Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Departamento de Matemática

Danilo Machado Tereza

Coloração de grafos via bases de Gröbner

Juiz de Fora
2018

Danilo Machado Tereza

Coloração de grafos via bases de Gröbner

Trabalho de conclusão de curso apresentado ao Departamento de Matemática da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do título de Bacharel em Matemática.

Orientador: Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2018

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Tereza, Danilo.
Coloração de grafos via bases de Gröbner / Danilo Machado Tereza. – 2018.
68 f.

Orientador: Beatriz Casulari da Motta Ribeiro
Trabalho de conclusão de curso – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Departamento de Matemática, 2018.

1. Bases de Gröbner. 2. Grafos. 3. Coloração. 4. Computação algébrica. I. Ribeiro, Beatriz, orient. II. Título.

Danilo Machado Tereza

Coloração de grafos via bases de Gröbner

Trabalho de conclusão de curso apresentado ao Departamento de Matemática da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do título de Bacharel em Matemática.

Aprovada em 2 de julho de 2018

BANCA EXAMINADORA

Profa. Dra. Beatriz Casulari da Motta Ribeiro
Orientadora
Universidade Federal de Juiz de Fora

Prof. Dr. Frederico Sercio Feitosa
Universidade Federal de Juiz de Fora

Prof. Dr. André Arbex Hallack
Universidade Federal de Juiz de Fora

AGRADECIMENTOS

Agradeço, primeiramente a Deus, por me instruir em toda essa trajetória de vida. À professora Beatriz pela confiança em meu potencial, e dedicação em não só transmitir os ensinamentos desse estudo, mas também em como despertar o pensamento crítico a respeito dele, parceria esta que foi fundamental ao longo de toda a graduação. Enfatizo um agradecimento especial ao restante dos professores que tive ao longo dessa caminhada e que auxiliaram no meu conhecimento científico, aos meus familiares e companheira pela compreensão nas horas dedicadas ao estudo e pelo suporte constante em todas elas.

RESUMO

Nesse trabalho, utilizamos as bases de Gröbner como ferramenta para decidir se um polinômio em várias variáveis com coeficientes em um corpo pertence a um ideal fixado. Em seguida, representamos um grafo como um polinômio em várias variáveis e utilizamos os resultados obtidos com bases de Gröbner para decidir se o mesmo pode ser colorido com certo número de cores.

Bases de Gröbner. Grafos. Coloração. Computação algébrica.

ABSTRACT

In this work, we use Gröbner basis as a tool to find out when a polynomial in several variables with coefficients in a field belongs to a fixed ideal. Following, we represent a graph as a polynomial in several variables and use the previous results to decide if it can be colored with certain number of colors.

Key-words: Gröbner basis. Graphs. Coloring. Computational algebra.

SUMÁRIO

INTRODUÇÃO 7

1 ANÉIS 9
1.1 CONCEITOS INICIAIS 9
1.2 IDEAIS 10

2 ANÉIS DE POLINÔMIOS EM UMA VARIÁVEL 13
2.1 CONCEITOS INCIAIS 13
2.2 ALGORITMO DA DIVISÃO EM $\mathbb{K}[x]$ 14
2.3 IDEAIS EM $\mathbb{K}[x]$ 19

3 ANÉIS DE POLINÔMIOS EM VÁRIAS VARIÁVEIS 21
3.1 CONCEITOS INICIAIS 22
3.2 ORDENS MONOMIAIS 23
3.3 ALGORITMO DA DIVISÃO EM $\mathbb{K}[x_1, \cdots, x_n]$ 27
3.4 IDEAIS EM $\mathbb{K}[x_1, \cdots, x_n]$ 30
3.5 ALGORITMO DA PSEUDO-DIVISÃO 33
3.6 IDEAIS RADICAIS DE POLINÔMIOS 36

4 BASES DE GRÖBNER 39
4.1 CONCEITOS INICIAIS 39
4.2 ALGORITMO DE BUCHBERGER 41
4.3 PROPRIEDADES DAS BASES DE GRÖBNER 49

5 COLORAÇÃO DE GRAFOS 54
5.1 POLINÔMIOS E GRAFOS 54
5.2 COLORAÇÃO DE GRAFOS 55

A Testando pertinência no Magma 66

REFERÊNCIAS 68

INTRODUÇÃO

A teoria dos Grafos é um ramo da matemática discreta que possui muitas aplicações em problemas na matemática, computação, engenharia e indústria. Em matemática, um grafo $G = (V, A)$ é um conjunto finito de vértices V e arestas A, onde cada aresta é um par de vértices, ditos vizinhos. É comum, no entanto, representar um grafo esquematicamente através de um diagrama de vértices e arestas similares às figuras usadas na geometria plana. Evidentemente, pode-se representar um mesmo grafo por desenhos aparentemente diferentes, de forma a ter os mesmos vértices e arestas. Nesse caso, a grosso modo, um grafo é dito planar se tem uma representação em figura onde não há interseção de arestas. Uma $k-$coloração (de vértices) de um grafo é um caso especial de rotulagem de grafos, que atribui a cada vértice um número natural chamado, no caso, uma cor. O caso interessante é quando impedimos que vértices vizinhos tenham a mesma cor.

A coloração de grafos tem diversas aplicações, sendo a mais clara e conhecida a coloração de mapas. Nesse caso, os países (ou estados ou cidades ou bairros) são representados pelos vértices e há uma aresta entre dois vértices sempre que dois países (ou estados ou cidades ou bairros) são vizinhos. Outras aplicações interessantes são o jogo Sudoku, escalas de aviões para voos, atribuição de frequência de rádio, entre outras. Há ainda aplicações teóricas na matemática: na geometria euclidiana, na álgebra abstrata, na teoria de códigos corretores de erros e na geometria algébrica.

Uma pergunta natural é quantas cores, no máximo, são necessárias para colorir um grafo (planar ou não) de forma que vértices vizinhos não tenham a mesma cor. Esse problema data do século XIX e, na década de 1970, o caso planar foi resolvido computacionalmente: qualquer grafo planar pode ser colorido com no máximo 4 cores distintas respeitando a regra anterior (veja [1]). Não se conhece prova algébrica do teorema, embora seja possível provar resultados análogos para 5 e 6 cores utilizando conceitos relativamente simples sobre grafos. Mesmo sabendo a quantidade máxima de cores necessárias para colorir um grafo planar, veja que não falamos como, algoritmicamente, a coloração pode ser feita. Temos que, coloridos certos vértices de um grafo, a decisão de como colorir o próximo pode ser complicada conforme crescem os números de vértices e arestas.

Nesse trabalho, estamos interessados em estudar uma ferramenta de álgebra computacional e geometria algébrica chamada base de Gröbner, que foi definida por Buchberger [3] em 1965 e nomeada em homenagem a seu orientador. A aplicação de tais bases na coloração de grafos apareceu pela primeira vez na tese de doutorado de Dave Bayer [2] em 1982, mas rendeu maiores resultados apenas após o ano 2000, estabelecendo então uma interessante conexão entre a álgebra abstrata e a matemática discreta. Uma base de Gröbner é um tipo particular de conjunto gerador de um ideal em um anel de polinômios

de várias variáveis, que pode ser vista como uma generalização não linear do algoritmo de Euclides para o cálculo do máximo divisor comum (em uma variável); do processo de eliminação de Gauss para sistemas lineares; entre outros. O principal objetivo do estudo de tais bases é resolver o problema de pertinência de um polinômio a um ideal fixado no anel de polinômios de várias variáveis. Em uma variável, esse problema é simples e completamente determinado pelo fato dos ideais de polinômios em uma variável com coeficientes em um corpo serem principais, isto é, gerados por um único elemento. Esse não é o caso dos polinômios em várias variáveis, sendo necessária, então, uma nova ferramenta.

No caso da aplicação das bases de Gröbner à coloração de grafos, um grafo de n vértices e d arestas é representado por um polinômio em n variáveis de grau d. No anel de polinômios de n variáveis, o problema da $k-$coloração passa então a ser equivalente a determinar se o polinômio representante do grafo pertence a um certo ideal. O algoritmo de Buchberger, desenvolvido pelo próprio ainda na década de 1960, permite determinar uma base de Gröbner para o ideal em questão, o que torna mais simples o processo de verificar se o polinômio está no ideal. Nossa referência principal para esse estudo foi [4].

A fim de alcançar o necessário para compreender tanto as bases de Gröbner quanto a aplicação à coloração de grafos, esse trabalho está dividido em cinco capítulos.

O primeiro capítulo traz resultados e definições básicas sobre anéis e ideais.

No segundo capítulo, abordamos o problema da pertinência de um polinômio a um ideal em uma variável, cuja solução é bastante intuitiva.

No terceiro capítulo, generalizamos esse problema para anéis de polinômios em várias variáveis, seguindo a mesma ideia intuitiva do caso anterior. Para isso, precisamos encontrar uma forma de ordenar as variáveis para estruturar um algoritmo de divisão relativamente similar ao caso de uma variável. Após isso, ainda que tenhamos, pelo teorema das bases de Hilbert (de 1890), a existência de um conjunto finito de geradores para um ideal em várias variáveis, vemos que isso não resolve o problema da pertinência.

No capítulo quatro, apresentamos as bases de Gröbner, que será nossa ferramenta algébrica para testar se um dado polinômio pertence ou não a um ideal em várias variáveis, conceito que será usado no capítulo final para dizer se um grafo pode ser ou não colorido com k cores.

No capítulo final, vemos ainda que a solução desse problema independe da forma como representamos o grafo esquematicamente, mas que está restrito apenas a resultados sobre o polinômio que representa o grafo e ao ideal construído através da quantidade de cores. Após isso, refinaremos o resultado ainda utilizando essas bases, para um teste que se restringe apenas ao polinômio. Por fim, enunciaremos um resultado que se baseia apenas na base de Gröbner, cujo custo computacional pode ser considerado reduzido, umas vez que essas bases estão implementadas em diversas ferramentas computacionais.

1 ANÉIS

1.1 CONCEITOS INICIAIS

Nesse capítulo, apresentamos alguns conceitos iniciais sobre anéis que serão utilizados ao longo do texto.

Definição 1.1.1. Seja $\mathbb{A}$ um conjunto não vazio onde estejam definidas duas operações, denotadas por

$$\begin{array}{cc} + : \mathbb{A} \times \mathbb{A} \to \mathbb{A} & e \quad * : \mathbb{A} \times \mathbb{A} \to \mathbb{A} \\ (a, b) \to a + b & (a, b) \to a * b \end{array}$$

Chamamos $(\mathbb{A}, +, *)$ de **anel**, se as seguintes propriedades são verificadas quaisquer que sejam $a, b, c \in \mathbb{A}$:

1. $a + (b + c) = (a + b) + c$ (associatividade da operação $+$);
2. $a + b = b + a$ (comutatividade da operação $+$);
3. Existe $0 \in \mathbb{A}$ tal que $a + 0 = 0 + a = a$, para todo $a \in \mathbb{A}$ (elemento neutro da operação $+$);
4. Para todo $a \in \mathbb{A}$ existe $s(a) \in \mathbb{A}$ tal que $a + s(a) = e$ (elemento simétrico ou oposto com relação a operação $+$);
5. $a(bc) = (ab)c$ (associatividade da operação $*$).
6. $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$ (distributividade das operações).

E mais, se existir $1 \in \mathbb{A}$ tal que $a * 1 = 1 * a = a$ para todo $a \in \mathbb{A}$, isto é, se existir o elemento neutro da operação $*$, o anel $(\mathbb{A}, +, *)$ é chamado de **anel com unidade**;

Se $a * b = b * a$ para todo $a, b \in \mathbb{A}$, ou seja, for válida a comutatividade da operação $*$, então o anel $(\mathbb{A}, +, *)$ é chamado de **anel comutativo**;

Definição 1.1.2. Um anel comutativo com unidade $\mathbb{A}$ é dito **domínio de integridade** se para todos $a, b \in \mathbb{A}$ tais que $a * b = 0$, então $a = 0$ ou $b = 0$.

Definição 1.1.3. Seja A um anel comutativo com unidade. Dizemos que o elemento não nulo $a \in A$ é **invertível** se existe $b \in A \setminus \{0\}$ tal que $a * b = b * a = 1$. Denotamos $b = a^{-1}$.

Definição 1.1.4. Um domínio $\mathbb{A}$ é **corpo** se todo elemento $a \in \mathbb{A} \setminus \{0\}$ possui inverso com relação a operação $*$.

Ao longo desse texto, $\mathbb{K}$ representará um corpo.

Exemplo 1.1.5. São exemplos de anéis comutativos com unidade: $\mathbb{Z}$ e $\mathbb{Z}_n$, onde $n \in \mathbb{Z}$. Ainda, $\mathbb{Z}$ é um exemplo de domínio. Por fim, são exemplos de corpos: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{Z}_p$, onde p é um número primo.

Definição 1.1.6. Sejam $\mathbb{A}$ um anel e $a \in \mathbb{A}$. Dizemos que um elemento não invertível $d \in \mathbb{A}$ é um **fator próprio** de a, se existe outro elemento não invertível $c \in \mathbb{A}$ tal que $a = dc$. O elemento c é dito o **cofator** de d em a.

1.2 IDEAIS

Definição 1.2.1. Seja $\mathbb{A}$ um anel comutativo com unidade, dizemos que um subconjunto não vazio $I \subseteq \mathbb{A}$ é um **ideal** se

1. $f + g \in I$ para quaisquer $f, g \in I$;
2. $hf \in I$ para todo $f \in I$ e todo $h \in \mathbb{A}$.

No que segue, chamaremos de anel um anel comutativo com unidade.

Definição 1.2.2. Sejam A um anel e I um ideal de A. Dizemos que I é um **ideal próprio** de A se $I \subsetneq A$.

Proposição 1.2.3. *Sejam $\mathbb{A}$ um anel e I um ideal de $\mathbb{A}$. Temos*

1. *$0 \in I$;*
2. *Se existe $f \in I$ invertível, então $I = \mathbb{A}$.*

Demonstração. 1. Se $I = \{0\}$ segue o que queríamos. Caso contrário, $I \neq \{0\}$ e existe $f \in I$ não nulo. Da propriedade (2) da definição 1.2.1 temos $0f = 0 \in I$.

2. Suponhamos que f é invertível, então existe $f^{-1} \in \mathbb{A}$. Da propriedade (2) da definição 1.2.1 temos $ff^{-1} = 1 \in I$. Novamente pela propriedade (2), temos $he = h \in I$ para todo $h \in \mathbb{A}$. Logo $\mathbb{A} \subset I$, mas $I \subset \mathbb{A}$, portanto $I = \mathbb{A}$. □

Podemos listar algumas propriedades sobre operações com ideais, cujas demonstrações seguem direto da definição 1.2.1.

Proposição 1.2.4. *Dados os ideais I e J de $\mathbb{A}$, temos*

1. *$I \cap J$ é o ideal interseção;*
2. *$I + J$ é o ideal soma;*
3. *IJ é o ideal produto;*

4. $I : J := \{f \mid fh \in I \forall h \in J\}$ *é o ideal quociente.*

Definição 1.2.5. Dado um subconjunto $S \neq \emptyset$ de $\mathbb{A}$, então

$$\langle S \rangle := \left\{ \sum_{i=1}^{m} a_i f_i \,\middle|\, m \in \mathbb{N} - \{0\}, f_i \in S \text{ e } a_i \in \mathbb{A} \right\}$$

é um ideal de $\mathbb{A}$ chamado de **ideal gerado** por S. Se S é finito, digamos $S = \{f_1, \cdots, f_n\}$, dizemos que $\langle S \rangle$ é um **ideal finitamente gerado** e denotamos $\langle S \rangle = \langle f_1, \cdots, f_n \rangle$. Mais ainda, se $\langle S \rangle = \langle f \rangle$ dizemos que $\langle S \rangle$ é um **ideal principal**. Se todo ideal de $\mathbb{A}$ é principal, então $\mathbb{A}$ é dito **anel principal**.

Proposição 1.2.6. *Seja I um ideal finitamente gerado de um anel A. Se S é um conjunto infinito de geradores de I, então existe um subconjunto finito de S que também gera I.*

Demonstração. Como I é finitamente gerado, existem $g_1, \cdots, g_s$ em I tais que $I = \langle g_1, \cdots, g_s \rangle$. Como S é um conjunto de geradores, cada g_i pode ser escrito como combinação linear finita de elementos de S. Isto é

$$g_i \in \langle s_1, \cdots, s_{r_i} \rangle,$$

para cada $i \in \{1, \cdots, s\}$. Denotando $m := \max\{r_k \,\big|\, 1 \leqslant k \leqslant s\}$, obtemos

$$g_i \in \langle s_1, \cdots, s_m \rangle$$

para todo $i \in \{1, \cdots, s\}$. Mas $S \subseteq I$, então

$$\langle g_1, \cdots, g_s \rangle \subseteq \langle s_1, \cdots, s_m \rangle \subseteq I.$$

Como $I = \langle g_1, \cdots, g_s \rangle$, temos $\langle s_1, \cdots, s_m \rangle = I$. □

Definição 1.2.7. Uma cadeia ascendente de ideais de um anel

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

é **estacionária** se existe $n \in \mathbb{N}$ tal que $I_k = I_n$ quando $k > n$.

Proposição 1.2.8. *Se $\mathbb{A}$ é um anel principal com unidade, então toda cadeia ascendente de ideais é estacionária.*

Demonstração. Seja

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

uma cadeia ascendente de ideais. Considere $I = \bigcup_{i \in \mathbb{N}} I_i$. Afirmamos que I é ideal. De fato, dados $a, b \in I$ existem $i, j \in \mathbb{N}$ tais que $a \in I_i$ e $b \in I_j$. Como a cadeia é ascendente, suponhamos sem perda de generalidade que $i < j$, então $a \in I_j$. Como I_j é ideal segue

que $a + b \in I_j \subseteq I$. Agora, dados $a \in I$ e $b \in \mathbb{A}$ existe $n \in \mathbb{N}$ tal que $a \in I_n$, como I_n é ideal segue que $ba \in I_n \subseteq I$.

Como $\mathbb{A}$ é um anel principal, temos que $I = \langle c \rangle$, para algum $c \in \mathbb{A}$. Como $1c = c \in I$ existe $n \in \mathbb{N}$ tal que $c \in I_n$. Logo, $I_n = \langle c \rangle$, portanto $I_r = I_n$ para todo $r \geqslant n$, isto é, essa cadeia é estacionária. □

Definição 1.2.9. Seja $\mathbb{A}$ um anel e $I \subseteq \mathbb{A}$ um ideal próprio. Dizemos que

1. I é ideal **primo** se para todo $ab \in I$, então $a \in I$ ou $b \in I$;
2. I é ideal **maximal** se para todo ideal $J \subseteq \mathbb{A}$ tal que $I \subseteq J$, então $J = I$ ou $J = \mathbb{A}$.

Proposição 1.2.10. *Um anel $\mathbb{A}$ é domínio se, e somente se, o ideal $I = \{0\}$ é primo.*

Demonstração. Se $\mathbb{A}$ é domínio, então dados $a, b \in I \subseteq \mathbb{A}$ tais que $ab = 0$, temos $a = 0$ ou $b = 0$, isto é, $a \in I$ ou $b \in I$, portanto I é ideal primo. Reciprocamente, se $I = \{0\}$ é primo, então dado $ab \in \mathbb{A}$ tal que $ab = 0$, temos $ab \in I$. Como I é primo então $a = 0$ ou $b = 0$, portanto $\mathbb{A}$ é domínio. □

Encerramos esse capítulo com o conceito de radical de um ideal, cuja motivação para o estudo nesse trabalho é o Teorema dos Zeros de Hilbert, cuja importância veremos no capítulo de Bases de Gröbner.

Definição 1.2.11. Sejam A um anel e I um ideal de A. Definimos o **ideal radical** $\sqrt{I}$ de I como o conjunto dos elementos $a \in A$ tais que existe $k \geq 0$ tal que $a^k \in I$.

Temos claramente que $I \subset \sqrt{I}$, porém podemos ter $\sqrt{I} \not\subset I$. De fato, por exemplo, no anel dos inteiros $\mathbb{Z}$, temos que 2 está no radical de $4\mathbb{Z}$, porém $2 \notin 4\mathbb{Z}$. Na verdade, podemos ver que $\sqrt{4\mathbb{Z}} = 2\mathbb{Z}$.

Definição 1.2.12. Se $I = \sqrt{I}$, dizemos que I é um ideal radical.

Por fim, observamos que $\sqrt{I}$ é um ideal radical e, mais ainda, $\sqrt{I}$ é o menor ideal radical que contém I.

