UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL - PROFMAT
(Mestrado)

Lígia Bittencourt Ferraz de Camargo

Sistemas de Equações Polinomiais e Coloração de Mapas

Maringá-PR
2013

Lígia Bittencourt Ferraz de Camargo

Sistemas de Equações Polinomiais e Coloração de Mapas

Trabalho de Conclusão de Curso apresentado ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre.

Área de concentração: Matemática.

Orientador: Dr. Marcelo Escudeiro Hernandes

Maringá

2013

Sistemas de Equações Polinomiais e Coloração de Mapas

Lígia Bittencourt Ferraz de Camargo

Trabalho de Conclusão de Curso apresentado ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários à obtenção do grau de Mestre.

COMISSÃO JULGADORA

Profa. Dra. Marcela Duarte da Silva

Representando Marcelo Escudeiro Hernandes - Orientador

Universidade Estadual de Maringá (UEM)

Prof. Jair da Silva

Universidade Federal do Mato Grosso do Sul

Prof. Wesley Vagner Inês Shrabayashi

Universidade Estadual de Maringá

Aprovada em: 12 de março de 2013.

Local de defesa: Auditório DMA , Bloco F-67, *campus* da Universidade Estadual de Maringá.

Agradecimentos

$\mathcal{A}$o concluir este trabalho, agradeço:

$\mathcal{A}$os meus pais Fábio Ferraz de Camargo e Rosa Maria Bittencourt Camargo que desde minha infância mostraram-me a importância de uma boa educação e ao meu irmão Fábio Bittencourt Ferraz de Camargo com quem pude contar em todos os momentos.

$\mathcal{A}$o meu orientador Professor Doutor Marcelo Escudeiro Hernandes, exemplo de dedicação que, ministrando uma disciplina da minha graduação, foi capaz de despertar meu interesse a ponto de dar continuidade nos estudos. Obrigada pela valiosa contribuição na elaboração deste trabalho.

$\mathcal{A}$o professor Doutor Juan Palomino Soriano, coordenador do PROFMAT - Mestrado Profissional em Matemática em Rede Nacional, que atuou comprometido com o projeto e atendendo, na medida do possível, às nossas necessidades.

$\mathcal{A}$os demais professores do PROFMAT da Universidade Estadual de Maringá que repassaram, durante suas aulas, valiosos ensinamentos tão importantes para nosso crescimento pessoal e profissional.

$\mathcal{À}$ CAPES pelo incentivo financeiro que viabilizou minha dedicação ao programa.

$\mathcal{A}$os meus colegas de turma pelo companheirismo e apoio recebido no decorrer do curso. Agradecimento especial a Lucimeire Adorno e Roberta Ferreira Xavier pelos bons momentos vivenciados e pela amizade que criamos. Também ao amigo Maciel Araujo que sempre se mostrou prestativo me auxiliando principalmente na parte técnica deste trabalho.

$\mathcal{À}$s amigas de longa data Jordana Ponchio de Oliveira e Ivnna Gurniski Carniel pelo apoio e incentivo oferecidos em todos os momentos.

$\mathcal{E}$, principalmente, a Deus, por estar presente em minha vida e me dar condições de prosseguir em meus estudos.

Resumo

O estudo das Bases de Gröbner foi motivado pelo que chamamos de Problema das Três Cores que consiste em decidir se um mapa pode ser colorido utilizando apenas três cores e, em caso afirmativo, como proceder a coloração. Para que pudéssemos "algebrizar" tal problema foi necessário o estudo de sistemas de equações polinomiais, uma das mais difundidas aplicações das Bases de Gröbner. Esse estudo, por sua vez, requereu conceitos e propriedades ligadas aos anéis de polinômios em várias indeterminadas e de ideais.

Palavras chave: Sistemas de Equações Polinomiais, Bases de Gröbner, Problema das Três Cores.

Abstract

In this work we study Gröbner basis to present an answer for the Three Color Problem that consist to decide if a given map can or not to paint using only three colors and, if is the case, how to paint it. The main idea is translate the geometric problem to an algebraic problem and for this we study system of polynomials equations, the more known application of Gröbner basis, concepts and properties of polynomial rings in several variables and ideals as well.

Key words: System of polynomials equations, Gröbner Basis, Three Color Problem.

Lista de Figuras

Sumário

Introdução

O estudo de sistemas polinomiais lineares é abordado no ensino médio por meio da regra de Cramer e da eliminação de Gauss ou escalonamento. No entanto, nenhuma menção a sistemas polinomiais em geral é apresentado, mesmo que estes surjam naturalmente quando se estuda a interseção de circunferências ou ainda objetos geométricos com elipses, esferas, cones, etc.

Neste trabalho, apresentamos um método para estudar sistemas polinomiais quaisquer, isto é, analisar quando possuem soluções, caso possuam como estimar o número de soluções e se as soluções forem em número finito como obtê-las. O método utiliza bases de Gröbner e, como veremos, omitindo as demonstrações e linguagem técnica, ou seja, restringindo-se apenas aos cálculos, pode ser entendido facilmente.

O conceito de bases de Gröbner foi introduzido em 1965 por Bruno Buchberger na sua tese de doutorado que as nomeou em homenagem ao seu orientador, Wolfgang Gröbner. Inicialmente, a importância de seu trabalho não foi devidamente reconhecida, apenas nos anos 80 pesquisadores começaram uma investigação mais profunda da nova teoria. Desde então muitas generalizações e uma ampla variedade de aplicações foram desenvolvidas.

Vamos admitir o conhecimento prévio das propriedades e operações do anel de polinômios em uma indeterminada. O capítulo 1 trata de anéis de polinômios em várias variáveis, maneiras de ordenar monômios e uma generalização do algoritmo da divisão, bem como apresentamos exemplos de como utilizar tal algoritmo.

O capítulo 2 inicia com o conceito de ideais que serão utilizados na sequência ao definir bases de Gröbner. Além disso, apresentamos um resultado que permitirá verificar se, dado um ideal e um elemento $f \in \mathbb{C}[x_1, ..., x_n]$, temos $f \in I$. Em seguida, visando apresentar o

resultado crucial que nos forneça o algoritmo de Buchberger, que é um método para obter uma base de Gröbner, introduzimos o conceito de S-polinômio. Finalizamos o capítulo com uma aplicação do referido algoritmo.

Tendo em vista que as aplicações mais difundidas das bases de Gröbner encontram-se no estudo de sistemas de equações polinomiais, o capítulo 3 aborda esse conceito e apresenta teoremas essenciais no que diz respeito a condição necessária e suficiente para um sistema de equações polinomiais admitir um número finito de soluções. Neste capítulo também será apresentada uma descrição do problema de coloração de mapas utilizando apenas três cores que será modelado por um sistema de equações polinomiais e resolvido utilizando a teoria das bases de Gröbner.

Capítulo 1

Anéis de Polinômios em Várias Indeterminadas

Seja $\mathbb{C}$ o corpo dos números complexos e considere o conjunto

$$\mathbb{C}[x] = \{a_n x^n + ... + a_1 x + a_0, n \in \mathbb{N}, a_i \in \mathbb{C} \text{ e } i = 0, ..., n\}.$$

Um elemento de $\mathbb{C}[x]$ é chamado um polinômio na indeterminada x com coeficientes em $\mathbb{C}$.

Nesta seção abordaremos conceitos ligados aos anéis de polinômios em várias indeterminadas.

Seja $\mathbb{C}[x_1]$. Se x_2 é uma indeterminada sobre o anel $\mathbb{C}[x_1]$, define-se

$$\mathbb{C}[x_1, x_2] = (\mathbb{C}[x_1])[x_2],$$

isto é, o anel de polinônios na indeterminada x_2 com coeficientes no anel $\mathbb{C}[x_1]$.

Pode-se então definir recursivamente,

$$\mathbb{C}[x_1, x_2, ..., x_n] = (\mathbb{C}[x_1, x_2, ..., x_{n-1}])\,[x_n]$$

que chamamos anel de polinômios nas indeterminadas $x_1, ..., x_n$ com coeficientes no corpo $\mathbb{C}$.

Um elemento não nulo $f \in \mathbb{C}[x_1, ..., x_n]$ é um elemento da forma

$$f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i},$$

com $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n, a_\alpha \in \mathbb{C}$ e $J \subset \mathbb{N}^n$ finito.

Definição 1.0.1. *Um* **termo** *de* $\mathbb{C}[x_1, ..., x_n]$ *é um elemento da forma* $a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i}$ *com* $\alpha = (\alpha_1, ..., \alpha_n) \in \mathbb{N}^n, a_\alpha \in \mathbb{C}$ *é chamado de* **coeficiente** *do termo e* $\prod_{i=1}^{n} x_i^{\alpha_i}$ *é chamado* **monômio**. *Chamamos de* **grau** *(total) do monômio* $\prod_{i=1}^{n} x_i^{\alpha_i}$ *o número natural dado por*

$$gr\left(\prod_{i=1}^{n} x_i^{\alpha_i}\right) = \sum_{i=1}^{n} \alpha_i.$$

Dado $f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} \in \mathbb{C}[x_1, ..., x_n]$ *não nulo, denotaremos por*

$$\mathbb{M}(f) = \left\{ \prod_{i=1}^{n} x_i^{\alpha_i}; a_\alpha \neq 0 \right\}$$

o conjunto de todos os monômios de f *e chamamos*

$$gr(f) = max \left\{ \sum_{i=1}^{n} \alpha_i; \prod_{i=1}^{n} x_i^{\alpha_i} \in \mathbb{M}(f) \right\}$$

de **grau** *(total) de* f.

