Universidade Estadual de Campinas
Instituto de Matemática, Estatística e
Computação Científica - IMECC

Bases de Gröbner Aplicadas à k-Coloração de Grafos

Frederico Fontes Staib

fredericostaib@gmail.com

Dissertação de Mestrado

Orientadora: **Profª. Drª. Patrícia Helena Araújo da Silva Nogueira**

Dezembro de 2010

Campinas - SP

Bases de Gröbner Aplicadas à k-Coloração de Grafos

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Frederico Fontes Staib** e aprovada pela comissão julgadora.

Campinas, 03 de Dezembro de 2010.

Profa. Dra. Patrícia Helena Araújo da Silva Nogueira
Orientadora

Banca Examinadora:

Profª. Drª. Patrícia Helena Araújo da Silva Nogueira (UERJ)

Prof. Dr. João Eloir Strapasson (FCA- UNICAMP)

Prof. Dr. Juscelino Bezerra dos Santos (ENCE)

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, **UNICAMP**, como requisito parcial para obtenção de Título de **Mestre em Matemática**.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Fabiana Bezerra Müller – CRB8 / 6162

Staib, Frederico Fontes
St15b Bases de Gröbner aplicadas à k-coloração de grafos/Frederico Fontes Staib-- Campinas, [S.P. : s.n.], 2010.

Orientador : Patrícia Helena Araújo da Silva Nogueira
Dissertação (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1.Bases de Gröbner. 2.Teoria dos grafos. I. Nogueira, Patrícia Helena Araújo da Silva. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Application of Gröbner bases in graph k-coloring

Palavras-chave em inglês (Keywords): 1. Grobner bases. 2. Graph theory.

Área de concentração: Algebra

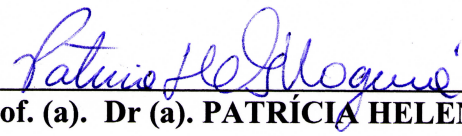
Titulação: Mestre em Matemática

Banca examinadora: Profª. Drª. Patrícia Helena Araújo da Silva Nogueira (UERJ)
Prof. Dr. João Eloir Strapasson (FCA - UNICAMP)
Prof. Dr. Juscelino Bezerra dos Santos (ENCE)

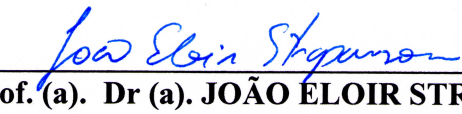
Data da defesa: 03/12/2010

Programa de Pós-Graduação: Mestrado Profissional em Matemática

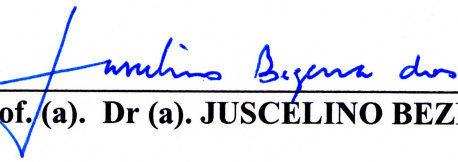
Dissertação de Mestrado Profissional defendida em 03 de dezembro de 2010 e aprovada pela Banca Examinadora composta pelos Profs. Drs.



Prof. (a). Dr (a). PATRÍCIA HELENA ARAÚJO DA SILVA NOGUEIRA



Prof. (a). Dr (a). JOÃO ELOIR STRAPASSON



Prof. (a). Dr (a). JUSCELINO BEZERRA DOS SANTOS

Dedico este trabalho ao GRANDE AMOR da minha vida, ***Samira****, e à minha filha* ***Sofia****.*

Agradecimentos

Agradeço aos meus pais Armando e Mirian por todo amor, carinho, compreensão, incentivo e educação que me deram. Aos meus irmãos Luísa e Leonardo que dividem comigo desde sempre as alegrias e percalços da vida. Aos meus avós por toda sabedoria acumulada e repassada de maneira simples e inesquecível.

Agradeço à minha esposa Samira, por ser minha razão de querer aproveitar a vida ao máximo, por estar sempre ao meu lado não importa o que aconteça e por ter sempre sido a minha melhor certeza absoluta. À minha filha Sofia, por tornar a minha vida mais feliz a cada sorriso, mesmo ainda não tendo a menor idéia disso.

Agradeço à minha orientadora Patrícia por todo o apoio constante, por toda atenção e paciência despendidas, por todas as idéias e críticas sempre muito importantes e, principalmente, por me fazer gostar ainda mais da Matemática ao transmití-la com tanta facilidade e competência.

Agradeço aos membros da banca examinadora - Prof. Dr. Juscelino Bezerra dos Santos, Prof. Dr. João Eloir Strapasson e Profa. Dra. Patrícia Helena Araújo da Silva Nogueira - pela grande contribuição dada nas correções e sugestões a esse trabalho.

Agradeço aos responsáveis pela realização deste Mestrado Profissional pelo convênio entre a AMAN e a UNICAMP, em especial à Profa. Dra. Sueli Irene Rodrigues Costa e Profa. Dra. Vera Lúcia da Rocha Lopes da UNICAMP e ao Coronel Tércio da AMAN, que não mediram esforços para que tudo desse certo.

Encerro agradecendo também a todos os professores, monitores e colegas com quem tive o prazer de passar ótimos momentos de muito estudo, discussões e risadas, que todos saibam do quanto me orgulho de conhecê-los.

Resumo

Neste trabalho, estudamos a teoria das bases de Gröbner e sua aplicação ao problema da k-coloração de grafos, estabelecendo assim uma interessante conexão entre a álgebra abstrata e a matemática discreta. Fazemos também uma abordagem de caráter lúdico, traduzindo o passatempo chamado Sudoku em um problema de 9-coloração e utilizando a teoria apresentada para resolvê-lo através das bases de Gröbner.

Abstract

In the present work, we study the Gröbner basis theory and its application on the graph k-coloring problem, establishing an interesting relation between abstract algebra and discrete mathematics. We make a ludic approach, translating the puzzle called Sudoku to a 9-coloring problem and using the given theory to solve it by the Gröbner basis.

Sumário

CAPÍTULO 1

INTRODUÇÃO

A teoria das bases de Gröbner é uma ferramenta fundamental na álgebra polinomial, respondendo a muitas questões importantes da álgebra comutativa, como o problema da pertinência a um ideal. As bases de Gröbner têm seu início em 1965 a partir da tese de doutorado de Bruno Burchberger, orientado por Wolfgang Gröbner, que foi homenageado com seu nome dado a estas bases. Como muitas "novas"idéias na Matemática, por muito anos não recebeu a atenção merecida, sem que percebessem toda sua importância. Com o avanço da computação, começou a ser valorizada por seu caráter altamente computacional, exercendo um importante papel na álgebra computacional. Atualmente, dificilmente encontramos um sistema de computação algébrica que não possua um pacote para utilizar bases de Gröbner.

A teoria dos Grafos é uma importante parte da matemática discreta bastante aplicada em diversos problemas na matemática, na informática, na engenharia e até mesmo na indústria. A própria teoria de Grafos surgiu e desenvolveu-se a partir de problemas aparentemente triviais, como o problema das pontes de Königsberg que recebeu bastante atenção de Leonhard Euler, e o problema da 4-coloração de um mapa que passou anos sem que conseguissem prová-lo.

Nosso principal objetivo neste trabalho, é aplicar as bases de Gröbner ao problema da k-coloração de grafos. Estabelcendo assim uma interessante conexão entra a álgebra abstrata e a matemática discreta. Muitos resultados interessantes são encontrados na aplicação das bases de Gröbner a problemas de coloração de grafos. Um grafo de n vértices é representado por um polinômio em n variáveis com grau igual ao número de arestas do grafo. No anel

de polinômios em n variáveis, o problema da k-coloração será equivalente a determinar se o polinômio que representa o grafo pertence a um dado ideal. Encontrando uma base de Gröbner para este ideal, o problema tornar-se-á simplificado.

Optamos por esse tema, por acreditar que esse tipo de relação entre áreas da matemática aparentemente desconexas é de grande valia para o aprendizado da matemática, já que pode ser visto como uma motivação para encontrar outras relações, incentivando assim o estudo da matemática.

Ainda a fim de contribuir para essa motivação, com intuito de fazer uma abordagem de caráter lúdico, aproveitamos a aplicação da teoria dos grafos em vários jogos e passatempos, e escolhemos o passatempo chamado Sudoku o qual podemos ver como um problema de k-coloração de grafos. Neste passatempo completa-se uma tabela com números de 1 a 9 de maneira lógica. Vamos traduzir este passatempo em um problema de 9-coloração onde iremos nos deparar com um sistema de equações polinomiais, o qual iremos resolver utilizando as bases de Gröbner.

No capítulo 2, Conceitos Básicos revemos os conceitos e resultados que vamos precisar em todo o trabalho, em especial as definições de anéis de polinômios em várias variáveis, o conceito de ideal associado a um sistema de equações, o das variedades algébricas afins e das ordens monomiais.

No capítulo3, Bases de Gröbner, fazemos mais algumas definições importantes como a de ideal de termos líderes, e definimos o que vem a ser uma Base de Gröbner para um ideal, dando alguns exemplos. Provamos a existência destas bases e obtemos como consequência dessa existência o Teorema de Hilbert onde todo ideal em um anel de polinômio em várias variáveis possui um conjunto finito de geradores. Definimos ainda base de Gröbner reduzida, muito importante por fornecer a unicidade tão desejada e necessária, razão especial da teoria das bases de Gröbner. E por último a relação das variedades afins e estas bases reduzidas.

No último capítulo, Aplicação em k-Coloração de Grafos, iniciamos com os conceitos básicos sobre grafos, definindo logo após o conceito de coloração de grafos, mas especificamente da coloração de vértices de um grafo, finalizando com o probema da k-coloração, onde iremos transformá-lo em um sistema de equações, por fim demonstraremos que um grafo será k-colorável se e somente se a variedade algébrica afim do ideal associado a este sistema for não vazia.

Concluímos o trabalho com o exemplo do passatempo sudoku resolvido aplicando-se toda a teoria vista. Utilizando, como ferramenta o sistema de computação algébrica chamado SINGULAR, gratuito e disponível na Internet. Fazemos ainda um apêndice com uma introdução básica ao SINGULAR, para servir de apoio ao leitor que desejar utilizar a mesma ferramenta, já que não encontramos manuais e tutoriais disponíveis em português.

CAPÍTULO 2

CONCEITOS BÁSICOS

Antes de iniciarmos nosso estudo das bases de Gröbner iremos rever alguns conceitos básicos, com os quais alunos de graduação em matemática estão bastante familiarizados.

Alguns resultados indispensáveis, também serão expostos neste capítulo a fim de nos auxiliar na prova dos teoremas relacionados à existência das bases de Gröbner.

2.1 Anéis de Polinômios

2.1.1 Polinômios em uma variável

Definição 2.1. *Seja K um corpo* [1]. *Chamamos de* ***polinômio em uma variável*** *x sobre K a soma formal:*

$$p = \sum_{i \geq 0} a_i x^i$$

onde $a_i \in K$ e $a_i = 0$ para todo $i \geq m \in \mathbb{Z}_{\geq 0}$.

Observamos que o polinômio p pode ser visto como uma sequência de elementos de A

$$\{a_i\}_{i \in \mathbb{Z}_{\geq 0}} = (a_0, a_1, \cdots, a_m, \cdots)$$

[1] podemos de forma análoga definir com um anel comutativo com unidade.

onde $a_i \neq 0$ somente para um número finito de $i \in \mathbb{Z}_{\geq 0}$. De fato, podemos associar cada sequência $(a_0, a_1, \cdots, a_m, \cdots)$ ao polinômio da forma $p = a_0 + a_1x + \ldots + a_mx^m$.

Dizemos que dois polinômios $p = a_0 + a_1x + \ldots + a_mx^m$ e $q = b_0 + b_1x + \ldots + b_nx^n$ são iguais se e somente se $m = n$ e $a_i = b_i$ para todo i com $0 \leq i \leq m$.

Podemos definir a adição e a multiplicação de dois polinômios como se segue:

$$p + q = \sum_{i=j}(a_i + b_j)x^i$$

e

$$p \cdot q = \sum_{k=0}^{m+n}\left(\sum_{i+j=k} a_i \cdot b_j\right)x^k$$

onde $m, n, i, j, k \in \mathbb{Z}_{\geq 0}$.

O polinômio $p = 0 + 0x + \ldots + 0x^n$ é chamado de ***polinômio identicamente nulo*** sobre K e é denotado simplesmente por 0. O conjunto de todos os polinômios na variável x sobre K é denotado por $K[x]$

Definição 2.2. *Se $p = \sum_{i\geq 0} a_ix^i$ é tal que $a_n \neq 0$ e $a_i = 0 \quad \forall i > n$, dizemos que n é o **grau do polinômio** p e denotamos por $\delta p = n$*

Definição 2.3. *Seja $p = a_0 + a_1x + \ldots + a_nx^n \in A$, onde $\delta p = n$. Chamamos*

$$TL(p) = a_nx^n$$

*de **termo líder** de p, e*

$$CL(p) = a_n$$

*de **coeficiente líder** de p. Quando $a_n = 1$, dizemos que p é **mônico**.*

Pode-se mostrar que se A é um anel, $A[x]$ é um anel; se D é um domínio de integridade, $D[x]$ é um domínio de integridade (ver em [1], pág. 200); porém, se K é um corpo, $K[x]$ não é um corpo, basta observarmos que $x \in K[x]$ não possui inverso multiplicativo, isto é, não existe $f \in K[x]$ tal que $fx = 1$.

Exemplo 2.1. *Seja o corpo $\mathbb{Z}_2 = \{0, 1\}$ das classes residuais dos inteiros módulo 2. Tomemos dois polinômios $p, q \in \mathbb{Z}_2[x]$ tais que:*

$$p = x^2 + x + 1 \qquad e \qquad q = x^3 + x^2 + 1$$

Os termos líderes de p e q são, respectivamente, x^2 e x^3. Os graus dos polinômios são $\delta p = 2$ e $\delta q = 3$.

Temos ainda,

$$\begin{aligned} p + q &= (x^2 + x + 1) + (x^3 + x^2 + 1) \\ &= x^3 + 2x^2 + x + 2 \\ &= x^3 + x \in \mathbb{Z}_2[x] \end{aligned}$$

$$\begin{aligned} p.q &= (x^2 + x + 1).(x^3 + x^2 + 1) \\ &= x^5 + x^4 + x^2 + x^4 + x^3 + x + x^3 + x^2 + 1 \\ &= x^5 + x + 1 \in \mathbb{Z}_2[x] \end{aligned}$$

Mais a frente, no exemplo 2.16, iremos relembrar a divisão de polinômios em $K[x]$.

Definição 2.4. *Um **Domínio Euclidiano** (D, φ) é um domínio de integridade D com uma função*

$$\varphi : D \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

que satisfaz as seguintes propriedades:

(i) $\forall a, b \in D, b \neq 0$*, existem* $t, r \in D$ *tais que*

$$a = bt + r \quad com \quad \begin{cases} \varphi(r) < \varphi(b) \\ ou \\ r = 0 \end{cases}$$

(ii) $\varphi(a) \leq \varphi(ab) \quad , \quad \forall a, b \in D \setminus \{0\}$

Teorema 2.1. *$(K[x], \delta)$ é um domínio euclidiano, isto é, para todo $a, b \in K[x]$ com $b \neq 0$ temos*

$$a = bq + r \text{ , onde } r = 0 \text{ ou } \delta r < \delta b$$

e para todo $a, b \in K[x]$

$$\delta a < \delta ab.$$

Demonstração. Ver [2], pág. 17.

□

Vemos claramente que o anel K é um subanel de $K[x]$, já que um elemento a de K pode ser visto como um polinômio de grau zero denotado por $p = a + 0x + \ldots + 0x^n = a$ que chamamos de ***polinômio constante*** a**.**

Lema 2.1 (Bezout)**.** *Sejam $f_1, \cdots, f_s \in K[x]$. Se $d = MDC(f_1, \cdots, f_s)$ então existem $a_1, \cdots, a_s \in K[x]$ tais que,*

$$d = a_1 f_1 + \cdots + a_s f_s$$

Demonstração. Ver em [3] pág. 128. □

2.1.2 Polinômios em Várias Variáveis

O anel de polinômios em várias variáveis possui uma estrutura bastante análoga aos polinômios em uma variável, porém encontraremos algumas particularidades que exigirão uma atenção especial, principalmente no que diz respeito à ordenação dos monômios e ao algoritmo da divisão.

Definição 2.5. *Um **monômio** em $x_1, x_2, \cdots, x_n$ é um produto da forma:*

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n}$$

onde os expoentes $\alpha_1, \alpha_2, \cdots, \alpha_n$ são números inteiros não negativos.

A fim de tornar mais simples a notação para monômios usamos o multi-índice

$$\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$$

uma n-upla de números inteiros não negativos, sendo, então, um monômio denotado por

$$X^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ldots \cdot x_n^{\alpha_n}.$$

Quando $\alpha = (0, 0, \cdots, 0)$ denotaremos simplesmente $X^\alpha = 1$. Chamaremos

$$|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$$

de **grau total** do monômio X^α.

Definição 2.6. *O **polinômio** p **em várias variáveis** $x_1, \cdots, x_n$ com coeficientes em K(corpo) será uma combinação linear finita (com coeficientes em K) de monômios. Portanto, escrevemos:*

$$p = \sum_\alpha a_\alpha X^\alpha \quad , \quad a_\alpha \in K$$

onde o somatório é sobre um número finito de n-uplas $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$.

Denotamos o conjunto de todos os polinômios nas variáveis $x_1, \cdots, x_n$ sobre K como $K[x_1, \cdots, x_n]$. Vale observar que podemos ver $K[x_1, \cdots, x_n]$ como o anel de polinômios na variável x_n com coeficientes no anel $K[x_1, \cdots, x_{n-1}]$, denotamos assim $K[x_1, \cdots, x_{n-1}][x_n]$.

Definição 2.7. *Seja $p = \sum_\alpha a_\alpha X^\alpha$ um polinômio em $K[x_1, \cdots, x_n]$. De forma análoga aos polinômios em uma variável,*

*(i) Chamamos a_α de **coeficiente do monômio** X^α;*

*(ii) Se $a_\alpha \neq 0$, chamamos $a_\alpha X^\alpha$ de **termo** de p.*

Definição 2.8. *O **grau total de um polinômio** $p = \sum_\alpha a_\alpha X^\alpha \in K[x_1, \cdots, x_n]$ é igual ao máximo $|\alpha|$ cujo coeficiente $a_\alpha \neq 0$.*

Definição 2.9. *Sejam $p, q \in K[X]$, polinômios em n variáveis, tais que $p = \sum_\alpha a_\alpha X^\alpha$ e $q = \sum_\beta b_\beta X^\beta$, com $|\alpha| \geq |\beta|$. Definimos a* soma $p + q$ *como:*

$$\sum_\alpha a_\alpha X^\alpha + \sum_\beta b_\beta X^\beta = \sum_\alpha (a_\alpha + b_\alpha) X^\alpha$$

E definimos o produto $p.q$ *como:*

$$\sum_{\alpha} a_\alpha X^\alpha . \sum_{\beta} b_\beta X^\beta = \sum_{\kappa} \left(\sum_{\alpha+\beta=\kappa} a_\alpha b_\beta \right) X^\kappa$$

Exemplo 2.2. *Seja o corpo* $\mathbb{Z}_3 = \{0, 1, 2\}$. *Tomemos dois polinômios* $p, q \in \mathbb{Z}_3[x, y]$ *tais que:*

$$p = x^3y^2 + xy^2 + 2 \qquad e \qquad q = x^2y^4 + x^2y + 1$$

Os graus dos polinômios são $\delta p = 5$ *e* $\delta q = 6$.