2 ANÉIS DE POLINÔMIOS EM UMA VARIÁVEL

2.1 CONCEITOS INCIAIS

Definição 2.1.1. Seja $(\mathbb{A}, +, *)$ um anel, considere

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

Um elemento de $\mathbb{A}[x]$ é dito um **polinômio** na indeterminada x com coeficientes em $\mathbb{A}$. Temos que $\mathbb{A}[x]$ é um anel com as operações:

$$\begin{array}{ccc} + : \mathbb{A}[x] \times \mathbb{A}[x] \to \mathbb{A}[x] & \quad e \quad & * : \mathbb{A}[x] \times \mathbb{A}[x] \to \mathbb{A}[x], \\ (f, g) \to f + g & & (f, g) \to f * g \end{array}$$

em que, dados $f = \sum_{i=0}^{n} a_i x^i$ e $g = \sum_{i=0}^{m} b_i x^i$, temos a soma dada por

$$f+g = \sum_{i=0}^{r} c_i x^i, \text{ com } r = \max\{n, m\} \quad \text{onde} \quad c_i = \begin{cases} a_i + b_i, & \text{se } i \leqslant \min\{n, m\} \\ a_i, & \text{se } \min\{n, m\} < i \text{ e } r = n \\ b_i, & \text{se } \min\{n, m\} < i \text{ e } r = m \end{cases}$$

e o produto dado por

$$fg = \sum_{i=0}^{n+m} c_i x^i \quad \text{com} \quad c_i = \sum_{i=j+k} a_j b_k.$$

Observamos que se $\mathbb{A}$ é comutativo (ou um domínio) então $\mathbb{A}[x]$ também é comutativo (ou um domínio). Além disso, se $\mathbb{A}$ tem unidade então $\mathbb{A}[x]$ também tem. Por fim, os invertíveis de $\mathbb{A}[x]$ são os invertíveis de $\mathbb{A}$.

Para encerrar essa seção, estabelecemos a nomenclatura a ser usada nesse texto sobre um polinômio $f = \sum_{i=0}^{n} a_i x^i$ em $\mathbb{A}[x]$. Temos:

1. Um **termo de** f é um $a_i x^i$, dado $i \in \{1, \cdots, n\}$, tal que $a_i \neq 0$;
2. Os **coeficientes de** f são os a_i, para todo $0 \leqslant i \leqslant n$;
3. Os **monômios de** f são os x^i, para todo $0 \leqslant i \leqslant n$;
4. Conjunto de todos os monômios de f é denotado por $\mathbb{M}(f)$;
5. O **grau de** f é o inteiro $gr(f) := \max\{i, x^i \in \mathbb{M}(f)\}$;
6. O **termo líder de** f é denotado como $tl(f) := a_n x^n$, onde $n = gr(f)$;
7. O **coeficiente líder de** f é denotado como $cl(f) := a_n$, onde $n = gr(f)$;

8. Convencionamos $gr(0) = -\infty$, $tl(0) := 0$ e $cl(0) := 0$;

9. O **monômio líder de** f é denotado como $ml(f) := x^n$, onde $n = gr(f)$;

10. f é dito **mônico** se $cl(f) = 1$;

Observação 2.1.2. Algumas propriedades intuitivas sobre operações com os graus de polinômios são listadas abaixo:

$$gr(f+g) \leqslant \max\{gr(f), gr(g)\} \quad \text{e} \quad gr(fg) = gr(f) + gr(g),$$

e se $gr(f) \neq gr(g)$, então

$$gr(f+g) = \max\{gr(f), gr(g)\}$$

2.2 ALGORITMO DA DIVISÃO EM $\mathbb{K}[x]$

Ao longo do texto, $\mathbb{K}$ denota um corpo. Já é conhecido o conceito de divisão euclidiana que temos em $\mathbb{Z}$, em que dado $a \in \mathbb{Z}$, para qualquer $b \in \mathbb{Z}\backslash\{0\}$, existem únicos $q, r \in \mathbb{Z}$, respectivamente o quociente e o resto da divisão de a por b, tais que

$$a = qb + r,$$

onde $0 \leqslant r < b$. O resultado a seguir é o análogo no anel $\mathbb{K}[x]$.

Teorema 2.2.1. *Seja $\mathbb{K}$ um corpo. Dado $f \in \mathbb{K}[x]$, para qualquer $g \in \mathbb{K}[x]\backslash\{0\}$ existem $q, r \in \mathbb{K}[x]$ unicamente determinados pelas condições*

$$f = qg + r \quad com \quad gr(r) < gr(g).$$

Embora o teorema nos garanta a existência e a unicidade de q e r ele não nos auxilia em determiná-los. Enunciamos então o *algoritmo da divisão*, que instrui passos sistemáticos que nos levam a determinar q e r tal como foram enunciados no teorema

acima.

Algoritmo: Divisão de polinômios de uma variável

Entrada: $f \in \mathbb{K}[x]$ e $g \in \mathbb{K}[x]\backslash\{0\}$

Saída: q e r satisfazendo a igualdade $f = qg + r$, onde $r = 0$ ou $gr(r) < gr(g)$

início
  $q = 0$
  $r = f$
  enquanto $r \neq 0$ *e* $gr(r) \geqslant gr(g)$ **faça**
    $q := q + \dfrac{tl(r)}{tl(g)}$
    $r := r - \dfrac{tl(r)}{tl(g)}g$
  fim
fim
retorna q, r

Ilustremos esse algoritmo de forma esquemática nos exemplos que seguem:

Exemplo 2.2.2. Seja $n \in \mathbb{N}$ com $n \neq 0$. Encontremos o quociente e o resto na divisão de $x^n - 1$ por $x - 1$ em $\mathbb{K}[x]$.

Façamos o cálculo de maneira esquemática, começamos com $q = 0$ e $r = x^n - 1$, temos na primeira execução

$$\begin{array}{r|l} x^n - 1 & x - 1 \\ \cline{2-2} r = x^{n-1} - 1 & q = x^{n-1} \end{array}$$

Como $r \neq 0$ e $gr(r) \geqslant gr(g)$ continuemos

$$\begin{array}{r|l} x^n - 1 & x - 1 \\ \cline{2-2} x^{n-1} - 1 & q = x^{n-1} + x^{n-2} \\ r = x^{n-2} - 1 & \end{array}$$

Novamente façamos

$$\begin{array}{r|l} x^n - 1 & x - 1 \\ \cline{2-2} x^{n-1} - 1 & q = x^{n-1} + x^{n-2} + x^{n-3} \\ x^{n-2} - 1 & \\ r = x^{n-3} - 1 & \end{array}$$

Note que a cada passo, o grau do coeficiente líder de r diminui em um. Repetindo finitas

vezes este passo obtemos:

$$\begin{array}{r|l} x^n - 1 & x - 1 \\ \hline x^{n-1} - 1 & q = x^{n-1} + x^{n-2} + x^{n-3} + \cdots + x \\ x^{n-2} - 1 & \\ x^{n-3} - 1 & \\ \vdots & \\ r = x - 1 & \end{array}$$

Por último,

$$\begin{array}{r|l} x^n - 1 & x - 1 \\ \hline x^{n-1} - 1 & q = x^{n-1} + x^{n-2} + x^{n-3} + \cdots + x + 1 \\ x^{n-2} - 1 & \\ x^{n-3} - 1 & \\ \vdots & \\ x - 1 & \\ r = 0 & \end{array}$$

Como $r = 0$, o algoritmo encerra e obtemos

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

Exemplo 2.2.3. Calculemos $a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{R}$ de modo que o quociente e o resto da divisão de $x^5 + 2x^4 + 2x^3 + a_1x^2 + x + a_2$ por $a_3x^2 + a_4x + 2$ são respectivamente $x^3 + a_5x^2 - x - 3$ e $a_6x + 7$.

Executemos esquematicamente o algoritmo da divisão de forma a obtermos o quociente pedido no exemplo. Temos

$$\begin{array}{r|l} x^5 + 2x^4 + 2x^3 + a_1x^2 + x + a_2 & a_3x^2 + a_4x + 2 \\ \hline -(a_3x^5 + a_4x^4 + 2x^3) & q = x^3 \\ \hline (2 - a_4)x^4 + a_1x^2 + x + a_2 & \end{array}$$

Note que pelo algoritmo devemos ter necessariamente que $1 - a_3 = 0$, então $a_3 = 1$. Continuemos

$$\begin{array}{r|l} x^5 + 2x^4 + 2x^3 + a_1x^2 + x + a_2 & a_3x^2 + a_4x + 2 \\ \hline -(a_3x^5 + a_4x^4 + 2x^3) & q = x^3 + a_5x^2 \\ \hline (2 - a_4)x^4 + a_1x^2 + x + a_2 & \\ -(a_3a_5x^4 + a_4a_5x^3 + 2a_5x^2) & \\ \hline -a_4a_5x^3 + (a_1 - 2a_5)x^2 + x + a_2 & \end{array}$$

Agora temos que $(2 - a_4) - a_3a_5 = 0$, então

$$2 - a_4 - a_5 = 0. \tag{2.1}$$

Prosseguimos

$$\begin{array}{r|l}
x^5+2x^4+2x^3+a_1x^2+x+a_2 & a_3x^2+a_4x+2 \\
\cline{2-2}
-(a_3x^5+a_4x^4+2x^3) & q=x^3+a_5x^2-x \\
\cline{1-1}
(2-a_4)x^4+a_1x^2+x+a_2 & \\
-(a_3a_5x^4+a_4a_5x^3+2a_5x^2) & \\
\cline{1-1}
-a_4a_5x^3+(a_1-2a_5)x^2+x+a_2 & \\
-(-a_3x^3-a_4x^2-2x) & \\
\cline{1-1}
(a_1-2a_5+a_4)x^2+3x+a_2 &
\end{array}$$

Desta etapa devemos ter $-a_4a_5+a_3=0$, então

$$a_4a_5=1. \tag{2.2}$$

Por fim,

$$\begin{array}{r|l}
x^5+2x^4+2x^3+a_1x^2+x+a_2 & a_3x^2+a_4x+2 \\
\cline{2-2}
-(a_3x^5+a_4x^4+2x^3) & q=x^3+a_5x^2-x-3 \\
\cline{1-1}
(2-a_4)x^4+a_1x^2+x+a_2 & \\
-(a_3a_5x^4+a_4a_5x^3+2a_5x^2) & \\
\cline{1-1}
-a_4a_5x^3+(a_1-2a_5)x^2+x+a_2 & \\
-(-a_3x^3-a_4x^2-2x) & \\
\cline{1-1}
(a_1-2a_5+a_4)x^2+3x+a_2 & \\
-(-3a_3x^3-3a_4x-6) & \\
\cline{1-1}
(3a_4+3)x+(a_2+6) &
\end{array}$$

E desta obtemos $a_1-2a_5+a_4+3a_3=0$, daí

$$a_1-2a_5+a_4+3=0 \tag{2.3}$$

Por (2.1) e (2.2) temos

$$2-a_4=a_5 \implies a_4(2-a_4)=1 \implies a_4=1 \implies a_5=1$$

Como informação do exemplo temos também que o resto é dado por a_6x+7, com o que obtemos do algoritmo, temos

$$3a_4+3=a_6 \quad \text{e} \quad a_2+6=7 \implies a_6=6 \quad \text{e} \quad a_2=1$$

Agora por (2.3) obtemos que $a_1=-2$. Com isso obtemos todas as constantes que queríamos.

Definição 2.2.4. Se o resto na divisão de a por b é nulo, dizemos que b **divide** a e denotamos por $b \mid a$.

Definição 2.2.5. Dados $f_1,\cdots,f_r \in \mathbb{K}[x]\backslash\{0\}$ dizemos que $d \in \mathbb{K}[x]$ é um **máximo divisor comum** de $f_1,\cdots,f_r$ se

- $d \mid f_i$ para todo $i \in \{1, \cdots, r\}$;
- Se $g \mid f_i$ para todo $i \in \{1, \cdots, r\}$ então $g \mid d$.

Se o máximo divisor comum for mônico então será denotado por $MDC(f_1, \cdots, f_r)$.

Exemplo 2.2.6. Se $f, g \in \mathbb{K}[x]\backslash\{0\}$ são tais que $f \mid g$ então

$$MDC(f, g) = \frac{f}{cl(f)}.$$

Proposição 2.2.7. *Sejam $f_1, \cdots, f_r \in \mathbb{K}[x]\backslash\{0\}$, podemos determinar de maneira recursiva o MDC fazendo*

$$MDC(f_1, \cdots, f_r) = MDC(MDC(f_1, \cdots, f_{r-1}), f_r).$$

Teorema 2.2.8. *Dados $f, g \in \mathbb{K}[x]\backslash\{0\}$. Se q e $r \neq 0$ são tais que $f = qg + r$, então*

$$MDC(f, g) = MDC(g, r).$$

O resultado deste teorema se faz claro no seguinte algoritmo para determinar o MDC entre dois polinômios.

Algoritmo: Cálculo do MDC

Entrada: $f \in \mathbb{K}[x]$ e $g \in \mathbb{K}[x]\backslash\{0\}$
Saída: $MDC(f, g)$

```
início
    f := q_0 g + r_1
    g := q_1 r_1 + r_2
    enquanto r_i não dividir r_{i-1} faça
        r_{i-1} := q_i r_i + r_{i+1}
    fim
    MDC(f, g) := r_s / cl(r_s)
fim
retorna MDC(f, g)
```

Utilizamos a existência de q e r no teorema 2.2.1 e executamos sucessivas divisões de forma que algum resto se torne divisor do anterior, garantindo que o próximo resto é nulo. Temos essa garantia, pois da forma como foram construídas as divisões temos, pelo teorema 2.2.1, que $gr(r_{i+1}) < gr(r_i)$, donde algum resto será nulo. Nesse passo, o resto anterior garante o resultado que queríamos.

Definição 2.2.9. Sejam $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$ e $k \in \mathbb{K}$. Denotamos $a_n k^n + \cdots + a_1 k + a_0$ por $f(k)$ e dizemos que k é **raiz** ou zero de f se $f(k) = 0$.

Definição 2.2.10. Um corpo $\mathbb{K}$ é dito **algebricamente fechado** se todo polinômio não constante $p \in \mathbb{K}[x]$ admite raiz em $\mathbb{K}$.

Considerando a definição 2.2.9, segue então do teorema 2.2.1:

Proposição 2.2.11. *Sejam $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$ e $k \in \mathbb{K}$. O resto da divisão de f por $x - k$ é $f(k)$.*

Corolário 2.2.12. *Seja $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$. Temos que $k \in \mathbb{K}$ é uma raiz de f se, e só se, f é divisível por $x - k$.*

Proposição 2.2.13. *Seja $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ com $a_n \neq 0$. Então se $\frac{p}{q} \in \mathbb{Q}$ irredutível é raiz de f com $p, q \in \mathbb{Z}$, então $q \mid a_n$ e $p \mid a_0$.*

Demonstração. Como $\frac{p}{q} \in \mathbb{Q}$ com $q \neq 0$ é raiz de f, então sendo $f = \sum_{i=0}^{n} a_i x^i$ temos que

$$f\left(\frac{p}{q}\right) = 0 = \sum_{i=0}^{n} a_i \left(\frac{p}{q}\right)^i = \sum_{i=0}^{n} a_i \frac{p^i}{q^i} \implies a_0 + \sum_{i=1}^{n} a_i \frac{p^i}{q^i} = 0 \implies a_0 q^n + \sum_{i=1}^{n} a_i p^i q^{n-i} = 0,$$

daí

$$q(a_0 q^{n-1} + a_1 p q^{n-2} + \cdots + a_{n-2} q + a_{n-1}) = -a_n p^n.$$

Como $q \nmid p$, pois $\frac{p}{q}$ é irredutível, então $q \nmid p^n$, portanto q divide a_n. Agora, note também que podemos escrever $f\left(\frac{p}{q}\right)$ da seguinte forma

$$f\left(\frac{p}{q}\right) = p\left(\frac{a_1}{q} + \cdots + \frac{a_n p^{n-1}}{q^n}\right) = -a_0,$$

portanto p divide a_0. □

2.3 IDEAIS EM $\mathbb{K}[x]$

Nesta seção, solucionaremos por completo o problema em decidir se um dado polinômio pertence ou não a um ideal fixado. Enunciaremos nesta seção apenas o necessário para solucionar este problema e deixaremos para o próximo capítulo resultados mais gerais em várias variáveis.

Proposição 2.3.1. *Todo ideal I de $\mathbb{K}[x]$ é principal.*

Demonstração. Seja I um ideal de $\mathbb{K}[x]$. Se $I = \{0\}$, então I é gerado por 0. Suponhamos que $I \neq \{0\}$. Seja $0 \neq p(x) \in I$ tal que $gr(p)$ seja o menor possível. Se $p(x) = a$ constante não nula, então $1 = a^{-1}a \in I$ e assim $1 * g(x) \in I$ para todo $g(x) \in \mathbb{K}[x]$, donde obtemos que $I = \mathbb{K}[x]$ e é gerado por 1.

Suponhamos então que $gr(p) > 0$. Como $p \in I$, claramente temos que $\langle p \rangle \subset I$, resta-nos mostrar que $\langle p \rangle \supset I$. De fato, seja $f \in I$, pelo teorema 2.2.1 existem $q, r \in \mathbb{K}[x]$ unicamente determinados por

$$f = qp + r \quad \text{com} \quad gr(r) < gr(p).$$

Agora, como $f, p \in I$, segue imediatamente que $r \in I$. Pela minimalidade do grau de p e pela condição $gr(r) < gr(p)$, temos necessariamente que r é identicamente nulo. Logo $f = qp$, isto é, f, um elemento qualquer de I, é múltiplo de p. Portanto $\langle p \rangle \supset I$, o que demonstra a proposição. □

Observação 2.3.2. Notamos que, pela demonstração da proposição 2.3.1, podemos notar que se $I = \langle f_1, \cdots, f_n \rangle$, então $I = \langle MDC\{f_1, \cdots, f_n\} \rangle$.

Observação 2.3.3. Pelas proposições 1.2.8 e 2.3.1, temos então que toda cadeia ascendente de ideais de $\mathbb{K}[x]$ é estacionária.

Encerramos essa seção com a solução do problema de pertinência de um polinômio f a um ideal I fixado. Sejam $f \in \mathbb{K}[x]$ e um ideal I de $\mathbb{K}[x]$. Pela proposição 2.3.1 existe $g \in \mathbb{K}[x]$ tal que $I = \langle g \rangle$ e, pelo teorema 2.2.1, existem $q, r \in \mathbb{K}[x]$ unicamente determinados por

$$f = qg + r \quad \text{com} \quad gr(r) < gr(g).$$

Por essas observações obtemos que f pertence a I se, e somente se, r é o polinômio nulo, isto é, f ser múltiplo de g é condição necessária e suficiente para garantir que $f \in I$. Obtemos isso devido a unicidade do resto ao dividir f pelo gerador de I.

3 ANÉIS DE POLINÔMIOS EM VÁRIAS VARIÁVEIS

No capitulo anterior, solucionamos o problema da pertinência de um polinômio em um ideal de $\mathbb{K}[x]$ sem muita dificuldade, bastou estudarmos o resto da divisão deste polinômio pelo polinômio que gera o ideal, uma vez que todo ideal é principal.

Neste capítulo, estudaremos os anéis de polinômios em várias varáveis, nos quais a solução para o problema da pertinência torna-se mais elaborado. Nosso caminho natural é seguir pelo mesmo raciocínio do capítulo anterior.

O primeiro problema a ser resolvido é: como dividir um polinômio de várias variáveis por outro. Devemos também estudar como são os ideais nos anéis de polinômios em várias variáveis, para só então estudar um método que resolva o problema da pertinência neste contexto. Para o primeiro problema consideramos o seguinte polinômio

$$x^2y^3 + x^4 + y^6 + z.$$

Primeiramente, devemos ordená-lo de tal forma a selecionarmos qual termo é o líder do polinômio. Se considerarmos a variável x mais "importante", o polinômio deveria ser ordenado da seguinte forma

$$x^4 + x^2y^3 + y^6 + z,$$

mas se fizermos o raciocínio análogo ao y o mesmo deveria ser ordenado da forma

$$y^6 + y^3x^2 + x^4 + z.$$

Porém, podemos ainda pensar outras formas de ordenar este polinômio, o que resultaria, por exemplo, em

$$y^6 + x^2y^3 + x^4 + z \quad \text{ou} \quad z + x^4 + x^2y^3 + y^6 \quad \text{ou} \quad z + y^6 + y^3x^2 + x^4$$

Nota-se um importante passo antes de buscarmos um algoritmo da divisão: estruturar de forma consistente essa ordem. Veremos mais deste conceito na seção sobre ordens monomiais. Após isso, somos levados a estruturar um algoritmo da divisão que nos possibilite determinar se este polinômio pertence ou não a um dado ideal.

Pelo mesmo principio do capítulo anterior, seríamos levados a dividir esse polinômio pelos geradores do ideal (saberemos da existência desta base pelo *teorema das bases de Hilbert* que veremos a seguir), porém esta base não nos auxilia para solucionar o problema da pertinência, que só será concluído ao definirmos uma *base de Gröbner* para este ideal, conceito que será visto no próximo capítulo.