Vejamos um exemplo de como obter o grau de monômios e de polinômios com várias indeterminadas.

Exemplo 1.0.2. *Dado o monômio* x^2yz^5 *e o polinômio* $x^3y^4 + xy^3z^5 + x^2y^2z^3 \in \mathbb{C}[x, y, z]$ *temos que:*

- $gr(x^2yz^5) = 2 + 1 + 5 = 8$
- $gr(x^3y^4 + xy^3z^5 + x^2y^2z^2) = gr(xy^3z^5) = 1 + 3 + 5 = 9$

1.1 Ordens Monomiais

Examinando em detalhes o algoritmo da divisão em $\mathbb{C}[x]$, vemos que uma noção de ordem de termos é um ingrediente chave. Assim, podemos imaginar que uma componente muito importante de alguma extensão da divisão para polinômios em várias variáveis é uma ordem de termos em polinômios em $\mathbb{C}[x_1, ..., x_n]$. Tal ordenação necessita se aplicar a qualquer monômio deste anel e possibilitará identificar o termo líder de um elemento $f \in \mathbb{C}[x_1, ..., x_n]$.

Definição 1.1.1. *O conjunto de todos os monômios de $\mathbb{C}[x_1, ..., x_n]$ será denotado por $\mathbb{M}_n$, ou seja,*

$$\mathbb{M}_n = \left\{ \prod_{i=1}^{n} x_i^{\alpha_i}; \alpha_1, ..., \alpha_n \in \mathbb{N} \right\}.$$

O monômio $x_1^0 \cdot ... \cdot x_n^0$ será denotado por 1.

Definição 1.1.2. *Uma* **ordem monomial** $\preceq$ *sobre $\mathbb{M}_n$ é uma relação de ordem total que satisfaz:*

1. *Se $m_1, m_2 \in \mathbb{M}_n$ são tais que $m_1 \preceq m_2$, então $m_1 m_3 \preceq m_2 m_3$ para todo $m_3 \in \mathbb{M}_n$.*
2. *Todo subconjunto não vazio de $\mathbb{M}_n$ admite um menor elemento com respeito à $\preceq$.*

O Lema a seguir nos dá uma outra interpretação para a condição da boa ordenação da parte (2) da definição acima.

Lema 1.1.3. *Seja $\preceq$ uma ordem monomial em $\mathbb{C}[x_1, ..., x_n]$, então qualquer sequência decrescente (com respeito à $\preceq$) de monômios é finita.*

Demonstração: Seja $m_1 \succeq m_2 \succeq m_3 \succeq ...$, uma sequência decrescente de elementos de $\mathbb{M}_n$, então $S = \{m_i;\ i = 1, 2, ...\}$, admite um menor elemento com respeito à $\preceq$, ou seja, a sequência é finita. □

No desenvolvimento deste trabalho serão utilizadas as ordens lexicográfica e lexicográfica graduada conforme enunciadas abaixo, contudo vale ressaltar que existem outras ordens monomiais. (Veja página 34 de [1]).

Definição 1.1.4. *(***Ordem Lexicográfica** $\preceq_L$*) Dados dois monômios* $\prod_{i=1}^{n} {x_i}^{\alpha_i}, \prod_{i=1}^{n} {x_i}^{\beta_i} \in \mathbb{M}_n$, *dizemos que*

$$\prod_{i=1}^{n} {x_i}^{\alpha_i} \preceq_L \prod_{i=1}^{n} {x_i}^{\beta_i}$$

se $\alpha_k = \beta_k$ *para todo* $k \in \{1, ..., n\}$ *isto é,* $\prod_{i=1}^{n} {x_i}^{\alpha_i} = \prod_{i=1}^{n} {x_i}^{\beta_i}$, *ou existe* $i \in \{1, ..., n\}$ *tal que* $\alpha_i < \beta_i$ *e* $\alpha_j = \beta_j$ *para todo* $j < i$.

Definição 1.1.5. *(***Ordem Lexicográfica Graduada** $\preceq_{LG}$*) Dados* $\prod_{i=1}^{n} {x_i}^{\alpha_i}, \prod_{i=1}^{n} {x_i}^{\beta_i} \in \mathbb{M}_n$, *dizemos que*

$$\prod_{i=1}^{n} {x_i}^{\alpha_i} \preceq_{LG} \prod_{i=1}^{n} {x_i}^{\beta_i}$$

se:

- $gr\left(\prod_{i=1}^{n} {x_i}^{\alpha_i}\right) < gr\left(\prod_{i=1}^{n} {x_i}^{\beta_i}\right)$ *ou*
- $gr\left(\prod_{i=1}^{n} {x_i}^{\alpha_i}\right) = gr\left(\prod_{i=1}^{n} {x_i}^{\beta_i}\right)$ *e* $\prod_{i=1}^{n} {x_i}^{\alpha_i} \preceq_L \prod_{i=1}^{n} {x_i}^{\beta_i}$

Ilustramos as definições acima com a ordenação de alguns monômios com relação às ordens lexicográfica e lexicográfica graduada.

Exemplo 1.1.6. *Considere os monômios* xy^3z^3, xy^2z^4, $x^2y^4z^2$, x^4y, $x^3y^2z^3$ *pertencentes a* $\mathbb{C}[x, y, z]$. *Temos que:*

- $xy^2z^4 \preceq_L xy^3z^3 \preceq_L x^2y^4z^2 \preceq_L x^3y^2z^3 \preceq_L x^4y$
- $x^4y \preceq_{LG} xy^2z^4 \preceq_{LG} xy^3z^3 \preceq_{LG} x^2y^4z^2 \preceq_{LG} x^3y^2z^3$

1.2 O Algoritmo da pseudo-divisão

Para estudar o problema da pertinência de polinômios de várias variáveis a um ideal, formularemos um algoritmo de divisão para polinômios em $\mathbb{C}[x_1, ..., x_n]$ que estende o algoritmo de $\mathbb{C}[x]$. No caso geral, a meta é dividir $f \in \mathbb{C}[x_1, ..., x_n]$ por $g_1, ..., g_s \in \mathbb{C}[x_1, ..., x_n]$. Como veremos, isto significa expressar f na forma:

$$f = q_1 g_1 + ... + q_s g_s + r$$

onde os quocientes $q_1, ..., q_s$ e o resto r estão em $\mathbb{C}[x_1, ..., x_n]$. Alguns cuidados serão necessários para caracterziar o resto e nesse momento usaremos as ordens monomiais introduzidas. 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 monomial fixada) multiplicando algum g_i por um monômio apropriado e subtraí-lo de f. Então esse monômio torna-se um termo correspondente de q_i. Em vez de descrever o algoritmo no caso geral, consideremos a definição abaixo e a seguir trabalharemos com alguns exemplos para ilustrar o método.

Definição 1.2.1. *Fixemos uma ordem monomial $\preceq$ sobre $\mathbb{M}_n$. Dado $f \in \mathbb{C}[x_1, ..., x_n] \setminus \{0\}$ chamamos $ml(f) = max_{\preceq}\mathbb{M}(f)$ de* **monômio líder de** *f.*

O termo $tl(f) = a \cdot ml(f)$ presente na expressão de f é chamado de **termo líder** *de f e $cl(f) = a \in \mathbb{C}$ é o* **coeficiente líder** *de f.*

Exemplo 1.2.2. *Primeiro dividiremos $f = xy^2 + 1$ por $g_1 = xy + 1$ e $g_2 = y + 1$ usando a ordem lexicográfica. Queremos empregar o mesmo esquema para divisão de polinômios de uma variável, sendo que a diferença é que existem vários divisores e quocientes.*

$$\begin{array}{l|l} f = xy^2 + 1 & g_1 = xy + 1 \\ & g_2 = y + 1 \end{array}$$

Os termos líderes $tl(g_1) = xy$ e $tl(g_2) = y$ ambos dividem o termo líder $tl(f) = xy^2$. Já que g_1 é listado primeiro, usaremos tal polinômio. Dividindo xy^2 por xy, temos y e então subtraímos yg_1 de f.

$$\begin{array}{rl|l} f = xy^2 + 1 & g_1 = xy + 1 & \\ & g_2 = y + 1 & \\ \hline \underline{-xy^2 - y} & & q_1 = y \\ -y + 1 & & \end{array}$$

