in I \Longrightarrow x - y \in \sqrt{I} \setminus I$. Ou seja, $I \neq \sqrt{I}$

G. Kemper em [7] propôs uma bela generalização do resultado de Seidenberg. Em seu artigo, é apresentado um novo algoritmo para computar os geradores do radical de um ideal zero-dimensional em que o corpo é finitamente gerado sobre um corpo perfeito. Ou seja, o nosso exemplo de que o algoritmo de Seidenberg não funciona pode ser resolvido pelo algoritmo de Kempler.

Capítulo 3

Computação do Radical de um Ideal em Característica Positiva

3.1 Alguns Resultados

Seja K um corpo qualquer, $K[x_1, ..., x_n]$ o anel de polinômios em n variáveis sobre K e $I \subseteq K[x_1, ..., x_n]$ um ideal. O radical de I é, como já vimos,

$$\sqrt{I} = \{f \in K[x_1, ..., x_n];\ \ existe\ \ e \in \mathbb{N}\ \ tal\ \ que\ \ f^e \in I\}$$

Definimos o índice de nilpotência de $x \in \sqrt{I}$ com respeito à I, como

$$nil(x, I) := min\{i > 0\ ; x^i \in I\}$$

A dimensão de um ideal I é a dimensão de Krull de seu anel de resíduos $K[x_1, ..., x_n]/I$. Se I é zero dimensional e K é um corpo perfeito, já apresentamos os resultados de Seidenberg em [11] para computar o ideal $\sqrt{I}$. Outro resultado interessante, é o método de Eisenbud em [4] que só é aplicável para um ideal I no qual o radical é gerado por elementos cujos índices de nilpotência com respeito à I

são menores que a característica. Assim, o corpo sobre o qual estamos estudando o anel de polinômios tem grande importância. Neste capítulo, a ideia principal é apresentar a proposta de Matsumoto em [10] para calcular o radical de um ideal arbitrário sobre um corpo perfeito de característica $p > 0$.

Sendo K um corpo qualquer de característica $p > 0$. Iremos encontrar o radical de um ideal próprio $I \subseteq K[x_1, ..., x_n]$. Seja q uma potência de p. Considere o endomorfismo φ:

$$K[x_1, ..., x_n] \to K[x_1, ..., x_n]$$

$$f \mapsto f^q$$

Como $(f + g)^q = f^q + g^q$ para todos f e g em $K[x_1, ..., x_n]$, então φ é um endomorfismo de $K[x_1, ..., x_n]$.

Agora vamos definir,

$$\varphi^{-1}(I) := \{f \in K[x_1, ..., x_n]/\varphi(f) \in I\}$$

O que nos fornece a seguinte ordem de inclusão,

$$I \subseteq \varphi^{-1}(I) \subseteq \sqrt{I}$$

A próxima proposição apresentará a importância dessas inclusões anteriores, dizendo que se $I \neq \sqrt{I}$, então $\varphi^{-1}(I)$ é estritamente maior que I.

Proposição 3.1.1. *Seja $I \subset K[x_1, ..., x_n]$ um ideal. Com as notações anteriores, temos:*

(i) Se $I \neq \sqrt{I}$, então $\varphi^{-1}(I)$ é estritamente maior que I.

(ii)Se $x \in \sqrt{I}$ e $x \neq 0$, então

$$nil(x, \varphi^{-1}(I)) = \lceil nil(x, I)/q \rceil,$$

onde $\lceil x \rceil = min\{n \in \mathbb{Z} | n \geq x\}$.

Demonstração: (i) Se existir $x \in \sqrt{I}$ e x não pertence a I, então vamos mostrar que $x^{\lceil nil(x,I)/q \rceil} \in \varphi^{-1}(I)$ e não pertence a I.

Se $nil(x,I) < q$, então $\lceil nil(x,I)/q \rceil = 1 \Rightarrow x^{(\lceil nil(x,I)/q \rceil)q} = x^q$ e como $nil(x,I) < q$, temos que $x^q \in I$; assim, $x^{(\lceil nil(x,I)/q \rceil)q} \in I$. Logo, $x^{\lceil nil(x,I)/q \rceil} \in \varphi^{-1}(I)$.