Temos ainda,

$$\begin{aligned} p + q &= (x^3y^2 + xy^2 + 2) + (x^2y^4 + x^2y + 1) \\ &= x^3y^2 + xy^2 + x^2y^4 + x^2y + 3 \\ &= x^3y^2 + xy^2 + x^2y^4 + x^2y \in \mathbb{Z}_3[x] \end{aligned}$$

$$\begin{aligned} p.q &= (x^3y^2 + xy^2 + 2).(x^2y^4 + x^2y + 1) \\ &= x^5y^6 + x^5y^3 + x^3y^2 + x^3y^6 + x^3y^3 + xy^2 + 2x^2y^4 + 2x^2y + 2 \in \mathbb{Z}_3[x] \end{aligned}$$

Teorema 2.2. $(K[X], +, .)$ *é um domínio de integridade.*

Demonstração. Sabemos que, para o caso de uma variável, $K[x]$ é um domínio de integridade. Considerando que podemos estender $K[x]$, adicionando-lhe variáveis até obtermos $K[X]$ com n variáveis, utilizamos indução sob o número de variáveis para, de forma imediata, estender a prova do caso em uma variável.

□

Veremos, mais a frente que $K[X]$ não é um Domínio Euclidiano.

2.2 Ideais

2.2.1 Ideal de um Anel

Definição 2.10. *Seja A um anel comutativo com unidade. Um subconjunto, não vazio, $I \subset A$ é um **ideal** se satisfaz:*

(i) Se $a, b \in I$, então $a + b \in I$

(ii) Se $a \in I$ e $c \in A$, então $ca \in I$

Exemplo 2.3. *O conjunto $F = \{fxy \mid f \in \mathbb{R}[x, y]\}$ é um ideal do anel de polinômios $\mathbb{R}[x, y]$. De fato:*

- *Não vazio, pois $1xy \in F$;*
- *Sejam f_1xy e $f_2xy \in F$, $f_1xy + f_2xy = (f_1 + f_2)xy \in F$;*
- *Sejam $f_1xy \in F$ e $g \in \mathbb{R}[x, y]$, $f_1xyg = (f_1g)xy \in F$.*

Definição 2.11. *Seja A um anel e $a \in A$. O conjunto*

$$\langle a \rangle = \{ba \mid b \in A\},$$

*de todos os múltiplos de a, é um ideal, chamado **ideal principal** . De fato,*

- *É não vazio, pois $1a \in \langle a \rangle$;*
- *Sejam $b_1a \in \langle a \rangle$ e $b_2a \in \langle a \rangle$. Então, $b_1a + b_2a = (b_1 + b_2)a \in \langle a \rangle$;*
- *Sejam $ba \in \langle a \rangle$ e $c \in A$, então $bac = (bc)a$.*

Definição 2.12. *Um domínio de integridade onde cada ideal é principal é chamado **domínio de ideais principais**.*

Proposição 2.1. *Seja (D, φ) um Domínio Euclidiano então D é um Domínio de Ideais Principais.*

Demonstração. Seja $I \subset D$ um ideal. Se $I = \{0\}$, então $I = \langle 0 \rangle$. Suponha que $I \neq \{0\}$. Como $\{\varphi(b) \mid b \in I\} \subseteq \mathbb{Z}_{\geq 0}$, este conjunto possui menor elemento, digamos $m \in \mathbb{Z}_{\geq 0}$. Seja $a \in I$, tal que $\varphi(a) = m$.

Dado $b \in I$, sendo D um domínio euclidiano, existem $q, r \in D$ satisfazendo

$$b = qa + r$$

onde $r = 0$ ou $\varphi(r) < \varphi(a)$.

Como $r = b - qa$ concluímos que $r \in I$. Sendo $m = \varphi(a)$ o menor elemento de $\{\varphi(b) \mid b \in I\}$ podemos concluir que $r = 0$ e portanto $b = qa$.

Sendo assim, $I = \langle a \rangle$. □

Corolário 2.1. *$K[x]$ é um Domínio de Ideais Principais.*

Demonstração. Como já visto no Teorema 2.1, $K[x]$ é um Domínio Euclidiano, daí segue diretamente da proposição anterior. □

Corolário 2.2. *Sejam (D, φ) um domínio euclidiano e $I \subset D$ um ideal de D. Então, $I = \langle a \rangle$ e $b = qa + r \in I$ se e somente se r é igual a zero.*

Demonstração. Segue diretamente da proposição anterior. □

Definição 2.13. *Sejam $a_1, \cdots, a_s \in A$. Definimos o conjunto*

$$\langle a_1, \cdots, a_s \rangle = \left\{ \sum_{i=1}^{s} h_i a_i \ \mid \ h_1, \cdots, h_s \in A \right\},$$

das combinações lineares dos elementos $a_i \in A$, com coeficientes no próprio anel A.

Lema 2.2. *Se $a_1, \cdots, a_s \in A$, então $\langle a_1, \cdots, a_s \rangle$ é um ideal de A. Chamamos $\langle a_1, \cdots, a_s \rangle$ de **ideal gerado por** $a_1, \cdots, a_s$.*

Demonstração. De fato, $0 \in \langle a_1, \cdots, a_s \rangle$ já que $0 = \sum_{i=1}^{s} 0a_i$. Agora, suponhamos que $a = \sum_{i=1}^{s} p_i a_i$ e $b = \sum_{i=1}^{s} q_i a_i$, e façamos $c \in A$. Assim,

$$\begin{aligned} a + b &= \sum_{i=1}^{s} (p_i + q_i)a_i \quad \in \langle a_1, \cdots, a_s \rangle \\ c.a &= \sum_{i=1}^{s} (cp_i)a_i \qquad \in \langle a_1, \cdots, a_s \rangle \end{aligned}$$

Portanto, $\langle a_1, \cdots, a_s \rangle$ é um ideal. □

Exemplo 2.4. *Seja $I = \langle x, y \rangle$ ideal de $K[x, y]$. Suponha por absurdo que $I = \langle g \rangle$ (ou seja, que I é principal). Sendo assim, $x = tg$ e $y = sg$, onde $t, s \in K[x, y]$.*

Olhando t, g e tg como elementos do anel $(K[x])[y]$, temos que, sendo $K[x]$ um domínio de integridade, vale que:

$$grau_y(tg) = grau_y(t) + grau_y(g)$$

Como $tg = x$, temos que $grau_y(g) = 0$ e portanto $g \in K[x]$.

Por outro lado, olhando s, g e sg como elementos do anel $(K[y])[x]$, um argumento análogo mostra que $grau_x(g) = 0$.

Portanto, g é uma constante, o que implica que $I = K[x, y]$, o que é um absurdo.

Definição 2.14. *Dizemos que um subconjunto $\{b_1, \cdots, b_n\}$ de polinômios de um ideal I é uma base de I se $I = \langle b_1, \cdots, b_n \rangle$.*

É importante ressaltar, que podemos ter mais de um conjunto de geradores distintos e com diferentes números de geradores para um mesmo ideal, como vemos no exemplo a seguir.

Exemplo 2.5. *Seja o ideal $I \subset \mathbb{Q}[x, y]$ onde*

$$I = \langle x + xy, y + xy, x^2, y^2 \rangle$$

podemos dizer que $I \subset \langle x, y\rangle$. De fato,

$$\begin{array}{rcrcrcl} x & + & xy & = & 1(x) & + & x(y) \\ y & + & xy & = & y(x) & + & 1(y) \\ x^2 & & & = & x(x) & + & 0(y) \\ & & y^2 & = & 0(x) & + & y(y) \end{array}$$

Ou seja, todo polinômio do primeiro conjunto gerador de I, é gerado pelos polinômios x e y, ou seja, $\langle x + xy, y + xy, x^2, y^2\rangle \subset \langle x, y\rangle$.

Agora, devemos mostrar que $\langle x, y\rangle \subset \langle x + xy, y + xy, x^2, y^2\rangle$. De fato,

$$\begin{array}{rcrcrcrcrcl} x & = & 1 & (x+xy) & + & (-x) & (y+xy) & + & y & (x^2)+0 & (y^2) \\ y & = & (-y) & (x+xy) & + & 1 & (y+xy) & + & 0 & (x^2)+x & (y^2) \end{array}$$

Portanto,

$$I = \langle x + xy, y + xy, x^2, y^2\rangle = \langle x, y\rangle.$$

Definição 2.15. *Um ideal $I \subset K[x_1, \cdots, x_n]$ é um **ideal monomial** se for gerado por um conjunto de monômios. Isto é, se existe um conjunto de expoentes $M \subseteq \mathbb{Z}^n_{\geq 0}$ tal que*

$$I = \langle X^\alpha | \alpha \in M\rangle.$$

Exemplo 2.6. *$\langle x^3y^2, x^4y^3, x^5y^4, y^2\rangle \subset \mathbb{R}[x, y]$, sendo os expoentes pertencentes ao conjunto $M = \{(3, 2), (4, 3), (5, 4), (0, 2)\}$*

Lema 2.3. *Sejam $M \subseteq \mathbb{Z}^n_{\geq 0}$ e $I = \langle X^\alpha | \alpha \in M\rangle$ um ideal monomial de $K[x_1, \cdots, x_n]$. Então um monômio X^β pertence a I se e somente se existe $\alpha \in M$ tal que X^β é divisível por X^α*

Demonstração. Se X^β for múltiplo de X^α para algum $\alpha \in M$, então, pela própria definição de ideal, X^β pertence a I.

Por outro lado, supondo $X^\beta \in I$ teremos $X^\beta = \sum_{i=1}^{s} h_{\alpha_i} X^{\alpha_i}$, com $h_{\alpha_i} \in K[x_1, \cdots, x_n]$ e $\alpha_i \in M$. Ao expandirmos cada h_{α_i}, como uma combinação linear de monômios, podemos reescrever a igualdade acima como combinação linear de monômios distintos:

$$X^\beta = \sum_{j=1}^{t} c_j X^{\beta_j}$$

com coefientes constantes $c_j \in K$ e cada monômio X^{β_j} sendo múltiplo de algum X^{α_i}, com $\alpha_i \in M$. Assim, pela definição de igualdade de polinômios, nesta última relação o lado direito contém um único termo, ou seja, $t = 1$, $c_1 = 1$ e $\beta_1 = \beta$.

□

Podemos notar na teoria dos ideais uma analogia com a álgebra linear. A definição de ideal é similar a definição de subespaço: ambas são fechadas quanto a adição e multiplicação, porém, em um subespaço, multiplicamos por escalares, já nos ideais, multiplicamos por polinômios. Mais ainda, observe que um ideal gerado por polinômios $f_1, \cdots, f_s$ é similar ao conjunto gerador de um subespaço. Em cada caso, pegamos combinações lineares, usando coeficientes no corpo no caso do conjunto gerador de um subespaço, e polinômios no caso dos ideais gerados. Agora, a maior diferença entre eles é na utilização do termo **base**, pois diferente da álgebra linear, como vimos no exemplo 2.5, as bases de um mesmo ideal podem ter um número diferente de polinômios.

2.2.2 Ideal associado a um Sistema de Equações Polinomiais

Podemos associar um ideal a um sistema de equações polinomiais, tomando as equações do sistema como polinômios geradores do ideal. Observamos que toda solução do sistema de equações será também a solução de qualquer elemento do ideal, isto é, seja o seguinte sistema:

$$\begin{cases} f_1 &= 0 \\ f_2 &= 0 \\ \vdots &= \vdots \\ f_n &= 0 \end{cases} \tag{2.1}$$

Agora tomemos o ideal gerado pelos polinômios das equações acima $I = \langle f_1, f_2, \cdots, f_n \rangle$ e seja $f \in I$, logo

$$f = h_1 f_1 + h_2 f_2 + \cdots + h_n f_n,$$

então, se X_1 é solução do sistema acima,

$$f(X_1) = h_1(X_1) f_1(X_1) + h_2(X_1) f_2(X_1) + \cdots + h_n(X_1) f_n(X_1) = 0,$$

ou seja, X_1 também é solução de qualquer elemento do ideal. Podemos então ver o conjunto solução do sistema (2.1), como sendo o conjunto de zeros comuns ao elementos do ideal $I = \langle f_1, f_2, \cdots, f_n \rangle$.

A relevância desse fato é que todo ideal em um anel de polinômios sobre um corpo, $K[X]$ é finitamente gerado, como veremos no próximo capítulo no Teorema de Hilbert; mais ainda, como vimos, não existe um único conjunto gerador de um ideal, poderemos encontrar um "melhor" conjunto gerador, o que tornará a busca pela solução do sistema de equações mais eficiente.

2.3 Variedade Algébrica Afim

Definição 2.16. *Sejam K um corpo e $f_1, \cdots, f_s$ polinômios em $K[x_1, \cdots, x_n]$. Definimos a variedade álgebrica afim definida por $f_1, \cdots, f_s$ como sendo o conjunto*

$$V(f_1, \cdots, f_s) = \{(a_1, \cdots, a_n) \in K^n \mid f_i(a_1, \cdots, a_n) = 0 \ \textit{para todo} \ 1 \leq i \leq s\}$$

De uma forma mais geral, a variedade afim $V(f_1, \cdots, f_s) \subseteq K^n$ é definida como o conjunto de todas as soluções do sistema

$$f_1(x_1, \cdots, x_n) = f_2(x_1, \cdots, x_n) = \ldots = f_s(x_1, \cdots, x_n) = 0$$

Exemplo 2.7. *Determinar* $V(x^2-y-1, x+y+1) \subseteq \mathbb{R}^2$*, é o mesmo de solucionar o sistema*

$$\begin{cases} x^2 - y - 1 = 0 \\ x + y - 1 = 0 \end{cases}$$

A solução do sistema acima é a intersecção de uma parábola e uma reta no plano, como vemos na figura abaixo.

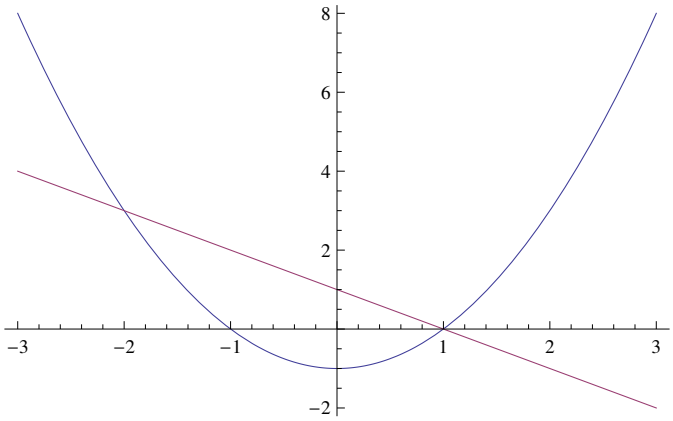


Figura 2.1: $V(x^2 - y - 1, x + y + 1) = \{(-2, 3), (1, 0)\}$

A variedade afim de um polinômio vai depender sempre do anel de polinômios em que estamos trabalhando, como vemos no exemplo a seguir.

Exemplo 2.8. *Seja o polinômio* $x^2 + 1 \in \mathbb{R}[x, y]$*, então*

$$V(x^2 + 1) = \emptyset;$$

Agora, se tomarmos o mesmo polinômio $x^2 + 1 \in \mathbb{C}[x, y]$*, teremos, como sua variedade afim, duas retas:*

$$V(x^2 + 1) = \{(-i, y) \mid y \in \mathbb{C}\} \cup \{(i, y) \mid y \in \mathbb{C}\}.$$

2.3.1 Variedade Afim de um Ideal

Definição 2.17. *Seja $I \subseteq K[X]$ um ideal. A* ***variedade afim do ideal*** *I*

$$V(I) = \{(a_1, \cdots, a_n) \in K^n \mid f(a_1, \cdots, a_n) = 0 \ \textit{para todo} \ \ f \in I\}.$$

Quando I é finitamente gerado, vemos que $V(I) = V(f_1, \cdots, f_s)$, ou seja, o conjunto solução do sistema infinito de equações polinomiais

$$f(x_1, \cdots, x_n) = 0 \ \ , \ \ f \in I;$$

é igual ao conjunto solução do sistema finito

$$f_1(x_1, \cdots, x_n) = f_2(x_1, \cdots, x_n) = \ldots = f_s(x_1, \cdots, x_n) = 0.$$

Vemos, claramente, que a solução do primeiro sistema é, também, uma solução do sistema finito, visto que $f_i \in I$ para $i = 1, \cdots, s$. Por outro lado, se $(a_1, \cdots, a_n) \in K^n$ é uma solução do sistema finito, e se f é um elemento qualquer de I, então $f(a_1, \cdots, a_n) = 0$, já que $f = \sum_{i=1}^{s} h_i f_i$, com $h_i \in K[x_1, \cdots, x_n]$. Portanto $(a_1, \cdots, a_n)$ é uma solução do sistema infinito.

Veremos, mais a frente, no Teorema da Base de Hilbert (Teorema 3.2), que todo ideal de $K[X]$ é finitamente gerado, e mais ainda, um ideal pode ter diversos conjuntos geradores com diferente número de elementos. Então se tivermos $I = \langle f_1, \cdots, f_s \rangle = \langle f'_1, \cdots, f'_t \rangle$, então $V(f_1, \cdots, f_s) = V(I) = V(f'_1, \cdots, f'_t)$. Isto é, a solução do sistema $f_1 = 0, \cdots, f_t = 0$ tem as mesmas soluções do sistema $f'_1 = 0, \cdots, f'_t = 0$, e portanto a variedade afim é determinada por um ideal, e não por um conjunto particular de equações.

Este fato, nos diz que para resolver um sistema extremamente trabalhoso, basta que encontremos polinômios que sejam mais simples e gerem o mesmo ideal associado ao sistema original. Em outras palavras, encontrar um "melhor" conjunto de geradores para o mesmo ideal, que nos permita entender de forma melhor sua variedade afim.

