Sistemas Polinomiais, Mapas e Origamis

Marcelo Escudeiro Hernandes[1]
Departamento de Matemática
Universidade Estadual de Maringá

[1]mehernandes@uem.br

Introdução

O que sistemas de equações polinomiais, coloração de mapas e origamis possuem em comum? Todos podem ser abordados utilizando Bases de Gröbner!

O objetivo destas notas é oferecer ao leitor uma introdução às Bases de Gröbner e algumas de suas muitas e interessantes aplicações.

O conceito de Bases de Gröbner e o algoritmo para obtê-las, apresentado por Bruno Buchberger em sua tese de doutorado em meados de 1960 sob orientação de Wolfgang Gröbner, impressiona pela genialidade, simplicidade e pelo grande número de aplicações nas mais diversas áreas. Inicialmente desenvolvida para ideais polinomiais, a teoria de Bases de Gröbner foi estendida para ideais dos anéis de séries de potências, módulos, subálgebras e outras estruturas algébricas.

Nestas notas serviremos um aperitivo desta teoria para ideais polinomiais. Esperamos que isto estimule o apetite do leitor na busca de mais detalhes, profundidade e aplicações deste assunto.

A estrutura destas notas segue a seguinte trilha: Iniciaremos (re)vendo o anel de polinômios em uma indeterminada passando na sequência para o estudo de anéis de polinômios em várias variáveis, maneiras de ordenar monômios, ideais e uma generalização do algoritmo da divisão.

Na sequência, introduziremos o conceito de Bases de Gröbner e nos concentraremos em sua construção, para tanto seguiremos os passos de Buchberger definindo S-polinômio e apresentando seu famoso algoritmo.

Como aplicações do algoritmo de Buchberger, veremos como resolver sistemas de equações polinomiais. Como subproduto desta aplicação, veremos como modelar algebricamente o problema da co-

loração de mapas com três cores sem que regiões adjacentes recebam uma mesma cor, de modo que sua solução possa ser obtida por meio de Bases de Gröbner. Finalizaremos abordando uma recente aplicação, dada pelo próprio Buchberger, que consiste em validar uma construção realizada com Origami via Bases de Gröbner. Em particular, veremos como um dos problemas clássicos da Geometria, a trisecção do ângulo, embora não possa ser realizado com régua (não graduada) e compasso, pode ser realizado via Origami.

Meus agradecimentos à Comissão Organizadora do I Colóquio de Matemática da Região Sul por ter aceitado a proposta do minicurso que originou estas notas, a Wesley Grütner Martins e Jorge Luiz Deolindo Silva que sob minha orientação desenvolveram trabalhos de iniciação científica no tema.

Registro ainda, um agradecimento mais do que especial à Maria Elenice Rodrigues Hernandes que leu, apontou sugestões e correções e a nossa pequena Laura, a quem dedico estas notas e que soube tirar minha atenção nos momentos certos.

Maringá, maio de 2010.

Marcelo Escudeiro Hernandes

Conteúdo

Introdução **i**

1 Anéis de Polinômios **1**
1.1 Um pouco da teoria geral de Anéis 1
1.2 Anéis de Polinômios em uma indeterminada 5
1.2.1 Algoritmo da divisão em $\mathbb{K}[x]$ 8
1.3 Anéis de Polinômios em várias indeterminadas 18
1.3.1 Ordens Monomiais 20
1.3.2 Algoritmo da divisão em $\mathbb{K}[x_1, \ldots, x_n]$ 29

2 Bases de Gröbner para ideais em $\mathbb{K}[x_1, \ldots, x_n]$ **36**
2.1 Ideais 36
2.2 O Algoritmo da divisão revisitado 45
2.3 Bases de Gröbner 53
2.4 Algoritmo de Buchberger 59
2.4.1 Implementações 69

3 Aplicações **70**
3.1 Sistemas de Equações Polinomiais 70
3.2 Coloração de Mapas 76
3.2.1 Raízes da Unidade 78
3.2.2 O Problema das Três Cores 78
3.3 Validação de Origamis 82

Bibliografia **89**

Índice Remissivo **91**

Capítulo 1

Anéis de Polinômios

A essência deste livro é apresentar uma introdução a teoria Bases de Gröbner para ideais de anéis de polinômios em várias variáveis, bem como aplicações desta teoria. Neste capítulo abordaremos conceitos e propriedades ligados aos anéis de polinômios sem a intenção de esgotar o assunto e sim de fornecer subsídios para o restante das notas.

Os pontos centrais do capítulo são: o anel de polinômios em várias variáveis, o conceito de ordens monomiais e o algoritmo da pseudo-divisão.

1.1 Um pouco da teoria geral de Anéis

Nesta seção introduziremos o conceito de *anel*, bem como algumas propriedades a ele relacionadas, o leitor que possui alguma familiaridade com tal estrutura pode avançar para a próxima seção sem prejuízo algum.

Várias vezes faremos uso da noção de *operação binária* sobre um conjunto C. Tal conceito se refere simplesmente a uma aplicação $\star$ que associa a cada par de elementos de C um outro elemento do conjunto C, ou seja,

$$\begin{array}{rccc} \star: & C \times C & \longrightarrow & C \\ & (a,b) & \mapsto & \star(a,b). \end{array}$$

Vamos sempre indicar $\star(a,b)$ por $a \star b$.