3.1 CONCEITOS INICIAIS

De maneira mais simplória, começamos com duas variáveis. Denotemos um elemento de $\mathbb{K}[x][y]$ como

$$f_n y^n + f_{n-1} y^{n-1} + \cdots + f_1 y + f_0$$

com $f_i = \sum_{j_0}^{m_i} a_{ij} x^j \in \mathbb{K}[x]$, onde $n, m_i \in \mathbb{N}$. Tem-se também que $\mathbb{K}[x][y]$ é um domínio se $\mathbb{K}[x]$ o for, e este será, como já foi visto, se $\mathbb{K}$ o for também. Note que da forma como definimos $\mathbb{K}[x][y] = \mathbb{K}[y][x]$. Denotemos então por

$$\mathbb{K}[x, y] := \mathbb{K}[x][y] = \mathbb{K}[y][x].$$

Definição 3.1.1. Um **termo** de $\mathbb{K}[x_1, \cdots, x_n]$ é um elemento da forma

$$a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i},$$

com $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$, onde $a_\alpha \in \mathbb{K}$ é o **coeficiente** e $\prod_{i=1}^{n} x_i^{\alpha_i}$ é o **monômio** do termo. Tem-se como **grau total** do monômio $\prod_{i=1}^{n} x_i^{\alpha_i}$ o número natural dado por

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

Definição 3.1.2. Um elemento $f \in \mathbb{K}[x_1, \cdots, x_n]$ é uma soma formal

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

com $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}^n$, $a_\alpha \in \mathbb{K}$ e $J \subset \mathbb{N}^n$ finito. Dado $(k_1, \cdots, k_n) \in \mathbb{K}^n$ definimos

$$f(k_1, \cdots, k_n) := \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} k_i^{\alpha_i}.$$

Consideramos ainda

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

como sendo o conjunto de todos os monômios de f ou **suporte** de f. E chamamos de **grau total** de f o número

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

Podemos generalizar de maneira intuitiva as operações de soma e produto dadas no capítulo anterior para polinômios em várias variáveis. Obtemos os mesmos resultados a respeito do grau, dados por

$$gr(f + g) \leqslant \max\{gr(f), gr(g)\} \quad \text{e} \quad gr(fg) = gr(f) + gr(g),$$

onde f e g são polinômios em $\mathbb{K}[x_1, \cdots, x_n]$.

3.2 ORDENS MONOMIAIS

Nesta seção, estudaremos o conceito de ordem monomial que estrutura os termos dos polinômios no anel $\mathbb{K}[x_1, \cdots, x_n]$ de forma a obtermos uma boa definição de termo líder na próxima seção.

Definição 3.2.1. O conjunto de todos os monômios de $\mathbb{K}[x_1, \cdots, x_n]$ será denotado por $\mathbb{M}_n$, ou seja,

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

onde consideramos o monômio $x_1^0 \cdots x_n^0 = 1$.

Definição 3.2.2. Uma **relação de ordem**, ou ordenação, sobre um conjunto $\mathcal{C}$ não vazio é uma relação denotada por $\preceq$ que satisfaz

1. **Reflexividade:** $c \preceq c$ para todo $c \in \mathcal{C}$;
2. **Antissimétrica:** Se $c_1 \preceq c_2$ e $c_2 \preceq c_1$, então $c_1 = c_2$;
3. **Transitiva:** Se $c_1 \preceq c_2$ e $c_2 \preceq c_3$, então $c_1 \preceq c_3$.

Exemplo 3.2.3. A relação "divisão" dada por

$$a \preceq b \iff \text{ existe } q \text{ tal que } b = qa$$

é uma relação de ordem em $\mathbb{Z}$, mas não é sobre $\mathbb{Q}$ ou $\mathbb{R}$.

Definição 3.2.4. Dizemos que a relação de ordem é **total** se para quaisquer c_1 e c_2 em $\mathcal{C}$ tem-se $c_1 \preceq c_2$ ou $c_2 \preceq c_1$ ou $c_1 = c_2$.

Exemplo 3.2.5. A relação de ordem "divisão" definida no exemplo anterior não é total em $\mathbb{Z}$. Basta observar que $3 \nmid 4$, $4 \nmid 3$ e $3 \neq 4$.

Exemplo 3.2.6. A relação sobre $\mathbb{C}$ dada por

$$a + bi \preceq c + di \iff \begin{cases} a < c & \text{ou} \\ a = c & \text{e} \quad b \leqslant d \end{cases}$$

$\preceq$ é uma relação de ordem total.

Definição 3.2.7. Sejam

$$f = a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} \quad \text{e} \quad g = a_\beta \prod_{i=1}^{n} x_i^{\beta_i},$$

dizemos que $g \,\Big|\, f$ se existe $m_1 = \prod_{i=1}^{n} {x_i}^{\lambda_i} \in \mathbb{M}_n$ e $a_\lambda \in \mathbb{K}$ tais que

$$f = a_\lambda m_1 g,$$

ou seja,

$$a_\alpha \prod_{i=1}^{n} {x_i}^{\alpha_i} = \left(a_\lambda \prod_{i=1}^{n} {x_i}^{\lambda_i}\right)\left(a_\beta \prod_{i=1}^{n} {x_i}^{\beta_i}\right) = a_\lambda a_\beta \prod_{i=1}^{n} {x_i}^{\lambda_i+\beta_i}.$$

Daí $\beta_i \leqslant \alpha_i$ para todo $i \in \{1, \cdots, n\}$.

Com estas definições somos capazes de enunciar a ordem monomial. A partir dela, definiremos uma série de exemplos de ordens deste tipo.

Definição 3.2.8. Uma **ordem monomial** $\preceq$ sobre $\mathbb{M}_n$ é uma relação de ordem total que satisfaz:

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

Lema 3.2.9. *Seja $\preceq$ uma ordem monomial em $\mathbb{K}[x_1, \cdots, x_n]$, então qualquer sequência decrescente de monômios é finita.*

Demonstração. Considere a sequência de monômios decrescente, segundo a ordem monomial $\preceq$, dados por

$$\cdots \preceq m_i \preceq \cdots \preceq m_1 \preceq m_0$$

Seja M o conjunto que contém os monômios dessa sequência. Como M é um subconjunto não vazio de $\mathbb{M}_n$ e $\preceq$ é uma ordem monomial, pela segunda propriedade da definição de ordem monomial temos que M admite um menor elemento m_j, desta forma

$$m_j \preceq \cdots \preceq m_i \preceq \cdots \preceq m_1 \preceq m_0,$$

seguindo o que queríamos. □

Definição 3.2.10. (Ordem lexicográfica $\preceq_L$): Sejam os monômios $\prod_{i=1}^{n} {x_i}^{\alpha_i}$ e $\prod_{i=1}^{n} {x_i}^{\beta_i} \in \mathbb{M}_n$, dizemos que

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

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

Definição 3.2.11. (Ordem lexicográfica graduada $\preceq_{LG}$): Sejam os monômios $\prod_{i=1}^{n} {x_i}^{\alpha_i}$ e $\prod_{i=1}^{n} {x_i}^{\beta_i} \in \mathbb{M}_n$, dizemos que

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

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

Definição 3.2.12. (Ordem lexicográfica graduada reversa $\preceq_{LGR}$): Sejam os monômios $\prod_{i=1}^{n} {x_i}^{\alpha_i}$ e $\prod_{i=1}^{n} {x_i}^{\beta_i} \in \mathbb{M}_n$, dizemos que

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

- se $gr\left(\prod_{i=1}^{n} {x_i}^{\alpha_i}\right) < gr\left(\prod_{i=1}^{n} {x_i}^{\beta_i}\right)$; ou
- se $gr\left(\prod_{i=1}^{n} {x_i}^{\alpha_i}\right) = gr\left(\prod_{i=1}^{n} {x_i}^{\beta_i}\right)$ e existe $k \in \{1, \cdots, n\}$ tal que $\alpha_k > \beta_k$ e $\alpha_j = \beta_j$ para todo $j > k$.

Definição 3.2.13. (Ordem ponderada $\preceq^P$): Considere $\preceq$ uma ordem monomial sobre $\mathbb{M}_n$ e $p = (p_1, \cdots, p_n) \in \mathbb{N}^n$. Dados dois monômios $\prod_{i=1}^{n} {x_i}^{\alpha_i}$ e $\prod_{i=1}^{n} {x_i}^{\beta_i} \in \mathbb{M}_n$, dizemos que

$$\prod_{i=1}^{n} {x_i}^{\alpha_i} \preceq^P \prod_{i=1}^{n} {x_i}^{\beta_i},$$

- se $\sum_{i=1}^{n} p_i\alpha_i < \sum_{i=1}^{n} p_i\beta_i$; ou
- se $\sum_{i=1}^{n} p_i\alpha_i = \sum_{i=1}^{n} p_i\beta_i$ e $\prod_{i=1}^{n} {x_i}^{\alpha_i} \preceq \prod_{i=1}^{n} {x_i}^{\beta_i}$.

Chamaremos $p \in \mathbb{N}^n$ de peso e o inteiro

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

de grau ponderado do monômio $\prod_{i=1}^{n} {x_i}^{\alpha_i}$ com respeito a p.

Observação 3.2.14. Se $p = (0, \cdots, 0)$ então $\preceq^P$ coincide com $\preceq$. Se $p = (1, \cdots, 1)$, então $\preceq^P$ é a $\preceq_{LG}$.

Exemplo 3.2.15. Sendo $xy^3z^3, xy^2z^4, x^2y^4z^2, x^4y, x^3y^2z^3 \in \mathbb{K}[x, y, z]$. Ordenando com respeito a cada uma das ordens monomiais definidas acima, temos

$$xy^2z^4 \preceq_L xy^3z^3 \preceq_L x^2y^4z^2 \preceq_L x^3y^2z^3 \preceq_L x^4y$$

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

$$x^4y \preceq_{LGR} xy^2z^4 \preceq_{LGR} xy^3z^3 \preceq_{LGR} x^3y^2z^3 \preceq_{LGR} x^2y^4z^2$$

$$x^4y \preceq^P xy^3z^3 \preceq^P x^2y^4z^2 \preceq^P x^3y^2z^3 \preceq^P xy^2z^4 \quad (\text{onde } p = (1,2,3))$$

Provemos a seguir que a ordem lexicográfica é, tal como foi definida, uma ordem monomial. As demonstrações de que as outras ordens definidas acima também são ordens monomiais seguem de forma análoga. Provemos:

Antissimetria: Dados $\prod_{i=1}^{n} {x_i}^{\alpha_i}$ e $\prod_{i=1}^{n} {x_i}^{\beta_i}$ em $\mathbb{M}_n$, tais que

$$\prod_{i=1}^{n} {x_i}^{\alpha_i} \preceq \prod_{i=1}^{n} {x_i}^{\beta_i} \quad \text{e} \quad \prod_{i=1}^{n} {x_i}^{\beta_i} \preceq \prod_{i=1}^{n} {x_i}^{\alpha_i}.$$

Suponhamos por contradição que $\prod_{i=1}^{n} {x_i}^{\alpha_i} \neq \prod_{i=1}^{n} {x_i}^{\beta_i}$, então existe $k \in \{1, \cdots, n\}$ tal que $\alpha_k \neq \beta_k$. Seja j o menor índice com essa propriedade.

Caso $\alpha_j < \beta_j$, então não podemos ter $\prod_{i=1}^{n} {x_i}^{\beta_i} \preceq \prod_{i=1}^{n} {x_i}^{\alpha_i}$. E se $\alpha_j > \beta_j$ não podemos ter $\prod_{i=1}^{n} {x_i}^{\alpha_i} \preceq \prod_{i=1}^{n} {x_i}^{\beta_i}$. Logo $\alpha_k = \beta_k$, o que é uma contradição, portanto $\prod_{i=1}^{n} {x_i}^{\alpha_i} = \prod_{i=1}^{n} {x_i}^{\beta_i}$.

Reflexividade: Dado qualquer $\prod_{i=1}^{n} {x_i}^{\alpha_i} \in \mathbb{M}_n$ é direto que $\prod_{i=1}^{n} {x_i}^{\alpha_i} \preceq \prod_{i=1}^{n} {x_i}^{\alpha_i}$.

Transitividade: Dados $a = \prod_{i=1}^{n} {x_i}^{\alpha_i}$, $b = \prod_{i=1}^{n} {x_i}^{\beta_i}$ e $c = \prod_{i=1}^{n} {x_i}^{\gamma_i}$ em $\mathbb{M}_n$ onde

$$a \preceq_L b \quad \text{e} \quad b \preceq_L c.$$

Se $a = b$ ou $b = c$ então é claro que $a \preceq_L c$. Suponhamos que $a \neq b$ e $b \neq c$, então existem $i, k \in \{1, \cdots, n\}$ tais que

$$\alpha_i < \beta_i \quad \text{e} \quad \alpha_j = \beta_j \ \forall j < i;$$

$$\beta_k < \gamma_k \quad \text{e} \quad \beta_\ell = \gamma_\ell \ \forall \ell < k.$$

Se $i = k$, então $\alpha_i < \gamma_i$ e $\alpha_j = \gamma_j$ para todo $j < i$. Porém, se $i < k$, então $\alpha_i < \beta_i = \gamma_i$ e $\alpha_j = \beta_j = \gamma_j$ para todo $j < i$. E se $k < i$ temos $\alpha_k = \beta_k < \gamma_k$ e $\alpha_\ell = \beta_\ell = \gamma_\ell$ para todo $\ell < k$. Em todos os casos, concluímos que $a \preceq_L c$.

Ordem total: Dados $\prod_{i=1}^{n} {x_i}^{\alpha_i}$ e $\prod_{i=1}^{n} {x_i}^{\beta_i}$ em $\mathbb{M}_n$. Se $\prod_{i=1}^{n} {x_i}^{\alpha_i} = \prod_{i=1}^{n} {x_i}^{\beta_i}$, não temos o que provar. Suponhamos que $\prod_{i=1}^{n} {x_i}^{\alpha_i} \neq \prod_{i=1}^{n} {x_i}^{\beta_i}$, então existe $k \in \{1, \cdots, n\}$ tal que

$\alpha_k \neq \beta_k$. Considere j o menor índice com essa propriedade, donde $\alpha_p = \beta_p$ para todo $p < j$. Temos que

$$\prod_{i=1}^{n} {x_i}^{\alpha_i} \preceq_L \prod_{i=1}^{n} {x_i}^{\beta_i}, \text{ se } \alpha_j < \beta_j \quad \text{ou} \quad \prod_{i=1}^{n} {x_i}^{\beta_i} \preceq_L \prod_{i=1}^{n} {x_i}^{\alpha_i}, \text{ se } \alpha_j > \beta_j$$

Produto: Dados $a = \prod_{i=1}^{n} {x_i}^{\alpha_i}$, $b = \prod_{i=1}^{n} {x_i}^{\beta_i}$ e $c = \prod_{i=1}^{n} {x_i}^{\gamma_i}$ em $\mathbb{M}_n$, onde $a \preceq_L b$. Se $a = b$, então é direto que $ac \preceq_L bc$. Se $a \neq b$, então existe $k \in \{1, \cdots, n\}$ tal que $\alpha_k < \beta_k$ e $\alpha_j = \beta_j$ para todo $j < k$. Mas

$$\alpha_k + \gamma_k < \beta_k + \gamma_k \quad \text{e} \quad \alpha_j + \gamma_j = \beta_j + \gamma_j \ \forall j < k,$$

então $ac \preceq_L bc$, pois

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

Menor elemento: Consideramos um subconjunto $S \subseteq \mathbb{M}_n$ e $gr_{x_i}(s)$ como sendo o grau da variável x_i de s. Temos que

$$S(1) = \{m \in S : gr_{x_1}(m) \leqslant gr_{x_1}(s) \ \forall s \in S\},$$

é não vazio, pois $\mathbb{N}$ é bem ordenado. Consideramos também

$$S(2) = \{m \in S(1) : gr_{x_2}(m) \leqslant gr_{x_2}(s) \ \forall s \in S(1)\},$$

que, pelo mesmo argumento, é não vazio. Continuando com essa construção obtemos

$$S(n) = \{m \in S(n-1) : gr_{x_n}(m) \leqslant gr_{x_n}(s) \ \forall s \in S(n-1)\},$$

que é não vazio e admite um elemento mínimo α, que é o mínimo de S.

3.3 ALGORITMO DA DIVISÃO EM $\mathbb{K}[x_1, \cdots, x_n]$

Definição 3.3.1. Fixamos uma ordem monomial $\preceq$ sobre $\mathbb{M}_n$ e consideramos o polinômio

$$f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} \neq 0.$$

em $\mathbb{K}[x_1, \cdots, x_n] \backslash \{0\}$. Definimos as seguintes nomenclaturas:

- O **monômio líder** de f é

$$ml_{\preceq}(f) := \max_{\preceq} \left\{ \prod_{i=1}^{n} x_i^{\alpha_i} \in \mathbb{M}(f) \right\}.$$

Usamos apenas $ml(f)$ quando a ordem monomial é claramente apresentada;

- O **termo líder**, ou termo inicial, de f é dado por $in_{\preceq}(f) := a_\alpha ml_{\preceq}(f)$, ou simplesmente $in(f)$ quando a ordem é clara;
- O **coeficiente líder** de f é $cl_{\preceq}(f) = a_\alpha \in \mathbb{K}$.

Exemplo 3.3.2. Seja $f = 2x^5y^2z - xy^3z^5 + 3x^2yz^6 + 5x^2y^3z^2 \in \mathbb{Q}[x, y, z]$. Temos os seguintes termos iniciais:

$$in_{\preceq_L}(f) = 2x^5y^2z\,, \quad in_{\preceq_{LG}}(f) = 3x^2yz^6\,, \quad in_{\preceq_{LGR}}(f) = -xy^3z^5$$

Lema 3.3.3. *Sejam $m \in \mathbb{M}_n$ e $f \in \mathbb{K}[x_1, \cdots, x_n]$, então $ml(mf) = ml(m)ml(f)$.*

Demonstração. Sejam

$$m = \prod_{i=1}^{n} {x_i}^{\alpha_i} \quad \text{e} \quad ml(f) = \prod_{i=1}^{n} {x_i}^{\beta_i},$$

temos então

$$mf = \prod_{i=1}^{n} {x_i}^{\alpha_i} \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} {x_i}^{\beta_i} = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} {x_i}^{\alpha_i+\beta_i}.$$

Portanto,

$$ml(mf) = \prod_{i=1}^{n} {x_i}^{\alpha_i+\beta_i} = \prod_{i=1}^{n} {x_i}^{\alpha_i} \prod_{i=1}^{n} {x_i}^{\beta_i} = ml(m)ml(f).$$

□

Teorema 3.3.4. *Fixada uma ordem monomial $\preceq$ e dado $g \in \mathbb{K}[x_1, \cdots, x_n]\backslash\{0\}$, para qualquer polinômio $f \in \mathbb{K}[x_1, \cdots, x_n]$ existem $q, r \in \mathbb{K}[x_1, \cdots, x_n]$ unicamente determinados pelas condições*

$$f = qg + r \quad com \quad r = 0 \quad ou \quad ml(g) \nmid m \ \forall m \in \mathbb{M}(r).$$

Algoritmo: Divisão de polinômios em várias variáveis

Entrada: $f \in \mathbb{K}[x_1 \cdots, x_n]$ e $g \in \mathbb{K}[x_1 \cdots, x_n]\backslash\{0\}$

Saída: q e r satisfazendo $f = qg + r$ com $r = 0$ ou $ml(g) \nmid m \ \forall m \in \mathbb{M}(r)$.

```
início
    q := 0;   r := 0;   h := f
    enquanto h ≠ 0 faça
        se ml(g) | ml(h) então
            q := q + in(h)/in(g)   e   h := h − (in(h)/in(g)) g
        fim
        senão
            r := r + in(h)   e   h := h − in(h)
        fim
    fim
fim
retorna q, r
```

Exemplo 3.3.5. Vamos dividir, pelo algoritmo descrito acima, $xy^4 + x^4 + x^3y + y^3$ por $y^3 + x^2$ segundo a ordem lexicográfica e, em seguida, pela ordem lexicográfica graduada.