Agora, repetimos o mesmo processo sobre $-y+1$*. Dessa vez usaremos* g_2 *já que* $tl(g_1) = xy$ *não divide* $tl(-y + 1) = -y$*. Assim obtemos:*

$$\begin{array}{rl|l} f = xy^2 + 1 & g_1 = xy + 1 & \\ & g_2 = y + 1 & \\ \hline \underline{xy^2 + y} & & q_1 = y \\ -y + 1 & & q_2 = -1 \\ \underline{y + 1} & & \\ 2 & & \end{array}$$

Já que $tl(g_1)$ *e* $tl(g_2)$ *não dividem* 2*, segue que o resto é* $r = 2$ *e desse modo concluímos a divisão. Então, temos escrito* $f = xy^2 + 1$ *na forma:*

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

Exemplo 1.2.3. *Neste exemplo, encontraremos uma sutileza inesperada que pode ocorrer quando estamos trabalhando com polinômios de mais de uma variável. Vamos dividir* $f = x^2y + xy^2 + y^2$ *por* $g_1 = xy - 1$ *e* $g_2 = y^2 - 1$*. Como no exemplo anterior, usaremos a ordem lexicográfica.*

Os dois primeiros passos do algoritmo são usuais, dando assim a seguinte divisão parcialmente completa.

$$\begin{array}{rl|l} f = x^2y + xy^2 + y^2 & g_1 = xy - 1 & \\ & g_2 = y^2 - 1 & \\ \hline \underline{-x^2y + x} & & q_1 = x + y \\ xy^2 + x + y^2 & & \\ \underline{-xy^2 + y} & & \\ x + y^2 + y & & \end{array}$$

Note que nem $tl(g_1) = xy$ nem $tl(g_2) = y^2$ dividem $tl(x + y^2 + y) = x$. Entretanto, $x + y^2 + y$ não transmite a ideia de resto da divisão, já que $tl(g_2)$ divide y^2. Neste caso, se movermos x para o resto, podemos continuar com a divisão.

Observação 1.2.4. *Este é um fato que nunca ocorre no caso de uma variável, uma vez que o termo líder do divisor não divide mais o termo líder de um polinômio também não dividirá os demais termos e assim o algoritmo termina.*

Para executar essa idéia, criamos uma coluna de resto r, do lado esquerdo, onde colocamos os termos que pertencem ao resto, e então, continuamos dividindo até o dividendo intermediário seja zero. Abaixo encontra-se tal etapa aplicado em nosso exemplo, onde movemos x para a coluna do resto (como indicado pela seta):

$$\begin{array}{rrl} f = & x^2y + xy^2 + y^2 & \begin{array}{|l} xy - 1 \\ y^2 - 1 \\ \hline \end{array} \\ & \underline{-x^2y + x} \qquad & x + y \\ & xy^2 + x + y^2 & \\ & \underline{-xy^2 + y} & \\ & x + y^2 + y & \\ & \underline{\qquad\qquad} & \\ x & \leftarrow \quad y^2 + y & \end{array}$$

Agora, continuamos dividindo. Se podemos dividir o polinômio resultante da eliminação do termo x por $tl(g_1)$ ou $tl(g_2)$, procedemos como usualmente, e se nenhum divide, moveremos o termo líder do dividendo intermediário para a coluna do resto. Assim, obtemos o seguinte processo:

$$
\begin{array}{rll}
f = & x^2y + xy^2 + y^2 & \left|\begin{array}{l} xy - 1 \\ y^2 - 1 \end{array}\right. \\
\hline
 & -x^2y + x & x + y \\
\hline
 & xy^2 + x + y^2 & 1 \\
 & -xy^2 + y & \\
\hline
 & x + y^2 + y & \\
\hline
x & \leftarrow \quad y^2 + y & \\
 & -y^2 + 1 & \\
\hline
 & y + 1 & \\
\hline
x + y & \leftarrow \quad 1 & \\
\hline
x + y + 1 & \leftarrow \quad 0 &
\end{array}
$$

Neste caso, o resto é $x + y + 1$, e obtemos:

$$x^2y + xy^2 + y^2 = (x + y)(xy - 1) + 1(y^2 - 1) + x + y + 1. \tag{1.1}$$

Observe que o resto é a soma de monômios, nenhum dos quais é divisível pelos termos líderes $tl(g_1)$ ou $tl(g_2)$.

O exemplo acima é uma ilustração bastante completa de como o algoritmo da divisão se aplica. Este exemplo nos mostra também qual propriedade desejamos que o resto possua: nenhum de seus termos pode ser divisível pelos termos líderes dos polinômios dos divisores.

Podemos agora enunciar a forma geral do algoritmo da divisão.

Teorema 1.2.5. *(***Algoritmo da Pseudo-Divisão***) Fixada uma ordem monomial $\preceq$ e dados $f, g_1, ..., g_s \in \mathbb{C}[x_1, ..., x_n]$ com $g_i \neq 0$ para todo $i = 1, ..., s$, existem polinômios $q_1, ..., q_s, r \in \mathbb{C}[x_1, ..., x_n]$ tais que*

$$f = \sum_{i=1}^{s} q_i g_i + r$$

com $ml(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$ e todo $i = 1, ..., s$.

Demonstração: Vamos demonstrar este teorema apresentando e justificando um procedimento que fornece o resultado esperado. Considere o seguinte algoritmo:

ALGORITMO DA PSEUDO-DIVISÃO EM $\mathbb{C}[x_1, ..., x_n]$

ENTRADA: $f, g_1, ..., g_s \in \mathbb{C}[x_1, ..., x_n]$ com $g_i \neq 0$

PARA TODO $i = 1, ..., s$ DEFINA $q_1 := ... := q_s := r := 0$

E $h := f$;

ENQUANTO $h \neq 0$ FAÇA

SE EXISTIR $i \in 1, ..., s$ TAL QUE $ml(g_i)|ml(h)$

ENTÃO

ESCOLHA O MENOR TAL ÍNDICE i E FAÇA

$q_i := q_i + \frac{tl(h)}{tl(g_i)}$;

$h := h - \frac{tl(h)}{tl(g_i)} g_i$;

SENÃO

$r := r + tl(h)$;

$h := h - tl(h)$;

SAÍDA: $q_1, ..., q_s$ E r TAIS QUE $f = \sum_{j=1}^{s} q_j g_j + r$,

$ml(g_i) \nmid m$ PARA TODO $m \in \mathbb{M}(r)$

E TODO $i = 1, ..., s$.

Como primeira observação, devemos notar que as instruções acima sempre nos fornecerão uma resposta, ou seja, independente dos dados de entrada, obteremos dados de saída após um número finito de passos. Tal garantia é dada, pois independente do resultado da condicional "SE"sempre redefinimos h de modo que seu monômio líder m_i satisfaz $m_i \preceq m_{i-1}$, onde m_{i-1} é o monômio líder de h no passo anterior.

De fato, se existe $i \in \{1, ..., s\}$ tal que $ml(g_i)|ml(h)$, então temos obrigatoriamente que $ml(h) \succ ml\left(h - \frac{tl(h)}{tl(g_i)} g_i\right)$. Caso contrário temos que $ml(h) \succ ml(h - tl(h))$.

Pelo Lema (1.1.3), toda sequência decrescente de monômios é finita, ou seja, em algum momento obteremos $h = 0$ e consequentemente o algoritmo finaliza.

Agora vamos justificar porque o algoritmo acima nos dá uma resposta adequada.

Note que em cada passo executado no algoritmo temos a igualdade

$$f = \sum_{j=1}^{s} q_j g_j + r + h.$$

De fato, iniciamos com $h = f$, $r = 0$ e $q_i = 0$ para todo $i = 1, ..., s$, assim a afirmação inicia verdadeira.

Se existe $i \in \{1, ..., s\}$ tal que $ml(g_i)|ml(h)$, então redefinimos q_i por $q_i + \dfrac{tl(h)}{tl(g_i)}$, h por $h - \dfrac{tl(h)}{tl()g_i}g_i$ e temos

$$\sum_{\substack{j=1 \\ j\neq i}}^{s} q_j g_j + \left(q_i + \frac{tl(h)}{tl(g_i)}\right) g_i + r + \left(h - \frac{tl(h)}{tl(g_i)}g_i\right) = \sum_{j=1}^{s} q_j g_j + r + h = f.$$

Caso contrário, redefinimos r por $r + tl(h)$, h por $h - tl(h)$ e temos

$$\sum_{j=1}^{s} q_j g_j + (r + tl(h)) + (h - tl(h)) = \sum_{j=1}^{s} q_j g_j + r + h = f.$$

Deste modo, a equação $f = \sum_{j=1}^{s} q_j g_j + r + h$ se verifica em todos os passos do procedimento. Como o algoritmo finaliza com $h = 0$, temos após um número finito de etapas $f = \sum_{j=1}^{s} q_j g_j + r$.