Se $nil(x,I) = q$, então $x^{(\lceil nil(x,I)/q \rceil)q} = x^q \in I$. Logo, $x^{\lceil nil(x,I)/q \rceil} \in \varphi^{-1}(I)$.

Se $nil(x,I) > q$, então efetuamos a divisão euclidiana do $nil(x,I)$ por q e escrevemos $nil(x,I) = qt + r$ com $0 \leq r < q$.

$$x^{(\lceil nil(x,I)/q \rceil)q} = x^{(\lceil (qt+r)/q \rceil)q} = x^{(\lceil t+r/q \rceil)q} = x^{(t+\lceil r/q \rceil)q},$$

como $\lceil r/q \rceil = 1$, temos $x^{(t+\lceil r/q \rceil)q} = x^{(t+1)q} = x^{qt+q}$, mas $q > r$ ou $r = 0$, então escrevemos $q = r + l$ para algum número natural l, e $x^{qt+q} = x^{qt+r+l} = x^{nil(x,I)+l} = x^{nil(x,I)}x^l$, o que pertence a I por definição.

O que mostra que $\varphi^{-1}(I)$ é estritamente maior que I.

(ii) Vamos mostrar que o menor expoente l tal que $x^l \in \varphi^{-1}(I)$ é $\lceil nil(x,I)/q \rceil$. Fazendo a mesma divisão euclidiana que no item (i), $nil(x,I) = qt + r$, onde $0 \leq r < q$. Obtemos

$$(\lceil nil(x,I)/q \rceil - 1)q = (\lceil (qt+r)/q \rceil - 1)q = qt + q\lceil r/q \rceil - q = qt,$$

Se $r = 0$, então $nil(x,I) = tq$. Ou seja, tq é o menor natural tal que $x^{tq} \in I$. Logo, $t = \lceil nil(x,I)/q \rceil = nil(x, \varphi^{-1}(I))$. Provando o item (ii).

Se $r \neq 0$, então

$$q(\lceil nil(x,I)/q \rceil - 1) = qt < qt + r = nil(x,I),$$

e, também

$$q\lceil nil(x,I)/q \rceil = qt + q > qt + r = nil(x,I).$$

Pela definição de $nil(x, I)$,

$$x^{\lceil nil(x,I)/q \rceil - 1} \notin \varphi^{-1}(I),$$

e, também

$$x^{\lceil nil(x,I)/q \rceil} \in \varphi^{-1}(I). \quad \square$$

Para computar os geradores do radical de um ideal, iremos tomar ideais tais que $I \neq \sqrt{I}$. Por isso, a proposição anterior será útil dizendo que, nesse caso, a seguinte cadeia é composta de inclusões estritas:

$$I \subsetneq \varphi^{-1}(I) \subsetneq \varphi^{-2}(I) \subsetneq ...$$

Pela condição de cadeia ascendente, essa cadeia deverá estacionar. Afirmamos que a cadeia para em $\sqrt{I}$, pois caso contrário ela estacionaria em um ideal J menor que $\sqrt{I}$ e aplicando $\varphi^{-1}(J)$ obtemos um ideal maior que J. Logo, existe j tal que a cadeia estaciona:

$$\varphi^{-j+1}(I) \subsetneq \varphi^{-j}(I) = \sqrt{I}.$$

Iremos apresentar uma limitação para esse valor j descrito acima. Antes disso, a seguinte proposição, que não demostraremos, limita os expoentes dos elementos do radical.

Proposição 3.1.2. *Suponhamos que $n \geq 2$. Seja d o máximo do grau total dos geradores de I e 3. Para $x \in \sqrt{I}$,*

$$nil(x, I) \leq d^n.$$

Demonstração: Ver demonstração em [12].

Note que d depende do conjunto de geradores do ideal I e não é unicamente determinado por I.