Por exemplo, no caso de polinômios em uma variável, encontramos o MDC, como o melhor conjunto gerador, utilizando para isso o algoritmo de Euclides. Já para os polinômios

lineares em várias variáveis utilizamos a eliminação gaussiana para encontrar polinômios mais simples. Vejamos alguns exemplos desses casos, relembrando que estes algoritmos servirão de analogia ao nosso objetivo maior: as bases de Gröbner.

Proposição 2.2. *Sejam os polinômios* $f_1, f_2, \cdots, f_s \in K[x]$ *e o ideal* $I = \langle f_1, f_2, \cdots, f_s \rangle$*, então,*

$$I = \langle g \rangle.$$

onde $g = MDC(f_1, f_2, \cdots, f_s)$.

Demonstração. Primeiramente vamos provar que $\langle f_1, f_2, \cdots, f_s \rangle \subset \langle MDC(f_1, f_2, \cdots, f_s) \rangle$.

De fato, como $g = MDC(f_1, f_2, \cdots, f_s)$, então temos que

$$\begin{aligned} f_1 &= g.h_1 \\ f_2 &= g.h_2 \\ \vdots &\quad \vdots \\ f_s &= g.h_s \end{aligned}$$

para $h_1, h_2, \cdots, h_s \in K[x]$.

Agora, seja $f \in \langle f_1, f_2, \cdots, f_s \rangle$, então

$$\begin{aligned} f &= a_1 f_1 + a_2 f_2 + \ldots + a_s f_s \\ &= a_1(g.h_1) + a_2(g.h_2) + \ldots + a_s(g.h_s) \\ &= g(a_1.h_1 + a_2.h_2 + \ldots + a_s.h_s) \end{aligned}$$

com $a_1, a_2, \cdots, a_s \in K$. Ou seja,

$$f \in \langle g \rangle,$$

e portanto

$$\langle f_1, f_2, \cdots, f_s \rangle \subset \langle MDC(f_1, f_2, \cdots, f_s) \rangle.$$

Por outro lado, se $f \in \langle g \rangle$, temos que $f = h.g$ para algum $h \in K[x]$. Agora, como $g = MDC(f_1, f_2, \cdots, f_s)$, pelo Lema de Bezout (Lema 2.1) existem $a_1, a_2, \cdots, a_n \in K[x]$ tais que,

$$g = a_1 f_1 + a_2 f_2 + \ldots + a_s f_s$$

então

$$f = h.g = h(a_1f_1 + a_2f_2 + \ldots + a_sf_s) = (ha_1)f_1 + (ha_2)f_2 + \ldots + (ha_s)f_s$$

ou seja, $f \in \langle f_1, f_2, \cdots, f_s\rangle$ para qualquer $f \in \langle g\rangle$.

Portanto, $\langle MDC(f_1, f_2, \cdots, f_s)\rangle \subset I$. Logo, $I = \langle g\rangle$. □

Exemplo 2.9. *Considere o seguinte sistema de polinômios em* $\mathbb{Q}[x]$*:*

$$\begin{cases} x^3 + x^2 - 12 = 0 \\ x^2 - 4x + 4 = 0 \end{cases}$$

onde $f_1 = x^3 + x^2 - 12$ *e* $f_2 = x^2 - 4x + 4$*. Tomemos* $I = \langle f_1, f_2\rangle$*, pela proposição 2.2, temos que* $I = \langle g\rangle$ *onde* $g = MDC(f_1, f_2)$*.*

De fato, ao fatorarmos cada um destes polinômios temos:

$$\begin{aligned} f_1 = x^3 + x^2 - 12 &= (x-2)(x^2+3x+6) \\ f_2 = x^2 - 4x + 4 &= (x-2)^2 \end{aligned}$$

Logo, o $MDC(f_1, f_2) = (x-2)$*.*

Agora, seja $f = h_1f_1 + h_2f_2 \in I$ *onde* $h_1, h_2 \in \mathbb{Q}(x)$*, temos que*

$$\begin{aligned} f &= h_1(x^3 + x^2 - 12) + h_2(x^2 - 4x + 4) \\ f &= h_1(x-2)(x^2+3x+6) + h_2(x-2)^2 \\ f &= [h_1(x^2+3x+6) + h_2(x-2)](x-2) \end{aligned}$$

Ou seja, $f \in \langle x-2\rangle$*. Portanto,* $I = \langle x-2\rangle$

Exemplo 2.10. *Seja o ideal* $J \subset \mathbb{R}[x, y, z]$ *tal que*

$$J = \langle\ x + y + z,\ 2x - 3y + z,\ x - y - 2z\ \rangle.$$

Vamos calcular $V(J)$, ou seja, vamos resolver o seguinte sistema de equações:

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

No caso de equações polinomiais lineares em várias variáveis, onde queremos encontrar uma solução para um sistema de equações, utilizamos a muito conhecida, eliminação gaussiana*, na qual operamos sobre as equações do sistema, a fim de eliminar o maior número de incógnitas possível, de três maneiras possíveis: permutando duas equações, adicionando o múltiplo de uma equação a outra e/ou multiplicando uma equação por um escalar não nulo.*

Com isso, reduzimos as equações originais a outras equações, diferentes, que nos dêem a solução de forma mais direta, como veremos abaixo.

$$\begin{cases} x + y + z = 0 \\ 2x - 3y + z = 0 \\ x - y - 2z = 0 \end{cases} \longrightarrow \begin{cases} x + y + z = 0 \\ -5y - z = 0 \\ -2y - 3z = 0 \end{cases} \longrightarrow$$

$$\longrightarrow \begin{cases} x + y + z = 0 \\ -5y - z = 0 \\ 13z = 0 \end{cases} \longrightarrow \begin{cases} x + y + z = 0 \\ y + \frac{1}{5}z = 0 \\ z = 0 \end{cases}$$

$$\longrightarrow \begin{cases} x = 0 \\ y = 0 \\ z = 0 \end{cases}$$

Vemos, facilmente, no sistema resultante a solução $S = \{(0, 0, 0)\}$.

Sendo assim, $J = \langle x, y, z \rangle$ e $V(J) = \{(0, 0, 0)\}$.

2.3.2 Ideal associado a um Sudoku

Um exemplo que usaremos por todo nosso trabalho com o intuito de ilustrar os conceitos desenvolvidos, é um passatempo muito conhecido no mundo todo como Sudoku.

O tabuleiro do Sudoku é formado por um quadrado dividido em 9×9 quadrados menores separados em 9 blocos de 3×3. O passatempo consiste em preencher os 81 espaços com algarismos de 1 a 9 de maneira que nenhuma linha, coluna ou bloco 3×3 possua algarismos repetidos.

Cada passatempo Sudoku é um subconjunto do tabuleiro completo que determina de forma única o restante do tabuleiro, isto é, o passatempo inicia-se com uma quantidade de espaços já preenchidos de maneira que só há uma possibilidade de completar os restantes.

Abaixo vemos um exemplo de um passatempo Sudoku a ser resolvido.

7		2		6				3
			7			2		
	4			2	1			9
		8					6	
4		3				1		2
	7					4		
8			9	4			1	
		7			3			
5				8		9		6

Figura 2.2: Sudoku

O que faremos é "reescrever" o Sudoku como um sistema de equações polinomiais em várias variáveis (sobre os números complexos) , da seguinte maneira:

Antes de mais nada, vamos considerar cada um dos 81 espaços como uma variável que chamaremos de x_i com i variando de 1 a 81, numerados da esquerda pra direita, de cima para baixo.

Como cada espaço deve ser preenchido com um algarismo de 1 a 9, vamos associar a cada um desses algarismos uma das raízes nonas da unidade $\zeta_n \in \mathbb{C}$ onde $\zeta_n^9 = 1$ com $1 \leq n \leq 9$, de forma que para cada espaço temos a seguinte equação:

$$x_i{}^9 - 1 = 0$$

onde $1 \leq i \leq 81$.

Como não podemos ter regiões (linha, coluna e bloco 3×3), com algarismos repetidos, teremos a seguinte equação:

$$G_{i,j}(x_i, x_j) = \frac{x_i{}^9 - x_j{}^9}{x_i - x_j} = x_i^8 + x_i^7 x_j + x_i^6 x_j^2 + x_i^5 x_j^3 + x_i^4 x_j^4 + x_i^3 x_j^5 + x_i^2 x_j^6 + x_i x_j^7 + x_j^8 = 0$$

para cada $\{i, j\} \in A$, com $i \neq j$, sendo A o conjunto dos pares não ordenados $\{i, j\}$ onde

$$\{i, j\} \in A \iff x_i, x_j \text{ } \textit{estão numa mesma linha, coluna ou bloco } 3 \times 3.$$

Observe que o conjunto A será sempre o mesmo qualquer que seja o Sudoku, contendo 810 elementos. Vejamos alguns destes elementos relacionados ao primeiro espaço com a primeira linha, coluna e bloco 3x3:

$$\begin{aligned} A \;=\; \big\{ & \{1,2\},\{1,3\},\{1,4\},\{1,5\},\{1,6\},\{1,7\},\{1,8\},\{1,9\}, \\ & \{1,10\},\{1,11\},\{1,12\},\{1,19\},\{1,20\},\{1,21\},\{1,28\}, \\ & \{1,37\},\{1,46\},\{1,55\},\{1,64\},\{1,73\},\ \cdots \big\} \end{aligned}$$

Além disso, temos as equações fornecidas pelos espaços já preenchidos do passatempo, onde sabemos que a raiz nona da unidade ζ_n está ocupando o espaço x_i atravé da equação:

$$x_i - \zeta_n = 0.$$

Portanto para encontrarmos uma solução para o Sudoku da figura 2.3.2, devemos resolver o seguinte sistema de equações polinomiais complexas em 81 variáveis:

$$
\begin{cases}
{x_i}^9 - 1 = 0 \quad , \quad 1 \leq i \leq 81 \\
\\
G_{i,j}(x_i, x_j) = 0 \quad , \quad \{i,j\} \in A \\
\\
\begin{array}{llllll}
x_1 - \zeta_7 = 0 & , & x_3 - \zeta_2 = 0 & , & x_5 - \zeta_6 = 0 & , & x_9 - \zeta_3 = 0 \\
x_{12} - \zeta_7 = 0 & , & x_{16} - \zeta_2 = 0 & , & x_{20} - \zeta_4 = 0 & , & x_{23} - \zeta_2 = 0 \\
x_{24} - \zeta_1 = 0 & , & x_{27} - \zeta_9 = 0 & , & x_{30} - \zeta_8 = 0 & , & x_{35} - \zeta_6 = 0 \\
x_{37} - \zeta_4 = 0 & , & x_{39} - \zeta_3 = 0 & , & x_{43} - \zeta_1 = 0 & , & x_{45} - \zeta_2 = 0 \\
x_{47} - \zeta_7 = 0 & , & x_{52} - \zeta_4 = 0 & , & x_{55} - \zeta_8 = 0 & , & x_{58} - \zeta_9 = 0 \\
x_{59} - \zeta_4 = 0 & , & x_{62} - \zeta_1 = 0 & , & x_{66} - \zeta_7 = 0 & , & x_{69} - \zeta_3 = 0 \\
x_{73} - \zeta_5 = 0 & , & x_{77} - \zeta_8 = 0 & , & x_{79} - \zeta_9 = 0 & , & x_{81} - \zeta_6 = 0
\end{array}
\end{cases}
$$

Totalizando,neste exemplo, 919 equações.

Sabemos que resolver um sistema dessa magnitude não é uma tarefa trivial, e demanda bastante tempo. Porém, o que vamos fazer é associar um ideal a esse sistema, na verdade, tomaremos o ideal gerado pelos 919 polinômios do sistema acima e calcularemos sua variedade afim, achando assim a solução do sistema, e consequentemente a do Sudoku.

Veremos nos próximos capítulos que poderemos calcular essa variedade afim, de uma forma menos trabalhosa, com o auxílio das bases de Gröbner. Além de conhecermos a relação do Sudoku com o problema da k-coloração de grafos.

2.4 Divisão em Várias Variáveis

Vimos que no caso da divisão de polinômios em uma variável, descobrir um bom conjunto gerador, equivale a determinar o MDC dos geradores através do algoritmo de Euclides; já no caso linear com várias variáveis, utilizamos a eliminação Gaussiana para encontrá-lo.

Em todos esses casos, para que se possa implementar um algoritmo de divisão é necessário que sejam determinados os termos líderes dos polinômios, e para isso uma ordenação sobre os monômios.

No entanto, nos casos de polinômios em uma variável não há dúvidas quanto a escolha do termo líder, visto que basta sabermos determinar o de maior grau. Já com os polinômios lineares em várias variáveis, como não temos a preocupação com o grau, nos guiamos pela ordem das variáveis, geralmente $x_i < x_j$ se $i < j$.

Para o caso geral definiremos nesta seção o que vem a ser uma ordem monomial e daremos alguns exemplos das ordens mais comumente utilizadas. Vale observar que, fixar uma ordem no conjunto dos monômios X^α equivale a fixar uma ordem em $\mathbb{Z}^n_{\geq 0}$

2.4.1 Ordens Monomiais

Definição 2.18. *Uma relação de ordem $\succ$ em $\mathbb{Z}^n_{\geq 0}$ é chamada uma **ordem monomial**, se satisfaz as seguintes propriedades:*

(i) $\succ$ é uma ordem total, isto é,

$$\forall \alpha, \beta \in \mathbb{Z}^n_{\geq 0},\ \textit{Se } \alpha \neq \beta \textit{ então } \alpha \succ \beta \textit{ ou } \beta \succ \alpha;$$

(ii) $\alpha \succ \beta \Longrightarrow \alpha + \gamma \succ \beta + \gamma, \forall \alpha, \beta, \gamma \in \mathbb{Z}^n_{\geq 0}$*;*

(iii) $\succ$ é uma boa ordem, ou seja, todo subconjunto não vazio de $\mathbb{Z}^n_{\geq 0}$ admite um menor elemento.

Definição 2.19. *Seja $\succ$ uma ordem em $\mathbb{Z}^n_{\geq 0}$. Podemos, então, definir uma ordem no conjunto dos monômios, a saber*

$$X^\alpha \succ X^\beta \iff \alpha \succ \beta.$$

Proposição 2.3. *Uma ordem total $\succ$ em $\mathbb{Z}^n_{\geq 0}$ é uma boa ordem se e somente se toda sequência decrescente ($\alpha_1 \succeq \alpha_2 \succeq \ldots$) em $\mathbb{Z}^n_{\geq 0}$ estabiliza, i.e., $\exists n_0$ talque $\alpha_n = \alpha_{n_0}\ \forall n \geq n_0$.*

Demonstração. Suponha que $\succ$ não é uma boa ordem. Então existe $M \subseteq \mathbb{Z}^n_{\geq 0}$, não vazio, tal que M não admite um menor elemento. Tome $\alpha_1 \in M$. Como M não admite um elemento

mínimo, podemos escolher um $\alpha_2 \in M$, tal que $\alpha_1 \succ \alpha_2$. Utilizando o mesmo raciocínio para α_2, e assim sucessivamente, podemos encontrar uma sequência estritamente decrescente infinita

$$\alpha_1 \succ \alpha_2 \succ \alpha_3 \succ \cdots .$$

Reciprocamente, dada uma sequência decrescente $(\alpha_1 \succeq \alpha_2 \succeq \cdots)$ em $\mathbb{Z}^n_{\geq 0}$, tome $M = \{\alpha_1, \alpha_2, \cdots\}$. Por hipótese M admite um menor elemento. Logo, $\exists\, n_o$ tal que $a_n = a_{n_0}\ \forall\ n \geq n_0$. □

Definição 2.20 (Ordem Lexicográfica). *Seja $\alpha = (\alpha_1, \cdots, \alpha_n)$ e $\beta = (\beta_1, \cdots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, dizemos que*

$$\alpha \succ_{LEX} \beta \textit{ se, e somente se, existe } j \in \{1, \cdots, n\} \textit{tal que}$$

$$\alpha_j > \beta_j \textit{ e } \alpha_k = \beta_k \textit{ para cada } k < j$$

Sendo assim $X^\alpha \succ_{LEX} X^\beta$ se $\alpha \succ_{LEX} \beta$.

Podemos observar que:

$$x_1 = X^{(1,0,\cdots,0)}$$

$$x_2 = X^{(0,1,\cdots,0)}$$

$$\cdots$$

$$x_n = X^{(0,0,\cdots,1)}$$

Assim, teremos

$$x_1 \succ_{LEX} x_2 \succ_{LEX} \cdots \succ_{LEX} x_n.$$

Exemplo 2.11. *Vejamos alguns exemplos:*

(a) $xy^4 \succ_{LEX} xyz^2$;

(b) $x^2y \succ_{LEX} xy \succ_{LEX} xz^3 \succ_{LEX} y^4z^2 \succ_{LEX} z^8$.

Definição 2.21. ***(Ordem Lexicográfica Graduada)*** *Seja α e $\beta \in \mathbb{Z}^n_{\geq 0}$, dizemos que*

$$\alpha \succ_{LEG} \beta \textit{ se, e somente se,} |\alpha| > |\beta| \textit{ ou } |\alpha| = |\beta| \textit{ e } \alpha \succ_{LEX} \beta$$

Exemplo 2.12. *Vejamos alguns exemplos:*

(a) $(3,1,4) \succ_{LEG} (1,1,2)$*, pois* $3+1+4 > 1+1+2$*;*

(b) $z^8 \succ_{LEG} y^4z^2 \succ_{LEG} xz^3 \succ_{LEG} y^4 \succ_{LEG} x^2y \succ_{LEG} xz \succ_{LEG} y^2$.

Definição 2.22. ***(Ordem Lexicográfica Inversa Graduada)*** *Seja* α *e* $\beta \in \mathbb{Z}^n_{\geq 0}$*, dizemos que*

$$\alpha \succ_{LIVG} \beta \textit{ se, e somente se,} |\alpha| > |\beta| \textit{ ou } |\alpha| = |\beta| \; e$$

$$existe\ j \in \{1, \cdots, n\} \textit{tal que } \alpha_k = \beta_k \; para \; k > j \; e \; \alpha_j < \beta_j$$

Neste caso, quando $|\alpha| = |\beta|$*, a decisão para* $\alpha \succ_{LIVG} \beta$ *depende da comparação das componentes de* α *e* β*, da direita pra esquerda, necessitando agora a coordenada correspondente diferente ser maior em* β*.*

Exemplo 2.13. *Vejamos alguns exemplos:*

(a) $(3,1,4) \succ_{LIVG} (1,1,2)$*, pois* $3+1+4 > 1+1+2$*;*

(b) $z^8 \succ_{LIVG} y^4z^2 \succ_{LIVG} y^4 \succ_{LIVG} xz^3 \succ_{LIVG} x^2y \succ_{LIVG} y^2 \succ_{LIVG} xz$.