Além disto, pelas instuções do procedimento acima, vemos claramente que $ml(g_j) \nmid m$ para todo $m \in \mathbb{M}(r)$ e todo $j = 1, ..., s$ o que prova o teorema. □

Um observação do algoritmo da pseudo-divisão é que o resto não é unicamente determinado. Para ilustrar isto considere o seguinte exemplo:

Exemplo 1.2.6. *Vamos dividir* $f = x^2y + xy^2 + y^2$ *por* $g_1 = y^2 - 1$ *e* $g_2 = xy - 1$. *Usaremos a ordem lexicográfica, porém, mudaremos a ordem dos divisores.*

$$\begin{array}{rrl|l}
f = & x^2y + xy^2 + y^2 & y^2 - 1 & \\
 & & xy - 1 & \\
\hline
 & -x^2y + x & & x + 1 \\
\hline
 & xy^2 + x + y^2 & & x \\
 & -xy^2 + x & & \\
\hline
 & \underline{2x + y^2} & & \\
2x & \leftarrow \quad y^2 & & \\
 & \underline{-y^2 + 1} & & \\
 & \underline{1} & & \\
2x + 1 & \leftarrow \quad 0 & &
\end{array}$$

desta forma temos que:

$$x^2y + xy^2 + y^2 = (x + 1)(y^2 - 1) + x(xy - 1) + 2x + 1. \tag{1.2}$$

Se compararmos a equação **(1.2)** com a equação **(1.1)**, veremos que o resto é diferente do que vimos no Exemplo (1.2.3). Assim, o resto pode não ser único, ou seja, pode depender da prioridade dada para os divisores $g_1, ...g_s$.

Capítulo 2

Ideais e Bases de Gröbner

Neste capítulo apresentaremos o objeto central do trabalho, a saber, Base de Gröbner, para tanto alguns conceitos algébricos se fazem necessários, para isto dedicamos a próxima seção.

2.1 Ideais em $\mathbb{C}[x_1, ..., x_n]$

No que segue vamos apresentar rapidamente o conceito de ideal, bem como as principais propriedades que utilizaremos no restante do trabalho.

Definição 2.1.1. *Considere* $\mathbb{C}[x_1, ..., x_n]$. *Dizemos que um subconjunto não vazio* $I \subseteq \mathbb{C}[x_1, ..., x_n]$ *é um* ***ideal*** *se:*

1. $f + g \in I$ para quaisquer $f, g \in I$.

2. $h \cdot f \in I$ para todo $f \in I$ e todo $h \in \mathbb{C}[x_1, ..., x_n]$.

Seja I um ideal de $\mathbb{C}[x_1, ..., x_n]$. Algumas propriedades seguem diretamente da definição, por exemplo, $0 \in I$. De fato, como I é não vazio, então existe $f \in I$, deste modo, $-f = (-1) \cdot f \in I$ e assim, $f + (-f) = 0 \in I$.

Além disto, note que se I é um ideal de $\mathbb{C}[x_1, ..., x_n]$ e um elemento inversível $f \in \mathbb{C}[x_1, ..., x_n]$ pertence a I, então $I = \mathbb{C}[x_1, ..., x_n]$. De fato, como $f \in I$ é invertível, temos que $f^{-1} \in \mathbb{C}[x_1, ..., x_n]$ e desta forma, $1 = f \cdot f^{-1} \in I$. Mas deste modo, dado $h \in \mathbb{C}[x_1, ..., x_n]$ temos que $h = h \cdot 1 \in I$, ou seja, $\mathbb{C}[x_1, ..., x_n] \subseteq I$, como obviamente $I \subseteq \mathbb{C}[x_1, ..., x_n]$, temos $I = \mathbb{C}[x_1, ..., x_n]$.

Exemplo 2.1.2. *Seja I um ideal de $\mathbb{C}[x_1, ..., x_n]$. Então, o conjunto*

$$\sqrt{I} = \{a \in \mathbb{C}[x_1, ..., x_n];\ a^n \in I \ \ para\ algum\ \ n \in \mathbb{N}\}$$

(radical de I) é ideal de $\mathbb{C}[x_1, ..., x_n]$.

Solução: De fato, inicialmente note que $\sqrt{I} \neq \emptyset$ uma vez que $I \subseteq \sqrt{I}$.

Sejam $f, g \in \sqrt{I}$ e $h \in \mathbb{C}[x_1, ..., x_n]$, em particular, existem $n, m \in \mathbb{N}$ tais que $f^n, g^m \in I$. Observe que em $(f+g)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} f^i g^{n+m-i}$ todas as parcelas pertencem a I, pois a potência de f é maior $n-1$ ou a potência de g é maior que m. Deste modo, segue que $(f+g)^{n+m} \in I$ e assim, $f+g \in \sqrt{I}$.

Além disto, temos que $(h.f)^n = h^n.f^n \in I$, ou seja, $h.f \in \sqrt{I}$. Portanto, $\sqrt{I}$ é um ideal de $\mathbb{C}[x_1, ..., x_n]$. □

A seguir apresentamos um resultado que permite construir ideais a partir de um subconjunto não vazio qualquer de um anel.

Proposição 2.1.3. *Dado um subconjunto não vazio S de $\mathbb{C}[x_1, ..., x_n]$, o conjunto*

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} a_1 \cdot f_i; m \in \mathbb{N}^*, f_i \in f\ \ e\ a_i \in \mathbb{C}[x_1, ..., x_n] \right\}$$

é um ideal de $\mathbb{C}[x_1, ..., x_n]$.

Demonstração: De fato, se $h_1 = \sum_{i=1}^{n_1} a_i \cdot f_i$, $h_2 = \sum_{j=1}^{n_2} b_j \cdot f_j \in \langle S \rangle$, então

$$h_1 + h_2 = \sum_{i=1}^{n_1} a_i \cdot f_i + \sum_{j=1}^{n_2} b_j \cdot f_j = \sum_{k=1}^{max\{n_1, n_2\}} c_k \cdot f_k \in \langle S \rangle,$$

com $c_k = a_k + b_k$. Além disto, se $a \in \mathbb{C}[x_1, ..., x_n]$, então claramente temos que

$$a \cdot h_1 = a \sum_{i=1}^{n_1} a_i \cdot f_i = \sum_{i=1}^{n_1} (a \cdot a_i) \cdot f_i \in \langle S \rangle.$$

□

Uma outra construção de ideais, vinculada a anéis de polinômios, nos será útil e portanto a apresentamos no resultado a seguir.

Proposição 2.1.4. *Sejam* $\mathbb{C}$ *e* $C \subseteq \mathbb{C}^n$*, o conjunto*

$$\mathcal{I}(C) = \{f \in \mathbb{K}[x_1, ..., x_n]; f(\underline{c}) = 0 \text{ para todo } \underline{c} = (c_1, ..., c_n) \in C\}$$

é um ideal de $\mathbb{C}[x_1, ..., x_n]$.

Demonstração: De fato, claramente $\mathcal{I}(C) \neq \emptyset$, pois $0 \in \mathcal{I}(C)$. Dados $f, g \in \mathcal{I}(C)$ e $h \in \mathbb{K}[x_1, ..., x_n]$ temos

$$(f + g)(\underline{c}) = f(\underline{c}) + g(\underline{c}) = 0 + 0 = 0$$

$$(h \cdot g)(\underline{c}) = h(\underline{c}) \cdot g(\underline{c}) = h(\underline{c}) \cdot 0 = 0$$

para todo $\underline{c} = (x_1, ..., x_n) \in C$. □

Note que $\mathcal{I}(\emptyset) = \mathbb{C}[x_1, ..., x_n]$. De fato, uma vez que o polinômio constante 1 nunca se anula, temos que $1 \in \mathcal{I}(\emptyset)$, mas desta forma, temos um elemento invertível no ideal $\mathcal{I}(\emptyset)$ donde segue a igualdade.

2.2 Bases de Gröbner para ideais em $\mathbb{C}[x_1, ..., x_n]$

Nesta seção apresentaremos as noções básicas da teoria de Bases de Gröbner que permitem, dentre outras coisas, decidir se um polinômio $f \in \mathbb{C}[x_1, ..., x_n]$ pertence ou não a um ideal I.

A resposta deste problema surgiu a partir dos estudos do matemático alemão Wolfgang Gröbner que garantem que todo ideal de $\mathbb{C}[x_1, ..., x_n]$ admite conjuntos finitos de geradores "especiais" que possibilitam decidir se um elemento pertence ou não ao ideal dado. Mas, apesar de provar que tais geradores existem, ele não dispunha de um método sistemático para determiná-los. Somente em 1967, Bruno Bruchberger, um dos alunos de Gröbner, formulou um algoritmo para obter tais geradores, os quais foram batizados de Bases de Gröbner, em

homenagem ao matemático alemão. Tal teoria desempenha um papel muito importante na Álgebra Computacional e a partir dela várias aplicações foram obtidas.

Iniciemos com a seguinte definição.

Definição 2.2.1. *Sejam $I \subset \mathbb{C}[x_1, ..., x_n]$ um ideal e $\preceq$ uma ordem monominal fixada. Um subconjunto não vazio e finito G de I é uma* **Base de Gröbner** *para I, com respeito à $\preceq$, se para todo $f \in I$ existe $g \in G$ de modo que $ml(g)|ml(f)$.*

O resultado a seguir será apresentado sem sua demonstração por ser demasiadamente técnica, mas a mesma pode ser encontrada nas referências bibliográficas que apresentamos no final do trabalho.