Proposição 3.1.3. *Sejam $I \subseteq K[x_1, ..., x_n]$ um ideal próprio e q uma potência do primo p.Com as notações anteriores, temos:*

(i) $j = \lceil log_q max\{nil(x, I) | x \in \sqrt{I}\}\rceil$.

(ii) $j \leq \lceil n log_q d\rceil$.

Demonstração: (i) Definimos,

$$\sigma(i) := \lceil i/q\rceil$$

$$\tau(i) := min\{m|\sigma^m(i) = 1\}.$$

Como $\sigma^m(i) = 1$ se, e somente se, $\lceil i/q^m\rceil \leq 1$; isto é, $i/q^m < 1$. Temos que $\tau(i) = min\{m|\ i < q^m\} = min\{m|\ log_q i \leq m\} = min\{m|\ \lceil log_q i\rceil \leq m\} = \lceil log_q i\rceil$. Sendo $j = log_q\{max\{nil(x, I)|\ x \in \sqrt{I}\}\}$, temos que $j = \tau(max\{nil(x, I)|x \in \sqrt{I}\})$. Seja $l := \lceil log_q i\rceil$. Chamando $t = log_q i$, sabemos que $i = q^t$. Também, $l = \lceil t\rceil$, assim $l - 1 < t$ e $t \leq l$. Logo,

$$q^{l-1} < i \leq q^l,$$

$$\sigma(q^{l-1}) = q^{l-2} < \sigma(i) \leq q^{l-1} = \sigma(q^l),$$

$$\vdots$$

$$\sigma^{l-1}(q^{l-1}) = 1 < \sigma^{l-1}(i) \leq q = \sigma^{l-1}(q^l).$$

Portanto, $\tau(i) = \lceil log_q i\rceil$.

O próximo passo será computar $\varphi^{-1}(I)$. Para isso, precisaremos de muitas ferramentas já vistas com as Bases de Groebner e, também, conceitos novos até então: como as funções polinomiais e os problemas de computar núcleos e imagens dessas funções.

Definição 3.1.4. *Sendo K um corpo de característica $p > 0$. Definimos o endomorfismo φ_c de $K[x_1, ..., x_n]$ como*

$$\sum a_{m_1...m_n} x_1^{m_1}...x_n^{m_n} \longmapsto \sum a^q_{m_1...m_n} x_1^{m_1}...x_n^{m_n}$$

e o endomorfismo φ_v como

$$f(x_1, ..., x_n) \longmapsto f(x_1^q, ..., x_n^q)$$

Observação 3.1.5. Como $\varphi = \varphi_c \circ \varphi_v = \varphi_v \circ \varphi_c$,

$$\varphi^{-1}(I) = \varphi_c^{-1}(\varphi_v^{-1}(I)) = \varphi_v^{-1}(\varphi_c^{-1}(I))$$

Poderemos calcular $\varphi_v^{-1}(I)$ transformando-o em um núcleo de uma aplicação especial, o que veremos na próxima seção.

3.2 Aplicações Polinomiais e Algoritmo de Matsumoto

Nesta seção estaremos interessados em estudar os homomorfismos entre os anéis de polinômios $K[y_1, ..., y_m]$ e $K[x_1, ..., x_n]$. Definimos uma única aplicação determinada por

$$\phi : y_i \longmapsto f_i$$

onde $f_i \in K[x_1, ..., x_n], 1 \leq i \leq m$. Isto é, se oferecemos um polinômio $h \in K[y_1, ..., y_m]$, escrevemos na forma $h = \sum_\nu c_\nu y_1^{\nu_1} ... y_m^{\nu_m}$, onde $c_\nu \in K$, $\nu = (\nu_1, ..., \nu_m) \in \mathbb{N}^m$, e somente finitos c_ν's são não nulos. Então, temos

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

Sabemos que o núcleo de ϕ é o ideal,

$$ker(\phi) = \{h \in K[y_1, ..., y_m];\ \phi(h) = 0\},$$

e a imagem de ϕ é uma K-subalgebra de $K[x_1, ..., x_n]$; essa subalgebra é denotada por $K[f_1, ..., f_m]$. Usando a teoria da eliminação podemos determinar:

(i) O núcleo de ϕ, mais precisamente, uma base de Groebner para $ker(\phi)$;

(ii)A imagem de ϕ, mais precisamente, um algoritmo para decidir quando um polinômio f está na imagem de ϕ.