Proposição 2.4. *As ordens Lexicográfica, Lexicográfica Graduada e Lexicográfica Inversa Graduada são ordens monomiais.*

Demonstração. Vamos provar somente para a ordem lexicográfica, já que as demais demonstrações são análogas. Para isso, vamos mostrar que a ordem $\succ_{LEX}$ satisfaz às três condições da definição 2.18.

De fato,

(i) $\succ_{LEX}$ é uma ordem total, pois ao compararmos componente a componente, α e $\beta \in \mathbb{Z}^n_{\geq 0}$, utilizamos a ordem $>$ em $\mathbb{Z}_{\geq 0}$, que é total.

(ii) Suponha $\alpha \succ_{LEX} \beta$, digamos, $\alpha_i = \beta_i$, para i de 1 até $j-1$, e $\alpha_j > \beta_j$. Logo, $\alpha + \gamma \succ_{LEX} \beta + \gamma$, pois $\alpha_i + \gamma_i = \beta_i + \gamma_i$, para i de 1 até $j-1$ e $\alpha_j + \gamma_j > \beta_j + \gamma_j$;

(iii) Suponha, por absurdo, que $\succ_{LEX}$ não é uma boa ordem. Então pela proposição 2.3, existe uma sequência infinita estritamente decrescente

$$\alpha_1 \succ_{LEX} \alpha_2 \succ_{LEX} \alpha_3 \succ_{LEX} \cdots .$$

em $\mathbb{Z}^n_{\geq 0}$. Mostraremos que isto é impossível.

Considere a sequência (a^i_1) formada pela primeira componente. Ora, esta é uma sequência decrescente em $\mathbb{Z}_{\geq 0}$, logo estabiliza. Passando para a segunda componente, utilizando o mesmo raciocínio, vemos que esta também se estabiliza. Como α_i admite um número finito, fixo de componentes, a sequência α_i tem que se estabilizar, o que é uma contradição.

Portanto, a ordem lexicográfica é uma ordem monomial.

□

Definição 2.23. *Seja $f \in K[x_1, \cdots, x_n]$ um polinômio não nulo. Fixada uma ordem monomial $\succ$ em $\mathbb{Z}^n_{\geq 0}$, podemos escrever f na forma*

$$f = a_\alpha X^\alpha + \sum_{\alpha \succ \beta} a_\beta X^\beta.$$

com $a_\alpha, a_\beta \in K$ e $a_\alpha \neq 0$. Definimos, então:

*(i) o **termo líder** de f como $TL(f) = a_\alpha X^\alpha$;*

*(ii) o **potência líder** de f como $PL(f) = X^\alpha$;*

*(iii) o **coeficiente líder** de f como $CL(f) = a_\alpha$;*

*(iv) o **grau do polinômio** f como $\delta f = |\alpha|$.*

Proposição 2.5. *Seja $f, g \in K[X]$ polinômios não nulos e $\succ$ uma ordem monomial. Então:*

(i) $PL(f.g) = PL(f) + PL(g)$;

(ii) $PL(f + g) \preceq max(PL(f), PL(g))$.

Demonstração. Sejam

$$f = \sum_{i=1}^{r} a_i X^{\alpha_i} \qquad e \qquad g = \sum_{i=1}^{s} b_j X^{\beta_j}$$

onde $a_i, b_j \in K$ e $X^{\alpha_1} \succeq X^{\alpha_2} \succeq \ldots \succeq X^{\alpha_r}$ e $X^{\beta_1} \succeq X^{\beta_2} \succeq \ldots \succeq X^{\beta_s}$.

Daí, as potências líderes de f e g são $PL(f) = X^{\alpha_1}$ e $PL(g) = X^{\beta_1}$.

Temos o produto fg dado por

$$fg = \Big(\sum_{i=1}^{r} a_i X^{\alpha_i}\Big)\Big(g = \sum_{i=1}^{s} b_j X^{\beta_j}\Big) = \sum_{i=1}^{r}\sum_{i=1}^{s} a_i b_j X^{\alpha_i} X^{\beta_j}.$$

Como $X^{\alpha_1} \succ X^{\alpha_i}$ para $i = 2, \cdots, r$, temos $X^{\alpha_1}X^{\beta_j} \succ X^{\alpha_i}X^{\beta_j}$ para $i = 2, \cdots, r$ e $j = 2, \cdots s$. Da mesma maneira temos $X^{\alpha_i}X^{\beta_1} \succ X^{\alpha_i}X^{\beta_j}$ para $j = 2, \cdots s$ e $i = 2, \cdots, r$. Daí,

$$X^{\alpha_1}X^{\beta_1} \succ X^{\alpha_1}X^{\beta_j} \succ X^{\alpha_i}x^{\beta_j}$$

para $i = 2, \cdots, r$ e $j = 2, \cdots, s$.

Portanto,

$$PL(fg) = X^{\alpha_1}X^{\beta_1} = PL(f)PL(g).$$

Agora, na soma dos polinômios $f + g$ teremos somente uma das duas possibilidades para os termos líderes,

$$TL(f) = -TL(g) \;\; \textit{ou} \;\; TL(f) \neq -TL(g).$$

Se $TL(f) = -TL(g)$, então os termos líderes de f e g cancelam-se na soma, restando apenas monômios menores, assim

$$PL(f + g) \prec \textit{max}\{PL(f), PL(g)\}$$

onde, $\textit{max}\{PL(f), PL(g)\} = \textit{max}\{X^{\alpha_1}, X^{\beta_1}\}$.

Se $TL(f) \neq -TL(g)$, então não há cancelamento dos termos líderes e

$$PL(f + g) = \textit{max}\{PL(f), PL(g)\}.$$

□

Corolário 2.3. *Seja $f, g \in K[X]$ polinômios não nulos, fixada uma ordem monomial. Então:*

(i) $\delta(f.g) = \delta f + \delta g$;

(ii) Se $f + g \neq 0$, *então,* $\delta(f + g) \leq max(\delta f, \delta g)$.

Se em (ii), $\delta f \neq \delta g$ *então vale a igualdade.*

Demonstração. Segue imediatamente da proposição 2.5 □

2.4.2 Algoritmo da Divisão

Fixada uma ordem monomial em $K[X]$, nosso próximo objetivo é obter um algoritmo da divisão.

O bom senso nos leva a tentar algo análogo aos polinômios em uma variável, e aos polinômios lineares de várias variáveis, onde o objetivo é reduzir os polinômios até certo ponto.

A idéia ao se dividir f por $f_1, \cdots, f_n$, é cancelar os termos de f usando os termos líderes dos f_i's (de tal maneira, que os novos termos sejam menores, segundo a ordem fixada, do que os cancelados) até quando não seja mais possível continuar, obtendo ao final, neste caso, uma lista de polinômios quociente e um resto. Veremos mais a frente, o algoritmo de uma forma mais completa.

Definição 2.24. *Dados polinômios $f, g, h \in K[X]$ com $g \neq 0$ dizemos que* ***f reduz-se a h módulo g****, denotado por*

$$f \xrightarrow{g} h$$

se e somente se $TL(g)$ divide algum termo $T(f)$ de f e

$$h = f - \frac{T(f)}{TL(g)}g.$$

Exemplo 2.14. *Sejam os polinômios $f = x^4 + y^2$, $g = x^2$ e $h = y^2$ com $f, g, h \in \mathbb{R}[x, y]$. Então, considerando a ordem lexicográfica com $x > y$, $f \xrightarrow{g} h$. De fato,*

$$y^2 = (x^4 + y^2) - \frac{x^4}{x^2}x^2.$$

Definição 2.25. *Sejam $f \in K[X]$ e $G = \{g_1, g_2, ..., g_s\} \subset K[X]$ com $g_i \neq 0$ para $1 \leq i \leq s$ Dizemos que f reduz-se a h módulo G, e denotamos*

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

se e somente se existe uma seqüência de índices $i_1, i_2, \cdots, i_t \in \{1, \cdots, s\}$ e uma seqüência de polinômios $h_1, \cdots, h_{t-1} \in K[X]$ tais que

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

Exemplo 2.15. *Sejam os polinômios*

$$\begin{aligned} f &= x^4 + y^2 \\ g_1 &= x^2 \\ g_2 &= y \\ h &= 0 \end{aligned}$$

com $f, g_1, g_2, h \in \mathbb{R}[x, y]$. Considerando a ordem lexicográfica com $x > y$, se $G = \{g_1, g_2\}$ então $f \xrightarrow{G}_+ h$.

De fato, existe h_1 tal que $f \xrightarrow{g_1} h_1$ onde

$$h_1 = (x^4 + y^2) - \frac{x^4}{x^2}x^2 = y^2$$

Além disso, $h_1 \xrightarrow{g_2} h$

$$h = y^2 - \frac{y^2}{y}y = 0$$

Portanto,

$$f \xrightarrow{g_1} h_1 \xrightarrow{g_2} h$$

$$x^4 + y^2 \xrightarrow{x^2} y^2 \xrightarrow{y} 0.$$

Isto é,

$$x^4 + y^2 \xrightarrow{G}_+ 0.$$

Definição 2.26. *O polinômio* ***r é reduzido módulo G*** $\subseteq K[X]$*, se* $r = 0$ *ou se nenhum termo de* r *é divisível por* $TL(g)$*, para qualquer* $g \in G$*.*

A fim de nos auxiliar no estudo do algoritmo da divisão em várias variáveis, vejamos um exemplo de divisão de polinômios em uma variável.

Exemplo 2.16. *Vamos dividir o polinômio*

$$f = x^6 - x^4 + x^3 - x$$

por

$$g = x^2 + x$$

com $f, g \in \mathbb{Q}[x]$*.*

No caso de uma variável, como já dissemos, não há dúvidas quanto a ordenação, visto que utilizamos o grau dos monômios do maior para o menor.

Primeiramente verificamos que

$$\frac{TL(f)}{TL(g)} = \frac{x^6}{x^2} = x^4$$

assim, obtemos

$$f = q_1 g + f_1$$

onde $q_1 = x^4$ *e* $f_1 = -x^5 - x^4 + x^3 - x$*.*

Na próxima etapa, temos

$$\frac{TL(f_1)}{TL(g)} = \frac{-x^5}{x^2} = -x^3$$

assim, obtemos

$$f_1 = q_2 g + f_2$$

onde $q_2 = -x^3$ *e* $f_2 = x^3 - x$*.*

Na terceira etapa, temos

$$\frac{TL(f_2)}{TL(g)} = \frac{x^3}{x^2} = x$$

assim, obtemos

$$f_2 = q_3 g + f_3$$

onde $q_3 = x$ *e* $f_3 = -x^2 - x$

Na quarta etapa, temos

$$\frac{TL(f_3)}{TL(g)} = \frac{-x^2}{x^2} = -1$$

obtemos

$$f_3 = q_4 g + f_4$$

onde $q_4 = -1$ *e* $f_4 = 0$.

Como $f_4 = 0$ *e portanto reduzido módulo* g *terminamos o processo obtendo*

$$f = q.g + r$$

onde $q = q_1 + q_2 + q_3 + q_4$ *e* $r = f_4$.

Podemos observar, que no exemplo acima, obtivemos como resto da divisão o polinômio nulo, como sempre acontece quando trabalhamos em domínios euclidianos em uma variável como $Q[x]$, garantimos que f pertence ao ideal gerado por g.

No entanto, no caso de várias variáveis, considerando esta anologia com o caso univariado, poderíamos ser induzidos a pensar que a condição para que um polinômio g pertença a um $I = \langle f_1, \cdots, f_s \rangle \subset K[X]$ é que o resto r da divisão de g por $f_1, \cdots, f_s$ seja nulo, o que não é sempre verdade, já que $K[X]$ não é um domínio euclidiano, o que veremos a frente. E é justamente por isso que precisaremos das bases de Gröbner, assunto do próximo capítulo.

Na página seguinte, encontraremos o algoritmo da divisão de um polinômio f por $f_1, \cdots, f_n$ em $K[X]$ em um formato mais apropriado.

Os dados de entrada serão o polinômio f e a lista de polinômios $F = \{f_1, \cdots, f_n\}$, todos pertencentes a $K[X]$. Vamos supor uma ordem monomial qualquer, previamente determinada, assim como um procedimento, também previamente definido, para a determinação do $TL(f)$, o qual omitiremos do processo. Obteremos como saída do algoritmo, a lista de polinômios quocientes $Q = \{q_1, \cdots, q_m\}$ e o polinômio resto r.

Vale ressaltar que no caso da divisão de um polinômio, em várias variáveis, por vários polinômios podemos obter uma lista com vários polinômios quocientes e não, necessariamente, somente um. Outra coisa, ainda mais relevante, é que não há no algoritmo algo que garanta a

unicidade do resto, isto é, se alterarmos a ordem em que encontram-se os polinômios do conjunto de divisores, geralmente obteremos outro resto diferente, como veremos nos exemplos a seguir.

Finalmente, o **algoritmo da divisão de um polinômio em várias variáveis** por uma lista de polinômios, todos pertencentes a $K[X]$.

Algoritmo 1: algoritmo da divisão em várias variáveis

Entrada: f, $F = \{f_1, \cdots, f_s\}$
Resultado: r, $Q = \{q_1, \cdots, q_m\}$
Dados: ordem monomial
$p = f$; `#dividendo inicial`
para $i = 1$ **até** m **faça**
  $q_i = 0$; `#quocientes iniciais`
fim para
$r = 0$; `#resto inicial`
início;
enquanto $p \neq 0$ **faça**
  se *existe* i *tal que* $TL(f_i)$ *divide* $TL(p)$ **então**
    escolha o menor i tal que $TL(f_i)$ divide $TL(p)$;
    $q_i = q_i + \frac{TL(p)}{TL(f_i)}$;
    $p = p - \frac{TL(p)}{TL(f_i)} f_i$;
    $r = r$;
  senão
    $p = p - TL(p)$;
    $r = r + TL(p)$;
  fim se
fim enqto
Saída: r e Q

Vejamos, agora, alguns exemplos de divisões de polinômios. Neste primeiro exemplo, faremos uma divisão entre dois polinômios em duas variáveis, a fim de ilustrar a semelhança entre as divisões em uma variável.

Exemplo 2.17. *Vamos dividir o polinômio*

$$f = 6x_1^6x_2^4 + 7x_1^5 + 8x_1^4x_2^7 + 1 \quad \textit{por} \quad f_1 = x_1^4x_2^2 + 1$$

com $f, f_1 \in \mathbb{Q}[x_1x_2]$*, considerando a ordenação lexicográfica com* $x > y$*.*

Iniciando o algoritmo teremos:

$$\begin{cases} p &= 6x_1^6x_2^4 + 7x_1^5 + 8x_1^4x_2^7 + 1 \\ f_1 &= x_1^4x_2^2 + 1 \end{cases} \quad \begin{cases} q_1 &= 0 \\ r &= 0 \end{cases}$$

Primeira etapa: $x_1^4x_2^2 = TL(f_1)$ *divide* $TL(p) = 6x_1^6x_2^4$

$$\begin{aligned} q_1 &= \tfrac{TL(p)}{TL(f_1)} = 6x_1^2x_2^2 \\ p &= 6x_1^6x_2^4 + 7x_1^5 + 8x_1^4x_2^7 + 1 - (x_1^4x_2^2 + 1)6x_1^2x_2^2 \\ &= 6x_1^6x_2^4 + 7x_1^5 + 8x_1^4x_2^7 + 1 - 6x_1^6x_2^4 - 6x_1^2x_2^2 \\ &= 7x_1^5 + 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1 \\ r &= 0 \end{aligned}$$

Segunda etapa: $x_1^4x_2^2 = TL(f_1)$ *não divide* $TL(p) = 7x_1^5$

$$\begin{aligned} p &= 7x_1^5 + 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1 - (7x_1^5) \\ &= 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1 \\ r &= 7x_1^5 \end{aligned}$$

Terceira etapa: $x_1^4x_2^2 = TL(f_1)$ *divide* $TL(p) = 8x_1^4x_2^7$

$$\begin{aligned} q_1 &= 6x_1^2x_2^2 + \tfrac{TL(p)}{TL(f_1)} = 6x_1^2x_2^2 + 8x_2^5 \\ p &= 8x_1^4x_2^7 - 6x_1^2x_2^2 + 1 - (x_1^4x_2^2 + 1)8x_2^5 \\ &= -6x_1^2x_2^2 - 8x_2^5 + 1 \\ r &= 7x_1^5 \end{aligned}$$

Quarta etapa: $x_1^4x_2^2 = TL(f_1)$ *não divide* $TL(p) = -6x_1^2x_2^2$

$$\begin{aligned} p &= -6x_1^2x_2^2 - 8x_2^5 + 1 - (-6x_1^2x_2^2) \\ &= -8x_2^5 + 1 \\ r &= 7x_1^5 - 6x_1^2x_2^2 \end{aligned}$$

Quinta etapa: $x_1^4x_2^2 = TL(f_1)$ *não divide* $TL(p) = -8x_2^5$

$$\begin{aligned} p &= -8x_2^5 + 1 - (-8x_2^5) \\ &= 1 \\ r &= 7x_1^5 - 6x_1^2x_2^2 - 8x_2^5 \end{aligned}$$

Sexta etapa: $x_1^4x_2^2 = TL(f_1)$ *não divide* $TL(p) = 1$

$$\begin{aligned} p &= 1 - (1) \\ &= 0 \\ r &= 7x_1^5 - 6x_1^2x_2^2 - 8x_2^5 + 1 \end{aligned}$$

Encerrando assim o algoritmo com

$$\begin{cases} p &= 0 \\ q_1 &= 6x_1^2x_2^2 + 8x_2^5 \\ r &= 7x_1^5 - 6x_1^2x_2^2 - 8x_2^5 + 1 \end{cases}$$

Portanto, podemos escrever

$$6x_1^6x_2^4 + 7x_1^5 + 8x_1^4x_2^7 + 1 = (6x_1^2x_2^2 + 8x_2^5)(x_1^4x_2^2 + 1) + 7x_1^5 - 6x_1^2x_2^2 - 8x_2^5 + 1$$

No exemplo a seguir, dividiremos um polinômio por uma lista de polinômios, todos em duas variáveis.

Exemplo 2.18. *Sejam*

$$f_1 = xy + 1 \quad e \quad f_2 = y^2 - 1$$

com $f_1, f_2 \in \mathbb{Q}[x, y]$.

e a ordem lexicográfica, com $x > y$.

Vamos dividir

$$f = xy^2 - x$$

por $F = \{f_1, f_2\}$.