Teorema 2.2.2. *Todo ideal não nulo I de $\mathbb{C}[x_1, ..., x_n]$ possui uma Base de Gröbner com respeito à uma ordem monomial fixada.*

Ilustremos a definição acima com alguns exemplos.

Exemplo 2.2.3. *Dado um ideal principal $I = \langle g \rangle \subseteq \mathbb{C}[x_1, ..., x_n]$, então $G = g$ é uma base de Gröbner para I com respeito à qualquer ordem monomial.*

Exemplo 2.2.4. *Se $I = \langle m_1, ..., m_r \rangle \subseteq \mathbb{C}[x_1, ..., x_n]$ é gerado por monômios, então $G = \{m_1, ..., m_r\}$ é uma Base de Gröbner para I com respeito à qualquer ordem monomial.*

Exemplo 2.2.5. *Considere o ideal $I = \langle y^2 - x, xy - y \rangle \subseteq \mathbb{C}[x, y]$, então $G = \{y^2 - x, xy - y\}$ não é uma Base de Gröbner para I com respeito à ordem lexicográfica graduada. De fato, temos que*

$$x^2 - x = (-x + 1)(y^2 - x) + y(xy - y) \in I,$$

mas considerando a ordem lexicográfica graduada temos $ml(x^2 - x) = x^2$ não é divisível pelos monômios líderes dos elementos de G.

Podemos reformular a definição de Base de Gröbner de várias formas, abaixo reunimos algumas.

Teorema 2.2.6. *Fixe uma ordem monomial $\preceq$. Dados I um ideal não nulo de $\mathbb{C}[x_1, ..., x_n]$ e $G = \{g_1, ..., g_s\} \subset I$, então são equivalentes:*

1. G é uma Base de Gröbner para o ideal I com respeito à ordem monomial $\preceq$;
2. $\langle ml(I)\rangle = \langle ml(G)\rangle$, onde $ml(I)$ e $ml(G)$ indicam o conjunto dos monômios líderes de todos os elementos de I e G, respectivamente;
3. $f \in I$ se, e somente se, o resto da pseudo-divisão de f pelos elementos de G é zero;
4. $f \in I$ se, e somente se, podemos escrever $f = \sum_{i=1}^{s} q_i \cdot g_i$ com $ml(f) = \max_{1 \leq i \leq s}\{ml(q_i)ml(g_i)\}$.

Demonstração:

1) $\Rightarrow$ 2)**.** Como $G \subset I$, certamente $ml(G) \subset ml(I)$ e consequentemente

$$\langle ml(G)\rangle \subseteq \langle ml(I)\rangle.$$

Por outro lado, seja $m \in ml(I)$, então existe $f \in I$, tal que $ml(f) = m$. Como G é Base de Gröbner para I, existe $g_i \in G$ tal que $ml(g_i)|m$, ou seja, existe um monômio $m_i \in \mathbb{M}_n$ de tal modo que $m = m_i \cdot ml(g_i)$, ou seja, $m \in \langle ml(G)\rangle$ e $ml(I) \subseteq \langle ml(G)\rangle$.

Deste modo, dado $h \in \langle ml(I)\rangle$ existem polinômos $h_1, ..., h_k$ em $\mathbb{C}[x_1, ..., x_n]$ e $f_1, ..., f_k \in I$ tais que

$$h = \sum_{i=1}^{k} h_i \cdot ml(f_i).$$

Como $ml(f_i) \in ml(I) \subseteq \langle ml(G)\rangle$, temos que $h \in \langle ml(G)\rangle$, ou seja, $\langle ml(I)\rangle \subseteq \langle ml(G)\rangle$.

2) $\Rightarrow$ 3)**.** Como $g_1, ..., g_s \in I$, se o resto da pseudo-divisão de f por $g_1, ..., g_s$ é zero, ou seja, existem $q_1, ..., q_s \in \mathbb{C}[x_1, ..., x_n]$ tais que podemos escrever $f = \sum_{i=1}^{s} q_i \cdot g_i$, então $f \in I$.

Por outro lado, suponha que $\langle ml(I)\rangle = \langle ml(G)\rangle$ e que $f \in I$. Aplicando o algoritmo da pseudo-divisão para f e $g_1, ..., g_s$, existem polinômios $r, q_1, ..., q_s \in \mathbb{C}[x_1, ..., x_n]$ tais que

$$f = \sum_{i=1}^{s} q_i \cdot g_i + r$$

com $r = 0$ ou $ml(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$.

Assim, temos que $r = f - \sum_{i=1}^{s} q_i \cdot g_i \in I$.

Se $r \neq 0$, então temos que $ml(r) \in ml(I) \subseteq \langle ml(I)\rangle = \langle ml(G)\rangle$, ou seja, existe $g_i \in G$ tal que $ml(g_j)|ml(r)$, o que é um absurdo! Seguindo, desta maneira, que $r = 0$.

3) $\Rightarrow$ 4)**.** Esta implicação segue imediatamente do algoritmo do teorema da pseudo divisão (Teorema 1.2.5).

4) $\Rightarrow$ 1)**.** Seja $f \in I$, como $ml(f) = \max_{1\leq i\leq r}\{ml(q_i) \cdot ml(g_i)\}$, existe $g_i \in G$ tal que $ml(g_j)|ml(f)$ e, por definição, G é uma Base de Gröbner para I. □

Como consequência do teorema anterior, temos o seguinte resultado.

Corolário 2.2.7. *Se $G = \{g_1, .., g_s\}$ é uma Base de Gröbner para um ideal I com respeito à uma ordem monomial, então o resto da pseudo-divisão de um elemento $f \in \mathbb{C}[x_1, ..., x_n]$ pelos elementos de G é único (não importando a enumeração de seus elementos).*

Demonstração: Consideremos r_1 e r_2 restos da pseudo-divisão de um polinômio $f \in \mathbb{C}[x_1, ..., x_n]$ pelos elementos de G enumerados de alguma forma. Assim, existem polinômios $p_1, ..., p_s, q_1, ..., q_s \in \mathbb{C}[x_1, ..., x_n]$ tais que

$$f - \sum_{i=1}^{s} q_i \cdot g_i = r_1 \text{ e } f - \sum_{i=1}^{s} p_i \cdot g_i = r_2.$$

Deste modo, temos que

$$r_1 - r_2 = \sum_{i=1}^{s} (p_i - q_i) \cdot g_i \in I.$$

Se $r_1 \neq r_2$, então como G é uma Base de Gröbner para I, deve existir $g_i \in G$ tal que $ml(g_i)|ml(r_1 - r_2) \in \mathbb{M}(r_1) \cup \mathbb{M}(r_2)$, o que não pode ocorrer, pois r_1 e r_2 são restos da pseudo-divisão de f pelos elementos de G. Segue assim, que $r_1 = r_2$. □

No restante do capítulo apresentaremos as ferramentas algébricas para formular um algoritmo para computar uma base de Gröbner para um ideal I de $\mathbb{C}[x_1, ..., x_n]$ a partir de um conjunto finito de geradores.

Definição 2.2.8. *O mínimo múltiplo comum, ou simplesmente MMC, de dois monômios $\prod_{i=1}^{n} {x_i}^{\alpha_i}, \prod_{i=1}^{n} {x_i}^{\beta_i} \in \mathbb{M}_n$ é o monômio*

$$MMC\left(\prod_{i=1}^{n} {x_i}^{\alpha_i}, \prod_{i=1}^{n} {x_i}^{\beta_i}\right) = \prod_{i=1}^{n} {x_i}^{\gamma_i}$$

onde $\gamma_i = max\{\alpha_i, \beta_i\}$ para todo $i = 1, ..., n$.

Definição 2.2.9. *Fixada uma ordem monomial em $\mathbb{M}_n$ e dados elementos $f, g \in \mathbb{C}[x_1, ..., x_n] \setminus \{0\}$, o* **S-polinômio** *ou* **S-processo** *de f e g, que denotamos $S(f, g)$ é o polinômio*

$$S(f, g) = MMC\left(ml(f), ml(g)\right) \cdot \left(\frac{f}{tl(f)} - \frac{g}{tl(g)}\right).$$

Ilustremos a definição acima com o seguinte exemplo.

Exemplo 2.2.10. *Fixemos a ordem lexicográfica graduada. O S-polinômio de $f = y^2 - x$ e $g = xy - y$ é*

$$S(f, g) = xy^2\left(\frac{y^2 - x}{y^2} - \frac{xy - y}{xy}\right) = -x^2 + y^2.$$

A ideia crucial de Buchberger se resume nos dois próximos resultados. A proposição a seguir apresenta uma condição equivalente para um conjunto ser uma Base de Gröbner

em termos de S-polinômios e o teorema na sequência, apresentado em forma de algoritmo, sintetiza o método provado por Buchberger para obter uma Base de Gröbner. Vamos omitir as demonstrações por serem técnicas e relativamente longas, mas o leitor interessado pode consultá-las nas referências que listamos no final do trabalho.