Pela ordem lexicográfica, onde $x \succeq y$, temos inicialmente

$$\begin{array}{r|l} x^4 + x^3y + xy^4 + y^3 & x^2 + y^3 \\ \hline -(x^4 + x^2y^3) & q = x^2 \\ \hline x^3y - x^2y^3 + xy^4 + y^3 & \end{array}$$

Continuando,

$$\begin{array}{r|l} x^4 + x^3y + xy^4 + y^3 & x^2 + y^3 \\ \hline -(x^4 + x^2y^3) & q = x^2 + xy \\ \hline x^3y - x^2y^3 + xy^4 + y^3 & \\ -(x^3y + xy^4) & \\ \hline -x^2y^3 + y^3 & \end{array}$$

Por fim,

$$\begin{array}{r|l} x^4 + x^3y + xy^4 + y^3 & x^2 + y^3 \\ \hline -(x^4 + x^2y^3) & q = x^2 + xy - y^3 \\ \hline x^3y - x^2y^3 + xy^4 + y^3 & \\ -(x^3y + xy^4) & \\ \hline -x^2y^3 + y^3 & \\ -(-x^2y^3 - y^6) & \\ \hline r = y^6 + y^3 & \end{array}$$

Daí obtemos

$$x^4 + x^3y + xy^4 + y^3 = (x^2 + y^3)(x^2 + xy - y^3) + y^6 + y^3$$

Agora, pela ordem lexicográfica graduada, onde $x \succeq y$, temos inicialmente

$$\begin{array}{r|l} xy^4 + x^4 + x^3y + y^3 & y^3 + x^2 \\ \hline -(xy^4 + x^3y) & q = xy \\ \hline x^4 + y^3 & r = 0 \end{array}$$

Como $y^3 \nmid x^4$, temos

$$\begin{array}{r|l} xy^4 + x^4 + x^3y + y^3 & y^3 + x^2 \\ \hline -(xy^4 + x^3y) & q = xy \\ \hline \cancel{x^4} + y^3 & r = x^4 \\ y^3 & \end{array}$$

Continuando

$$\begin{array}{r|l} xy^4 + x^4 + x^3y + y^3 & y^3 + x^2 \\ \hline -(xy^4 + x^3y) & q = xy + 1 \\ \hline \cancel{x^4} + y^3 & r = x^4 \\ y^3 & \\ -(y^3 + x^2) & \\ \hline -x^2 & \end{array}$$

E por fim

$$\begin{array}{r|l} xy^4 + x^4 + x^3y + y^3 & y^3 + x^2 \\ \hline -(xy^4 + x^3y) & q = xy + 1 \\ \hline \cancel{x^4} + y^3 & r = x^4 - x^2 \\ y^3 & \\ -(y^3 + x^2) & \\ \hline \cancel{y^2} & \end{array}$$

Daí obtemos

$$xy^4 + x^4 + x^3y + y^3 = (y^3 + x^2)(xy + 1) + x^4 - x^2$$

3.4 IDEAIS EM $\mathbb{K}[x_1, \cdots, x_n]$

Nas seções anteriores desse capítulo, construímos uma relação que nos permitiu ordenar e dividir polinômios em várias variáveis. Nessa seção, a partir da definição 1.2.1, estamos interessados em abordar resultados mais gerais sobre ideais de $\mathbb{K}[x_1, \cdots, x_n]$.

A partir disso, veremos que alguns resultados em $\mathbb{K}[x]$ não podem ser generalizados para $\mathbb{K}[x_1, \cdots, x_n]$, como é o caso da proposição 2.3.1, que nos garante que todo ideal em $\mathbb{K}[x]$ é principal. Contudo, esta propriedade não ocorre com todos os ideais de $\mathbb{K}[x_1, \cdots, x_n]$, como pode ser visto no seguinte exemplo:

Exemplo 3.4.1. O ideal $I = \langle x_1, x_2 \rangle$ de $\mathbb{K}[x_1, \cdots, x_n]$ com $n \geqslant 2$ não é principal.

De fato, suponhamos que $g \neq 0$ seja o gerador de I. Neste caso, deveria existir um polinômio $h \in \mathbb{K}[x_1, \cdots, x_n]$ tal que

$$x_1 = hg.$$

Logo g tem grau no máximo 1 como polinômio na indeterminada x_1 e grau 0 relativo a todas as outras indeterminadas de $\mathbb{K}[x_1, \cdots, x_n]$. Como o mesmo vale para x_2, então g deve ser constante, o que implicaria em

$$I = \mathbb{K}[x_1, \cdots, x_n],$$

o que é um absurdo. Portanto, I não pode ser principal.

Por indução em n, utilizando um argumento análogo ao usado acima, podemos obter:

Proposição 3.4.2. *O ideal $\langle x_1, \cdots, x_n \rangle$ de $\mathbb{K}[x_1, \cdots, x_n]$ não pode ser gerado por menos de n polinômios.*

Definição 3.4.3. O ideal I_k de $\mathbb{K}[x_1, x_2]$ é dado por

$$I_k := \langle x_1^k, x_1^{k-1}x_2, \cdots, x_1x_2^{k-1}, x_2^k \rangle.$$

Temos, em particular, $I_1 = \langle x_1, x_2 \rangle$ e $I_2 = \langle x_1^2, x_1x_2, x_2^2 \rangle$.

Proposição 3.4.4. *O ideal I_k não pode ser gerado por menos do que $k+1$ polinômios.*

Demonstração. Suponha que I_k possa ser gerado por polinômios não nulos $g_1, \cdots, g_s$ onde $s < k+1$. Como I_k é gerado pelos monômios de grau k (segundo a definição anterior), o termo de menor grau de cada g_i tem que ter grau pelo menos k. Seja t_i o termo de grau k de g_i. Temos, então que $g_i - t_i$ só tem termos de grau maior que k. Portanto $g_i - t_i \in I_{k+1}$.

Escrevemos o monômio $x_1^j x_2^{k-j}$ como combinação dos geradores $g_1, \cdots, g_s$, obtemos

$$x_1^j x_2^{k-j} = q_1 g_1 + \cdots + q_s g_s.$$

Disto, segue que

$$x_1^j x_2^{k-j} - (c_1 t_1 + \cdots + c_s t_s) \in I_{k+1},$$

em que c_i é o termo constante de q_i. Como I_{k+1} só tem polinômios não nulos de grau maior ou igual a $k+1$, obtemos

$$x_1^j x_2^{k-j} = c_1 t_1 + \cdots + c_s t_s$$

Isto significa que os polinômios $t_1, \cdots, t_s$, geram o $\mathbb{K}$-espaço vetorial V_k dos polinômios homogêneos de grau k. Obtivemos um conjunto de geradores para o espaço vetorial V_k com apenas s elementos. Entretanto, os $k+1$ monômios de grau k formam uma base de V_k como espaço vetorial, de modo que $\dim_k(V_k) = k+1$. Como uma base é um conjunto mínimo de geradores, temos uma contradição com $s < k+1$. □

As proposições 3.4.2 e 3.4.4 mostram que $\mathbb{K}[x_1, \ldots, x_n]$ não é um domínio de ideais principais, o que foi fundamental, no capítulo anterior, para resolver o problema da pertinência em ideais no anel $\mathbb{K}[x]$. Temos, no entanto, o seguinte teorema que nos garante a existência de uma base finita para qualquer ideal de $\mathbb{K}[x_1, \ldots, x_n]$.

Teorema 3.4.5 (Teorema das bases de Hilbert)**.** *Todo ideal de $\mathbb{K}[x_1, \cdots, x_n]$ é finitamente gerado.*

Adiaremos a demonstração do teorema até introduzirmos o conceito das bases de Gröbner no próximo capítulo. O principal objetivo do estudo dessa base é solucionar o problema da pertinência em ideais em $\mathbb{K}[x_1, \cdots, x_n]$.

No restante da seção solucionaremos este problema para um caso particular, em ideais monomiais. Para isto, enunciaremos o Lema de Dickson e, ainda que seja um resultado restrito a ideais monomiais, será uma ferramenta necessária, junto às bases de Gröbner, para provar o teorema das bases de Hilbert.

Definição 3.4.6. Um ideal $I \subset \mathbb{K}[x_1, \cdots, x_n]$ é chamado de **ideal monomial** se existe um conjunto de monômios que geram I.

Exemplo 3.4.7. O ideal $I = \langle x^3 + xy^4, y^2 \rangle$ é monomial. Basta observar que $I = \langle x^3, y^2 \rangle$.

Teorema 3.4.8 (Lema de Dickson)**.** *Seja I um ideal monomial de $\mathbb{K}[x_1, \cdots, x_n]$, então I é finitamente gerado por monômios.*

Demonstração. Mostraremos que se $\mathbb{K}[x_1, \cdots, x_n]$ admite um ideal monomial que não é finitamente gerado, então $\mathbb{K}[x_1, \cdots, x_{n-1}]$ também admite um tal ideal. Dessa forma, $\mathbb{K}[x_1]$ admitiria ideais monomiais que não são finitamente gerados, o que contradiz a proposição 2.3.1.

Suponha que $I \subset \mathbb{K}[x_1, \cdots, x_n]$ seja este ideal. Escolhemos uma sequência de monômios em I tais que

- $\mu_1 \in I$ e $gr_{x_n}(\mu_1)$ é o menor possível;
- $\mu_2 \in I \backslash \langle \mu_1 \rangle$ e $gr_{x_n}(\mu_2)$ é o menor possível;
- $\mu_3 \in I \backslash \langle \mu_1, \mu_2 \rangle$ e $gr_{x_n}(\mu_3)$ é o menor possível;

  $\cdots$

- $\mu_s \in I \backslash \langle \mu_1, \cdots, \mu_{s-1} \rangle$ e $gr_{x_n}(\mu_s)$ é o menor possível;

  $\cdots$

Como I não é finitamente gerado, esta sequência é infinita e fixada uma ordem monomial podemos sempre obter estes monômios de menor grau. Temos que $\mu_i = v_i x_n^{k_i}$, onde v_i é um monômio nas indeterminadas $x_1, \cdots, x_{n-1}$. Consideramos o ideal J de $\mathbb{K}[x_1, \cdots, x_{n-1}]$ gerado pelos $v's$.

Se J fosse finitamente gerado, então pela proposição 1.2.6 poderia ser gerado pelos monômios $v_1, \cdots, v_m$, para algum inteiro $m > 0$. Mas v_{m+1} também é um monômio, o que implica

$$v_{m+1} = v_\ell \eta,$$

para algum $1 \leqslant \ell \leqslant m$ e algum monômio $\eta \in \mathbb{K}[x_1, \cdots, x_{n-1}]$. Porém, a escolha dos $\mu's$ implica que $k_{m+1} \geqslant k_\ell$, daí

$$\mu_{m+1} = v_{m+1} x_n^{k_{m+1}} = \eta x_n^{k_{m+1} - k_\ell} \mu_\ell.$$

O que implica em $\mu_{m+1} \in \langle \mu_1, \cdots, \mu_m \rangle$, contradizendo a escolha de μ_{m+1}. Portanto, J não pode ser finitamente gerado.

□

Proposição 3.4.9. *Sejam* $\mathbb{K}$ *um corpo e*

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots$$

uma sequência ascendente de subconjuntos formados por monômios do anel de polinômios $\mathbb{K}[x_1, \cdots, x_n]$. *Então existe um inteiro* $k > 0$ *tal que* $\langle S_t \rangle = \langle S_k \rangle$ *para todo* $t \geqslant k$.

Sua demonstração segue direto da proposição 1.2.6 e do teorema 3.4.8 obtemos a seguinte proposição:

Proposição 3.4.10. *Um polinômio* $f \in \mathbb{K}[x_1, \cdots, x_n]$ *pertence a um ideal monomial* $I = \langle m_1, \cdots, m_s \rangle$ *se, e somente se,* $m \in I$ *para todo* $m \in \mathbb{M}(f)$.

O resultado acima nos dá um modo de decidir se um elemento $f \in \mathbb{K}[x_1, \cdots, x_n]$ pertence a um ideal monomial I. Para isto, consideramos um conjunto finito de geradores $\{m_1, \cdots, m_s\}$ de I (garantido pelo Lema de Dickson) e verificamos se cada monômio de f pertence ao ideal I. Isto ocorre se, e somente se, cada monômio é divisível por um dos monômios que geram I.

Exemplo 3.4.11. Consideramos o ideal $I = \langle x^3 + xy^4, y^2 \rangle$ e os polinômios

$$f = 6x^4 + 4xy^2 - 3x^3y \quad \text{e} \quad g = 2x^4 + 5xy^2 - 8x^2y.$$

Do exemplo anterior temos que I é um ideal monomial dado por $I = \langle x^3, y^2 \rangle$. Da proposição 3.4.10 temos para o polinômio f:

$$x^3 \,\Big|\, 6x^4\,, \qquad y^2 \,\Big|\, 4xy^2\,, \qquad x^3 \,\Big|\, -3x^3y,$$

portanto $f \in I$. Já para o polinômio g, temos que $-8x^2y$ não é divisível por nenhum dos monômios geradores de I, portanto $g \notin I$.

3.5 ALGORITMO DA PSEUDO-DIVISÃO

Até o momento somos capazes de ordenar os monômios a fim de determinarmos o termo inicial de um polinômio de várias variáveis. Vimos também que nem todo ideal de $\mathbb{K}[x_1, \cdots, x_n]$ é principal, seguindo o raciocínio do capítulo anterior seríamos levados a solucionar o problema da pertinência estudando o resto da divisão de um dado polinômio pelos geradores de um ideal.

Para isto, nesta seção, enunciaremos um método que estrutura a divisão de um polinômio por outros ao mesmo tempo: o algoritmo da pseudo-divisão e veremos ao final que utilizar qualquer conjunto de geradores de um dado ideal não nos auxilia a solucionar o problema da pertinência, isto só será resolvido no próximo capítulo com as bases de Gröbner.

Teorema 3.5.1. *Fixada uma ordem monomial $\preceq$ e dados $f, g_1, \cdots, g_s \in \mathbb{K}[x_1, \cdots, x_n]$ com $g_i \neq 0$ para todo $i \in \{1, \cdots, s\}$, existem polinômios $q_1, \cdots, q_s \in \mathbb{K}[x_1, \cdots, x_n]$ tais que*

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

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

Definição 3.5.2. Denotaremos o polinômio r, obtido pelo teorema 3.5.1, que representa o resto da pseudo-divisão de f pelos elementos de $G = \{g_1, \cdots, g_s\}$ como sendo $R_G(f)$.

Algoritmo: PSEUDO-DIVISÃO

Entrada: $f \in \mathbb{K}[x_1 \cdots, x_n]$ e $g_1, \cdots, g_s \in \mathbb{K}[x_1 \cdots, x_n] \backslash \{0\}$

Saída: $q_1, \cdots, q_s \in \mathbb{K}[x_1, \cdots, x_n]$ tais que $f = \sum_{i=1}^{s} q_i g_i + r$, com $ml(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$ e todo $i \in \{1, \cdots, s\}$

início
  $q_1 := \cdots := q_s := r := 0$ e $h := f$;
  enquanto $h \neq 0$ **faça**
    se $\exists i \in \{1, \cdots, s\}$ *tal que* $ml(g_i) \mid ml(h)$ **então**
      Escolha o menor índice i com essa propriedade
      $q_i := q_i + \dfrac{in(h)}{in(g_i)}$ e $h_i := h - \dfrac{in(h)}{in(g_i)} g_i$
    fim
    senão
      $r := r + in(h)$ e $h := h - in(h)$
    fim
  fim
fim
retorna $q_1, \cdots, q_s$

Exemplo 3.5.3. Façamos a divisão, pelo algoritmo da pseudo-divisão, de

$$f = y^4 - x^2y - xy^2 + x^2 + xy + y^2 + x \quad \text{por} \quad g_1 = y^2 - x \quad \text{e} \quad g_2 = xy - y$$

segundo a ordem lexicográfica graduada. Resolvemos de maneira esquemática tal como segue abaixo:

Inicialmente, temos

$$\begin{array}{r|l} & y^2 - x \\ y^4 - x^2y - xy^2 + x^2 + xy + y^2 + x & xy - y \\ \hline -(y^4 - xy^2) & q_1 = y^2 \\ \hline -x^2y - x^2 + xy + y^2 + x & q_2 = 0 \\ & r = 0 \end{array}$$

Agora,

$$\begin{array}{r|l}
 & y^2 - x \\
y^4 - x^2y - xy^2 + x^2 + xy + y^2 + x & xy - y \\
\cline{2-2}
-(y^4 - xy^2) & q_1 = y^2 \\
\cline{1-2}
-x^2y - x^2 + xy + y^2 + x & q_2 = -x \\
-(-x^2y + xy) & r = 0 \\
\cline{1-2}
x^2 + y^2 + x & \\
\end{array}$$

Como o monômio líder não é divisível nem pelo monômio líder de g_1 e nem pelo de g_2, temos

$$\begin{array}{r|l}
 & y^2 - x \\
y^4 - x^2y - xy^2 + x^2 + xy + y^2 + x & xy - y \\
\cline{2-2}
-(y^4 - xy^2) & q_1 = y^2 \\
\cline{1-2}
-x^2y - x^2 + xy + y^2 + x & q_2 = -x \\
-(-x^2y + xy) & r = x^2 \\
\cline{1-2}
\cancel{x^2} + y^2 + x & \\
y^2 + x & \\
\end{array}$$

Por fim,

$$\begin{array}{r|l}
 & y^2 - x \\
y^4 - x^2y - xy^2 + x^2 + xy + y^2 + x & xy - y \\
\cline{2-2}
-(y^4 - xy^2) & q_1 = y^2 + 1 \\
\cline{1-2}
-x^2y - x^2 + xy + y^2 + x & q_2 = -x \\
-(-x^2y + xy) & r = x^2 + 2x \\
\cline{1-2}
\cancel{x^2} + y^2 + x & \\
y^2 + x & \\
-(y^2 - x) & \\
\cline{1-2}
\cancel{2x} & \\
\end{array}$$

Exemplo 3.5.4. Façamos a divisão de $f = xy^2 - x$ por $g_1 = y^2 - x$ e $g_2 = xy - y$ fixada a ordem lexicográfica graduada. Depois refaçamos os cálculos invertendo a ordem de g_1 e g_2. Temos

$$\begin{array}{r|l}
 & y^2 - x \\
xy^2 - x & xy - y \\
\cline{2-2}
-(xy^2 - x^2) & q_1 = x \\
\cline{1-2}
\cancel{x^2} + \cancel{x} & q_2 = 0 \\
 & r = x^2 - x \\
\end{array}
\qquad \text{e} \qquad
\begin{array}{r|l}
 & xy - y \\
xy^2 - x & y^2 - x \\
\cline{2-2}
-(xy^2 - y^2) & q_1 = y \\
\cline{1-2}
y^2 - x & q_2 = 1 \\
-(y^2 - x) & r = 0 \\
\cline{1-2}
0 & \\
\end{array}$$

Neste exemplo, podemos ver que a forma de escolher os divisores influencia os valores de q_1, q_2 e r. Desta forma, o polinômio f pertence ao ideal $\langle g_1, g_2 \rangle$, pois pela

segunda maneira que dividimos obtemos resto zero. Porém, pela primeira ordem de divisão este resultado não se faria claro.

Somos levados a pensar que bastaria testar todas as $s!$ possíveis formas de se listar os polinômios $g_1, \cdots, g_s$ que geram o ideal $I = \langle g_1, \cdots, g_s \rangle$ para determinar se o polinômio f pertence a I ao resultar $r = 0$ em alguma dessas permutações. Entretanto, o próximo exemplo nos mostra que independente de obtermos restos não nulos para todas as formas de divisão, um polinômio pode pertencer ao ideal.

Exemplo 3.5.5. O polinômio $f = x^2y^4 - x^2$ pertence ao ideal $I = \langle y^2 - x, xy - y \rangle$, basta observar que

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

Porém, utilizando a ordem lexicográfica graduada, os restos de f, segundo o algoritmo da pseudo-divisão, em todas as possíveis permutações são não nulos.

$$\begin{array}{r|l} & y^2 - x \\ x^2y^4 - x^2 & xy - y \\ \hline -(x^2y^4 - x^3y^2) & q_1 = x^2y^2 + x^3 \\ \hline x^3y^2 - x^2 & q_2 = 0 \\ -(x^3y^2 - x^4) & r = x^4 - x^2 \\ \hline \cancel{x^4} \cancel{-x^3} \cancel{+x^2} & \end{array} \quad \text{e} \quad \begin{array}{r|l} & xy - y \\ x^2y^4 - x^2 & y^2 - x \\ \hline -(x^2y^4 - xy^4) & q_1 = xy^3 + y^3 + y \\ \hline xy^4 - x^2 & q_2 = y^2 + 1 \\ -(xy^4 - y^4) & r = -x^2 + x \\ \hline y^4 - x^2 & \\ -(y^4 - xy^2) & \\ \hline xy^2 - x^2 & \\ -(xy^2 - y^2) & \\ \hline \cancel{-x^2} \cancel{+y^2} + y^2 & \\ y^2 & \\ -(y^2 - x) & \\ \hline \cancel{x} & \end{array}$$

Observamos que se o resto for nulo em alguma permutação escolhida, então o polinômio que foi dividido pertence ao ideal, porém a recíproca não é verdadeira conforme o exemplo visto acima.