Iniciando o algoritmo teremos:

$$\begin{cases} p &= xy^2 - x \\ f_1 &= xy + 1 \\ f_2 &= y^2 - 1 \end{cases} \quad \begin{cases} q_1 &= 0 \\ q_2 &= 0 \\ r &= 0 \end{cases}$$

Primeira etapa:

- $xy = TL(f_1)$ *divide* $TL(p) = xy^2$

$$\begin{aligned} q_1 &= y \\ p &= xy^2 - x - (xy + 1).y = -x - y \\ r &= 0 \end{aligned}$$

Segunda etapa:

- $xy = TL(f_1)$ *não divide* $TL(p) = -x$
- $y^2 = TL(f_2)$ *não divide* $TL(p) = -x$

$$\begin{aligned} p &= -x - y - (-x) = -y \\ r &= -x \end{aligned}$$

Terceira etapa:

- $xy = TL(f_1)$ *não divide* $TL(p) = -y$
- $y^2 = TL(f_2)$ *não divide* $TL(p) = -y$

$$\begin{aligned} p &= -y - (-y) = 0 \\ r &= -x - y \end{aligned}$$

Encerrando assim o algoritmo.

Portanto temos que o polinômio f pode ser escrito como:

$$f = f_1q_1 + f_2q_2 + r$$

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

Agora, vamos dividir $f = xy^2 - x$ por $F = \{f_1, f_2\}$ sendo agora $f_1 = y^2 - 1$ e $f_2 = xy + 1$, ou seja, trocamos a ordem dos divisores.

Iniciando o algoritmo teremos:

$$\begin{cases} p &= xy^2 - x \\ f_1 &= y^2 - 1 \\ f_2 &= xy + 1 \end{cases} \quad \begin{cases} q_1 &= 0 \\ q_2 &= 0 \\ r &= 0 \end{cases}$$

Primeira etapa:

- $y^2 = TL(f_1)$ *divide* $TL(p) = xy^2$

$$\begin{aligned} q_1 &= x \\ p &= xy^2 - x - (y^2 - 1).x = 0 \\ r &= 0 \end{aligned}$$

Encerrando assim o algoritmo.

Obtemos, então,

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

No exemplo 2.18, podemos observar uma peculiaridade que não encontramos nos casos de uma variável, e que irá nos levar a necessidade das bases de Gröbner. Na divisão de um polinômio em uma variável por um conjunto G de polinômios, obtemos sempre o mesmo resto, independente da ordem que dividimos os polinômios, na verdade, isso significa, como já sabemos, $f \xrightarrow{G}_+ 0 \iff f \in \langle G \rangle$, por estar num domínio euclidiano.

Porém, o mesmo não acontece com polinômios em várias variáveis, já que $K[X]$ não é um domínio Euclidiano. Ou seja, ainda teremos $f \xrightarrow{G}_+ 0 \implies f \in \langle G \rangle$, mas como vimos no exemplo 2.18, a recíproca nem sempre é verdadeira. De fato, vimos que dividindo

o polinômio f por f_1 depois por f_2 encontramos um resto diferente de zero, no entanto, quando dividimos por f_2 e depois por f_1 obtemos resto nulo, implicando que $f \in \langle f_1, f_2 \rangle$.

Proposição 2.6. *Seja $F = \{f_1, \cdots, f_s\}$ uma lista de polinômios em $K[X]$ com uma ordem monomial fixada. Então qualquer $f \in K[X]$ pode ser escrito como*

$$f = q_1 f_1 + \ldots + q_s f_s + r$$

onde os q_i's e r pertencem a $K[X]$, $\delta q_i f_i \leq \delta f$ e r é reduzido módulo F.

Demonstração. Inicialmente vamos provar que existem $q_1, \cdots, q_s$ e r satisfazendo as condições acima, mostrando que o Algoritmo 1 funciona.

Devemos mostrar que

$$f = q_1 f_1 + \ldots + q_s f_s + p + r \tag{2.2}$$

vale a qualquer instante. Isto claramente é verdadeiro para os valores iniciais de $q_1 = \ldots = q_s = 0$, $p = f$ e $r = 0$. Agora, suponhamos que (2.2) vale também em algum momento do algoritmo. Se no próximo passo algum $TL(f_i)$ divide $TL(p)$, então a igualdade

$$q_i f_i + p = \left(q_i + \frac{TL(p)}{TL(f_i)}\right) f_i + \left(p - \left(\frac{TL(p)}{TL(f_i)}\right) f_i\right)$$

mostra que $q_i f_i + p$ não se altera, já que todas as outras variáveis não são alteradas e portanto (2.2) é verdadeiro neste caso. Por outro lado, se $TL(f_i)$ não divide $TL(p)$ para $i = 1, 2, \cdots, s$, então embora p e r se alterem, a soma $p + r$ se mantém inalterada já que

$$p + r = (p - TL(p)) + (r + TL(p)),$$

e portanto, também neste caso, 2.2 é verdadeiro.

Temos ainda que provar que o algoritmo termina, e isto acontece quando $p = 0$. Nesta situação temos de (2.2) que

$$f = q_1 f_1 + \ldots + q_s f_s + r$$

uma vez que os termos são adicionados a r somente quando não são divisíveis por $TL(f_i)$, para $i = 1, 2, \cdots, s$. Segue que r tem as propriedades desejadas quando o algoritmo termina. Para ver que o algoritmo termina, observe que toda vez que redefinimos a variável p seu grau diminui (ou torna-se nulo). Para ver isto, suponhamos inicialmente que p é redefinido por

$$p' = p - \frac{TL(p)}{TL(f_i)} f_i;$$

Pelo Corolário 2.3 temos então

$$TL\left(\frac{TL(p)}{TL(f_i)} f_i\right) = \frac{TL(p)}{TL(f_i)} TL(f_i) = TL(p)$$

e portanto p e $\left(\frac{TL(p)}{TL(f_i)}\right) f_i$ têm o mesmo termo líder. Logo a sua diferença p' deve ter grau estritamente menor quando $p' \neq 0$.

Vamos supor agora que $TL(f_i)$ não divide $TL(p)$ para $i = 1, 2, \cdots, s$. Então p é redefinido como

$$p' = p - TL(p)$$

e neste caso claramente o grau de p diminui, como no caso anterior. Suponhamos que o algoritmo nunca termine, teremos então uma sequência decrescente infinita formada pelos sucessivos graus de p', mas como estamos trabalhando com uma ordem monomial, isto não pode ocorrer. Portanto $p = 0$ e o algoritmo termina.

□

CAPÍTULO 3

BASES DE GRÖBNER

Agora que já temos uma ordem determinada, vamos precisar de um algoritmo e de algo mais que garanta o fim deste algoritmo. E é sobre isso que vamos tratar neste capítulo.

3.1 Ideal dos Termos Líderes

Primeiramente, seja K um corpo e $I \subseteq K[x_1, \cdots, x_n]$ um ideal. Vamos associar a cada ideal I um outro ideal sendo este monomial.

Definição 3.1. *Definimos o* ***ideal dos termos líderes de*** I *como*

$$\langle TL(I)\rangle = \langle\{TL(f) \mid f \in I\}\rangle.$$

Ou seja, o ideal gerado pelos termos líderes dos elementos de I*.*

Exemplo 3.1. *Seja* $I = \langle x^2 - y, x - y\rangle \subset K[x, y]$*. Temos então, considerando a ordem lexicográfica,*

$$\langle TL(x^2 - y), TL(x - y)\rangle = \langle x^2, x\rangle = \langle x\rangle$$

Porém, $y^2 - y \in I$*, pois*

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

mas seu termo líder não pertence a $\langle x\rangle$*.*

Isto é, $\langle TL(x^2 - y), TL(x - y)\rangle \neq \langle TL(I)\rangle$

Isto mostra que em geral $\langle TL(I)\rangle$ *pode ser estritamente maior que* $\langle TL(G)\rangle$ *onde* G *é um conjunto qualquer de geradores de* I.

3.2 Bases de Gröbner

3.2.1 Definições e exemplos

Definição 3.2. *Seja* I *um ideal de* $K[X]$. *Um subconjunto* finito $G = \{g_1, \cdots, g_t\} \subset I$ *é chamado de* ***base de Gröbner*** *para* I *se e somente se para todo* $f \in I$ *tal que* $f \neq 0$, *existe* $i \in \{1, \cdots, t\}$ *tal que* $TL(g_i)$ *divide* $TL(f)$.

Em outras palavras, se G é uma base de Gröbner para I, então o único polinômio em I reduzido módulo G é o polinômio nulo.

O Teorema a seguir nos dará outras definições para uma base de Gröbner, o que será de extrema relevância para provarmos alguns resultados importantes.

Teorema 3.1. *Seja* I *um ideal não nulo de* $K[X]$. *As seguintes sentenças são equivalentes para um conjunto de polinômios não nulos* $G = \{g_1, \cdots, g_t\} \subseteq I$.

(i) G *é uma base de Gröbner.*

(ii) $f \in I$ *se e somente se* $f \xrightarrow{G}_+ 0$.

(iii) $f \in I$ *se e somente se* $f = \sum_{i=1}^{t} h_i g_i$ *com* $TL(f) = max_{1 \leq i \leq t}\{TL(h_i)TL(g_i)\}$.

(iv) $\langle TL(G)\rangle = \langle TL(I)\rangle$

Demonstração. $(i) \Rightarrow (ii)$. Vamos supor, primeiramente, que $f \xrightarrow{G}_+ 0$. Logo, pela proposição 2.6

$$f = h_1 g_1 + h_2 g_2 \ldots + h_s g_s + 0$$

e portanto, como $G \subset I$, $f \in I$. Por outro lado se $f \in I$ e $f = h_1 g_1 + h_2 g_2 \ldots + h_s g_s + r$ temos que $r \in I$. Pela proposição 2.6, r é reduzido módulo G. Pela definição, 3.2 , de base de Gröbner, r é necessariamente o polinômio nulo.

$(ii) \Rightarrow (iii)$. Para $f \in I$, sabemos por hipótese que $f \xrightarrow{G}_+ 0$, e como o processo de redução é exatamente o mesmo do Algoritimo da Divisão, teremos

$$f = h_1 g_1 + h_2 g_2 + \cdots + h_t g_t + 0$$

logo, cada termo de f será do tipo $h_i g_i$ para $1 \leq i \leq t$. Desta maneira, o $TL(f)$ deverá ser o maior produto do tipo $TL(h_i)TL(g_i)$.

$(iii) \Rightarrow (iv)$. Claramente, $\langle TL(G)\rangle \subseteq \langle TL(I)\rangle$. Para a volta, é suficiente que mostremos que para todo $f \in I$, $TL(f) \in \langle TL(G)\rangle$, já que os $TL(f)$ geram $\langle TL(I)\rangle$. Escrevendo f como na hipótese, segue de imediato que

$$TL(f) = max\{TL(h_i)TL(g_i)\},$$

onde o somatório é sobre todo i tal que $TL(f) = TL(h_i)TL(g_i)$. O resultado segue imediatamente.

$(iv) \Rightarrow (i)$. Seja $f \in I$. Então $TL(f) \in \langle TL(G)\rangle$, e portanto

$$TL(f) = \sum_{i=1}^{t} h_i TL(g_i),$$

para algum $h_i \in K[X]$. Se expandirmos o lado direito da equação acima, vemos que cada termo é divisível por algum $TL(g_i)$. Portanto $TL(f)$, o único termo do lado esquerdo, é também divisível por algum $TL(g_i)$, como queríamos. □

Corolário 3.1. *Se $G = \{g_1, \cdots, g_t\}$ é uma base de Gröbner para o ideal I, então*

$$I = \langle g_1, \cdots, g_t\rangle.$$

Demonstração. Claramente $\langle g_1, \cdots, g_t\rangle \subseteq I$, já que cada $g_i \in I$. Para a volta, seja $f \in I$. Pelo Teorema 3.1, $f \xrightarrow{G}_+ 0$ e portanto $f \in \langle g_1, \cdots, g_t\rangle$. □

Vejamos agora exemplos de base de Gröbner.

Exemplo 3.2. *Considere os polinômios*

$$\begin{array}{rcl} g_1 & = & z+x \\ g_2 & = & y-x \end{array} \quad \in \mathbb{Q}[x,y,z]$$

Sejam $G = \{g_1, g_2\}$ *e* $I = \langle G \rangle$*. Considerando a ordem lexicográfica em* $\mathbb{Q}[x,y,z]$ *com* $x < y < z$*. Vamos provar que* G *é uma base de Gröbner para* I*.*

Suponha, por contradição, que existe $f \in I$ *tal que*

$$TL(f) \notin \langle TL(g_1), TL(g_2) \rangle = \langle z, y \rangle.$$

Então, z *não divide* $TL(f)$*, e* y *não divide* $TL(f)$*. Portanto, pela ordem determinada,* z *e* y *não aparecem em nenhum termo de* f*, logo* $f \in \mathbb{Q}[x]$*.*

Seja $f = (z+x)h_1 + (y-x)h_2$*, onde* $h_1, h_2 \in \mathbb{Q}[x,y,z]$*. Como* y *não aparece em* f*, devemos fazer* $h_2 = 0$*, assim teremos*

$$f = (z+x).h_1(x,x,z)$$

e, portanto, $z + x$ *divide* f*, o que é uma contradição pois* $f \in \mathbb{Q}[x]$*.*

Logo,

$$TL(f) \in \langle TL(g_1), TL(g_2) \rangle$$

isto é, G *é uma base de Gröbner para* I*.* □

É muito importante observar que uma base de Gröbner em relação a uma ordem monomial, pode não ser uma base de Gröbner se considerarmos outra ordenação.

No exemplo 3.2, acima, se tomarmos a ordem lexicográfica com $x > y > z$, veremos que $G = \{g_1, g_2\}$ não será mais uma base de Gröbner para I.

De fato, tomando $f = z + y \in I$,

$$TL(f) = y \notin \langle TL(g_1), TL(g_2) \rangle = \langle x \rangle.$$

isto é, $\langle TL(G) \rangle \neq \langle TL(I) \rangle$. Ou seja, G não é uma base de Gröbner para I.

Exemplo 3.3. *Consideremos $\mathbb{Q}[x, y]$ com a ordem lexicográfica graduada, com $x > y$.*

Sejam

$$f_1 = x^3 - 2xy \;\; e \;\; f_2 = x^2y - 2y^2 + x$$

ambos em $\mathbb{Q}[x, y]$. Tomemos $F = \{f_1, f_2\}$ e $I = \langle F \rangle$ um ideal.

Vemos que F não é uma base de Gröbner para I. De fato,

$$f_1.y - f_2.x = -x^2 \in I,$$

mas $x^2 \notin \langle TL(f_1), TL(f_2) \rangle = \langle x^3, x^2y \rangle$

Agora, seja

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

uma base de Gröbner para I. Ao adicionarmos os dois polinômios f_1 e f_2 ao conjunto G, teremos o conjunto

$$G_* = \{\ x^3 - 2xy\ ,\ x^2y - 2y^2 + x\ ,\ x^2\ ,\ 2xy\ ,\ 2y^2 - x\ \}$$

que também é uma base de Gröbner para I.

Podemos observar que no exemplo acima, mostramos duas bases de Gröbner diferentes para um mesmo ideal. Em outras palavras, uma base de gröbner para um ideal não é unicamente determinada. Mais ainda, pode-se adicionar vários polinômios a uma base de Gröbner, que mesmo assim ela continuará sendo uma base de Gröbner. Na verdade, essa não unicidade não é algo desejável, e é por essa razão que impondo algumas restrições na escolha dos polinômios do conjunto G, conheceremos mais a frente as bases de Gröbner reduzidas.

3.2.2 Existência das Bases de Gröbner

Agora, veremos o principal Teorema deste trabalho, resultado esse que garantirá o sucesso da nossa busca por uma base especial, o *Teorema de existência das Bases de Gröbner*.

Seguiremos a demonstração utilizada por André Vieira Costa e Israel Vainsencher em *Bases de Gröbner: Resolvendo Equações Polinomiais* [4], onde, ao contrário de outros textos da bibliografia, utilizam o Teorema da existência das bases de Gröbner para provar, aqui como

corolário, o *Teorema da Base de Hilbert*, que prova que todo ideal em $K[X]$ é finitamente gerado.

Proposição 3.1. *Seja $I \subseteq K[X]$ um ideal monomial. Então I admite uma base finita, i.e., existe um subconjunto finito de monômios $F \subseteq I$ tal que $I = \langle F \rangle$. Mais ainda, tal conjunto pode ser extraído de qualquer conjunto de monômios que gere I.*

Demonstração. (Por indução sobre o número n de variáveis) O caso n=1 é imediato pelo já visto que todo ideal em $K[x]$ é gerado por um único elemento. Agora, para a etapa indutiva, vamos supor verdadeiro para $K[X]$ e adicionaremos uma nova variável y, considerando o ideal $I \subseteq K[X][y]$. Podemos supor $I \neq \langle 0 \rangle$. Assim, existe $f_1 = f_1^*(X)y^{d_1} \in I/\langle 0 \rangle$, onde $f_1^*(X) \in K[X]$ denota um monômio e d_1 é mínimo. Agora, se $I = \langle f_1 \rangle$, nada mais temos a provar. Senão, escolhemos $f_2 = f_2^*(X)y^{d_2} \in I/\langle f_1 \rangle$, onde novamente $f_2^*(X) \in K[X]$ denota um monômio e d_2 é mínimo, sendo $d_2 \geq d_1$, caso contrário a escolha de f_1 teria sido mal feita. Se I não fosse finitamente gerado, poderíamos prosseguir na escolha de uma sequência infinita $f_1, f_2, \cdots$ com cada

$$f_m = f_m^*(X)y^{d_m} \in I/\langle f_1, \cdots, f_{m-1} \rangle,$$

onde $f_m^*(X) \in K[X]$ denota um monômio e d_m é mínimo. Seja $I^* \subseteq K[X]$ o ideal gerado por $f_1^*, \cdots, f_m^*, \cdots$. Pela hipótese de indução, existe N tal que $I^* = \langle f_1^*, \cdots, f_N^* \rangle$. Em particular, teremos o monômio $f_{N+1}^* \in I^*$, e portanto divisível por algum dos anteriores, digamos $f_{N+1}^* = g.f_m^*$ com $1 \leq m \leq N$ e $g \in K[X]$. Lembrando que na sequência dos graus tínhamos $d_m \leq d_{m+1} \leq \cdots$ podemos escrever

$$f_{N+1} = f_{N+1}^* y^{d_{N+1}} = g f_m^* y^{d_{N+1}} = g y^{d_{N+1}-d_m}(f_m^* y^{d_m})$$

mostrando que $f_{N+1} \in \langle f_m \rangle \subseteq \langle f_1, \cdots, f_N \rangle$ o que é uma contradição.