Proposição 2.2.11. *Fixada uma ordem monomial $\preceq$ sobre $\mathbb{M}_n$, temos que um conjunto $G = \{g_1, ..., g_s\} \subset \mathbb{C}[x_1, ..., x_n]$ é uma Base de Gröbner para o ideal $I = \langle g_1, ..., g_s \rangle$ com respeito à $\preceq$ se, e somente se, o resto da pseudo-divisão de todo S-polinômio $S(g_i, g_j)$ pelos elementos de G é nulo.*

Teorema 2.2.12. *(***Algoritmo de Buchberger***) Fixada uma ordem monomial e dado $g_1, ..., g_s \subset \mathbb{C}[x_1, ..., x_n]$, podemos obter uma Base de Gröbner G para o ideal $I = \langle g_1, ..., g_s \rangle$ aplicando o seguinte algoritmo:*

ALGORITMO DE BUCHBERGER

ENTRADA: $g_1, ..., g_s \subset \mathbb{C}[x_1, ..., x_n]$;
DEFINA $G_0 := \emptyset, G_1 := g_1, ..., g_s$ E $i := 1$;
ENQUANTO $G_{i-1} \neq G_i$ FAÇA
    SE EXISTIREM $f, h \in G_i$ TAIS QUE
    O RESTO r DA PSEUDO-DIVISÃO DE $S(f, h)$ POR
    G_i É NÃO NULO
        ENTÃO
            $G_{i+1} := G_i \cup r$;
        SENÃO
            $G_{i+1} := G_i$;
    $i := i + 1$;
SAÍDA: $G := G_i$ É BASE DE GRÖBNER PARA I.

A seguir apresentamos um exemplo de como calcular uma Base de Gröbner utilizando o algoritmo acima.

Exemplo 2.2.13. *Considere o ideal* $I = \langle y^2 - x, xy - y\rangle \subseteq \mathbb{C}[x, y]$. *Como vimos em um dos exemplos anteriores, o conjunto* $\{f = y^2 - x, g = xy - y\}$ *não é uma Base de Gröbner para* I *com respeito à ordem lexicográfica graduada. Assim, vamos aplicar o algoritmo de Buchberger a fim de obter uma Base de Gröbner para o ideal* $I = \langle f, g\rangle$.

Passo 1*: Consideramos* $G_1 = \{f, g\}$. *Como vimos no exemplo (2.2.10),* $S(f, g) = -x^2 + y^2$, *cujo resto da pseudo-divisão pelos elementos de* G_1 *é* $h = -x^2 + x$.

Passo 2*: Agora consideramos* $G_2 = \{f, g, h\}$. *Os S-polinômios que merecem análise são* $S(f, h) = -x^3 + xy^2$ *e* $S(g, h) = 0$ *já que não necessitamos nos atentar à* $S(f, g)$ *neste passo.*

Como $S(f, h) = x \cdot f + 0 \cdot g + x \cdot h$, *ou seja, o resto da divisão por* G_2 *é nulo, temos que* $G_2 = \{y^2 - x, xy - y, -x^2 + x\}$ *é uma Base de Gröbner para* I *com respeito à ordem lexicográfica graduada.*

Capítulo 3

Sistemas de Equações Polinomiais e Coloração de Mapas

Dentre as diversas aplicações de Base Gröbner para ideais de $\mathbb{C}[x_1, ..., x_n]$, abordaremos o estudo de sistemas de equações polinomiais visando, na sequência, apresentar o problema da coloração de mapas com três cores.

No capítulo anterior, vimos que dado um subconjunto $C \subseteq \mathbb{C}^n$ podemos associar um ideal $\mathcal{I}(C) \subseteq \mathbb{C}[x_1, ..., x_n]$ definido por

$$\mathcal{I}(C) = \{f \in \mathbb{K}[x_1, ...x_n]; f(\underline{c}) = 0 \text{ para todo } \underline{c} = (c_1, ..., c_n) \in C\},$$

ou seja, temos uma aplicação:

$$\begin{array}{ccc} \mathcal{I} : \{C; C \subseteq \mathbb{C}^n\} & \to & \{I; I \text{ é ideal de } \mathbb{C}[x_1, ..., x_n]\} \\ C & \mapsto & \mathcal{I}(C). \end{array}$$

Embora a aplicação acima não seja uma bijeção, dado um ideal $I \subseteq \mathbb{C}[x_1, ..., x_n]$, podemos associar um conjunto $\mathcal{Z}(I) \subseteq \mathbb{C}^n$ dado por

$$\mathcal{Z}(I) = \{\underline{c} = (c_1, ..., c_n) \in \mathbb{C}^n; f(\underline{c}) = 0 \text{ para todo } f \in I\}.$$

Estudar as soluções de um sistema de equações polinomiais é, na verdade, analisar o conjunto $\mathcal{Z}(I)$ em que I é o ideal gerado pelos polinômios que definem o ideal I. Nesse sentido, o teorema a seguir é de grande importância, omitiremos sua demonstração uma vez que para inclui-la teríamos que nos delongar demasiadamente em tópicos algébricos.

Teorema 3.0.14 (Teorema dos Zeros de Hilbert-Versão Forte)**.** *Para qualquer ideal* $\mathcal{I}$ *de* $\mathbb{C}[x_1, ..., x_n]$ *temos que* $\mathcal{I}(\mathcal{Z}(\mathcal{I}))=\sqrt{\mathcal{I}}$.

Como consequência podemos destacar o seguinte resultado.

Corolário 3.0.15. $\mathcal{Z}(I) \neq \emptyset$ *para qualquer ideal* $I \subsetneq \mathbb{C}[x_1, ..., x_n]$.

Demonstração: Se $\mathcal{Z}(I) = \emptyset$, teríamos $\mathcal{I}(\emptyset) = \mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$. Como $1 \in \mathcal{I}(\emptyset)$, então $1 \in \sqrt{I}$, isto é, existe $r \in \mathbb{N}^*$ tal que $1^r \in I$, ou seja, $1 \in I$. Assim $I = \mathbb{C}[x_1, ..., x_n]$, o que é um absurdo. Portanto, devemos ter $\mathcal{Z}(I) \neq \emptyset$. □

Note que o corolário (3.0.15) permite analisarmos quando um sistema de equações polinomiais tem solução.

3.1 Sistemas de Equações Polinomiais

Um sistema de equações polinomiais é dado por

$$f_1 = ... = f_m = 0$$

com $f_i \in \mathbb{C}[x_1, ..., x_n]$ para $i = 1, ..., m$. Assim, uma solução para esse sistema é $(k_1, ..., k_n) \in \mathbb{C}^n$ tal que $f_i(k_1, ..., k_n) = 0$ para todo $i = 1, ..., m$.

Note que

$$\sum_{i=1}^{m} h_i(k_1, ..., k_n) \cdot f_i(k_1, ..., k_n) = 0$$

para todo $h_i \in \mathbb{C}(x_1, ..., x_n)$, ou seja, $(k_1, ..., k_n) \in \mathcal{Z}(I)$ com $I = \langle f_1, ..., f_m \rangle$.

Uma vez que ao sistema acima associamos o ideal $I = \langle f_1, ..., f_m \rangle$, estudar se ele admite solução(ões) é o mesmo que analisar se $\mathcal{Z}(I) \neq \emptyset$. Da mesma forma, se o sistema admite solução, estimar quantas soluções existem é equivalente a analisar quantos elementos $\mathcal{Z}(I)$ apresenta. Por fim, caso o sistema admita um número finito de soluções, conhecê-las equivale a conhecer os elementos de $\mathcal{Z}(I)$.

Antes de prosseguirmos com o estudo de um sistema polinomial qualquer, vejamos um exemplo de um sistema linear.

Exemplo 3.1.1. *Considere o sistema*

$$\begin{cases} 2x + y + z + 1 = 0 \\ 3x - y + 2z + 1 = 0 \\ -x + y - z = 0. \end{cases} \tag{3.1}$$

Uma Base de Gröbner G, com respeito à ordem lexicográfica para o ideal

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

é

$$G = \{2x + y + z + 1, 3x - y + 2z + 1, -x + y - z, 5y - z + 1, -2z + 2\}.$$

Note que $1 \notin I$, isto é, o sistema admite solução. Temos que os conjuntos $G_1 = \{2x + y + z + 1, 5y - z + 1, -2z + 2\}$ e $G_2 = \{x + 1, y, z - 1\}$ também são bases de Grobner para I.

Tendo em vista que o sistema $f_1 = ... = f_m = 0$ é equivalente, ou seja, possui as mesmas soluções de $g_1 = ... = g_s = 0$ onde $G = \{g_1, ..., g_s\}$ é uma Base de Gröbner para um ideal dado $I = \langle f_1, ..., f_m \rangle$, no exemplo anterior, temos que A base de Grobner G_1 para o ideal gerado pelas equações do sistema, nos dá um novo sistema equivalente ao original, porém, mais simples de ser resolvido. A base de Gröbner G_2, por sua vez, nos forneceu um sistema, equivalente ao original, de onde podemos obter facilmente a solução

$$x = -1, \ y = 0 \ e \ z = 1.$$

A seguir, apresentamos um resultado que além de nos fornecer uma condição para termos um número finito de soluções também mostra que a situação que abordamos no exemplo anterior, ou seja, a relação íntima do sistema escalonado com uma base de Gröbner, não é uma mera coincidência e sim um caso particular de um método mais geral e que pode ser utilizado para sistemas polinomiais quaisquer.