No próximo capítulo, veremos que para obter esta equivalência e solucionarmos o problema da pertinência, será necessário definir um tipo especial de geradores, conhecidos como bases de Gröbner de um ideal. Mas antes disso, de passar ao próximo capítulo, vamos discutir um pouco sobre ideais radicais em anéis de polinômios.

3.6 IDEAIS RADICAIS DE POLINÔMIOS

Nessa seção, queremos obter um critério para determinar se um ideal $I \subset K[x_1, \ldots, x_n]$ é radical. Para isso, precisamos de um pouco de Geometria Algébrica.

Definição 3.6.1. Sejam os corpos $K \subset L$ e um subconjunto $S \subset K[x_1, \cdots, x_n]$, o **conjunto algébrico** $Z_L(S)$ é o conjunto dos pontos de L^n que se anulam em todos os polinômios de S, isto é,

$$Z(S) = \{p \in L^n \mid f(p) = 0 \ \forall f \in S\}$$

Por outro lado, dado $X \subset L^n$, o **ideal** de X em $\mathbb{K}[x_1, \cdots, x_n]$ é definido por

$$I(X) = \{f \in K[x_1, \cdots, x_n] \mid f(P) = 0 \, \forall \, P \in X\}$$

Exemplo 3.6.2. Seja $I = \langle S \rangle$ um ideal de L, então $Z(I) = Z(S)$. E se $1 \in I$, então $Z(I) = \emptyset$.

Teorema 3.6.3 (Teorema dos Zeros de Hilbert)**.** *O conjunto algébrico $Z(I)$ não é vazio se, e somente se, I é um ideal próprio de $\mathbb{K}[x_1, \cdots, x_n]$.*

Basicamente, o Teorema dos Zeros de Hilbert afirma que um ideal próprio é aquele que tem zeros e sua principal aplicação nesse trabalho é o Teorema 3.6.4, cuja ideia da demonstração será discutida a seguir.

Sejam f um polinômio e $I \subset K[x_1, \ldots, x_n]$ um ideal. Sabemos que se $f \in \sqrt{I}$, então existe $k \in \mathbb{N}$ tal que $f^k \in I$. Assim, $(f(P))^k = f^k(P) = 0$ para todo $P \in Z(I)$, ou seja, $f(P) = 0$ para todo $P \in Z(I)$. Agora, observamos que $f(P) \neq 0$ se e somente se existe $z_0 \in K$ tal que $z_0 f(P) = 1$, ou seja, $1 - zf$ se anula no ponto $(P, z_0) \in Z(I) \times K$. Considerando então o ideal de $\mathbb{K}[x_1, \ldots, x_n, z]$ dado por

$$J(I, f) = \langle 1 - zf \rangle + K[x_1, \ldots, x_n]I$$

obtemos, a partir de seus zeros, um conjunto algébrico em K^{n+1} tal que

$$(P, z_0) \in Z(J(I, f)) \Leftrightarrow f(P) \neq 0, \ P \in Z(I)$$

o que é equivalente a

$$f(P) \neq 0, \ P \in Z(I) \Leftrightarrow Z(J(I, f)) \neq \emptyset \Leftrightarrow 1 \notin J(I, f)$$

onde a última equivalência vem do Teorema dos Zeros de Hilbert.

Esse argumento é conhecido como truque de Rabinowitch e é o principal ingrediente na demonstração do seguinte Teorema.

Teorema 3.6.4. *Sejam I um ideal e f um elemento do anel de polinômios $\mathbb{K}[x_1, \cdots, x_n]$, então $f(p) = 0$ para todo $p \in Z(I)$ se, e somente se, $f \in \sqrt{I}$.*

Como conseqüência, temos:

Teorema 3.6.5. *Seja I um ideal de $\mathbb{K}[x_1, \ldots, x_n]$. Então, $I(Z(I)) = \sqrt{I}$. Reciprocamente, se X é um conjunto algébrico, então $Z(I(X)) = X$.*

Concluimos, então, que os ideais radicais são parte importante da decisão sobre a pertinência ou não de um polinômio f em um ideal de $\mathbb{K}[x_1, \cdots, x_n]$. Surge então uma pergunta: como decidir se um ideal $I \subset K[x_1, \cdots, x_n]$ é radical, isto é, se $I = \sqrt{I}$?

Vamos começar com uma definição.

Definição 3.6.6. Dizemos que um ideal $I \subset K[x_1, \cdots, x_n]$ tem **dimensão zero** se o conjunto algébrico correspondente tem um número finito de elementos.

Existem infinitos exemplos de conjuntos algébricos com um número finito de elementos, o que é o caso, por exemplo, do conjunto de pontos na interseção entre curvas algébricas (onde, por curva algébrica, entendemos o conjunto de zeros de um polinômio em duas variáveis). É possível provar que $I \subset \mathbb{K}[x_1, \cdots, x_n]$ é um ideal de dimensão zero se e somente se $I \cap \mathbb{K}[x_j] \neq \{0\}$ para todo $1 \leqslant j \leqslant n$, o que representa um critério de fácil aplicação. Agora, lembramos que $I \cap \mathbb{K}[x_j]$ é um ideal de $\mathbb{K}[x_i]$ e, por isso, é principal, gerado digamos por f_j. Fatorando $f_j = cp_1^{e_1} \ldots p_s^{e^s}$ e tomando $e = \max\{e_1, \ldots, e_s\}$, podemos concluir que

$$(p_1 \ldots p_s)^e = \left(\frac{1}{c} p_1^{e-e_1} \ldots p_s^{e-e_s}\right) f_k \in I$$

Assim, se I for radical, temos que $p_1 \ldots p_s \in I$. Notando que, como os polinômios p_j são irredutíveis, o que provamos foi que se I é um ideal radical de dimensão zero, então existe um polinômio livre de quadrados em $I \cap K[x_j]$. Esse argumento pode ser feito para todo $1 \leqslant j \leqslant n$. Supreendentemente, a recíproca desse resultado também é verdadeira e pode ser provada usando indução em n (veja [4], pg 299).

Lema 3.6.7 (Critério de Seidenberg)**.** *Seja I um ideal de dimensão zero do anel de polinômios $\mathbb{K}[x_1, \cdots, x_n]$. O ideal I é radical se, e somente se, para cada $1 \leqslant j \leqslant n$, existe um polinômio livre de quadrados em $I \cap \mathbb{K}[x_j]$.*

4 BASES DE GRÖBNER

Ainda que tenhamos, pelo teorema das bases de Hilbert, a garantia da existência de um conjunto finito de geradores para um ideal I em $\mathbb{K}[x_1, \cdots, x_n]$, utilizar o algoritmo da pseudo-divisão apresentou problemas em determinar se um polinômio f pertence ou não ao ideal I. Como foi visto nos exemplos do capítulo anterior, não tínhamos a unicidade do resto, que dependia da ordem de divisão escolhida sob uma certa ordem monomial $\succeq$.

Com isso, fomos levados a questionar o algoritmo da pseudo-divisão ou a base de geradores escolhida para solucionar o problema da pertinência. Neste capítulo, veremos que o algoritmo da forma que foi proposta é um passo necessário para a solucão deste problema e que a mudança necessária está em determinar uma base melhor para a divisão.

4.1 CONCEITOS INICIAIS

Suponhamos que esteja fixada uma ordem monomial $\succeq$, nosso objetivo agora é formular um algoritmo que nos permite determinar um conjunto de geradores para um ideal com certas propriedades de modo que um polinômio pertença ao ideal se, e somente se, deixa resto zero na divisão por estes geradores.

Definição 4.1.1. Sejam I um ideal e $\succeq$ uma ordem monomial de $\mathbb{K}[x_1, \cdots, x_n]$. O **ideal inicial** $in(I)$ de I é o ideal de $\mathbb{K}[x_1, \cdots, x_n]$ gerado pelos termos iniciais $in(f)$ de cada polinômio $f \in I$.

Como I é finitamente gerado por uma coleção de polinômios $g_1, \cdots, g_s$, desta definição podemos questionar se $in(g_1), \cdots, in(g_s)$ gerariam $in(I)$. Isto não é verdade e pode ser visto no seguinte exemplo:

Exemplo 4.1.2. Sob a ordem lexicográfica, consideramos o ideal I de $\mathbb{K}[x_1, x_2]$ gerado por $g_1 = x_1^2$ e $g_2 = x_1x_2 + x_2^2$. O ideal inicial $in(I)$ não é gerado por $in(g_1)$ e $in(g_2)$.

De fato, sob a ordem lexicográfica considerando $x_1 \succeq x_2$, temos que

$$in(g_1) = {x_1}^2 \quad \text{e} \quad in(g_2) = x_1x_2.$$

Daí

$$f = x_2g_1 - x_1g_2 = -x_1x_2^2 \in I \implies h = f + x_2g_2 = x_2^3 \in I$$

Portanto $x_2^3 = in(h) \in in(I)$, mas $x_2^3 \notin \langle in(g_1), in(g_2)\rangle$

Definição 4.1.3. Um subconjunto finito $G \subset I$ é uma **base de Gröbner** para I se $in(I)$ for gerado pelos termos inciais $in(g)$ para cada $g \in G$.

Concluímos direto da definição que se G é uma base de Gröbner, então $in(G)$ gera $in(I)$, no entanto não é direto que G gera I. A seguinte proposição estabelece um corolário em que isto torna-se verificado.

Proposição 4.1.4. *Sejam $J \subseteq I$ ideais de $\mathbb{K}[x_1, \cdots, x_n]$. Se $in(J) = in(I)$, então $I = J$.*

Demonstração. Seja $\succeq$ uma ordem monomial. Suponhamos por contradição que $J \neq I$. Como $\succeq$ é uma boa ordem, então $I \backslash J$ tem um elemento f cujo termo inicial é mínimo em relação a $\succeq$. Porém, por hipótese, $in(J) = in(I)$, então $in(f) \in in(J)$, portanto existe $g \in J$ tal que $in(g) = in(f)$. O que implica em $in(f) \succeq in(f - g)$. Pela minimalidade de f, $f - g \in J$. Como $g \in J$, então $f \in J$, uma contradição. Portanto $I = J$. □

Corolário 4.1.5. *Seja I um ideal de $\mathbb{K}[x_1, \cdots, x_n]$. Se G é uma base de Gröbner de I, então G gera I.*

Demonstração. Como $\langle G \rangle \subseteq I$ e $in(I) = \langle in(G) \rangle = in(\langle G \rangle)$, então, pela proposição 4.1.4, $I = \langle G \rangle$. □

Estamos em condição de demonstrar agora o Teorema das Bases de Hilbert.

Teorema 4.1.6 (Teorema das bases de Hilbert)**.** *Todo ideal de $\mathbb{K}[x_1, \cdots, x_n]$ é finitamente gerado.*

Demonstração. Sejam I um ideal e uma ordem monomial $\succeq$ em $\mathbb{K}[x_1, \cdots, x_n]$. Pelo Lema de Dickson (Teorema 3.4.8), existe um conjunto finito de monômios $\{\mu_1, \cdots, \mu_s\}$ que geram $in(I)$. Para cada j, seja $g_j \in I$ tal que seu termo inicial é μ_j. Seja J o ideal gerado pelos $g_1, \cdots, g_s$. Então, $J \subseteq I$ e $in(J) = in(I)$, pela proposição anterior $I = J$, portanto I é gerado por $g_1, \cdots, g_s$. □

Exemplo 4.1.7. Sob a ordem lexicográfica, consideramos o ideal I de $\mathbb{K}[x_1, x_2]$ gerado por $g_1 = x_1^2$ e $g_2 = x_1x_2 + x_2^2$ tal como foi enunciado no exemplo 4.1.2. Vamos mostrar que o conjunto $G = \{g_1, g_2, h\}$ é uma base de Gröbner de $I = \langle g_1, g_2 \rangle$.

Temos $G \subseteq I$ resta mostrar que $in(g_1)$, $in(g_2)$ e $in(h)$ geram $in(I)$. Dado $f \in \mathbb{K}[x_1, x_2]$ podemos escrevê-lo da forma

$$f = x_1^2 f_1(x_1, x_2) + x_1 f_2(x_2) + f_3(x_2),$$

com a ordem lexicográfica em que $x_1 \succeq x_2$. Temos que, se $f_1 \neq 0$ então

$$in(f) = in(x_1^2 f_1) = x_1^2 in(f_1) \in in(I) \implies in(f) \in in(I)$$

Logo para todo $f \in I$ onde $f_1 \neq 0$, temos $in(f) \in in(I)$. Suponhamos agora que $f_1 = 0$ e $f_2 \neq 0$. Temos $in(f) = in(x_1 f_2) = x_1 in(f_2)$. Se f_2 não se reduz a uma constante,

então $in(f_2)$ é divisível por x_2 o que implica que $in(f)$ é divisível por $in(g_2)$. Se f_2 se reduz a uma constante então $f = ax_1 + f_3(x_2)$ com a constante não nula. Mas como $f \in I$, então existem $q_1, q_2 \in \mathbb{K}[x_1, x_2]$ tais que $f = q_1g_1 + q_2g_2$.

Fazendo $x_1 = 0$ então $f(0, x_2) = f_3(x_2) = q_2(0, x_2)x_2^2$ logo $f = ax_1 + x_2^2q_2(0, x_2)$. E fazendo $x_2 = 0$ temos $f(x_1, 0) = ax_1 = q_1(x_1, 0)g_1(x_1, 0) = q_1(x_1, 0){x_1}^2$ então $a = 0$ que é uma contradição. Portanto, não existe este caso.

Falta apenas o caso $f_1 = 0 = f_2$ então $f = f_3(x_2)$. Se f_3 for divisível por x_2^3, então $in(f)$ é divisível por $in(h)$. Caso contrário $f_3 = a{x_2}^2 + bx_2 + c$ com a, b, c constantes. Pelo mesmo argumento escrevemos $f = q_1g_1 + q_2g_2$ e fazemos $x = 0$, obtendo $f(0, x_2) = ax_2^2 + bx_2 + c = q_2(0, x_2)x_2^2$, então $b = 0 = c$ e $f = ax_2^2$.

Já temos que $\langle x_1^2, x_1x_2 + x_2^2\rangle \subseteq \langle x_1^2, x_1x_2, x_2^2\rangle$. E como $a \neq 0$, então $g_2 - \frac{1}{a}f = x_1x_2$, donde $\langle x_1^2, x_1x_2, x_2^2\rangle \subseteq \langle x_1^2, x_1x_2 + x_2^2\rangle \subseteq I$. Portanto os ideais são iguais, mas pela proposição 3.4.4 o ideal I não pode ser gerado por dois elementos, então não ocorre este caso. Daí, $G = \{g_1, g_2, h\}$ é base de Gröbner do ideal I.

O primeiro questionamento que podemos fazer é na forma que determinamos o polinômio h no exemplo 4.1.2 para então mostrarmos que $G = \{g_1, g_2, h\}$ é base de Gröbner de I. E ainda que o exemplo seja simples, a demonstração de que G é uma base de Gröbner é exaustiva, o que nos leva a buscar um algoritmo que auxilie na construção de uma base.

Veremos este algoritmo na próxima seção, onde a construção do polinômio h em 4.1.2, se tornará mais sugestiva.

4.2 ALGORITMO DE BUCHBERGER

Nesta seção enunciaremos o algoritmo de Buchberger, que auxiliará na construção de uma base de Gröbner para um determinado ideal I em $\mathbb{K}[x_1, \cdots, x_n]$ munido de uma ordem monomial $\succeq$. A próxima definição traz a estrutura do polinômio h do exemplo 4.1.2, que utilizamos para a construção da base de Gröbner.

Definição 4.2.1. Definimos $\mathcal{S}(g_1, g_2)$ como sendo o **$\mathcal{S}$-polinômio** de g_1 e g_2 dado por:

$$\mathcal{S}(g_1, g_2) = \frac{in(g_2)}{\delta}g_1 - \frac{in(g_1)}{\delta}g_2,$$

onde $\delta = mdc(in(g_1), in(g_2))$.

Algoritmo: Algoritmo de Buchberger

Entrada: Subconjunto finito $\mathcal{S} \subset \mathbb{K}[x_1, \cdots, x_n]$

Saída: Base de Gröbner G do ideal gerado pelos polinômios de $\mathcal{S}$ em $\mathbb{K}[x_1, \cdots, x_n]$

```
1  início
2      G := S                                                    // (etapa 1)
3      P := {(g, g') | g, g' ∈ G e g ≠ g'}
4      enquanto P ≠ ∅ faça                                       // (etapa 2)
5          Escolher (g, g') ∈ P
6          Remover (g, g') de P
7          Calcular o resto r da divisão do S-polinômio S(g, g') por G
8          se r ≠ 0 então
9              Acrescente r a G
10             Acrescente a P os pares do tipo (h, r) para cada h ∈ G\{r}
11         fim
12     fim
13 fim
14 retorna G                                                     // (etapa 3)
```

Devemos provar que o algoritmo de Buchberger funciona e para isto é necessário mostrar que ele executa uma quantidade finita de passos e que ao final destes o algoritmo retorna uma base de Gröbner. Começamos pela finitude de etapas:

Digamos que $G_0 = \mathcal{S}$ e G_j seja o conjunto de geradores resultante ao final do j-ésimo passo. Então

$$G_{j+1} = G_j \cup \{r_{j+1}\}$$

onde r_{j+1} é o resto da divisão de algum $\mathcal{S}$-polinômio por G_j relativo a ordem monomial $\succeq$. Então

$$G_0 \subseteq G_1 \subseteq \cdots \subseteq G_j \subseteq \cdots \implies in(\langle G_0 \rangle) \subseteq in(\langle G_1 \rangle) \subseteq \cdots \subseteq in(\langle G_j \rangle) \subseteq \cdots,$$

isto é, uma cadeia ascendente de ideais, pela proposição 3.4.9, existe inteiro $k > 0$ tal que

$$in(\langle G_k \rangle) = in(\langle G_t \rangle) \quad \forall\, t \geqslant k.$$

Logo $in(r_{t+1}) \in (\langle G_k \rangle)$ para todo $t \geqslant k$, portanto $r_{t+1} = 0$, caso contrário iria contradizer a minimalidade de r_{t+1} com respeito a G_t.

Desta forma, após k passos, obtemos a propriedade acima que nos garante que $r_{t+1} = 0$ para todo $t \geqslant k$. Portanto o algoritmo não executará mais o último passo da *etapa 2*, levando mais um número finito de procedimentos até obter $\mathcal{P} = \emptyset$ e, finalmente, parar. Resta-nos mostrar que ao atingirmos esta propriedade, isto é, o resto de todos os $\mathcal{S}$-polonômios na divisão por G_k são nulos, então G_k é uma base de Gröbner. Antes de

provarmos essa propriedade, tida como o critério de Buchberger, enunciemos o seguinte lema técnico:

Lema 4.2.2. *Sejam g_1, g_2, u_1 e u_2 polinômios não nulos em $\mathbb{K}[x_1, \cdots, x_n]$. Se $in(u_1 g_1)$ é múltiplo constante de $in(u_2 g_2)$, então existem constantes $c_1, c_2 \in \mathbb{K}$ e um monômio $\theta \in \mathbb{T}^n$ tais que*

$$in(u_1) = c_1 \theta v_2 \quad e \quad in(u_2) = c_2 \theta v_1$$

em que v_i é o monômio obtido dividindo $in(g_i)$ pelo $MDC(in(g_1), in(g_2))$.

Demonstração. Por hipótese, existe $a \in \mathbb{K}$, tal que

$$in(u_1) in(g_1) = a\ in(u_2) in(g_2). \tag{4.1}$$

Por outro lado, considerando δ o máximo divisor comum entre $in(g_1)$ e $in(g_2)$, obtemos

$$in(g_i) = \delta v_i \quad \text{com} \quad v_1, v_2 \in \mathbb{T}^n.$$

Substituindo a igualdade acima em (4.1) e cancelando δ, temos

$$in(u_1) v_1 = a\ in(u_2) v_2,$$

e como v_1 e $in(g_2)$ não têm monômios em comum, concluímos que

$$in(u_2) = c_2 v_1 \theta,$$

para algum $\theta \in \mathbb{T}^n$ e alguma constante não nula $c_2 \in \mathbb{K}$. Obtemos ainda que $in(u_1) = c_1 v_2 \theta$, onde $c_1 = a c_2$, tal como queríamos. □

Teorema 4.2.3 (Critério de Buchberger)**.** *Seja $G \subset \mathbb{K}[x_1, \cdots, x_n]$ finito e I o ideal gerado pelos elementos de G. Temos que G é uma base de Gröbner de I se, e somente se, $R_G(\mathcal{S}(g, g')) = 0$ para todo $(g, g') \in G \times G$.*

Demonstração. Seja $G \subset \mathbb{K}[x_1, \cdots, x_n]$ finito e I o ideal gerado pelos elementos de G. Suponhamos que G seja uma base de Gröbner de I. Se $g, g' \in G$, então $\mathcal{S}(g, g') \in \langle G \rangle$. Portanto, pela propriedade 4.3.1 que veremos na próxima seção, $\mathcal{S}(g, g')$ deixa resto zero na divisão por G.