Agora, Seja $M \subseteq I$ um conjunto de monômios tal que $I = \langle M \rangle$ e seja $F = \{f_1, \cdots, f_N\}$ um conjunto fininto de geradores de I. Desprezando alguns elementos se necessário, podemos supor que nenhuma relação de divisibilidade ocorre entre os elementos de F, isto é, $f_i = g f_j$ com $g \in K[X] \Rightarrow f_i = f_j$. Provaremos que $F \subseteq M$. Com efeito, temos f_1 divisível por algum $g \in M$, digamos $f_1 = g.h$ para algum $h \in K[X]$. Temos igualmente

$g = f_i.q$ para algum $q \in K[X]$, $f_i \in F$. Logo f_i divide f_1. Por não haver divisão em F, segue que $f_1 = f_i$. Das relações $g = f_1 q = ghq$ (lembrando que g e f_1 são monômios) deduzimos que $h = q = 1$ e $f_1 = g \in M$. □

Teorema 3.2. *Seja $I \subseteq K[X]$ um ideal (não necessariamente monomial). Então I admite uma base de Gröbner G.*

Demonstração. Seja o ideal monomial $\langle TL(I)\rangle$, dos termos líderes de I, pela proposição anterior existe $G^* = \{g_1^*, \cdots g_t^*\} \subseteq TL(I)$, finito, tal que $\langle TL(I)\rangle = \langle G^*\rangle$.

Como $G^* \subseteq TL(I)$, existem $g_1, \cdots, g_s \in I$ tais que $g_i^* = TL(g_i)$.

Agora, seja $G = \{g_1, \cdots, g_s\}$, podemos escrever que $\langle TL(I)\rangle = \langle TL(G)\rangle$, isto é, pela definição de base de Gröbner, G é uma base de Gröbner de I. □

Corolário 3.2 (Teorema da Base de Hilbert). *Todo ideal $I \subseteq K[x_1, \cdots, x_n]$ é finitamente gerado.*

Demonstração. Segue imediato do Teorema 3.2. □

3.2.3 Base de Gröbner Reduzida

Vimos, até aqui, que as Bases de Gröbner existem, porém não são únicas, o que pode tornar tudo mais trabalhoso do que o desejado. Por isso, precisamos definir algumas restrições quanto a escolha dessas bases. Faremos isso, restringindo os polinômios pertencentes as bases de Grobner

Definição 3.3. *Uma base de Gröbner $G = \{g_1, \cdots, g_t\}$ é chamada de **base de Gröbner mínima** se para todo i, $CL(g_i) = 1$ e para todo $i \neq j$, $TL(g_i)$ não divide $TL(g_j)$.*

Lema 3.1. *Seja $G = \{g_1, \cdots, g_t\}$ uma base de Gröbner para um ideal I. Se $TL(g_2)$ divide $TL(g_1)$, então $\{g_2, \cdots, g_t\}$ também é uma base de Gröbner.*

Demonstração. Claramente, se um polinômio f é tal que $TL(f)$ é divisível por $TL(g_1)$, então é divisível também por $TL(g_2)$. Portanto , usando a Definição 3.2, $\{g_2, \cdots, g_t\}$ é uma base de Gröbner para I. □

Agora, uma consequência direta desse lema é como conseguimos obter uma base de Gröbner mínima de uma base de Gröbner.

Corolário 3.3. *Seja $I \subseteq K[X]$ um ideal. Então I admite uma base de Gröbner mínima.*

Demonstração. Seja $G = \{g_1, \cdots, g_t\}$ uma base de Gröbner para o ideal I. Ao retirarmos de G todo polinômio g_i para os quais existem $j \neq i$ tal que $TL(g_j)$ divide $TL(g_i)$ e dividindo cada g_i restante pelo $CL(g_i)$, pelo Lema 3.1 e pela definição 3.3, obtemos uma base de Gröbner mínima. □

Proposição 3.2. *Se $G = \{g_1, \cdots, g_t\}$ e $F = \{f_1, \cdots, f_s\}$ são bases de Gröbner mínimas para um ideal I, então $s = t$ e após renumeradas se necessário, $TL(f_i) = TL(g_i)$ para todo $i = 1, \cdots, t$.*

Demonstração. Como f_1 pertence a I e G é uma base de Gröbner para I, existe i tal que $TL(g_i)$ divide $TL(f_1)$. Após renumerarmos se necessário, podemos tomar $i = 1$. Agora, g_1 pertence também a I, e portanto, como F é uma base de Gröbner para I, existe j tal que $TL(f_j)$ divide $TL(g_1)$. Então $TL(f_j)$ divide $TL(f_1)$, e portanto, como F é uma base de Gröbner mínima, $j = 1$. Logo, $TL(f_1) = TL(g_1)$.

Agora f_2 pertence a I, e portanto existe i tal que $TL(g_i)$ divide $TL(f_2)$, pois G é uma base de Gröbner. A minimalidade de F e o fato de $TL(g_1) = TL(f_1)$ implica em $i \neq 1$, e, após renumerarmos se necessário, podemos tomar $i = 2$. Como anteriormente, pegamos $TL(g_2) = TL(f_2)$. Esse processo continua até esgotarmos todos os f's e g's. Logo, após renumerarmos $TL(f_i) = TL(g_i)$ para todo $i = 1, \cdots, t$, teremos $s = t$. □

Como foi dito no corolário acima, uma base de Gröbner mínima não é única. Para termos essa unicidade, precisamos adicionar uma condição mais forte aos polinômios da base de Gröbner. Essa unicidade será de fundamental importância nas aplicações da base de Gröbner.

Definição 3.4. *Uma base de Gröbner $G = \{g_1, \cdots, g_t\}$ é chamada de **base de Gröbner reduzida** se, para todo i, $CL(g_i) = 1$ e g_i é reduzido em relação a $G - \{g_i\}$. Isto é, para todo i, nenhum termo não nulo em g_i é divisível por qualquer $TL(g_j)$ com $j \neq i$.*

Observe que uma base de Gröbner reduzida é também mínima. Agora, vamos provar que as bases de Gröbner reduzidas existem.

Corolário 3.4. *Seja $G = \{g_1, \cdots, g_t\}$ uma base de Gröbner mínima para o ideal I. Vamos considerar o seguinte processo de redução:*

$g_1 \xrightarrow{H_1}_+ h_1$, *onde* h_1 *é reduzido módulo* $H_1 = \{g_2, \cdots, g_t\}$

$g_2 \xrightarrow{H_2}_+ h_2$, *onde* h_2 *é reduzido módulo* $H_2 = \{h_1, g_3, \cdots, g_t\}$

$g_3 \xrightarrow{H_3}_+ h_3$, *onde* h_3 *é reduzido módulo* $H_3 = \{h_1, h_2, g_3, \cdots, g_t\}$

$\vdots$

$g_t \xrightarrow{H_t}_+ h_t$, *onde* h_t *é reduzido módulo* $H_t = \{h_1, h_2, \cdots, h_{t-1}\}$

Então $H = \{h_1, \cdots, h_t\}$ é uma base de Gröbner reduzida.

Demonstração. Observe que, como G é uma base de Gröbner mínima, temos que $TL(h_i) = TL(g_i)$ para cada $i = 1, \cdots, t$. Daí, H também é uma base de Gröbner para I (mínima). Como a divisão de g_i por $h_1, \cdots, h_{i-1}, g_{i+1}, \cdots, g_t$ é feita eliminando os termos de g_i utilizando $TL(h_1), \cdots, TL(h_{i-1}), TL(g_{i+1}), \cdots, TL(g_t)$, e como $TL(h_j) = TL(g_j)$, para todo j, H é uma base de Gröbner reduzida. □

Teorema 3.3 (Buchberger)**.** *Fixada uma ordem monomial. Então todo ideal I, não nulo, possui uma única base de Gröbner reduzida em relação a esta ordem monomial.*

Demonstração. Acabamos de provar que todo ideal possui uma base de Gröbner reduzida. Portanto, vamos provar a sua unicidade. Seja $G = \{g_1, \cdots, g_t\}$ e $H = \{h_1, \cdots, h_t\}$ bases de Gröbner reduzidas de I. Observemos que pela Proposição 3.2, como uma base de Gröbner reduzida é mínima, tanto G como H possuem o mesmo número de elementos, logo reordenando os elementos de G e H de maneira conveniente, podemos tomar $TL(g_i) = TL(h_i)$ para cada i. Agora, vamos mostrar que $h_i = g_i$ para todo $1 < i < t$.

Suponha por absurdo que $h_1 \neq g_1$. Então $g_1 - h_1 \in I$ não nulo. Como H é uma base de Gröbner existe h_j tal que $TL(h_j) \,|\, TL(g_1 - h_1)$.

Como $TL(g_1 - h_1) < TL(h_1)$, pois $TL(g_1) = TL(h_1)$ temos que $j \neq 1$. Como $TL(g_1 - h_1)$ é igual a $c.T(g_1)$ ou $c.T(h_1)$ onde $c \in K$, temos que $TL(h_j)$ divide $T(h_1)$ ou $TL(h_j)$ divide $T(g_1)$. O primeiro caso contradiz o fato de que H é uma base de Gröbner reduzida e o segundo caso contradiz o fato de que G é uma base de Gröbner reduzida pois $TL(h_j) = TL(g_j)$ com $j \neq 1$. E portanto devemos ter $h_1 = g_1$.

De forma análoga podemos provar que $h_i = g_i$ para todo $1 < i < t$.

□

3.2.4 Algoritmo de Buchberger

Em todos os exemplos e resultados deste capítulo, não calculamos, efetivamente, as bases de Gröbner, simplesmente provamos a existência e verificamos as bases previamente dadas.

Na verdade, até sabemos calcular bases de Gröbner para dois casos específicos. No caso linear, o conjunto dos polinômios obtidos, na eliminação gaussiana, pelo escalonamento de uma matriz associada a um sistema de equações, constitui uma base de Gröbner do ideal gerado pelos polinômios originais do sistema, sendo a ordenação das variáveis determinada pela posição ocupada por elas na matriz original. No caso de uma variável, a base de Gröbner do ideal gerado por alguns polinômios será o MDC desses polinômios, o qual calculamos com o algoritmo de Euclides, considerando, naturalmente, a ordenação pelo grau do polinômio.

Para o cálculo das bases de Gröbner no caso de várias variáveis, utiliza-se um algoritmo que, a grosso modo, pode ser visto como uma generalização do algoritmo de Euclides e da eliminação Gaussiana, o chamado *algoritmo de Buchberger*, apresentado em 1976, por Bruno Buchberger, que o inventou e provou sua finitude. Algoritmo esse que permitiu, por seu caráter computacional, com o avanço dos computadores, cálculos que antes seriam inviáveis pela extensão das contas, além do tempo dispensado. Atualmente, existe uma grande quantidade de softwares matemáticos, inclusive softwares livres, com pacotes específicos para o cálculo das bases de Gröbner, muitos deles baseados no algoritmo de Buchberger, alguns deles são: Singular, Cocoa, Maxima, Gap, Mathematica, Maple, sendo os quatro primeiro gratuitos e disponíveis para baixar na Internet.

Por nosso trabalho tratar da aplicação das bases de Gröbner, iremos omitir aqui, a exposição do referido algoritmo, assim como os resultados relacionados a ele. No entanto, encontra-

mos na bibliografia material onde podemos nos aprofundar neste estudo, como Loustaunau e Adams em [5] .

Portanto, utilizaremos um dos softwares citados, no caso, o Singular, para fazermos os cálculos. Explicitaremos sempre que necessário as funções utilizadas nas contas, além de disponibilizarmos um pequeno tutorial, no Apêndice.

3.2.5 Variedades Algébricas Afins e as Bases de Gröbner

Um dos principais resultados utilizados no nosso trabalho relaciona as variedades algébricas afins às bases de Gröbner. Vale ressaltar que iremos trabalhar somente com corpos algebricamente fechados. Lembrando que um corpo é *algebricamente fechado* se para todo polinômio $f \in K[x]$ em uma variável, a equação $f = 0$ possui solução em K. Assim, em todos os exemplos daqui em diante iremos considerar o corpo dos números complexos $\mathbb{C}$.

Teorema 3.4 (Teorema dos zeros de Hilbert)**.** *Seja I um ideal contido em $K[X]$. Então $V_{\overline{K}}(I) = \emptyset$ se e somente se $I = K[X]$.*

Demonstração. Ver em [6] pág. 82.

□

Teorema 3.5. *Seja $I \subset K[X]$ um ideal e seja $G = \{g_1, \cdots, g_t\}$ uma base de Gröbner reduzida para I em relação a uma ordem monomial fixada. Então, $V_{\overline{K}}(I) = \emptyset$ se e somente se $G = \{1\}$.*

Demonstração. Pelo Teorema 3.4, $V_{\overline{K}}(I) = \emptyset$ se e somente se $I = K[X]$. Mas isto é o mesmo de dizer que $1 \in I$, já que pela definição de ideal $f = f.1 \in I$ para todo $f \in K[X]$. Agora, como $G = \{g_1, g_2, \cdots, g_t\}$ é uma base de Gröbner reduzida para I, temos que

$$\langle TL(I)\rangle = \langle TL(g_1), TL(g_2), \cdots, TL(g_t)\rangle$$

Como $1 \in \langle TL(I)\rangle$, então $1 \in \langle TL(g_1), TL(g_2), \cdots, TL(g_t)\rangle$ e pelo Lema 2.3 temos que 1 é divisível por algum $TL(g_i)$, digamos $TL(g_1)$. Isso obriga que g_1 seja um polinômio constante. Mas como todo $TL(g_i)$ é múltiplo de uma constante, então $g_2, \cdots, g_t$ podem ser removidos da base de Gröbner G, pelo Corolário 3.3.

Como $TL(g_1)$ é constante, temos que o próprio g_1 é uma constante, já que todo monômio não constante é maior do que 1. Assim, como G é uma base de Gröbner reduzida, por definição temos que g_1 é mônico, isto é, $TL(g_1) = 1$. Portanto, $G = \{1\}$.

Por outro lado, se $G = \{1\}$, temos que $I = \langle 1 \rangle$, e obviamente, $1 \in I$. Novamente, pelo Teorema 3.4, concluímos que

$$V_{\overline{K}}(I) = \emptyset.$$

□

3.2.6 Exemplos

Exemplo 3.4. *Vejamos como resolver o sistema abaixo, em* $\mathbb{C}[x, y, z]$*:*

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

Primeiramente, vamos considerar $f_1 = x^2 + y^2 + z^2 - 1$*,* $f_2 = x^2 - 2x + y^2 + z^2 - 1$ *e* $f_3 = 2x^3 - 3x^2y - x^2z$ *polinômios em* $\mathbb{C}[x, y, z]$ *e tomar o ideal* $I = \langle f_1, f_2, f_3 \rangle$*, considerando a ordem lexicográfica. Utilizando o SINGULAR, calculamos a base de Gröbner reduzida para este ideal, com os seguintes comandos:*

```
> ring C = complex,(x,y,z), lp ;
> ideal I = x2+y2+z2-1 , x2-2x+y2+z2 , 2x3-3x2y-x2z ;
> option(redSB) ;
> ideal G = groebner(I);
> G ;
```

Obtemos,

$$G = \left\{ z^2 - \frac{1}{5}z - \frac{5}{8} \ , \ y + \frac{1}{3}z - \frac{1}{3} \ , \ x - \frac{1}{2} \right\}.$$

Como $G \neq \{1\}$ *então* $V(I) \neq \emptyset$*, ou seja, nosso sistema possui solução. Calculando, então, a variedade de* G*, por substituição, obtemos as duas soluções do sistema:*

$$V(G) = \left\{ \left(\frac{1}{2}, \frac{18+\sqrt{254}}{60}, \frac{2-\sqrt{254}}{20} \right), \left(\frac{1}{2}, \frac{18-\sqrt{254}}{60}, \frac{2+\sqrt{254}}{20} \right) \right\}$$

Exemplo 3.5. *Agora, vejamos outro sistema, também em* $\mathbb{C}[x, y, z]$*:*

$$\begin{cases} x^3y + xz + y^2 = 5 \\ -x^2 + xyz^4 + y^3z = -1 \\ xy + y^3 - yz = 2 \\ x^5 + xy^7z^2 + yz^2 = -2 \end{cases}$$

Vamos considerar o ideal gerado pelos polinômios, em $\mathbb{C}[x, y, z]$, $f_1 = x^3y + xz + y^2 - 5$, $f_2 = -x^2 + xyz^4 + y^3z + 1$, $f_3 = xy + y^3 - yz - 2$ e $f_4 = x^5 + xy^7z^2 + yz^2 + 2$.

Utilizando novamente o SINGULAR, calculamos a base de Gröbner reduzida para este ideal, obtendo $G = \{1\}$, o que significa que $V(I) = \emptyset$, ou seja, o sistema não possui solução

CAPÍTULO 4

APLICAÇÃO EM K-COLORAÇÃO DE GRAFOS

Neste capítulo vamos aplicar as bases de Gröbner para resolver um problema bastante conhecido da matemática discreta, chamado k-coloração de grafos.

Primeiramente vamos fazer uma breve introdução sobre o que vem a ser um grafo, e uma k-coloração. Vale ressaltar que a teoria de grafos é bastante extensa, portanto vamos restringir essa introdução as definições e resultados os quais iremos utilizar.

Para esse capítulo utilizamos basicamente como bibliografia os livros de Bondy-Murty ([7]), Wallis ([8]) e Feofiloff-Kohayakawa-Wakabayashi ([9]), este último em português, disponível na internet. Para o leitor que desejar conhecer mais sobre Grafos, encontrará na bibliografia citada material suficiente.

4.1 Grafos

Muitas situações do dia a dia podem ser descritas como diagramas consistindo de um conjunto de pontos com linhas unindo pares desses pontos. Por exemplo, os pontos podem representar pessoas, com as linhas unindo pares de amigos; ou os pontos podem ser telefones, com as linhas representando uma ligação. Observe que nesses diagramas o que mais interessa é se dois pontos dados estão unidos por uma linha; a maneira de como estão unidos é irrelevante. Na Matemática, situações como essas nos levam ao conceito de um grafo.

4.1.1 Definições e exemplos

Definição 4.1. *Um **grafo***[1] $\mathcal{G}$ *é um par* (V, A) *consistindo de um conjunto* V *(chamado de vértices), e um conjunto* A *(chamado de arestas), subconjunto de* $V^{(2)} = \Big\{\{u, v\} \mid u, v \in V, u \neq v\Big\}$. *Denotaremos uma aresta* $\{u, v\}$ *simplesmente por* uv *ou por* vu.

Definição 4.2. *Se* uv *é uma aresta, então dizemos que* uv *incide em* u *e em* v*, e os vértices* u *e* v *são chamados de* pontas da aresta.

Definição 4.3. *Se* uv *é uma aresta, diremos que os vértices* u *e* v *são vizinhos ou adjacentes.*

Vale ressaltar que pela definição de grafo dada acima não há duas arestas diferentes com as mesmas pontas (ou seja, não existem arestas paralelas). Também não pode ter uma aresta com pontas coincidentes (ou seja,não existem laços).