Teorema 3.1.2. *Fixemos a ordem lexicográfica e considere o ideal*

$$I = \langle f_1, ..., f_m \rangle \subseteq \mathbb{C}[x_1, ..., x_n].$$

O sistema $f_1 = ... = f_m = 0$ *admite um número finito de soluções, ou seja,* $\mathcal{Z}(I)$ *é finito se, e somente se,* ${x_i}^{\gamma_i} = ml(g_i)$ *para* $g_i \in I, \gamma_i \in \mathbb{N} \setminus 0$ *e todo* $i = 1, ..., n$.

Demonstração: Suponha que um sistema $f_1 = ... = f_m = 0$ admite um número $k > 0$ de soluções $(z_{11}, ...z_{n1}), \ldots, (z_{1k}, ...z_{nk}) \in \mathbb{C}^n$. Temos que os possíveis valores para as i-ésimas coordenadas das soluções satisfazem $h_i = \prod(x_i - z_{ij}) = {x_i}^{\alpha_i} + ... + a_{i1}x_i + a_{i0}$ com $0 < \alpha_i \leq k$. Deste modo, $h_i \in \mathcal{I}(\mathcal{Z}(I))$ e segue que $h_i \in \sqrt{I}$, ou seja, existe $\beta_i \in \mathbb{N} \setminus 0$ tal que $h_i^{\beta_i} \in I$ com $ml(h_i^{\beta_i}) = x_i^{\alpha_i \beta_i}$ para todo $i = 1, ..., n$.

Para a recíproca, lembremos que com respeito à ordem lexicográfica temos

$x_n \prec_L x_{n-1} \prec_L ... \prec_L x_2 \prec_L x_1$. Por hipótese, existe $\gamma_i \in \mathbb{N} \setminus \{0\}$ de modo que $x_i^{\gamma_i} = ml(g_i)$ com $g_i \in I$ para todo $i = 1, ..., n$. Assim, a ordem lexicográfica nos garante que $g_n \in \mathbb{C}[x_n]$ e o número de soluções de $g_n = 0$ é limitado por $gr_{x_n}(g_n) = \gamma_n$.

Como $ml(g_{n-1}) = {x_{n-1}}^{\gamma_{n-1}}$ novamente, de acordo com a ordem lexicográfica, segue que $g_{n-1} \in \mathbb{C}[x_{n-1}, x_n]$. Para cada solução $z_n \in \mathbb{C}$ de $g_n = 0$, temos um número finito de soluções para $g_{n-1}(x_{n-1}, z_n)$, a saber, limitado por $gr_{x_{n-1}}(g_{n-1}) = \gamma_{n-1}$.Deste modo, o número de soluções de $g_n = g_{n-1} = 0$ é finito e limitado por $\gamma_{n-1} \cdot \gamma_n$. Procedendo deste modo, temos que o número de soluções do sistema $g_1 = ... = g_n = 0$ é finito e limitado por $\gamma_1 \cdot ... \cdot \gamma_n$. Agora, como $g_i \in I$, ou seja, $g_i = \sum q_j f_j$ com $q_j \in \mathbb{C}[x_1, ...x_n]$, temos que todas as soluções de $f_1 = ... = f_m = 0$ são também soluções de $g_1 = ... = g_n = 0$.

Como o último sistema admite um número finito de soluções, o mesmo acontece com o sistema original. □

Exemplo 3.1.3. *Considere o sistema*

$$\begin{cases} x^2 + y^2 + z^2 = 4 \\ x^2 + 2y^2 = 5 \\ xz + y^2 = 1. \end{cases} \tag{3.2}$$

Vamos encontrar as soluções, caso existam e sejam em um número finito. Para isto, ao computarmos uma Base de Gröbner para o ideal I dado por

$$\langle x^2 + y^2 + z^2 - 4, x^2 + 2y^2 - 5, xz + y^2 - 1 \rangle$$

com respeito à ordem lexicográfica, obtemos

$$G = \{x^2 + 2z^2 - 3, xz + z^2, y^2 - z^2 - 1, z^3 - z\}.$$

Como $1 \notin I$, temos que o sistema admite solução e, uma vez que x^2, y^2 e z^3 são monômios líderes de elementos de I, o último teorema garante que o sistema dado tem um número de soluções menor ou igual a $gr(x^2) \cdot gr(y^2) \cdot gr(z^3) = 12$.

Vamos obter todas as soluções $(k_1, k_2, k_3) \in \mathbb{C}^3$.

Temos que a equação $z^3 - z = 0$ admite como solução 0 e ± 1.

Se $k_3 = 0$, então as equações $y^2 - z^2 - 1 = xz + z^2 = x^2 + 2z^2 - 3 = 0$ nos dão que $k_2 = \pm 1$ e $k_1 = \pm\sqrt{3}$.

Considerando $k_3 = 1$, a equação $y^2 - z^2 - 1 = 0$ indica que $k_2 = \pm\sqrt{2}$. Substituindo z por 1 as equações $xz + z^2 = x^2 + 2z^2 - 3 = 0$ se tornam $x + 1 = x^2 - 1 = 0$, ou seja, $k_1 = -1$.

Tomando $k_3 = -1$ temos $k_2 = \pm\sqrt{2}$ e para $k_3 = -1$ obtemos $-x + 1 = x^2 - 1 = 0$ e assim, $k_1 = 1$.

Portanto, as soluções do sistema são:

$$(\pm\sqrt{3}, \pm 1, 0), (1, \pm\sqrt{2}, -1), (-1, \pm\sqrt{2}, 1).$$

Note que tínhamos estimado o número de soluções em $gr(x^2) \cdot gr(y^2) \cdot gr(z^3) = 12$, no entanto, verificamos que tal número é 8.

3.2 Coloração de Mapas

O Problema das Quatro Cores trata da determinação do número mínimo de cores necessárias para colorir um mapa, de países reais ou imaginários, de forma a que países com fronteira comum tenham cores diferentes. Em 1852, Francis Guthrie conjecturou que 4 era esse número mínimo. Somente após mais de cem anos, em 1976, se conseguiu provar que realmente a conjectura estava certa e o resultado ficou conhecido como Teorema das Quatro Cores.

Assim, como todo mapa pode ser colorido com quatro cores e é imediato decidir se um mapa pode ser colorido com duas cores, basta não termos regiões com tríplice fronteira, ou seja, uma região que tem fronteira com outras duas. Uma questão interessante é: como decidir se um mapa pode ser colorido utilizando apenas três cores? E, sendo possível, como proceder a coloração? A essa pergunta chamaremos de Problema das Três Cores e, para respondê-la utilizaremos como ferramenta matemática as Bases de Gröbner.

Primeiramente é necessário expressar por meio de equações polinomiais todas as situações geométricas na questão da coloração de um mapa por três cores.

Cada uma das cores será representada por uma raíz do polinômio $f = x^3 - 1$, que se chama raiz cúbica da unidade, e são denotadas por $1, \omega$ e ω^2. Na verdade, elas são os elementos do conjunto

$$\mathcal{Z}(\langle x^3 - 1 \rangle) = \left\{ \{\omega_k = cos\left(\frac{2k\pi}{3}\right) + i \cdot sen\left(\frac{2k\pi}{3}\right); k = 0, 1, 2\} \right\}$$

Assim, pode-se verificar que as únicas soluções da equação $y_1 + y_2 + y_3 = 0$ tais que $y_i \in U_3 = \{1, \omega, \omega^2\}$ são aquelas para os quais y_1, y_2 e y_3 assumem valores todos distintos.

Cada uma das regiões do mapa será representada por uma variável, isto é, no caso de n regiões considera-se o anel de polinômios $\mathbb{C}[x_1, ..., x_n]$. Assim, como cada uma das regiões pode ser colorida por uma das cores, a resposta para o problema está entre as soluções do sistema

$$x_i{}^3 - 1 = 0 \text{ para todo } i = 1, ..., n.$$

Porém, deve-se ainda inserir a restrição de que duas regiões vizinhas x_i e x_j não podem ser coloridas da mesma cor. Isto pode ser obtido observando que ${x_i}^3 = {x_j}^3$, ou seja,

$$ {x_i}^3 = {x_j}^3 \Leftrightarrow {x_i}^3 - {x_j}^3 = 0 \Leftrightarrow (x_i - x_j)({x_i}^2 + x_i x_j + {x_j}^2) = 0. $$

A última igualdade acarreta $x_i - x_j = 0$ ou ${x_i}^2 + x_i x_j + {x_j}^2 = 0$. Já que $x_i - x_j \neq 0$, pois caso contrário x_i receberia a mesma cor que x_j, deve-se ter ${x_i}^2 + x_i x_j + {x_j}^2 = 0$.