Reciprocamente, podemos supor sem perda de generalidade que todos os elementos de G sejam mônicos. Consideramos $G = \{g_1, \cdots, g_t\}$. Por hipótese, o resto da divisão por G dos $\mathcal{S}$-polinômios

$$\mathcal{S}_{ij} = \mathcal{S}(g_i, g_j')$$

é nulo quaisquer que sejam $1 \leqslant i, j \leqslant t$. Basta mostrarmos que se f pertence ao ideal I gerado por G em $\mathbb{K}[x_1, \cdots, x_n]$, então $in(f)$ é divisível por algum $in(g_i)$ onde $1 \leqslant i \leqslant t$ para concluírmos a demonstração.

Como cada polinômio em I pode ser escrito como combinação dos elementos de G, existem $u_1, \cdots, u_t \in \mathbb{K}[x_1, \cdots, x_n]$ tais que

$$f = u_1 g_1 + \cdots + u_t g_t. \tag{4.2}$$

Diremos que o vetor $u = (u_1, \cdots, u_t) \in \mathbb{K}[x_1, \cdots, x_n]^t$ é uma **associação** de f em G e definiremos

$$\rho(u) := \max\{in(u_i g_i); 1 \leqslant i \leqslant t\} \geqslant in(f),$$

um elemento de $\mathbb{T}^n$ e

$$\sigma(u) := \#\{i : in(u_i g_i) \text{ é múltiplo constante de } \rho(u)\} \tag{4.3}$$

que é um número entre 1 e t.

Suponhamos, inicialmente, que $\rho(u) = in(f)$. Neste caso, existem $1 \leqslant k \leqslant t$ e uma constante não nula $\alpha \in \mathbb{K}$, tais que

$$in(f) = \alpha\ in(u_k g_k) = \alpha\ in(u_k) in(g_k).$$

O que implica em $in(g_k)$ dividir $in(f)$, tal como queríamos mostrar. Portanto, para concluirmos o critério basta mostrar que todo f admite uma associação cujo ρ é múltiplo constante de $in(f)$. Para isto, construiremos um algoritmo que transforma uma associação qualquer em outra que satisfaz a propriedade desejada. Então, seja u uma associação de f em G para a qual $\rho(u) > in(f)$.

Como os $in(u_i)$ proporcionais a $\rho(u)$ são maiores que $in(f)$, eles terão que se cancelar entre si para que em (4.2) o termo inicial do lado direito seja $in(f)$. Contudo, o cancelamento só é possível se houver mais de um índice $1 \leqslant i \leqslant t$ para o qual $in(u_i)$ seja múltiplo constante de $\rho(u)$.

Portanto, $\rho(u) > in(f)$ implica em $\sigma(u) \geqslant 2$. A partir de u construiremos uma nova associação v tal que

$$\rho(v) < \rho(u) \quad \text{ou} \quad \sigma(v) < \sigma(u).$$

Reenumerando os $g's$, se necessário, podemos supor que $in(u_1 g_1)$ e $in(u_2 g_2)$ são múltiplos constantes de $\rho(u)$. Em particular, estes dois termos têm $\rho(u)$ como suporte, de modo que seus termos iniciais são múltiplos constantes um do outro. Portanto, pelo lema anterior, existem constantes $c_1, c_2 \in \mathbb{K}$ e $\theta \in \mathbb{T}^n$ para os quais

$$in(u_1) = c_1 \theta v_2 \quad e \quad in(u_2) = c_2 \theta v_1, \tag{4.4}$$

em que δ é o máximo divisor comum entre $in(g_1)$ e $in(g_2)$ e v_i é o cofator de δ em $in(g_i)$. A partir dessas expressões façamos o que segue para os termos iniciais de u_1 e u_2,

$$u_1 g_1 + u_2 g_2 = c_2 v_2 \theta g_1 + c_1 v_1 \theta g_2 + M \tag{4.5}$$

onde M representa uma soma de termos cujos suportes são monômios menores que

$$\rho(u) = in(u_1 g_1) = in(u_2 g_2).$$

Reescrevemos (4.5) de forma a obtermos $\mathcal{S}_{12}$. No entanto,

$$c_2 v_2 \theta g_1 + c_1 v_1 \theta g_2 = (c_2 + c_1) v_2 \theta g_1 + c_1 \theta (v_1 g_2 - v_2 g_1),$$

ao passo que

$$\mathcal{S}_{12} = v_1 g_2 - v_2 g_1.$$

Assim,

$$c_2 v_2 \theta g_1 + c_1 v_1 \theta g_2 = (c_2 + c_1) v_2 \theta g_1 + c_1 \theta \mathcal{S}_{12} \tag{4.6}$$

A partir da hipótese sobre os $\mathcal{S}$-polinômios e do teorema 3.5.1 temos

$$\mathcal{S}_{12} = q_1 g_1 + \cdots + q_t g_t,$$

com

$$in(\mathcal{S}_{12}) = max\{in(q_i g_i) : 1 \leqslant i \leqslant t\}.$$

Mas, pela definição de $\mathcal{S}$-polinômio, e por (4.4), obtemos $in(\mathcal{S}_{12}) < in(g_1 v_2) \leqslant in(u_1 g_1)$. Deste modo,

$$in(q_i g_i) < in(u_1 g_1) = \rho(u),$$

para todo $1 \leqslant i \leqslant t$. Combinando este resultado com (4.6) podemos concluir que

$$u_1 g_1 + u_2 g_2 = v_1 g_1 + \cdots + v_t g_t, \tag{4.7}$$

em que apenas $v_1 g_1$ pode ter termo inicial igual a $\rho(u)$, pois $in(v_1 g_1) = (c_1 + c_2) v_2 \theta \; in(g_1)$. Notamos que pode ocorrer $in(v_1 g_1) < \rho(u)$, basta que $c_1 + c_2 = 0$. Substituindo (4.7) em (4.2), obtemos

$$f = v_1 g_1 + v_2 g_2 + (u_3 + v_3) g_3 + \cdots + (u_t + v_t) g_t$$

e as condições sobre os $v's$ garantem que a relação w dada por

$$w_i = \begin{cases} v_i & \text{se } i = 1, 2 \\ v_i + u_i & \text{se } i \neq 1, 2 \end{cases}$$

satisfaz

$$\sigma(w) < \sigma(u).$$

Como a construção acima decresce o valor de σ definido em (4.3), eventualmente obteremos uma associação cujo σ é igual a um. Entretanto, já observamos que isso não é possível. Portanto, ao final de finitos passos, teremos uma associação cujo ρ é menor que $\rho(u)$. Repetindo este procedimento geramos uma sequência estritamente decrescente de monômios em $\mathbb{T}^n$ que não pode ser infinita, pois toda ordem monomial é boa ordem. Portanto, após uma quantidade finita de etapas, teremos uma associação cujo ρ é igual a $in(f)$, caindo no caso inicial.

□

Observação 4.2.4. Para concluirmos a demonstração acima utilizamos a propriedade 4.3.1. Embora esteja enunciada e demonstrada apenas na próxima seção, ela não faz uso de nenhum resultado que segue. Nosso objetivo em apresentar depois este resultado é apenas com o intuito de manter uma lista de propriedades em uma única seção, embora ela pudesse ser naturalmente enunciada antes deste critério.

Com isso, garantimos a eficiência do algoritmo de Buchberger para a construção de uma base de Gröbner de um ideal I gerado pelos polinômios $g_1, \cdots, g_s$. Ilustremos sua aplicação no seguinte exemplo:

Exemplo 4.2.5. Calculemos a base de Gröbner para o ideal $\langle x^2y - 1, xy^2 - x\rangle$, sob a ordem monomial $\succeq_{LG}$ pelo algoritmo de Buchberger.

Etapa 1: $G = \{h_1 = x^2y - 1, h_2 = xy^2 - x\}$ e $\mathcal{P} = \{(h_1, h_2)\} \neq \emptyset$;

Etapa 2:

(1) Selecione (h_1, h_2). Temos $\mathcal{P} = \emptyset$, calculemos:

$$\mathcal{S}(h_1, h_2) = \frac{xy^2}{xy}(x^2y - 1) - \frac{x^2y}{xy}(xy^2 - x) = x^2 - y$$

e

$$\begin{array}{r|l} & x^2y - 1 \\ x^2 - y & xy^2 - x \\ \hline -y & q_1 = 0 \\ 0 & q_2 = 0 \\ & r = x^2 - y \end{array}$$

Como $h_3 := r = x^2 - y \neq 0$, então $G = \{h_1, h_2, h_3\}$ e $\mathcal{P} = \{(h_1, h_3), (h_2, h_3)\}$.

(2) Selecione (h_2, h_3). Temos $\mathcal{P} = \{(h_1, h_3)\}$, calculemos:

$$\mathcal{S}(h_2, h_3) = \frac{x^2}{x}(xy^2 - x) - \frac{xy^2}{x}(x^2 - y) = y^3 - x^2$$

e

$$\begin{array}{r|l} & x^2y-1 \\ & xy^2-x \\ y^3-x^2 & x^2-y \\ \hline -x^2 & q_1=0 \\ 0 & q_2=0 \\ & q_3=0 \\ & r=y^3-x^2 \end{array}$$

Como $h_4 := r = y^3 - x^2 \neq 0$, então

$$G = \{h_1, h_2, h_3, h_4\} \text{ e } \mathcal{P} = \{(h_1, h_3), (h_1, h_4), (h_2, h_4), (h_3, h_4)\}$$

(3) Selecione (h_3, h_4). Temos $\mathcal{P} = \{(h_1, h_3), (h_1, h_4), (h_2, h_4)\}$, calculemos:

$$\mathcal{S}(h_3, h_4) = \frac{y^3}{1}(x^2 - y) - \frac{x^2}{1}(y^3 - x^2) = x^4 - y^4$$

e

$$\begin{array}{r|l} & x^2y-1 \\ & xy^2-x \\ & x^2-y \\ x^4-y^4 & y^3-x^2 \\ \hline -y^4+x^2y & q_1=0 \\ 0 & q_2=0 \\ & q_3=x^2 \\ & q_4=-y \\ & r=0 \end{array}$$

Como $r = 0$, temos $G = \{h_1, h_2, h_3, h_4\}$ e $\mathcal{P} = \{(h_1, h_3), (h_1, h_4), (h_2, h_4)\}$.

(4) Selecione (h_2, h_4). Temos $\mathcal{P} = \{(h_1, h_3), (h_1, h_4)\}$, calculemos:

$$\mathcal{S}(h_2, h_4) = \frac{y^3}{y^2}(xy^2 - x) - \frac{xy^2}{y^2}(y^3 - x^2) = x^3 - xy$$

e

$$\begin{array}{r|l} & x^2y-1 \\ & xy^2-x \\ & x^2-y \\ x^3-xy & y^3-x^2 \\ \hline 0 & q_1=0 \\ & q_2=0 \\ & q_3=x \\ & q_4=0 \\ & r=0 \end{array}$$

Como $r=0$, temos $G=\{h_1,h_2,h_3,h_4\}$ e $\mathcal{P}=\{(h_1,h_3),(h_1,h_4)\}$.

(5) Selecione (h_1,h_3). Temos $\mathcal{P}=\{(h_1,h_4)\}$, calculemos:

$$\mathcal{S}(h_1,h_3)=\frac{x^2}{x^2}(x^2y-1)-\frac{x^2y}{x^2}(x^2-y)=y^2-1$$

e

$$\begin{array}{r|l} & x^2y-1 \\ & xy^2-x \\ & x^2-y \\ y^2-1 & y^3-x^2 \\ \hline -1 & q_1=0 \\ 0 & q_2=0 \\ & q_3=0 \\ & q_4=0 \\ & r=y^2-1 \end{array}$$

Como $h_5:=r=y^2-1\neq 0$, então

$$G=\{h_1,h_2,h_3,h_4,h_5\} \quad \text{e} \quad \mathcal{P}=\{(h_1,h_4),(h_1,h_5),(h_2,h_5),(h_3,h_5),(h_4,h_5)\}.$$

Pode-se notar através de um cálculo sistemático que qualquer outro par (h_i,h_j) pertencente ao atual $\mathcal{P}$ tem $R_G(\mathcal{S}(h_i,h_j))=0$, ou seja, o conjunto G não agrega nenhum outro polinômio e consequentemente $\mathcal{P}$ se tornará nulo, encerrando o algoritmo.

Desta forma, segundo o algoritmo de Buchberger, a base de Gröbner do ideal $\langle x^2y-1, xy^2-x\rangle$ será

$$G=\{x^2y-1, xy^2-x, x^2-y, y^3-x^2, y^2-1\}$$

Note que o processo para construção torna-se mecânico, e como o algoritmo nos dá a garantia de termos obtido uma base de Gröbner o processo que fizemos no exemplo 4.1.7

torna-se desnecessário. Na próxima seção refinaremos esta base obtida ao introduzirmos os conceitos de bases de Gröbner reduzidas e mínimas. Terminamos a seção apresentando o seguinte resultado que será utilizado no último capítulo.

Lema 4.2.6. *Sejam $\mathbb{K}$ um corpo, F um subconjunto finito de $\mathbb{K}[x_1, \cdots, x_n]$ e $\preceq$ uma ordem monomial definida neste anel. Se*

$$mdc(in(f), in(g)) = 1,$$

para todo $f \neq g$ em F, então o conjunto F é uma base de Gröbner do ideal $\langle F \rangle$.

Demonstração. Suponhamos que os polinômios em F são mônicos e dados $f, g \in F$ consideremos

$$f = in(f) + f_1 \quad \text{e} \quad g = in(g) + g_1. \tag{4.8}$$

Desta forma, temos $f_1 \preceq f$ e $g_1 \preceq g$. Por hipótese, $mdc(in(f), in(g)) = 1$, então

$$S(f, g) = in(g)f - in(f)g. \tag{4.9}$$

Substituindo (4.9) em (4.9) obtemos

$$S(f, g) = f_1 g - g_1 f.$$

Suponhamos, por absurdo, que $in(f_1)in(g) = in(g_1)in(f)$, então como os termos iniciais de f e g são primos entre si, teríamos necessariamente que $in(f_1) = \eta in(g)$ e $in(g_1) = \eta in(f)$ para algum monômio η, o que contradiz $f_1 \preceq f$ e $g_1 \preceq g$. Podemos supor que

$$in(g_1)in(f) \preceq in(f_1)in(g)$$

e assim,

$$R_F(S(f, g)) = 0.$$

Como isso é válido para qualquer par de polinômios em F, pelo critério de Buchberger, podemos concluir que F é uma base de Gröbner do ideal $\langle F \rangle$. □

4.3 PROPRIEDADES DAS BASES DE GRÖBNER

Nesta última seção, poderemos, finalmente, resolver o problema da pertinência em ideais de $\mathbb{K}[x_1, \cdots, x_n]$.

Propriedade 4.3.1 (Pertinência)**.** Sejam I um ideal de $\mathbb{K}[x_1, \cdots, x_n]$ e G uma base de Gröbner para I. Então $f \in I$ se, e somente se, $R_G(f) = 0$.

Demonstração. Sabemos que G gera I e, se o resto da divisão de f por G for zero, então $f \in I$. Reciprocamente, suponhamos por contradição que $f \in I$, mas $R_G(f) = r \neq 0$. Neste caso, como $f - r \in I$ temos que $r \in I$. Portanto $in(r) \in in(I)$. Logo, pela definição da base de Gröbner, $in(g_0) \mid in(r)$ para algum $g_0 \in G$. Contradizendo a minimalidade do resto, concluímos então que $R_G(f) = 0$. □

Propriedade 4.3.2 (Unicidade do resto)**.** Sejam $G = \{g_1, \cdots, g_s\}$ uma base de Gröbner e f um polinômio do anel $\mathbb{K}[x_1, \cdots, x_n]$. Então existe um único polinômio r tal que

$$f = q_1 g_1 + \cdots + q_s g_s + r, \tag{4.10}$$

em que $q_1, \cdots, q_s \in \mathbb{K}[x_1, \cdots, x_n]$ e nenhum mônomio de r pertence ao ideal gerado pelos termos iniciais dos $g_i's$

Demonstração. Suponhamos por contradição que seja possível reescrever sob as mesmas condições (4.10) da seguinte forma

$$f = q_1' g_1 + \cdots + q_s' g_s + r'$$

Obtemos

$$(q_1 g_1 + \cdots + q_s g_s + r) - (q_1' g_1 + \cdots + q_s' g_s + r') = 0 \tag{4.11}$$

$$(q_1 - q_1') g_1 + \cdots + (q_s - q_s') g_s + (r - r') = 0 \tag{4.12}$$

$$(q_1' - q_1) g_1 + \cdots + (q_s' - q_s) g_s = (r - r'), \tag{4.13}$$

daí $(r - r') \in \langle g_1, \cdots, g_s \rangle$. Pela proposição anterior $R_G(r - r') = 0$, mas por hipótese nenhum monômio de r ou r' é divisível por nenhum termo inicial de qualquer $g \in G$. Donde o $R_G(r - r')$ é o próprio $r - r'$, isto é, $r - r' = 0$, como queríamos. □

Com estas duas propriedades garantimos uma consistência melhor no algoritmo da pseudo-divisão, com a unicidade do resto quando dividimos um polinômio f por uma base de Gröbner G, e mais, podemos agora garantir de forma determinista se f pertence ou não ao ideal gerado por G.

Proposição 4.3.3. *Seja G uma base de Gröbner no anel $\mathbb{K}[x_1, \cdots, x_n]$ com respeito a alguma ordem monomial. Suponhamos que g e h são elementos de G e que $in(g)$ divide $in(h)$. Então $H = G \backslash \{h\}$ também é uma base de Gröbner de $\langle G \rangle$.*

Demonstração. Basta mostrarmos que para cada $f \in \langle G \rangle$ o termo $in(f)$ é divisível pelo termo inicial de algum polinômio de H. G é base de Gröbner, portanto $in(f)$ é divisível pelo termo inicial de algum polinômio de G. Se este polinômio não for h então pertence a H. Por outro lado, se for h, temos por hipótese que $in(g)$ divide $in(h)$ que por sua vez divide $in(f)$, tal como queríamos. □

Observação 4.3.4. Este resultado combinado com a proposição 4.1.4 garantem que G e H geram o mesmo ideal.

Usando a Proposição 4.3.3, vemos que uma base de Gröbner pode ser refinada, uma vez que preservamos a propriedade de ser base ainda que retiremos elementos que tenham seus termos iniciais divisíveis por outros termos iniciais desta base. Com isto, definimos:

Definição 4.3.5. Seja $G = \{g_1, \cdots, g_t\}$ uma base de Gröbner em $\mathbb{K}[x_1, \cdots, x_n]$ com a ordem monomial $\succeq$. Dizemos que G é uma **base de Gröbner mínima** se

1. $in(g_i)$ tem coeficiente 1 para todo $i \in \{1, \cdots, t\}$ e
2. se $i \neq j$ então $in(g_i)$ não divide $in(g_j)$

As bases de Gröner mínimas possuem as seguintes propriedades:

Propriedade 4.3.6. Sejam $G = \{g_1, \cdots, g_s\}$ e $H = \{h_1, \cdots, h_t\}$ bases de Gröbner mínimas de um mesmo ideal. Então

1. $s = t$;
2. é possível reordenar os elementos de H de modo que $in(h_i) = in(g_i)$ para todo $i \in \{1, \cdots, s\}$.

Demonstração. Suponhamos que $s \leqslant t$. Como H é base de Gröbner de $I = \langle G \rangle$, então o termo inicial de cada elemento de G será divisível por algum elemento de H. Renumerando os $h's$obtemos um h_i cujo termo inicial divide $in(g_i)$. Reciprocamente, $h_i \in I$, então $in(h_i)$ é divisível pelo termo inicial de algum elemento de G. Seja g_j este elemento. Assim, $in(g_j)$ divide $in(h_i)$ que por sua vez divide $in(g_i)$. Como G é base mínima então $in(g_j) = in(g_i)$ donde $in(g_i) = in(h_i)$. Necessariamente, $s = t$ é verificado. □

Propriedade 4.3.7. Fixemos uma ordem monomial e suponhamos que G e G' são bases de Gröbner mínimas, distintas, de um mesmo ideal. Então, $in(G) = in(G')$.

Demonstração. Como G e G' são bases de Gröbner mínimas, temos pela primeira propriedade que ambas têm a mesma quantidade de elementos, digamos $G = \{g_1, \cdots, g_s\}$ e $G' = \{g'_1, \cdots, g'_s\}$.

Pela segunda propriedade, podemos ordenar os elementos de G' de forma a obtermos $in(g'_i) = in(g_i)$, para todo $i \in \{1, \cdots, s\}$. Assim, pela definição 4.1.1 temos o resultado. □

Exemplo 4.3.8. Calculemos a base de Gröbner mínima do ideal $\langle x^2y - 1, xy^2 - x \rangle$, sob a ordem monomial $\succeq_{LG}$.