Algumas vezes é necessário que o conjunto dos vértices e das arestas de um grafo $\mathcal{G}$ seja representado referindo-se a qual grafo pertencem, dessa maneira denotaremos $V(\mathcal{G})$ e $A(\mathcal{G})$ como sendo o conjunto dos vértices e de arestas de $\mathcal{G}$, respectivamente.

Exemplo 4.1. *Em um tabuleiro de xadrez podemos olhar as casas como sendo os vértices de um grafo. Dizemos que dois vértices são adjacentes se uma dama do jogo pode saltar de um deles para o outro em um só movimento. Este é o grafo dos movimentos da dama, ou simplesmente,o grafo da dama. Para deixar claras as dimensões do tabuleiro, podemos dizer que esse é o grafo da dama 8 por 8.*

4.1.2 Desenho de um Grafo

Grafos são chamados assim porque podem ser representados graficamente, e é exatamente a sua representação gráfica que nos permite entender muitas de suas propriedades. Cada vértice é indicado por um ponto e cada aresta uma linha que une suas pontas. Não existe uma única maneira correta de se desenhar um grafo; geralmente, não há um posicionamento obrigatório dos pontos ou formas específicas das linhas representantes das arestas. O diagrama de um grafo serve meramente para nos mostrar as relações entre os vértices e as

[1] Encontramos na bibliografia esta definição como sendo a de um *grafos simples*.

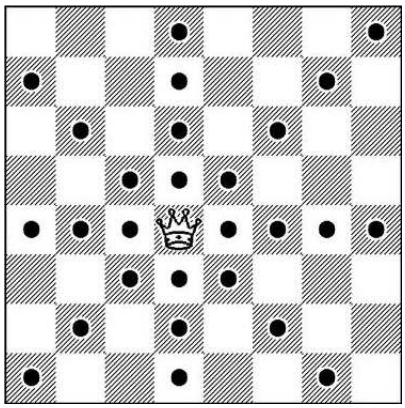


Figura 4.1: grafo da dama

arestas. No entanto, geralmente nos referimos ao diagrama do grafo como sendo o próprio grafo; dessa forma, chamamos seus pontos de ”vértices”e suas linhas de ”arestas”.

Exemplo 4.2. *O grafo dos estados do Brasil é definido assim: cada vértice é um dos estados da República Federativa do Brasil; dois estados são adjacentes se têm uma fronteira comum.*

4.2 Coloração de Grafos

Em muitas áreas da Matemática, a busca de soluções para problemas não resolvidos conduziram o desenvolvimento de idéias e técnicas. No caso da teoria dos grafos, um problema aparentemente inofensível de coloração de mapas motivou seu desenvolvimento por muitos anos. Este problema teve origem, em 23 de Outubro de 1852, na correspondência entre Hamilton e Augusto De Morgan, problema esse levantado por Francis Guthrie, aluno de De Morgan. O enunciado era aproximadamente o seguinte: *”porque razão, quando dividimos qualquer figura em zonas coloridas, de modo que duas zonas que tenham fronteira comum fiquem com cores diferentes, precisamos, no máximo, de quatro cores”*. Esse problema é conhecido como *Problema das 4 cores.*

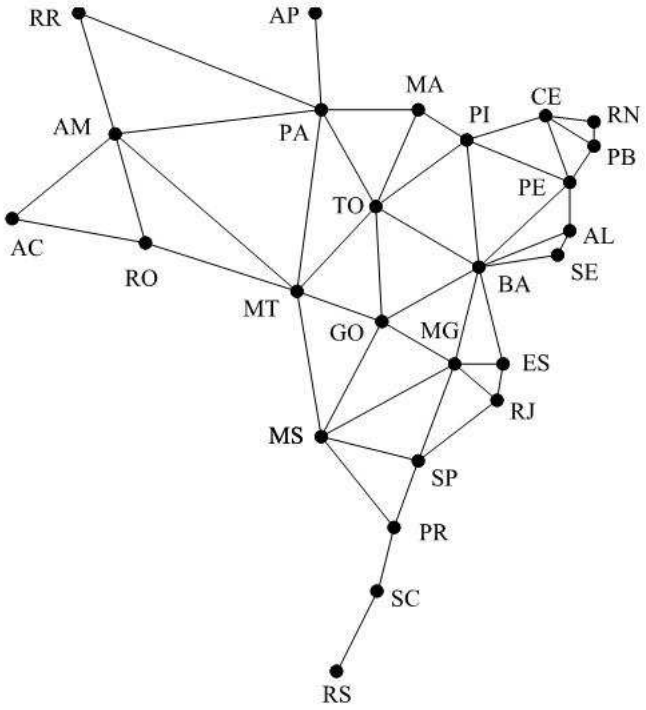


Figura 4.2: grafo dos estados do Brasil

4.2.1 Coloração de vértices

Ao traduzirmos este ”Problema das 4 cores”para a linguagem da teoria dos grafos, podemos considerar o mapa como um grafo, onde cada face do mapa é um vértice, e duas faces que façam fronteira sejam ligadas por uma aresta. Desta maneira vamos associar uma cor para cada vértice, lembrando que dois vértices unidos por uma aresta não possuem a mesma cor. Vejamos as duas figuras abaixo, mostrando o mapa do Brasil colorido e o seu grafo correspondente também colorido.

Definição 4.4. *Uma C-**coloração de um grafo** é a atribuição de cores aos vértices de um grafo. De maneira mais formal, suponha $C = \{c_1, c_2, \cdots c_k\}$ um conjunto de objetos chamados cores. Uma C-coloração de um grafo $\mathcal{G}$ é uma função*

$$\psi : V(\mathcal{G}) \to C.$$

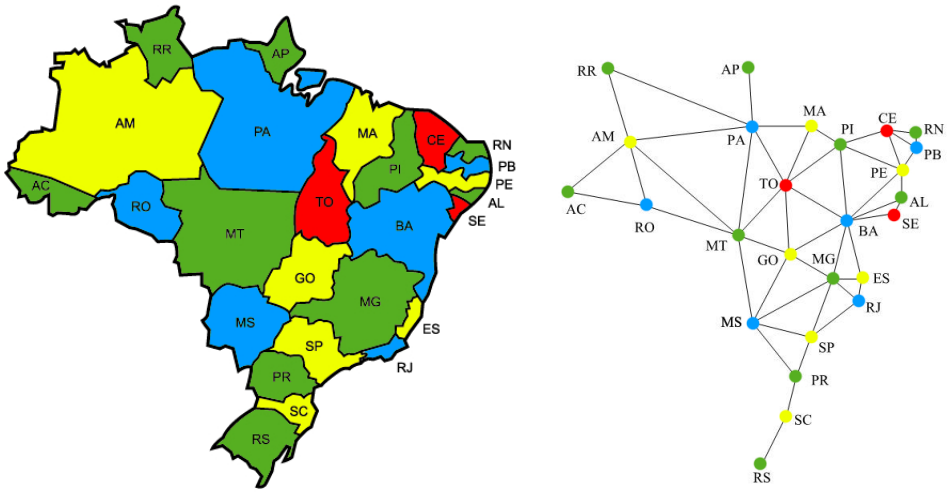


Figura 4.3: mapa do Brasil e seu grafo correspondente

Definição 4.5. *Uma coloração de $\mathcal{G}$ é dita **própria** se, numa coloração ψ de um grafo, dois vértices adjacentes não possuem a mesma cor.*

Definição 4.6. *Dizemos que uma coloração própria de $\mathcal{G}$ é chamada de k-coloração se C possui k elementos. Se $\mathcal{G}$ possui uma k-coloração, então $\mathcal{G}$ é dito k-colorável.*

Existem inúmeras situações, em diversas áreas, onde podemos considerá-las como um problema de k-coloração de um grafo para resolvê-las. Vejamos um deles no exemplo a seguir.

Exemplo 4.3. *Uma indústria produz n tipos de produtos químicos $v_1, \cdots, v_n$. Alguns destes produtos podem explodir se entrarem em contato com outros. Para previnir acidentes, a empresa quer construir k armazéns para armazenar os produtos químicos de tal forma que produtos incompatíveis fiquem em armazéns diferentes. Deseja-se saber qual é o menor número k de armazéns que devem ser construídos.*

Sabendo quais os produtos incompatíveis, podemos ver essa situação como um problema de k-coloração de um grafo, onde os produtos químicos são os vértices e os armazéns são as cores. Os produtos incompatíveis, que não podem ficar no mesmo armazém, são unidos por arestas, e portanto vértices adjacentes não podem ter a mesma cor.

Definição 4.7. *O número cromático $\chi(\mathcal{G})$ de um grafo $\mathcal{G}$ é o menor inteiro k tal que $\mathcal{G}$ tem um k-coloração.*

Obviamente, $\mathcal{G}$ é n-colorável para todo $n \geq \chi(\mathcal{G})$.

Definição 4.8. *Um grafo é planar se pode ser desenhado no plano sem que as curvas que representam arestas se cruzem.*

Teorema 4.1 (Teorema das quatro cores)**.** *Se um grafo $\mathcal{G}$ é planar então $\chi(\mathcal{G}) \leq 4$.*

Demonstração. Ver em [10] □

4.2.2 O problema da k-coloração

Este problema resume-se a determinar quando um grafo dado é k-colorável.

Primeiramente, faremos $\zeta = e^{\frac{2\pi i}{k}} \in \mathbb{C}$ a k-ésima raiz da unidade, ou seja, $\zeta^k = 1$. Representamos as k cores por $1, \zeta, \zeta^2, \cdots, \zeta^{k-1}$ as k raízes distintas da unidade. Agora, seja $x_1, \cdots, x_n$ as variáveis representando os distintos vértices do grafo $\mathcal{G}$. Cada vértice é associado a uma das k cores. Esse fato, pode ser representado pelas n equações seguintes

$$x_i^k - 1 = 0 \quad , \ 1 \leq i \leq n \tag{4.1}$$

Também, se os vértices x_i e x_j estão conectados, precisam ter cores diferentes. Como $x_i^k = x_j^k \implies x_i^k - x_j^k = 0$, teremos

$$x_i^k - x_j^k = (x_i - x_j)(x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i^{k-1-h}x_j^h + \cdots + x_i x_j^{k-2} + x_j^{k-1}) = 0$$

Portanto, x_i e x_j terão cores diferentes se e somente se

$$(x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i^{k-1-h}x_j^h + \cdots + x_i x_j^{k-2} + x_j^{k-1}) = 0 \tag{4.2}$$

Agora, seja o ideal $I_{\mathcal{G},k} \subset \mathbb{C}[x_1, \cdots, x_n]$ gerado pelos polinômios das equações 4.1 e 4.2.

Vamos considerar $V(I_{\mathcal{G},k}) \subset \mathbb{C}^n$ a variedade afim do ideal $I_{\mathcal{G},k}$. Assim:

Teorema 4.2. *O grafo $\mathcal{G}$ é k-colorável se e somente se $V(I_{\mathcal{G},k}) \neq \emptyset$*

Demonstração. Se $\mathcal{G}$ é k-colorável então cada vértice de $\mathcal{G}$ possui uma das k cores, isto é, existe ζ^i com $0 \leq i < k$ tal que as equações que dão origem aos polinômios de $I_{\mathcal{G},k}$ sejam satisfeitas, logo $V(I_{\mathcal{G},k}) \neq \emptyset$.

Agora, se $V(I_{\mathcal{G},k}) \neq \emptyset$, então existe algum ζ^i com $0 \leq i < k$ tal que os polinômios de $I_{\mathcal{G},k}$ sejam anulados, isto é, satisfazem as equações que originam os polinômios, e portanto dizemos que cada vértice possui uma das k cores. □

4.2.3 Sudoku

Voltando agora ao nosso exemplo principal, podemos enxergar o Sudoku como um grafo onde cada um dos 81 espaços é um vértice que vamos considerar estarem ligadas por arestas quando estiverem em uma mesma região(linha, coluna e bloco 3×3). Portanto, ao querer resolver este Sudoku encontramos um problema de k-coloração, mais precisamente de 9-coloração, isto é, vamos considerar cada algarismo de 1 a 9 como uma cor diferente associando a cada cor a uma das 9 raízes da unidade $\zeta_j \in \mathbb{C}$ onde $\zeta_j^9 = 1$ com $1 \leq j \leq 9$, e vamos colorir os 81 vértices sem que vértices ligados possuam a mesma cor.

Abaixo revemos o exemplo de um passatempo Sudoku a ser resolvido.

7		2		6				3
			7			2		
	4			2	1			9
		8					6	
4		3				1		2
	7					4		
8			9	4			1	
		7			3			
5				8		9		6

Figura 4.4: Sudoku

Novamente, o que faremos é associar o Sudoku a um sistema de equações polinomiais em várias variáveis (sobre os números complexos), já visto na Seção 2.3.2. Então devemos resolver o seguinte sistema de equações polinomiais complexas em 81 variáveis:

$$
\begin{cases}
{x_i}^9 - 1 = 0 \ , \quad 1 \leq i \leq 81 \\
\\
G_{i,j}(x_i, x_j) = 0 \ , \quad \{i,j\} \in A \\
\\
\begin{array}{llllll}
x_1 - \zeta_7 = 0 & , & x_3 - \zeta_2 = 0 & , & x_5 - \zeta_6 = 0 & , \quad x_9 - \zeta_3 = 0 \\
x_{12} - \zeta_7 = 0 & , & x_{16} - \zeta_2 = 0 & , & x_{20} - \zeta_4 = 0 & , \quad x_{23} - \zeta_2 = 0 \\
x_{24} - \zeta_1 = 0 & , & x_{27} - \zeta_9 = 0 & , & x_{30} - \zeta_8 = 0 & , \quad x_{35} - \zeta_6 = 0 \\
x_{37} - \zeta_4 = 0 & , & x_{39} - \zeta_3 = 0 & , & x_{43} - \zeta_1 = 0 & , \quad x_{45} - \zeta_2 = 0 \\
x_{47} - \zeta_7 = 0 & , & x_{52} - \zeta_4 = 0 & , & x_{55} - \zeta_8 = 0 & , \quad x_{58} - \zeta_9 = 0 \\
x_{59} - \zeta_4 = 0 & , & x_{62} - \zeta_1 = 0 & , & x_{66} - \zeta_7 = 0 & , \quad x_{69} - \zeta_3 = 0 \\
x_{73} - \zeta_5 = 0 & , & x_{77} - \zeta_8 = 0 & , & x_{79} - \zeta_9 = 0 & , \quad x_{81} - \zeta_6 = 0
\end{array}
\end{cases}
$$

Bem sabemos que resolver um sistema como esse, com 910 equações e 81 variáveis, sem o auxilio de um computador é inconcebível, portanto vamos utilizar o SINGULAR para resolvê-lo.

Vimos que ao utilizarmos o SINGULAR devemos, após determinar o anel de polinômios em que estamos trabalhando, entrar com os polinômios geradores do nosso ideal para então calculando a base de Gröbner reduzida obtermos um conjunto gerador onde podemos encontrar a solução de maneira mais evidente. No caso dos problemas de k-coloração de grafos, a base de Gröbner reduzida nos mostra geralmente a solução de maneira bem direta, como veremos neste exemplo.

Agora, mesmo utilizando um programa para fazer os cálculos, entrar com 910 polinômios já é uma tarefa bem trabalhosa. Por isso vamos utilizar um pacote do SINGULAR (librarie) chamado `sudoku.lib` (veja como no Apêndice A), o qual criamos a fim de aproveitarmos as equações e o procedimento do SINGULAR chamado *sudoku* escrito pelos autores do artigo *Sudokus and Gröbner bases: not only a Divertimento* em [11], procedimento esse disponível na Internet[2]. Convém ressaltar que o procedimento utilizado em [11] associa a cada cor um número inteiro de 1 a 9, enquanto nós associamos às raízes nonas da unidade, porém isso

[2] http://www-en.us.es/gmcedm/sudoku

não incorrerá em resultados distintos ao nosso. Por isso mesmo resolvemos utilizá-lo, já que assim podemos, em tempo hábil, aplicar tudo o que vimos neste trabalho, e ver que realmente funciona.

Vejamos como devemos utilizar o sudoku no SINGULAR:

```
> ring R = 0,x(1..81),Dp;
> LIB"sudoku.lib"
> intmat A[9][9] = 7,0,2,0,6,0,0,0,3,
  0,0,0,7,0,0,2,0,0,  0,4,0,0,2,1,0,0,9,
  0,0,8,0,0,0,0,6,0,  4,0,3,0,0,0,1,0,2,
  0,7,0,0,0,0,4,0,0,  8,0,0,9,4,0,0,1,0,
  0,0,7,0,0,3,0,0,0,  5,0,0,0,8,0,9,0,6;
> def G =sudoku(A);
> G;
```

O último comando nos retorna 81 polinômios do tipo $g_i = x_j - n$ que no formato do SINGULAR é $G[i] = x(j) - n$, onde temos que $1 \leq i, j \leq 81$ e $1 \leq n \leq 9$. Isso por que, como dissemos, são associados as cores os algarismos de 1 a 9. Vejamos:

$$
\begin{aligned}
G = \{&(x_{81}-6),\ (x_{80}-3),\ (x_{79}-9),\ (x_{78}-7),\ (x_{77}-8),\ (x_{76}-1),\ (x_{75}-4),\\
&(x_{74}-2),\ (x_{73}-5),\ (x_{72}-4),\ (x_{71}-2),\ (x_{70}-8),\ (x_{69}-3),\ (x_{68}-5),\\
&(x_{67}-6),\ (x_{66}-7),\ (x_{65}-9),\ (x_{64}-1),\ (x_{63}-5),\ (x_{62}-1),\ (x_{61}-7),\\
&(x_{60}-2),\ (x_{59}-4),\ (x_{58}-9),\ (x_{57}-6),\ (x_{56}-3),\ (x_{55}-8),\ (x_{54}-8),\\
&(x_{53}-5),\ (x_{52}-4),\ (x_{51}-6),\ (x_{50}-9),\ (x_{49}-3),\ (x_{48}-1),\ (x_{47}-7),\\
&(x_{46}-2),\ (x_{45}-2),\ (x_{44}-9),\ (x_{43}-1),\ (x_{42}-8),\ (x_{41}-7),\ (x_{40}-5),\\
&(x_{39}-3),\ (x_{38}-6),\ (x_{37}-4),\ (x_{36}-7),\ (x_{35}-6),\ (x_{34}-3),\ (x_{33}-4),\\
&(x_{32}-1),\ (x_{31}-2),\ (x_{30}-8),\ (x_{29}-5),\ (x_{28}-9),\ (x_{27}-9),\ (x_{26}-7),\\
&(x_{25}-6),\ (x_{24}-1),\ (x_{23}-2),\ (x_{22}-8),\ (x_{21}-5),\ (x_{20}-4),\ (x_{19}-3),\\
&(x_{18}-1),\ (x_{17}-4),\ (x_{16}-2),\ (x_{15}-5),\ (x_{14}-3),\ (x_{13}-7),\ (x_{12}-9),\\
&(x_{11}-8),\ (x_{10}-6),\ (x_9-3),\ (x_8-8),\ (x_7-5),\ (x_6-9),\ (x_5-6),\\
&(x_4-4),\ (x_3-2),\ (x_2-1),\ (x_1-7)\}.
\end{aligned}
$$

Calculamos facilmente a variedade $V(G)$, obtendo assim o valor de cada x_i, por exemplo, $x_{81} = 6$. Portanto, vemos claramente quais cores cada vértive deve possuir, ou ainda neste caso, com qual algarismo devemos preencher cada espaço no sudoku.