Assim, o problema da coloração do mapa utilizando apenas três cores se resume a estudar o sistema (3.3) abaixo:

$$ \begin{cases} {x_i}^3 - 1 = 0 \\ {x_j}^2 + x_i x_j + {x_k}^2 = 0 \end{cases} \tag{3.3} $$

sendo $i = 1, ..., n$ e x_j e x_k percorrem todas as regiões que possuem fronteira em comum.

Este sistema admite solução se $1 \notin I$, onde I é o ideal gerado pelos polinômios do sistema (3.3). Deve-se observar que, se o problema tem solução, então qualquer permutação das três cores também é solução.

Verificaremos se o mapa da região nordeste do Brasil pode ser colorido com três cores e, em caso afirmativo, como fazer esta coloração. O mapa em questão está apresentado na Figura (3.1) abaixo.

Figura 3.1: Região Nordeste do Brasil

Note que a região nordeste brasileira é composta por nove estados e assim a cada um deles será atribuída uma variável do anel de polinômios $\mathbb{C}[x_1, ..., x_9]$, a saber:

x_1 = Maranhão	x_4 = Rio Grande do Norte	x_7 = Alagoas
x_2 = Piauí	x_5 = Paraíba	x_8 = Sergipe
x_3 = Ceará	x_6 = Pernambuco	x_9 = Bahia

Assim, temos a Figura (3.2):

Figura 3.2: Região Nordeste nas Variáveis x_i; $i = 1, ..., 9$.

Levando em conta as regiões vizinhas do mapa, obtém-se o sistema (3.4) a seguir.

$$\begin{cases} x_i^3 - 1 = 0 \\ x_j^2 + x_j x_k + x_k^2 = 0 \end{cases} \tag{3.4}$$

sendo $i = 1, ..., 9$ e $(j, k) \in \{(1, 2), (2, 3), (2, 6), (2, 9), (3, 4), (3, 5), (3, 6), (4, 5), (5, 6), 6, 7),$ $(6, 9), (7, 8), (7, 9), (8, 9)\}$. O par (j, k) indica que o estado x_j é vizinho do estado x_k e que, portanto, não podem receber a mesma cor.

Usando o software Maple, devido ao grande número de operações, calcula-se uma base de Gröbner G para o ideal gerado pelos polinômios do sistema (3.4) com respeito a ordem lexicográfica e obtém-se

$$\begin{aligned} G &= \{\ x_9^3 - 1\ ,\ x_8^2 + x_8x_9 + x_9^2\ ,\ x_7 + x_8 + x_9\ ,\ x_6 - x_8,\ x_5 + x_8 + x_9, \\ &\quad x_4 - x_8\ ,\ x_3 - x_9\ ,\ x_2 + x_8 + x_9\ ,\ x_1^2 - x_1x_8 - x_1x_9 + x_8x_9\ \}. \end{aligned} \tag{3.5}$$

Portanto, o sistema(3.4) é equivalente ao sistema (3.6):

$$\begin{cases} x_9^3 - 1 = 0 \\ x_8^2 + x_8x_9 + x_9^2 = 0 \\ x_7 + x_8 + x_9 = 0 \\ x_6 - x_8 = 0 \\ x_5 + x_8 + x_9 = 0 \\ x_4 - x_8 = 0 \\ x_3 - x_9 = 0 \\ x_2 + x_8 + x_9 = 0 \\ x_1^2 - x_1x_8 - x_1x_9 + x_8x_9 = 0 \end{cases} \tag{3.6}$$

Agora cada uma das equações do sistema (3.6) é interpretada geometricamente, lembrando que as variáveis podem assumir como valor as raízes cúbicas da unidade, convencionamos que: 1 = azul, ω = amarelo e ω^2 = vermelho.

- A primeira equação indica que podemos escolher qualquer cor para x_9, sem perda de generalidade, atribuímos a cor 1.

- A segunda equação é interpretada como o fato de que a cor de x_8 não pode ser a mesma que x_9 assume. Assim, atribuímos à x_8 a cor ω.

- A terceira equação dada por $x_7 + x_8 + x_9 = 0$, deve admitir soluções entre as raízes cúbicas complexas da unidade, mas como vimos, x_7, x_8 e x_9 devem assumir valores distintos, ou seja, x_7 deve ser colorida com uma cor distinta das cores utilizadas para x_8 e x_9, isto é, ω^2.

- A quarta equação corresponde a informação de que x_6 assume o mesmo valor de x_8, neste caso, a cor ω.

- A quinta equação adverte que x_5 não pode assumir as mesmas cores que x_8 e x_9, ou seja, x_5 deverá assumir a cor ω^2.
- A sexta equação indica que x_4 assume o mesmo valor de x_8, ou seja, ω.
- A sétima equação mostra que x_3 assume o mesmo valor de x_9. Logo x_3 assume a cor 1.
- A oitava equação mostra que x_2 não pode assumir as mesmas cores que x_8 e x_9, isto é, x_2 deverá ser colorida da cor ω^2.
- A nona equação dada por $x_1^2 - x_1x_8 - x_1x_9 + x_8x_9 = 0$, pode ser reescrita na forma $(x_1 - x_8).(x_1 - x_9) = 0$. Deste modo, temos as possibilidades: $x_1 - x_8 = 0$ ou $x_1 - x_9 = 0$. Portanto, atribuímos à x_1 a mesma cor de x_8 ou a cor usada em x_9.

Portanto, mediante a interpretação das equações obtidas pelos elementos da Base de Gröbner reduzida G, temos duas situações, como é mostrado nas figuras (3.3) e (3.4) abaixo:

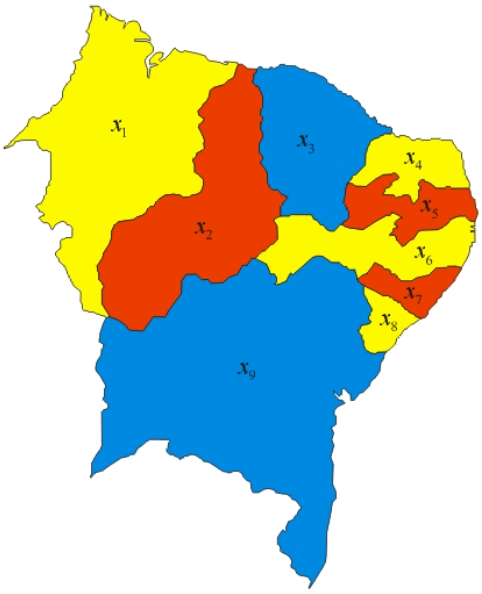

Figura 3.3: A cor de x_1 é igual a de x_8.

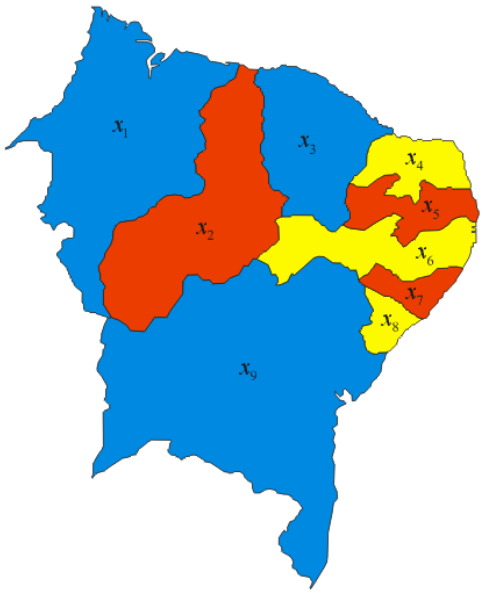

Figura 3.4: A cor de x_1 igual é a de x_9.

Conclusão

Neste trabalho apresentamos uma generalização do processo de escalonamento, que é usualmente utilizado na resolução de sistemas lineares, que permite estudar sistemas de equações polinomiais em geral.

No decorrer de nosso estudo, vimos como decidir se um polinômio $f \in \mathbb{C}[x_1, ..., x_n]$ pertence ou não a um ideal $I = \langle f_1, ..., f_s \rangle$. A resposta a esta questão permite decidir se um sistema de equações polinomiais $f_1(x_1, ..., x_n) = ... = f_s(x_1, ...x_n) = 0$ admite ou não solução. Vimos também, no caso do número de solução serem finitas, um método que permite obtê-las.

Como uma aplicação, apresentamos um modo de modelar o **Problema das Três Cores**, ou seja, como decidir se um mapa pode ser colorido utilizando apenas três cores de forma que regiões vizinhas não recebam a mesma cor, de modo algébrico, de tal forma que o problema se torne equivalente a estudar um sistema de equações polinomiais.

Bibliografia

[1] HERNANDES, Marcelo Escudeiro; **Um Primeiro Contanto com Bases de Grobner**, 28º Colóquio Brasileiro de Matemática, Rio de Janeiro (2011).

[2] COX, D; LITTLE, J. & O'SHEA, D; **Ideals, Varieties and Algorithms**, 2º edition, Springer-Verlag, New York, (1996).