O passo importante dessa seção será escrever $\varphi_v^{-1}(I)$ como um núcleo de uma aplicação polinomial e com o próximo lema e teorema seremos capazes de caracterizar esses núcleos, completando o item (i), e tendo como consequência um processo para computar o desejado $\varphi_v^{-1}(I)$.

Lema 3.2.1. *Seja $a_1, a_2, ..., a_n, b_1, ..., b_n$ elementos de um anel comutativo R. Então o elemento $a_1a_2...a_n - b_1b_2...b_n$ está no ideal $\langle a_1 - b_1, a_2 - b_2, ..., a_n - b_n\rangle$.*

Demonstração: A prova é simples, usando indução em n e o fato de que

$$a_1a_2...a_n - b_1b_2...b_n = a_1(a_2...a_n - b_2...b_n) + b_2...b_n(a_1 - b_1).$$

Teorema 3.2.2. *Sejam $\phi : y_i \longmapsto f_i$ um aplicação polinomial de $K[y_1, ..., y_m]$ em $K[x_1, ..., x_n]$ e $J = \langle y_1 - f_1, ..., y_m - f_m\rangle$ um ideal em $K[y_1, ..., y_m, x_1, ..., x_n]$. Então, $ker(\phi) = J \cap K[y_1, ..., y_m]$.*

Demonstração: Seja $g \in J \cap K[y_1, ..., y_m]$. 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 $h_i \in K[y_1, ..., y_m, x_1, ..., x_n]$. Como g é zero quando aplicamos em $(y_1, ..., y_m) = (f_1, ..., f_m)$. Então $g \in ker(\phi)$.

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

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

onde $c_\nu \in K, \nu = (\nu_1, ..., \nu_m) \in \mathbb{N}^m$. Como $g(f_1, ..., f_m) = 0$, temos que

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

Pelo lema anterior, cada termo da soma acima está no ideal J, e então $g \in J \cap K[y_1, ..., y_m]$. $\square$

Agora, lembramos que a proposição 1.6.14 nos mostrou que é possível computar uma base de Groebner para o ideal de eliminação $G_l = G \cap K[x_{l+1}, ..., x_n]$, sendo suficiente possuirmos uma base de Groebner G para o ideal J. Portanto, possuímos um algoritmo para computar uma base de Groebner para o kernel da aplicação ϕ. Primeiro, computamos uma base de Groebner G para o ideal

$$J = \langle y_1 - f_1, ..., y_m - f_m \rangle \subseteq K[y_1, ..., y_m, x_1, ..., x_n]$$

com respeito a uma ordem de eliminação cujas as variáveis em x sejam maiores do que as variáveis em y. Os polinômios em G sem qualquer variável x formam uma base de Groebner para o kernel da ϕ.

Exemplo 3.2.3. *Seja* $\phi : \mathbb{Q}[r, u, v, w] \longrightarrow \mathbb{Q}[x, y]$ *definida por*

$$r \longmapsto x^4$$

$$u \longmapsto x^3y$$

$$v \longmapsto xy^3$$

$$w \longmapsto y^4$$

Primeiro, calculamos uma base de Groebner G para o ideal

$$J = \langle r - x^4, u - x^3y, v - xy^3, w - y^4 \rangle \subseteq \mathbb{Q}[r, u, v, w, x, y]$$

com a ordem deglex $y > x$ *e a ordem degrevlex sobre as variáveis* r, u, v, w *tal que* $r > u > v > w$. *Na ordem de eliminação usamos qualquer ordem monomial que faça as variáveis* x, y *maiores que as variáveis* r, u, v, w. *Obtemos uma base de Groebner* $G = \{x^4 - r, x^3y - u, xy^3 - v, y^4 - w, yv - xw, yr - xu, y^2u - x^2v, x^2y^2w -$