Como resultado do exemplo 4.2.5, temos a seguinte base de Gröbner do ideal $\langle x^2y - 1, xy^2 - x\rangle$:

$$G = \{h_1 = x^2y - 1, h_2 = xy^2 - x, h_3 = x^2 - y, h_4 = y^3 - x^2, h_5 = y^2 - 1\}$$

. Notamos que $in(h_3) \mid in(h_1)$; $in(h_5) \mid in(h_2)$; e $in(h_5) \mid in(h_4)$, logo os polinômios h_1, h_2 e h_4, segundo a proposição 4.3.3, podem ser removidos que ainda teremos uma base de Gröbner. Como $G_m = \{h_3, h_5\}$ atende às condições da definição 4.3.5, então G_m é base de Gröbner mínima do ideal $\langle x^2y - 1, xy^2 - x\rangle$.

Com relação a base de Gröbner mínima obtemos uma quantidade mínima de polinômios que pertencem a mesma (condição 1 da definição) e mais, obtemos também uma invariância dos termos iniciais (condição 2). Porém para cada par $g_i \in G$ e $h_i \in H$, tais que $in(g_i) = in(h_i)$ onde G e H são bases de Gröbner mínimas, não garantimos que $g_i = h_i$. A definição a seguir resolve esse problema:

Definição 4.3.9. Seja $G = \{g_1, \cdots, g_t\}$ uma base de Gröbner em $\mathbb{K}[x_1, \cdots, x_n]$ com a ordem monomial $\succeq$. Dizemos que G é uma **base de Gröbner reduzida** se

1. G é mínima e
2. cada $g \in G$ é *reduzido* com relação a $G' = G\backslash\{g\}$, isto é, $R_{G'}(g) = 0$.

Ilustremos sua aplicação no exemplo que segue e logo mais enunciemos algumas propriedades que justificam esta definição.

Exemplo 4.3.10. Calculemos a base de Gröbner reduzida do exemplo 4.2.5.

Já obtemos que a base de Gröbner dada por

$$G = \{h_1 = x^2y - 1, h_2 = xy^2 - x, h_3 = x^2 - y, h_4 = y^3 - x^2, h_5 = y^2 - 1\}$$

tem base mínima

$$G_m = \{h_3, h_5\}.$$

Por cálculo direto, temos que os polinômios h_3 e h_5 são reduzidos, então G_m também será base de Gröbner reduzida.

Propriedade 4.3.11. (unicidade da base de Gröbner reduzida) Cada ideal de $\mathbb{K}[x_1, \cdots, x_n]$ admite uma única base de Gröbner reduzida relativamente a uma ordem monomial dada.

Demonstração. Suponhamos que G e H são duas bases de Gröbner reduzidas de um ideal I de $\mathbb{K}[x_1, \cdots, x_n]$ com respeito a uma ordem monomial $\succeq$. Em particular, são bases mínimas e, pela proposição 4.3.6, têm o mesmo número de elementos, digamos

$$G = \{g_1, \cdots, g_s\} \quad \text{e} \quad H = \{h_1, \cdots, h_s\},$$

onde $in(g_i) = in(h_i)$ para todo $i \in \{1, \cdots, s\}$. Segue então que cada h_i é reduzido não apenas com respeito a $H\backslash\{h_i\}$, mas também com relação a $G\backslash\{g_i\}$.

Suponhamos, por contradição, que $g_i \neq h_i$ para algum $1 \leqslant i \leqslant s$. Então, o suporte de $g_i - h_i$ não é vazio. Mas $g_i - h_i \in I$, donde $R_G(g_i - h_i) = 0$. Assim, dado um monômio do suporte de $g_i - h_i$, existirá um $in(g_i)$ que o divide. Entretanto, como $in(g_i) = in(h_i)$, os monômios em $sup(g_i - h_i)$ são menores que $in(g_i)$. Portanto $i \neq j$, contradizendo g_i e h_i serem reduzidos em relação a $G\backslash\{g_i\}$ □

Segue da propriedade 4.3.11, a última propriedade que listaremos:

Propriedade 4.3.12. Dois ideais de um anel de polinômios sobre um corpo são iguais se, e somente se, suas bases de Gröbner reduzidas são iguais.

Finalizamos esse capítulo com uma observação sobre a determinação do ideal radical de um ideal $I \subset K[x_1, \cdots, x_n]$ de dimensão zero decorrente do critério de Seidenberg (Lema 3.6.7).

Observação 4.3.13. Para calcular o radical de um ideal de dimensão zero $I \subset K[x_1, \cdots, x_n]$, começamos calculando as bases de Gröbner de $I \cap K[x_j]$ para cada $1 \leqslant j \leqslant n$. Como esses ideais são principais, cada base terá apenas um elemento $g_j \in K[x_j]$. Determinando a representação livre de quadrados de g_j denotada por q_j (existe um algoritmo para isso, veja [4], pg 295), temos que o ideal $J = \langle I, q_1, \ldots, q_n \rangle$ é radical pelo critério de Seidenberg. Lembrando que $\sqrt{I}$ é o menor ideal radical que contém I, segue que $J = \sqrt{I}$.

5 COLORAÇÃO DE GRAFOS

Neste último capítulo, apresentaremos uma aplicação importante de bases de Gröbner, abordando, inicialmente, algumas definições básicas sobre grafos e como representá-los através de polinômios. Na seção 5.2, discutiremos a coloração de grafos e como a teoria das bases de Gröbner que construímos no capítulo anterior pode ser aplicada a esse problema.

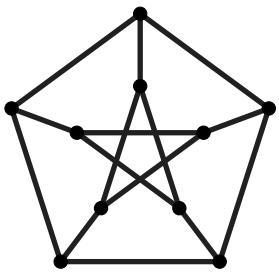
5.1 POLINÔMIOS E GRAFOS

Definição 5.1.1. Um **grafo** G é um conjunto finito de pontos, alguns dos quais podem estar ligados por um segmento. Os pontos são chamados de **vértices** e os segmentos de **arestas**. Sendo V o conjunto de vértices e A o conjunto de arestas do grafo G, denotamos: $G = (V, A)$.

Definição 5.1.2. Quando dois vértices estão ligados por uma aresta são chamados de **vértices adjacentes**. O **grau** de um vértice v é a quantidade de arestas que incide sobre v.

Definição 5.1.3. Seja G um grafo, dizemos que G é um grafo **simples** se cada par de vértices está ligado por no máximo um segmento (não orientado). Em particular, um grafo simples é dito grafo **completo** quando todo vértice é adjacente a todos os outros vértices. Ainda, G é **regular** quando todos os vértices possuem o mesmo grau.

Exemplo 5.1.4. Podemos representar as arestas e os vértices de um grafo esquematicamente. Por exemplo, a seguir apresentamos o grafo de Petersen, que é um grafo simples e regular de grau 3.



Seja $G = (V, A)$ um grafo com $\#V = n$. Numeramos os vértices de G com os inteiros de 1 a n e associamos uma indeterminada x_i ao vértice i para todo $1 \leq i \leq n$. Com isso, tornamos possível associar o grafo G ao produto homogêneo dado por

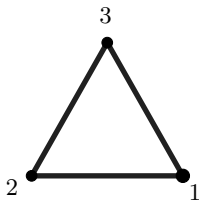
$$P = \prod_{i<j} (x_i - x_j)^{\alpha_{ij}},$$

em que o fator $(x_i - x_j)^{\alpha_{ij}}$ aparece no produto P se, e somente se, existem α_{ij} arestas ligando os vértices x_i e x_j de G. Notamos que, pela condição $i < j$ imposta a P, o número

α_{ij} representa a quantidade de arestas entre os vértices x_i e x_j. Além disso, G tem arestas múltiplas se algum $\alpha_{ij} > 1$. Em particular, quando o grafo $G = (V, A)$ é simples, o produto homogêneo P_G a ele associado é dado por

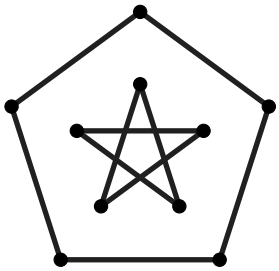
$$P_G = \prod_{(i,j)\in A} (x_i - x_j),$$

Exemplo 5.1.5. O produto homogêneo $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ está relacionado ao seguinte grafo completo regular de grau dois:



Definição 5.1.6. Seja $G = (V, A)$ um grafo. Dizemos que o grafo $H = (V', A')$ é **subgrafo** de G se $V' \subseteq V$ e $A' \subseteq A$. Quando $V = V'$ dizemos que H é **subgrafo gerador** de G. Um k**-fator** de G é um subgrafo gerador que é regular, cujos vértices têm grau k.

Exemplo 5.1.7. Um 2-fator do grafo de Petersen (exemplo 5.1.4) pode ser dado esquematicamente por



Numerando os vértices do pentágono de 1 a 5 e os vértices da estrela de 6 a 10, esse 2-fator do grafo de Petersen pode ser representado pelo seguinte polinômio

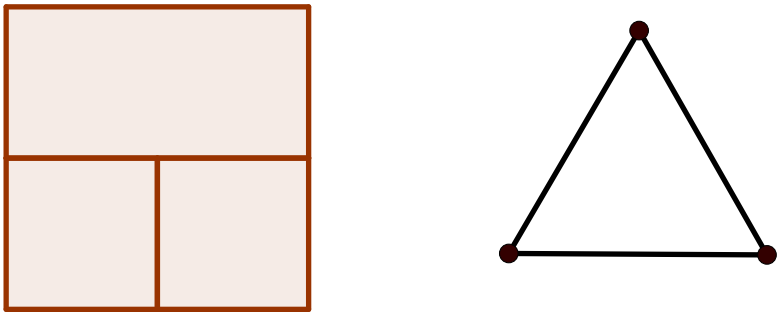
$$(x_7 - x_{10})(x_6 - x_9)(x_1 - x_5)\prod_{i=1}^{4}(x_i - x_{i+1})\prod_{j=1}^{3}(x_{j+5} - x_{j+7}).$$

5.2 COLORAÇÃO DE GRAFOS

Consideramos um mapa que representa uma região subdividida em várias outras. Uma pergunta natural é: como determinar o número de cores necessárias para colorir este mapa de tal forma que duas regiões que compartilham uma linha de fronteira não sejam coloridas com a mesma cor? Esta questão foi levantada pela primeira vez em 1852 por Francis Guthrie, que conjecturou a quantidade máxima de quatro cores para se colorir

qualquer mapa. O problema foi resolvido apenas em 1976 por Kenneth Appel e Wolfgang Haken com auxilio computacional e em 1994 sua demonstração foi simplificada por Paul D. Seymour, Neil Robertson, Daniel P. Sanders e Robin Thomas, que ainda utilizaram o recurso computacional.

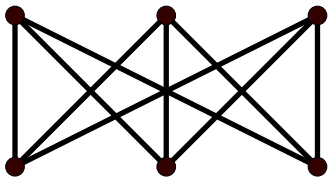
Esse problema foi resolvido associando um mapa a um grafo correspondendo cada uma de suas regiões por um vértice, e cada fronteira entre duas regiões por uma aresta que conecta os respectivos vértices. Como por exemplo:



Por esta associação, podemos dizer que um grafo é planar quando está associado a um mapa, ou seja, se existe uma representação esquemática do grafo em que nenhuma aresta intercepte ou sobreponha outra. Assim, resolver o problema da coloração de mapas está associado com a coloração de grafos, nos motivando a definir:

Definição 5.2.1. Uma **coloração** de um grafo simples $G = (V, A)$ é uma forma de rotular os vértices com um conjunto C de cores de tal maneira que vértices que estejam ligados por uma aresta não sejam pintados com uma mesma cor de C.

A partir desta definição podemos observar que o estudo de coloração de grafos não se limita a resolver o problema da coloração de mapas, pois é possível obter grafos que não sejam planares. Nossos resultados não se limitarão aos grafos planares, portanto não teremos como objetivo apresentar formas de decidir se um grafo é ou não planar. Entretanto, para apresentarmos essa diferença, trazemos como exemplo de um grafo não planar o grafo $K_{3,3}$, dado por:



No contexto da coloração de grafos, podemos observar que o número mínimo de cores de C está associado diretamente ao grafo em questão. Um grafo G com n vértices pode ser colorido com uma única cor, bastaria não ter arestas; como também, pode ser colorido com no mínimo n cores, para isto, bastaria que cada vértice esteja associado a todos os outros $n-1$ vértices. Fazendo sentido a seguinte definição:

Definição 5.2.2. Dado um grafo G, o **número cromático** de G, denotado por $\mathcal{X}(G)$, é o número mínimo de cores para se colorir o grafo G.

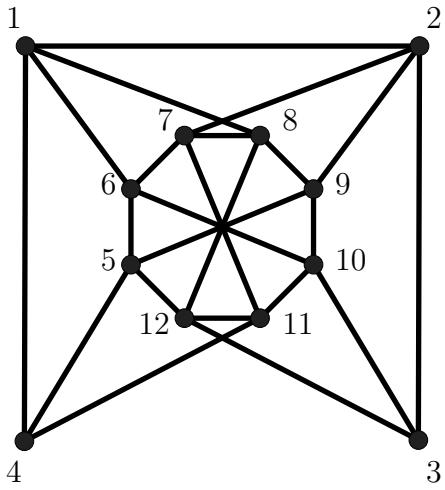
Impondo restrições específicas a um determinado tipo de grafo, podemos obter $\mathcal{X}(G)$ facilmente.

Exemplo 5.2.3. Dizemos que um grafo $G = (V, A)$ é **bipartido** se for possível decompor $V = V_1 \cup V_2$, onde V_1 e V_2 são conjuntos disjuntos de modo que só haja arestas ligando vértices de V_1 a V_2. Assim, como não há arestas ligando vértices de V_1 entre si e o mesmo ocorre em V_2, podemos colorir todos os vértices de V_1 com uma cor e todos os de V_2 com outra resultando que $\mathcal{X}(G) = 2$ qualquer que seja o grafo bipartido. O grafo $K_{3,3}$ é um exemplo de bipartido.

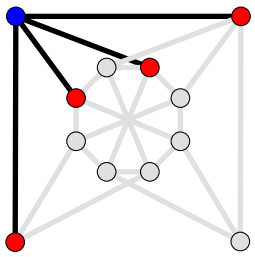
Até este momento, associamos um grafo a sua forma esquemática e polinomial e vimos também o que é uma coloração do grafo. Porém, em termos práticos, colorir um grafo em sua forma esquemática com uma quantidade mínima de cores pode ser uma tarefa complicada conforme a complexidade do grafo aumenta.

No seguinte exemplo veremos que a quantidade de cores está atrelada a forma como colorimos o grafo esquematicamente, isto é, o algoritmo de coloração induz uma quantidade k ou k' de cores, portanto determinar quando foi atingido o número mínimo pode não ser facilmente respondido apenas observando a estrutura do grafo.

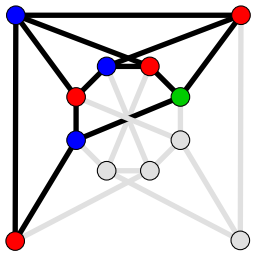
Exemplo 5.2.4. Considere o grafo de Chao e Chen, dado esquematicamente por:



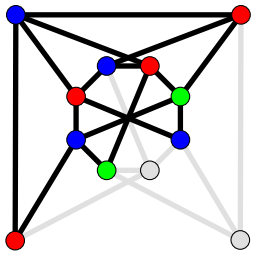
Em uma tentativa de colorir o grafo, colorimos inicialmente o vértice 1 com uma cor (azul). Como os vértices adjacentes a ele não são adjacentes entre si, podemos colori-los com apenas mais uma cor (vermelho), assim obtemos:



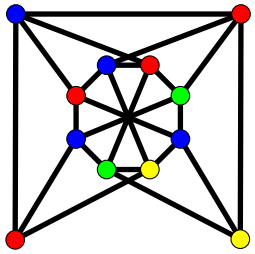
Em cada vizinho repetimos o processo, colorimos assim os vértices 5 e 7 com a cor azul, pois estes não são adjacentes ao vértice 1. Observe que no vértice 9 será necessário uma nova cor, pois este é adjacente aos vértices 5 e 8, logo colorimos na cor verde.



Seguindo este processo em cada vizinho colorimos os vértices 10 e 12, obtendo:



Neste momento, resta-nos apenas os vértices 3 e 11, que não podem ser coloridos com nenhuma das cores existentes, então obtemos a seguinte coloração do grafo:



Logo começar a coloração por 1 induz uma necessidade de colorir com 4 cores. A mesma quantidade é obtida começando por alguns outros, a pergunta que pode ser feita é: seria possível colorir com menos cores? Em um grafo mais complexo essa tarefa torna-se mais trabalhosa, e mesmo neste exemplo em dois momentos vimos a necessidade de adicionar mais uma cor, mas essas cores são realmente necessárias para uma coloração que use a quantidade mínima?

Para compreendermos melhor a coloração de um grafo façamos uso da notação polinomial descrita anteriormente. Para isso, somos levados a transcrever o conjunto de cores que colorem um grafo em linguagem polinomial para então abordar a coloração apenas neste contexto.

Representaremos as cores do conjunto C como sendo as raízes da unidade, ou seja, se o conjunto C possui k cores, associaremos cada uma delas a uma raiz do polinômio $x^k - 1 = 0$ em $\mathbb{C}$, que possui k raízes, pois $\mathbb{C}$ é algebricamente fechado. Assim podemos reescrever o conjunto C como sendo o seguinte conjunto:

$$\mathcal{U}_k = \left\{ \zeta^j \;\middle|\; 0 \leqslant j \leqslant k-1 \right\} \quad \text{onde} \quad \zeta = \cos\left(\frac{2\pi}{k}\right) + \imath \operatorname{sen}\left(\frac{2\pi}{k}\right)$$

Seja G um grafo simples com n vértices e $\mathcal{U}_k$ um conjunto de k cores. Numeramos cada vértice de 1 a n e associamos a indeterminada x_i ao $i-$ésimo vértice. Associamos uma escolha de cores para os vértices de G como sendo uma n-upla

$$v = (v_1, \cdots, v_n) \in \mathcal{U}_k^n,$$

em que o vértice i, associado a x_i é colorido com a $k-$ésima raiz da unidade v_i. Construída dessa forma, a n-upla não representa uma coloração do grafo, apenas uma disposição possível das cores de $\mathcal{U}_k$ nos vértices de G. A seguinte proposição nos permite concluir quando uma n-upla será considerada uma coloração de G.

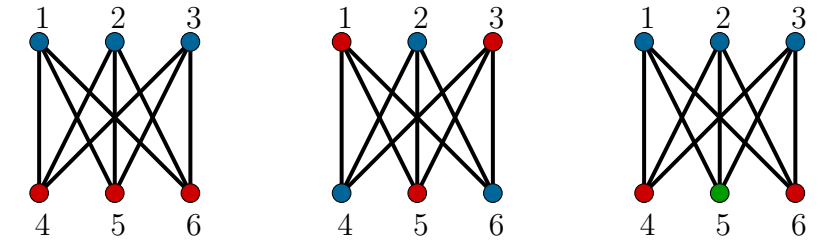
Proposição 5.2.5. *Uma escolha de cores $v = (v_1, \cdots, v_n) \in \mathcal{U}_k^n$ é uma coloração de G se, e somente se, $P_G(v) \neq 0$, onde P_G é o polinômio associado a G.*

Demonstração. Sejam G um grafo, $\mathcal{U}_k$ um conjunto de cores, P_G o polinômio associado a G e $v \in \mathcal{U}_k^n$. $P_G(v) = 0$ se, e só se, existe pelo menos um fator $(x_i - x_j)$ onde $i < j$ em P_G tal que $v_i - v_j = 0$, isto é, $v_i = v_j$. Como $(x_i - x_j)$ aparece em P_G se, e só se, existe aresta associando o vértice i a j, e v será coloração de G se, e só se, vértices adjacentes não compartilham a mesma cor se faz claro o resultado da proposição. □

Exemplo 5.2.6. Considere o seguinte polinômio associado ao grafo $K_{3,3}$:

$$P = \prod_{j=1}^{3} \prod_{i=4}^{6} (x_j - x_i)$$

e o conjunto de cores $\mathcal{U}_3 = \{\zeta^0, \zeta^1, \zeta^2\}$. Abaixo, temos algumas formas de colorir o grafo,



$(\zeta^0, \zeta^0, \zeta^0, \zeta^1, \zeta^1, \zeta^1)$ $(\zeta^1, \zeta^0, \zeta^1, \zeta^0, \zeta^1, \zeta^0)$ $(\zeta^0, \zeta^0, \zeta^0, \zeta^1, \zeta^2, \zeta^1)$

Destas, observe que $P((\zeta^0, \zeta^0, \zeta^0, \zeta^1, \zeta^1, \zeta^1))$ e $P((\zeta^0, \zeta^0, \zeta^0, \zeta^1, \zeta^2, \zeta^1))$ são não nulas, portanto colorações. E em $(\zeta^1, \zeta^0, \zeta^1, \zeta^0, \zeta^1, \zeta^0)$ o fator $(x_2 - x_4) = 0$, pois os vértices 2 e 4 são coloridos com a mesma cor ζ^0, portanto não é uma coloração.