Para finalizar, vamos completar o sudoku 4.2.3 com os valores obtidos na variedade V(G).

7	1	2	4	6	9	5	8	3
6	8	9	7	3	5	2	4	1
3	4	5	8	2	1	6	7	9
9	5	8	2	1	4	3	6	7
4	6	3	5	7	8	1	9	2
2	7	1	3	9	6	4	5	7
8	3	6	9	4	2	7	1	5
1	9	7	6	5	3	8	2	4
5	2	4	1	8	7	9	3	6

Figura 4.5: Sudoku Resolvido

Referências Bibliográficas

[1] FRALEIGH, J. B. *A first course in abstract algebra*. Addison Wesley, 2002.

[2] GARCIA, A.; LEQUAIN, Y. *Álgebra: um curso de introdução*. Instituto de Matemática Pura e Aplicada, 1988.

[3] WELLS, C. Discrete mathematics. disponível em: http://www.cwru.edu/artsci/math/wells/home.html. 01 2010.

[4] VAINSENCHER, I.; COSTA, A. V. *Bases de gröbner : Resolvendo equações polinomiais*. Atas da XIII Escola de Álgebra, Campinas, julho 1994, 111-184, 1995.

[5] ADAMS, W.; LOUSTAUNAU, P. *An introduction to grobner bases*. Graduate Studies in Mathematics, Vol. 3 American Mathematical Society, 289, 2000.

[6] ATIYAH, M. F.; MACDONALD, I. *Introduction to commutative algebra*. Addison-Wesley Publishing Company, 1969.

[7] BONDY, J. A.; MURTY, U. *Graph theory*. Springer, 2008.

[8] W.D.WALLIS. *A beginner's guide to graph theory*. Birkhäuser, 2008.

[9] FEOFILOFF, P.; KOHAYAKAWA, Y.; WAKABAYASHI, Y. Uma introdução sucinta à teoria dos grafos. disponível em: http://www.ime.usp.br/ pf/teoriadosgrafos/. 01 2010.

[10] APPEL, K.; HAKEN, W. *Every planar map is four colorable*. Contemporany Mathematics, v.98, 1989.

[11] GAGO-VARGAS, J.; HARTILLO-HERMOSO, I.; MARTíN-MORALES, J. Sudokus and gröbner bases: not only a divertimento, 2006.

[12] DECKER, W.; GREUEL, G. M.; PFISTER, G.; SCHÖNEMANN, H. SINGULAR 3-1-2 — A computer algebra system for polynomial computations. 2010. http://www.singular.uni-kl.de.

[13] COX, D.; LITTLE, J.; O'SHEA, D. *Ideals, varieties, and algorithms*. Springer, 2007.

[14] DECKER, W.; LOSSEN, C. *Computing in algebraic geometry - a quick start using singular*. Springer, 2006.

[15] BUCHBERGER, B.; WINKLER, F. *Gröbner bases and applications*. London Mathematical Society Lecture Note Series 251, Cambridge University Press and the London Mathematical Society, 1998.

APÊNDICE A

SINGULAR

Neste apêndice, apresentamos um pequeno tutorial para o software SINGULAR, dando algumas noções básicas sobre as funcionalidades do programa, como instalá-lo e alguns comandos com o objetivo de permitir que o leitor possa também fazer os cálculos dos exemplos apresentados neste trabalho, especialmente o exemplo do Sudoku.

Baseamo-nos para a elaboração deste apêndice, basicamente, no livro *Computing in Algebraic Geometry (A Quick Start using SINGULAR)* de Wolfram Decker e Christoph Lossen [14].

A.1 Visão Geral

SINGULAR é um sistema computacional algébrico para cálculos polinomiais, visando a álgebra comutativa, geometria algébrica e teoria das singularidades. É um software de licença livre (gratuito), desenvolvido pela " equipe SINGULAR"(SINGULAR team) do Departamento de Matemática da Universidade de Kaiserslautern, na Alemanha, sob a direção de Gert-Martin Greuel, Gerhard Pfister e Hans Schönemann. disponível para download no site (em inglês):

http://www.singular.uni-kl.de

Para tanto devemos ir a seção *Download 3-1-2* (última atualização em 19/10/2010), onde escolhemos qual sistema operacional utilizamos, logo após selecionando o instalador desejado.

Para rodar no Windows, o SINGULAR utiliza um programa chamado CYGWIN que simula um abiente LINUX, portanto encontramos duas opções:

- para quem já possui o CYGWIN instalado;
- para instalar ambos os programas com um único instalador.

temos ainda, na segunda opção, que decidir entre uma *versão "completa"* (*full*) ou*"simplificada"* (*small*). Utilizaremos aqui a versão simplificada, por ser o suficiente para o nosso objetivo.

Podemos encontrar no site do SINGULAR, um manual em diversos formatos (somente em inglês), além de diversas publicações envolvendo o software.

Vamos considerar a partir deste ponto o sistema sendo executado no Windows, podendo haver assim algumas divergências de informações dependendo do sistema operacional utilizado pelo leitor.

A.2 *Libraries* e *Procedures*

O SINGULAR possui implementado em seu núcleo uma grande quantidade de algoritmos, além de permitir o uso de "pacotes"(*libraries*) compostos por procedinentos (*procedures*) que podem ser carregados a qualquer momento com um comando específico, todas escritas numa linguagem própria do software.

Por ter seu núcleo pré compilado na linguagem de programação C/C++, muito da sintaxe do SINGULAR assemelha-se a esta linguagem, utilizando, por exemplo, caracteres como:

- Para atribuições: $\langle$***variável***$\rangle = \langle$***valor***$\rangle$
- Para comparações: $==, <, >, !=$
- Para declaração condicional: **if, else**;
- Para loops: **for, while**
- Para blocos: $\{ \quad \}$
- Para comentários: **// , /* */**

Convém ressaltar que a linguagem do SINGULAR é interpretada, não compilada.

A.3 Utilizando o SINGULAR

Após a instalação concluída, devemos iniciar o programa escolhendo o ícone "SINGULAR (Terminal)", será assim aberta uma janela de fundo preto (semelhante a um prompt DOS), com o nome do programa, sua versão e o nome dos criadores, além de um prompt $>$ onde iremos digitar os comandos a serem executados. Importante ressaltar que cada comando deve ser finalizado com um ponto e vírgula (**;**).

Ao ser pressionada a tecla ENTER do teclado, o sistema executa o comando, apresentando o resultado (dependendo do comando) e abre um novo prompt de entrada. Vejamos alguns exemplos, sem a necessidade de muitos esclarecimentos:

$> 7 + 2 + 1;$

10

$>$

Podemos digitar um comando por entrada, ou até mesmo, vários comandos de uma vez, sempre finalizando cada um com o ponto e vírgula (**;**), obteremos assim cada linha como resposta a um dos comandos, obedecendo a ordem de entrada:

$> 2 + 5; 4 + 7;$

7

11

$>$

Ao executarmos o comando " **help;** "é aberto uma nova janela com um manual, em inglês, onde podemos encontrar diversas informações sobre o software, pacotes e procedimentos disponíveis, além de um index com todos os comandos do SINGULAR, muito útil para consultas de referência.

A maior parte dos pacotes (libraries) do SINGULAR não são acessadas diretamente, havendo a necessidade, como já foi dito, de carregá-las. Para isso utilizamos o comando:

```
> LIB ``sudoku.lib";   // carregando assim o pacote ``sudoku.lib"[1]
>
```

O SINGULAR oferece diversos pacotes para cálculos em álgebra linear, álgebra comutativa, entre outras.

[1] Mais adiante criaremos esse pacote

O maior diferencial do SINGULAR em relação a outros sistemas de cálculo algébrico é a necessidade de definir, primeiramente, o anel em qual iremos trabalhar com os polinômios. Caso não seja definido nenhum anel, ao tentarmos efetuar a sequinte soma, o programa irá fornecer uma mensagem de erro, justamente atentando para a falta de um anel, como essa:

```
> 1/3+1/5;
    ? no ring active
    ? error occurred in STDIN line ... :' 1/3+1/5;'
```

A.3.1 Definindo Anéis de Polinômios

Para definirmos um anel de polinômio utilizamos o comando `ring`, onde nomeamos o anel (por exemplo, R), e ainda declaramos o anel dos coeficientes, as variáveis e a ordem monomial. Vejamos o exemplo:

```
> ring R = 0 , (x,y), dp;
```

Após definir um anel, podemos a qualquer momento ver tudo que foi declarado para o anel utilizando o comando R;.

```
> R;
// characteristic :  0
// number of vars :  2
// block 1 :  ordering dp
// :  names x y
// block 2 :  ordering C
```

Basicamente o SINGULAR utiliza para o anel dos coeficientes, os chamados *corpos primos* que são especificados por sua característica. Ao declarar 0 estamos no corpo $\mathbb{Q}$, dos números racionais. Ao colocarmos um número primo p estaremos declarando o corpo do $\mathbb{Z}_p$ com p elementos. Ao entrarmos com as palavras `real` ou `complex`, definimos o corpo dos números reais ou dos números complexos. Podemos ainda entrar com parâmetros, extendendo assim o corpo declarado. Vejamos alguns exemplos:

- $\mathbb{Q}[x_1, \cdots, x_7]$:

```
> ring R1 = 0, x(1..7), dp;
```

- $\mathbb{Q}(\sqrt{-1})[x, y]$:

  `> ring R2 = (0,i) , (x,y), dp;`

  `> minpoly =`$i^2 + 1$`;`

No anel `R2` do exemplo definimos o parâmetro i, nesse caso devemos especificar o polinômio mínimo com o comando `minpoly`, neste caso $i^2 + 1$.

Declarado o corpo dos coeficientes, definimos as variáveis que já vimos nos exemplos acima como fazemos, colocando-as entre parênteses, em ordem crescente. No caso de muitas variáveis definimos uma letra e entre parênteses colocamos o primeiro e o último índice desejado separado por dois pontos seguidos "..".

Quanto a ordem monomial a ser usada o SINGULAR já possui ordens pré-definidas, algumas delas são:

- `lp` - ordem lexicográfica;
- `Dp` - ordem lexicográfica graduada;
- `dp` - ordem lexicográfica inversa graduada;

Portanto se quisermos definir um anel de polinômios com 81 variáveis nos números complexos utilizando a ordem lexicográfica graduada, teremos:

```
> ring C = complex , x(1..81), Dp;
```

A.3.2 Definindo Polinômios e Ideais

Agora que já definimos um anel de polinômios, podemos definir elementos dentro destes anéis, para isso utlizamos o comando `poly` como no exemplo:

```
> ring C = complex , x(1..81), Dp;
```

`> poly f =`$x(1) + x(2) * x(3) - x(4)^2 + (x(15) * x(17))^3$

O SINGULAR ordena automaticamente o polinômio, dependendo da ordem escolhida. Assim o polinômio `f`$= x(15)^3 * x(17)^3 + x(2) * x(3) - x(4)^2 + x(1)$.

Agora, que já sabemos definir um polinômio vamos definir um ideal.

Existem três maneiras de se definir um ideal gerado por polinômios, ambas utilizam o comando `ideal`, vejamos:

```
> ring C = 0 , (x,y) , lp;
> ideal I = x2+3xy , xy4 - 7y3 - 5y2;
```

ou,

```
> ring C = 0 , (x,y) , lp;
> poly f = x2+3xy;
> poly g = xy4 - 7y3 - 5y2;
> ideal I = f, g;
```

ou ainda,

```
> ring C = 0 , (x,y) , lp;
> ideal I;
> I[1] = x2;
> I[2] = 7y - 5x2;
```

Convém observar que quando trabalhamos com variáveis compostas por uma letra podemos omitir o $*$ para contas de multiplicação assim com escrever um potência dele simplesmente colocando o número após a variável, portanto `3xy` = $3xy$ e `x2` = x^2.

A.3.3 Calculando Bases de Gröbner

Após definido um ideal, podemos querer calcular uma base de gröbner para esse ideal, para isso basta utilizarmos o comando `groebner` (ou ainda, `std;`) seguido do nome do ideal entre parênteses. Como no exemplo:

```
> ring C = 0 , (x,y) , lp;
> ideal I = x+y , y4 - y3 - y2;
> groebner(I);
```

Fazendo isso, o SINGULAR após os cálculos exibirá todos os polinômios da base. Devemos destacar que o tempo de resposta do comando dependenrá do tamanho e da complexidade do ideal.

Agora, se nessecitarmos de calcular uma base de Gröbner reduzida para esse ideal, devemos adicionar o comando `option(redSB);` antes do comando acima.

Outra observação é que podemos definir um ideal gerado por essa base de Gröbner, como vemos no próximo exemplo.

```
> ring C = 0 , (x,y) , lp;
> ideal I = x+y , y4 - y3 - y2;
> option(redSB);
> ideal G = groebner(I);
```

Desta forma, o ideal `G` é gerado pela base de Gröbner reduzida do ideal `I`.

Existe ainda um comando `simplify(G,1)` que quando necessário torna os polinômios da base obtida mônicos.

Vejamos um exemplo com tudo que vimos até aqui.

```
> ring R = 0, (x,y,z), lp;
> ideal I = 2y+z,3x-y;
> std(I);
 _[1]=2y+z
 _[2]=3x-y
> option(redSB);
> ideal G = std(I);
> G;
G[1]=2y+z
G[2]=6x+z
> G = simplify(G,1);
> G;
G[1]=y+1 / 2 z
G[2]=x+ 1 / 6 z
```

A.4 Como criar o pacote sudoku.lib

Vimos até aqui o que acreditamos seja o suficiente para que o leitor tenha uma idéia de como utilizar o SINGULAR, pelo menos no que diz respeito ao cálculo de bases de Gröbner. Lembramos que o SINGULAR possui extensa bibliografia entre manuais e livros nos quais podemos encontrar todos os comandos disponíveis e como utilizá-los.

Para encerrar esse tutorial, no entanto, vamos explicar como "montar"o pacote que utilizamos no exemplo do SUDOKU na Seção 4.2.3. Lembrando que utilizamos as equações e o procedimento sudoku disponíveis na Internet no site *http://www-en.us.es/gmcedm/sudoku*.

Estamos fazendo isso, pois a interface do SINGULAR na versão simplificada, não permite que você simplesmente "copie"e "cole"as equações no programa, tornando o aproveitamento de todas aquelas equações impossivel, por ser extremamente extensa.

Então, para montarmos nosso pacote sudoku vamos precisar utilizar um editor de texto (como o bloco de notas do windows) e acessar o site acima.

Após abrirmos um novo arquivo no editor de texto vamos digitar na primeira linha

```
// Singular-library
```

logo depois acessamos o site e copiamos todo o arquivo para o editor de texto. Vemos que na primeira linha é definido o anel em que vamos trabalhar, devemos no entanto excluir essa linha, já que quando formos utilizar o pacote este anel já estará definido no SINGULAR. Agora todas as linha seguintes serão mantidas. Vemos que há um ideal sendo definido com 810 polinômios, mas logo após o último há a seguinte linha:

```
proc sudoku (intmat A) {
```

vamos recortá-la e colá-la logo após a primeira linha do documento criado. Finalizando assim o arquivo, que deve estar parecido com o modelo na página a seguir.

```
// Singular-library

proc sudoku (intmat A)
{
option(set,intvec(100663298,10321));
timer=1;
ideal I;

// ***** AQUI  ESTARÃO AS 810 EQUAÇÕES ***** //

 ideal J;
  int i,j;
  for (i=1; i<=9; i++) {
  for (j=1; j<=9; j++) {
  if (A[i,j]!=0)
  { J=J + ideal( x((i-1)*9+j)- A[i,j] ); }}}
  option(redSB);
  ideal G = std(I+J);
return(G);
}
```

Para que possamos carregar o pacote que acabamos de montar, devemos salvar este arquivo com o nome de `sudoku.lib` atentando para a extensão `.lib`, na pasta

`/usr/share/Singular/LIB`

localizada no diretório onde foi instalado o programa CYGWIN. Feito isso, acessamos o SINGULAR, definimos o ideal (o mesmo da primeira linha que retiramos na montagem do pacote) e com o comando `LIB"sudoku.lib"` carregamos o pacote. Agora, para utilizá-lo devemos definir uma matriz com o comando `intmat` como vemos no exemplo a seguir:

9								8
5			2		8		6	
		3	7	1				9
				7	3		5	
2								4
	5		1	6				
8				2	7	3		
	4		3		9			1
7								2

Figura A.1: Sudoku

Exemplo A.1. *Utilizando o SINGULAR para resolver o sudoku da Figura A.1.*

```
> ring R = 0,x(1..81), Dp;
> LIB"sudoku.lib"
> intmat A[9][9] = 9,0,0,0,0,0,0,0,8,
    5,0,0,2,0,8,0,6,0,    0,0,3,7,1,0,0,0,9,
    0,0,0,0,7,3,0,5,0,    2,0,0,0,0,0,0,0,4,
    0,5,0,1,6,0,0,0,0,    8,0,0,0,2,7,3,0,0,
    0,4,0,3,0,9,0,0,1,    7,0,0,0,0,0,0,0,2;
> def G=sudoku(A);
> G;
```

O que dará todas os polinômios da base de Gröbner reduzida do ideal associado ao sudoku do exemplo. Ao analisarmos estes polinômios vemos claramente quais algarismos ocupam cada espaço, solucionando o sudoku como na figura A.1

9	2	6	5	3	4	7	1	8
5	7	1	2	9	8	4	6	3
4	8	3	7	1	6	5	2	9
1	9	8	4	7	3	2	5	6
2	6	7	9	8	5	1	3	4
3	5	4	1	6	2	9	8	7
8	1	9	6	2	7	3	4	5
6	4	2	3	5	9	8	7	1
7	3	5	8	4	1	6	9	2

Figura A.2: Sudoku

Índice Remissivo