$v^2, uv - rw, v^3 - uw^2, rv^2 - u^2w, yuw - xv^2, u^3 - r^2v, yu^2 - xrv\}$. *Assim, como vimos no teorema anterior, uma base de Groebner para* $ker(\phi)$ *é*

$$G \cap K[r, u, v, w] = uv - rw, v^3 - uw^2, rv^2 - u^2w, u^3 - r^2v.$$

Agora, com todas as ferramentas necessárias, estamos prontos para apresentar a maneira de computar $\varphi_v^{-1}(I)$. Basta considerar a seguinte aplicação,

$$\varphi : K[x_1, ..., x_n]/I \longrightarrow K[X_1, ..., X_n]/I$$

$$x_i \longmapsto f_i = X_i^q$$

onde X_i é uma nova variável para $i = 1, ..., n$. Conforme o teorema anterior, devemos construir o ideal

$$J = \langle I, x_1 - X_1^q, ...x_n - X_n^q \rangle.$$

Então, como no exemplo anterior, podemos computar

$$\varphi_v^{-1}(I) = ker(\varphi) = J \cap K[x_1, ..., x_n].$$

Para finalizar, o problema restante é saber como computar $\varphi_c^{-1}(I)$. Quando K é um corpo perfeito, a restrição $\varphi_c|K$ é um automorfismo de K, assim φ_c^{-1} é um automorfismo de $K[x_1, ..., x_n]$ e

$$\varphi_c^{-1}(I) = \{f \in K[x_1, ..., x_n]; \varphi_c(f) \in I\} = \{\varphi_c^{-1}(y); y \in I\}.$$

Logo, se I é gerado por $f_1, ..., f_s$, $\varphi_c^{-1}(I)$ é gerado por $\varphi_c^{-1}(f_1), ..., \varphi_c^{-1}(f_s)$. Resta apenas mostrar quem é o automorfismo inverso $\varphi_c^{-1}(f_i)$, onde $f_i \in K[x_1, ..., x_n]$.

Se K é um corpo finito com p^m elementos, então a restrição de φ_c a F_{p^m} é

$$\alpha \longmapsto \alpha^{p^{(log_p q) mod m}}.$$

Assim, o automorfismo inverso φ_c^{-1} é

$$\alpha \longmapsto \alpha^{p^{m-(log_p q mod m)}}.$$

Se K não é perfeito, não é conhecido ainda um método para computar $\varphi_c^{-1}(I)$. Agora, vamos descrever o algoritmo que apresentamos nessa seção e oferecer um exemplo para computar o radical de um ideal.

Algoritmo 3.2.4. (Algoritmo de Matsumoto)

Entrada: *Uma base de Groebner B, com qualquer ordem monomial, para um ideal próprio I de $K[x_1, ..., x_n]$ e q um potência da característica p.*

Saída: *Uma base de Groebner para o radical $\sqrt{I}$.*

Descrição do Algoritmo:

1. Seja $B = \{f_1, ..., f_s\}$. Calcule $\varphi_c^{-1}(f_i)$ para $i = 1, ..., s$.

2. Calcule uma base de Groebner B' para $\{\varphi_c^{-1}(f_1), ..., \varphi_c^{-1}(f_s), y_1 - x_1^q, ...y_n - x_n^q\}$ com uma ordem em que as variáveis x são maiores que as variáveis y, através do algoritmo de Buchberger. Seja $B'' = B' \cap K[y_1, ..., y_n]$, com y_i trocado por x_i para cada i.

3. Se o ideal gerado por B'' é igual ao B, então tome B'' e termine o algoritmo. Caso contrário, tome B como B'' e retorne ao primeiro passo.