Observamos que o conjunto $\mathcal{U}_k^n$ é um conjunto algébrico, mais precisamente,

$$\mathcal{U}_k^n = Z(\langle x_1^k - 1, \cdots, x_n^k - 1 \rangle) \subset \mathbb{C}\,,$$

através do qual podemos refinar a proposição 5.2.5 no seguinte resultado:

Proposição 5.2.7. *Seja G um grafo simples com n vértices e seja*

$$I = \langle x_1^k - 1, \cdots, x_n^k - 1 \rangle$$

um ideal do anel $\mathbb{Q}[x_1, \cdots, x_n]$. As seguintes afirmações são equivalentes:

1. $\mathcal{X}(G) > k$;

2. $P_G(v) = 0$ *para todo* $v \in Z(I)$;

3. $P_G \in I$.

Demonstração. A proposição 5.2.5 nos garante a equivalência entre 1 e 2. O fato de que 3 implica em 2 é direto das definições. Resta apenas mostrar que 2 implica em 3, mas pelo teorema 3.6.4, obtemos

$$P_G(v) = 0 \ \forall \ v \in Z(I) \Leftrightarrow P_G \in \sqrt{\langle x_1^k - 1, \cdots, x_n^k - 1\rangle}.$$

Como $Z(I)$ é finito e os polinômios $x_i^k - 1$ não possuem raízes repetidas, segue do critério de Seidenberg (Lema 3.6.7) que I é um ideal radical, assim $P_G \in \sqrt{I} = I$ provando assim a proposição. □

Observamos que a terceira afirmação é facilmente verificada ao determinar uma base de Gröbner para o ideal I.

Exemplo 5.2.8. Consideramos novamente o grafo de Chao e Chen apresentado no exemplo 5.2.4, cujo polinômio é dado por

$$\begin{aligned} P &= (x_1 - x_2)(x_1 - x_4)(x_1 - x_6)(x_2 - x_3)(x_2 - x_7)(x_3 - x_{12}) \\ &\quad (x_4 - x_5)\left(\prod_{k=1}^{5}(x_k - x_{k+7})\right)\left(\prod_{j=5}^{8}(x_j - x_{j+1})(x_j - x_{j+4})\right)\left(\prod_{i=9}^{11}(x_i - x_{i+1})\right) \end{aligned}$$

através de cálculo computacional observamos que este polinômio pertence ao ideal

$$I = \langle x_1^2 - 1, \cdots, x_{12}^2 - 1\rangle,$$

e assim, pela proposição anterior, $\mathcal{X}(G) > 2$. Portanto não é possível obter uma coloração do grafo com apenas duas cores. No exemplo 5.2.4 construímos uma coloração com 4 cores e, em breve, vamos verificar se é possível com apenas 3 cores.

Considerando a ordem lexicográfica, temos $in(x_i^k - 1) = x_i^k$ para todo $1 \leqslant i \leqslant n$. Portanto, se $F = \{x_1^k - 1, \cdots, x_n^k - 1\}$, pelo lema 4.2.6, temos que F é uma base de Gröbner para $\langle F\rangle$ em $\mathbb{Q}[x_1, \cdots, x_n]$. A partir disso, demonstraremos o seguinte teorema que nos permite estudar a coloração apenas com a expansão do polinômio.

Teorema 5.2.9. *Seja G um grafo simples. Se a expansão do polinômio P_G contém um termo cujo grau em cada uma das variáveis é menor do que k, então $\mathcal{X}(G) \leqslant k$.*

Demonstração. Seja $F = \{x_1^k - 1, \cdots, x_n^k - 1\}$. Dado um monômio não nulo η em $\mathbb{Q}[x_1, \cdots, x_n]$, obtemos $R_F(\eta) = \eta$ se η tiver grau menor que k em todas as variáveis. Caso

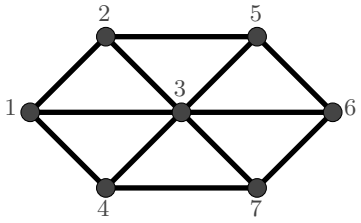
contrário, $R_F(\eta)$ terá grau total menor que η. Assim, por P_G ser homogêneo, sua divisão por F retorna um resto onde seu componente homogêneo de maior grau contém todos os monômios de P_G em seu suporte no qual as variáveis têm grau menor que k. Mas se os monômios não se cancelavam em P_G, então não se cancelarão em $R_F(P_G)$. Como, por hipótese, P_G contém um termo cujo grau em cada uma das variáveis é menor do que k, o resto $R_F(P_G)$ não pode ser nulo, donde $P_G \notin \langle F \rangle$.

Mas, sabemos que $Z(F)$ é finito e os polinômios geradores não possuem raízes repetidas, então segue do critério de Seidenberg (Lema 3.6.7) que $\langle F \rangle$ é um ideal radical. Portanto $P_G \notin \langle F \rangle = \sqrt{\langle F \rangle}$. Mas vimos que isso é equivalente a negação da afirmação 2 da proposição 5.2.7, donde $\mathcal{X}(G) \leqslant k$, isto é, G pode ser colorido com k cores. □

Exemplo 5.2.10. Consideramos o polinômio

$$P = \prod_{i=2}^{4}(x_1 - x_i) \cdot \prod_{j=4}^{7}(x_3 - x_j) \cdot (x_2 - x_3)(x_2 - x_5)(x_5 - x_6)(x_6 - x_7)$$

que corresponde ao seguinte grafo:



Observamos que a expansão de P tem termos em que cada variável aparece com grau dois ou menor. Portanto pelo teorema anterior este grafo pode ser colorido com apenas 3 cores.

Exemplo 5.2.11. Retornando ao grafo de Chao e Chen (exemplo 5.2.4), utilizando esse teorema, verificamos que existe um termo da expansão do polinômio em que as variáveis possuem grau menor que 3, donde é possível colorir com 3 cores. Portanto a coloração apresentada para esse grafo, faz uso de uma cor a mais. Mais a diante veremos como se dá essa coloração.

Observação 5.2.12. É claro que dependendo do problema ao qual o grafo está relacionado, um Sudoku por exemplo, alguns valores iniciais podem ser exigidos (que em linguagem de coloração significaria dizer que alguns vértices já assumiriam uma cor específica), levando isso em consideração "minimizar" a quantidade de cores pode estar relacionado ao problema inicialmente proposto.

Notamos que quando a complexidade do grafo aumenta, uma expansão dos fatores pode-se tornar inviável. Como último resultado deste texto, abordaremos uma forma de solucionar a coloração baseado apenas em uma base de Gröbner específica.

Um grafo $G = (V, A)$ com n vértices pode ser colorido com k cores se, e somente se, existe $v \in Z(x_1^k - 1, \cdots, x_n^k - 1)$ tal que $(i, j) \in A$ implica em $v_i \neq v_j$, isto é, se o fator $x_i - x_j$ aparece em P_G, então $v_i - v_j \neq 0$. Assim v deve satisfazer:

$$x_i^k - x_j^k = (x_i^k - 1) - (x_j^k - 1) = 0 \quad \text{e} \quad x_i - x_j \neq 0, \quad \forall\ (i, j) \in A.$$

Considerando

$$h_{i,j}^{k-1} = \sum_{\ell=0}^{k-1} x_i^\ell x_j^{k-1-\ell},$$

obtemos

$$(x_i - x_j)h_{i,j}^{k-1} = x_i \sum_{\ell=0}^{k-1} x_i^\ell x_j^{k-1-\ell} - x_j \sum_{\ell=0}^{k-1} x_i^\ell x_j^{k-1-\ell} \tag{5.1}$$

$$= \sum_{\ell=0}^{k-1} x_i^{\ell+1} x_j^{k-1-\ell} - \sum_{\ell=0}^{k-1} x_i^\ell x_j^{k-\ell} \tag{5.2}$$

$$= x_i^k - x_j^k + \sum_{\ell=0}^{k-2} x_i^{\ell+1} x_j^{k-1-\ell} - \sum_{\ell=1}^{k-1} x_i^\ell x_j^{k-\ell} \tag{5.3}$$

$$= x_i^k - x_j^k \tag{5.4}$$

Mas $x_i^k - x_j^k = 0$ e $x_i - x_j \neq 0$, portanto $h_{i,j}^{k-1} = 0$.

Por outro lado, se $w = (w_1, \cdots, w_n) \in \mathcal{U}_k^n$ satisfaz $w_i = w_j$, então

$$h_{i,j}^{k-1}(w) = \sum_{\ell=0}^{k-1} w_i^\ell w_i^{k-1-\ell} = k w_i^{k-1} \neq 0.$$

Por construção os pontos de $\mathcal{U}_k^n$ que são colorações do grafo G com k cores são os zeros dos polinômios $h_{i,j}^{k-1}$ para os quais $(i, j) \in A$.

Definição 5.2.13. Dado um grafo $G = (V, A)$ e k cores, dizemos que $x_i^k - 1$ para cada i de V é um **polinômio do tipo vértice**. E $h_{i,j}^{k-1}$ para cada (i, j) de A é um **polinômio do tipo aresta**. Denotamos B_G^k como sendo o ideal gerado por esses polinômios.

Por essa construção, colorações de G com k cores são os zeros de B_G^k. A partir disso e do teorema dos zeros de Hilbert, obtemos o seguinte resultado:

Proposição 5.2.14. *$\mathcal{X}(G) \leqslant k$ se, e somente se, $1 \notin B_G^k$.*

Demonstração. Por contrapositiva, suponhamos que 1 pertença ao ideal B_G^k, então, pelo exemplo 3.6.2, $Z(B_G^k) = \emptyset$. Como as colorações do grafo G são obtidas pelos zeros de B_G^k, isto é, por elementos de $Z(B_G^k)$, concluímos que G não admite coloração com este número de cores, portanto $\mathcal{X}(G) > k$.

Reciprocamente, se $1 \notin B_G^k$, então B_G^k é próprio em $Q[x_1, \cdots, x_n]$ e pelo teorema dos zeros de Hilbert $Z(B_G^k)$ é não vazio, donde existe pelo menos um $v \in Z(B_G^k)$, como

os zeros de B_G^k são colorações de G, segue que v é uma coloração do grafo, portanto $\mathcal{X}(G) \leqslant k$. □

Como isso pode ser testado usando apenas bases de Gröbner, esta proposição torna-se um critério computacionalmente mais viável que os anteriores como veremos no seguinte exemplo:

Exemplo 5.2.15. Consideramos novamente o grafo de Chao e Chen (exemplo 5.2.4). Como o grafo tem 12 vértices, B_G^k será um ideal de $\mathbb{Q}[x_1, \cdots, x_{12}]$. Tomando $k = 3$, obtemos que B_G^k é gerado pelos

- 12 polinômios do tipo vértice: $x_i^3 - 1$ para $1 \leqslant i \leqslant 12$;
- 23 polinômios do tipo aresta: $x_i^2 + x_i x_j + x_j^2$ toda vez que houver uma aresta entre os vértices $1 \leqslant i < j \leqslant 12$.

Utilizando o software Magma [7] (veja apêndice A) obtemos uma base de Gröbner de B_G^3 em relação a ordem lexicográfica:

$$\langle x_1 - x_{12},\ x_2 - x_{11}, x_3 + x_{11} + x_{12},\ x_4 + x_{11} + x_{12},\ x_5 - x_{11},\ x_6 + x_{11} + x_{12},$$
$$x_7 - x_{12},\ x_8 - x_{11},\ x_9 + x_{11} + x_{12},\ x_{10} - x_{12},\ x_{11}^2 + x_{11}x_{12} + x_{12}^2,\ x_{12}^3 - 1\rangle$$

Ainda com auxílio do Magma, podemos verificar que 1 não pertence a este ideal, portanto concluímos que o grafo de Chao e Chen pode ser colorido com apenas 3 cores.

O mais interessante é que a base obtida nos guia ainda na coloração do grafo. De fato, primeiro, lembramos que as cores são as raízes unidade de ordem 3, ou seja, ζ^0, ζ^1 e ζ^2, onde $\zeta = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Em seguida, notamos que a tripla $(\zeta^0, \zeta^1, \zeta^2)$ é um zero de $x + y + z = 0$, pois

$$\zeta^0 + \zeta^1 + \zeta^2 = 1 - \frac{1}{2} + i\frac{\sqrt{3}}{2} - \frac{1}{2} - i\frac{\sqrt{3}}{2} = 0.$$

Além disso, as duplas: (ζ^0, ζ^1), (ζ^0, ζ^2), (ζ^1, ζ^2) são zeros do polinômio $x^2 + xy + y^2$, pois

$$(\zeta^0)^2 + \zeta^0\zeta^1 + (\zeta^1)^2 = \zeta^0 + \zeta^1\zeta^0 + \zeta^2 = \zeta^0 + \zeta^1 + \zeta^2 = 0,$$

$$(\zeta^0)^2 + \zeta^0\zeta^2 + (\zeta^2)^2 = \zeta^0 + \zeta^2 + \zeta^4 = \zeta^0 + \zeta^2 + \zeta^1 = 0,$$

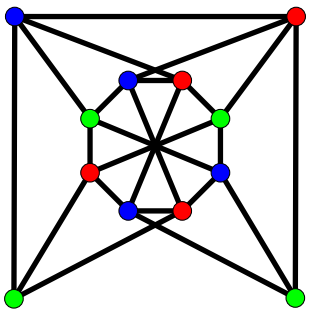
$$(\zeta^1)^2 + \zeta^1\zeta^2 + (\zeta^2)^2 = \zeta^2 + \zeta^3 + \zeta^4 = \zeta^2(\zeta^0 + \zeta^1 + \zeta^2) = 0.$$

Assim, estamos prontos para colorir o grafo de Chao e Chen, isto é, estamos prontos para procurar os zeros dos polinônios da base de Gröbner obtida pelo Magma.

Vamos começar com o último polinômio da base e seguir até o primeiro:

- $x_{12}^3 - 1$: Indica que podemos pintar o vértice 12 com qualquer cor entre as 3;
- $x_{11}^2 + x_{11}x_{12} + x_{12}^2$: Indica que o 11 não pode ter a mesma cor do 12;
- $x_{10} - x_{12}$: Indica que 10 e 12 têm a mesma cor;
- $x_9 + x_{11} + x_{12}$: Indica que 9 tem cor diferente de 11 e 12, isto é, uma terceira cor;
- $x_8 - x_{11}$: Indica que 8 a tem a mesma cor de 11;
- $x_7 - x_{12}$: Indica que 7 a tem a mesma cor de 12;
- $x_6 + x_{11} + x_{12}$: Indica que 6 tem cor diferente de 11 e 12;
- $x_5 - x_{11}$: Indica que 5 tem a mesma cor de 11;
- $x_4 + x_{11} + x_{12}$: Indica que 4 tem cor diferente de 11 e 12;
- $x_3 + x_{11} + x_{12}$: Indica que 3 tem cor diferente de 11 e 12;
- $x_2 - x_{11}$: Indica que 2 tem a mesma cor de 11;
- $x_1 - x_{12}$: Indica que 1 tem a mesma cor de 12.

Dessa forma, colorimos os vértices 1, 7, 10 e 12 com uma das cores, digamos azul; os vértices 2, 5, 8 e 11 com uma outra, digamos vermelho; e por fim os vértices 3, 4, 6 e 9 com a última cor, verde. Portanto, obtemos a seguinte coloração:



A Testando pertinência no Magma

Magma é um software projetado para cálculos em álgebra, teoria dos números, geometria algébrica e combinatória algébrica. Como código nativo, encontramos os algoritmos de Buchberger e pseudo-divisão, além de ter a ordem lexicográfica como padrão ao trabalharmos com polinômios em várias variáveis. A calculadora online do magma, pode ser acessada em

http://magma.maths.usyd.edu.au/calc/

e para aplicarmos a proposição 5.2.14 no exemplo 5.2.15 compilamos o seguinte bloco de comandos:

```
1  Q := RationalField();
2  P<x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_10,x_11,x_12> :=
       PolynomialRing(Q, 12);
3  I := ideal<P |  /* Polinômios do tipo vértice */
4                  x_1^3-1, x_2^3-1, x_3^3-1, x_4^3-1,
5                  x_5^3-1, x_6^3-1, x_7^3-1, x_8^3-1,
6                  x_9^3-1, x_10^3-1, x_11^3-1, x_12^3-1,
7                  /* Polinômios do tipo aresta */
8                  x_1^2+x_1*x_2+x_2^2, x_1^2+x_1*x_4+x_4^2, x_1^2+
                      x_1*x_8+x_8^2,
9                  x_1^2+x_1*x_6+x_6^2, x_2^2+x_2* x_7+x_7^2, x_2^2+
                      x_2*x_9+x_9^2,
10                 x_2^2+x_2*x_3+x_3^2, x_3^2+x_3*x_10+x_10^2, x_3
                      ^2+x_3*x_12+x_12^2,
11                 x_4^2+x_4*x_5+x_5^2, x_4^2+x_4*x_11+x_11^2, x_5
                      ^2+x_5*x_6+x_6^2,
12                 x_5^2+x_5*x_12+x_12^2, x_5^2+x_5*x_9+x_9^2, x_6
                      ^2+x_6*x_7+x_7^2,
13                 x_6^2+x_6*x_10+x_10^2, x_7^2+x_7*x_8+x_8^2, x_7
                      ^2+x_7*x_11+x_11^2,
14                 x_8^2+x_8*x_9+x_9^2, x_8^2+x_8*x_12+x_12^2, x_9
                      ^2+x_9*x_10+x_10^2,
15                 x_10^2+x_10*x_11+x_11^2, x_11^2+x_11*x_12+x_12
                      ^2>;
16 B := GroebnerBasis(I);
17 B;
18 1 in B;
```

Observamos que o ideal I definido na linha 3 do código representa o ideal B_G^3 e os polinômios que o geram são os do tipo vértice e aresta enunciados no exemplo.

Após isso, solicitamos o cálculo e a impressão da base (nas linhas 16 e 17) e por fim, testamos a afirmação da proposição (na linha 18). Ao compilarmos, o Magma nos retorna o seguinte bloco:

```
1  [
2      x_1 - x_12,
3      x_2 - x_11,
4      x_3 + x_11 + x_12,
5      x_4 + x_11 + x_12,
6      x_5 - x_11,
7      x_6 + x_11 + x_12,
8      x_7 - x_12,
9      x_8 - x_11,
10     x_9 + x_11 + x_12,
11     x_10 - x_12,
12     x_11^2 + x_11*x_12 + x_12^2,
13     x_12^3 - 1
14 ]
15 false
```

Portanto, 1 não pertence a este ideal, logo o grafo de Chao e Chen pode ser colorido com apenas 3 cores. É importante ressaltar, como já havíamos mencionado, a viabilidade computacional deste teste. O Magma corrobora essa afirmação ao necessitar de 0.210 segundos para o cálculo da base e o teste da pertinência. Dessa forma, a solução do problema de coloração de grafos através das bases de Gröbner é eficiente.

REFERÊNCIAS

[1] K. APPEL e W. HAKEN, *The Solution of the Four-Color-Map Theorem* Scientific American Vol. 237, N. 4 (1977), pp. 108-121. doi:10.1038/scientificamerican1077-108.

[2] D. BAYER, The division algorithm and the Hilbert scheme, Tese de Doutorado, Estados Unidos: Harvard, 1982.

Disponível em: https://www.math.columbia.edu/∼bayer/papers/Bayer-thesis.pdf (acesso em 15 de julho de 2018).

[3] B. BUCHBERGER, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Tese de Doutorado, Áustria: Univ. Innsbruck, 1965.

Tradução publicada em: Journal of Symbolic Computation, Vol. 41, N. 3-4 (2006), pp. 475-511. doi:10.1016/j.jsc.2005.09.007.

[4] S. C. COUTINHO. Polinômios e Computação Algébrica. *Coleção Matemática e Aplicações*, Rio de Janeiro: IMPA, 2012.

[5] A. GONÇALVES. Introdução à Álgebra. 5^a edição. *Projeto Euclides*, Rio de Janeiro: IMPA, 2015.

[6] M. E. HERNANDES. Um primeiro contato com Bases de Gröbner. *28^o Colóquio Brasileiro de Matemática*, Rio de Janeiro: IMPA, 2011.

[7] W. BOSMA, J. CANNON e C. PLAYOUST, *The Magma algebra system.* I. The user language, J. Symbolic Comput., 24 (1997), pp. 235-265.