Já vimos na primeira seção que o número de iterações desse algoritmo é menor ou igual a $\lceil n\ log_q d \rceil$, onde d é o máximo do grau total dos geradores de I e 3. Mostraremos agora um exemplo presente em [4] que ilustra o algoritmo anterior em característica 7.

$$I = \langle z^7 - xyu^5, y^4 - x^3u \rangle.$$

O primeiro passo do algoritmo não mudará nada os geradores, pois φ_c é a função identidade nesse caso. No segundo passo do algoritmo, vamos computar $\varphi_v^{-1}(I)$.

Como já vimos, devemos considerar um seguinte novo ideal em $K[x, y, z, u, X, Y, Z, U]$ e eliminar as variáveis u, x, y, z:

$$\langle z^7 - xyu^5, y^4 - x^3u, u^7 - U, x^7 - X, y^7 - Y, z^7 - Z\rangle.$$

Podemos eliminar as variáveis por computação de uma base de Groebner com respeito a ordem de eliminação com u, x, y, z maiores que U, X, Y, Z, que é:

$$\begin{array}{ccc}
-UX + YZ, & -Y^3 + X^2Z, & -UY^2 + XZ^2, \\
U^2Y - Z^3, & -ux^3 + y^4, & z^7 - Z, \\
y^7 - Y, & x^7 - X, & u^7 - U, \\
-u^5xy + z^7, & -x^4y^4 + uX, & u^2X - xyY, \\
-u^2y^6Y + xXZ, & -u^4y^5 + x^2Z, & -xyU + u^2Z, \\
-y^5U + u^3x^2Z, & u^3x^2y^2Z - UY, & -u^2y^6Z + xUY, \\
u^2UY - xyZ^2, & -u^2Y^2 + xyXZ, & -u^6y^4 + x^3U, \\
uy^3X - x^4Y, & -u^4Y + x^2y^2Z, & x^4U - uy^3Z, \\
uy^3UY - x^4Z^2, & -uy^3Y^2 + x^4XZ, & -u^3y^2Y + x^5Z,
\end{array}$$

O conjunto dos polinômios que não possuem as variáveis u, x, y, z é $\{-UX + YZ, -Y^3 + X^2Z, -UY^2 + XZ^2, U^2Y - Z^3\}$. Como já mostramos no algoritmo, basta agora trocar as variáveis e concluímos que $\sqrt{I}$ é gerado por

$$\{-ux + yz, -y^3 + x^2z, -uy^2 + xz^2, u^2y - z^3\}.$$

Referências Bibliográficas

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

[2] Atiyah, M. F.; Macdonald, I. G., *"Introduction to Commutative Algebra"*, Addison - Wesley Publishing Company, Massachusetts, 1969.

[3] Cox D.; Little J. e D. O'Shea, *Ideals, Varieties and Algorithms*, Springer Verlag, New York - Berlin - Heidelberg, 1997.

[4] Eisenbud D.; Huneke C. e W. Vasconcelos. *Direct methods for primary decomposition*, Invent. Math., 110 (1992), 207-235.

[5] Gianni P.; Trager B. e Zacharias G., *Bases and primary decomposition of ideals*, J. Symbolic Computation, 6, 149-167, 1988.

[6] Kaplansky, I., *"Commutative Rings"*, Univ. of Chicago Press, Chicago, 1974.

[7] Kemper G. , *"The calculation of radical ideals in positive characteristic"*, J. Symbolic Computation, 34 (2002), 229-238.

[8] Kreuzer,M.; Robbiano, L., *"Computational Commutative Algebra"*, Springer, Regensburg e Genova, 2000.

[9] Krick T.; A. Logar, *An algorithm for the computation of the radical of an ideal in the ring of polynomials*, AAECC9, Springer LNCS, 539, 195-205, 1991

[10] Matsumoto R. , *Computing the radical of an ideal in positive characteristic*, J. Symbolic Computation, 32 (2001), 263-271.

[11] Seidenberg A. , *Constructions in algebra*, Trans. Amer. Math. Soc., 197, 273-313, 1974.

[12] Vasconcelos, W.V., *Computational Methods in Commutative Algebra and Algebraic Geometry*, Springer, 1998.