Definição 1.1. *Seja A conjunto não vazio munido de duas operações binárias*

$$\begin{array}{rccc} \oplus: & A\times A & \longrightarrow & A \\ & (a,b) & \mapsto & a\oplus b \end{array} \quad e \quad \begin{array}{rccc} \odot: & A\times A & \longrightarrow & A \\ & (a,b) & \mapsto & a\odot b. \end{array}$$

Dizemos que $(A,\oplus,\odot)$ é um **anel** *se as seguintes propriedades são satisfeitas:*

1. *$a\oplus(b\oplus c)=(a\oplus b)\oplus c$ para quaisquer $a,b,c\in A$ (Associatividade de $\oplus$).*
2. *Para todos $a,b\in A$, temos $a\oplus b=b\oplus a$ (Comutatividade de $\oplus$).*
3. *Existe $z\in A$ tal que $a\oplus z=a$ para todo $a\in A$. O elemento z será chamado* **elemento neutro** *de $\oplus$.*
4. *Para todo $a\in A$, existe $s(a)\in A$ tal que $a\oplus s(a)=z$. Denominaremos o elemento $s(a)$ de* **simétrico** *ou* **oposto** *de a.*
5. *Para quaisquer $a,b,c\in A$, temos $a\odot(b\odot c)=(a\odot b)\odot c$ (Associatividade de $\odot$).*
6. *Temos $a\odot(b\oplus c)=(a\odot b)\oplus(a\odot c)$ e $(a\oplus b)\odot c=(a\odot c)\oplus(b\odot c)$ para todos $a,b,c\in A$ (Distributividade de $\odot$ com respeito a $\oplus$).*

Dizemos que um anel $(A,\oplus,\odot)$ tem **elemento unidade**, se existe $u\in A$ tal que $a\odot u=u\odot a=a$ para todo $a\in A$. Neste caso, um elemento $a\in A$ é chamado de **invertível**, se existe um elemento $i(a)\in A$ tal que $a\odot i(a)=i(a)\odot a=u$. Chamamos $i(a)$ de **inverso** do elemento a. Um anel $(A,\oplus,\odot)$ é dito **comutativo** se $a\odot b=b\odot a$ para todos $a,b\in A$.

Exemplo 1.2. *O conjunto $(\mathbb{N},+,\cdot)$ dos números naturais munido com as operações usuais de adição e multiplicação não é um anel. Por outro lado, o conjunto $(\mathbb{Z},+,\cdot)$ dos números inteiros, $(\mathbb{Q},+,\cdot)$ dos números racionais, $(\mathbb{R},+,\cdot)$ dos números reais e $(\mathbb{C},+,\cdot)$ dos números complexos, com as operações de adição e multiplicação usualmente adotadas, são exemplos de anéis comutativos e com unidade. Nestes*

casos, $z = 0$, $s(a) = -a$ *e* $u = 1$. *Além disto, os únicos elementos invertíveis de* $(\mathbb{Z}, +, \cdot)$ *são* -1 *e* 1, *enquanto para os outros anéis todos os elementos distintos de* 0 *são invertíveis.*

Para aliviar as notações e não sobrecarregarmos o texto de uma simbologia desnecessária, sempre que nos referirmos a um anel qualquer, utilizaremos a notação $(A, +, \cdot)$, 0 para o elemento neutro, 1 para o elemento unidade (quando A o admitir), $-a$ para o simétrico de a, a^{-1} para o inverso de a (se a o admitir) e ab para indicar $a \cdot b$ com $a, b \in A$. Além disto, quando tratarmos de um anel $(A, +, \cdot)$ cujas operações são as usualmente adotadas, o denotaremos simplesmente por A.

Os exemplos de anéis dados anteriormente, podem sugerir erroneamente que um anel deve possuir obrigatoriamente um número infinito de elementos. Para afastar totalmente esta ideia apresentamos abaixo, exemplo de anéis com um número finito de elementos.

Exemplo 1.3. *Dado um inteiro* $n > 1$, *denotemos por* $\mathbb{Z}_n$ *o conjunto* $\{0, 1, \ldots, n-1\}$ *e consideremos as operações*

$$\begin{array}{rccc} \oplus: & \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & (a,b) & \mapsto & a + b \ mod \ n \end{array} \quad e \quad \begin{array}{rccc} \odot: & \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & (a,b) & \mapsto & a \cdot b \ mod \ n \end{array}$$

onde $a + b \ mod \ n$ *e* $a \cdot b \ mod \ n$ *indicam respectivamente, o resto da divisão de* $a + b$ *e* $a \cdot b$ *por* n.

O leitor pode verificar, sem maiores dificuldades, que $(\mathbb{Z}_n, \oplus, \odot)$ *é um anel comutativo com unidade cujo simétrico de um elemento* a *é* $n - a$.

Dizemos que um anel comutativo $(A, \oplus, \odot)$ é um **domínio (de integridade)**, se dados quaisquer $a, b \in A$ tais que $ab = 0$ temos que $a = 0$ ou $b = 0$.

Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são domínios. Enquanto o anel $(\mathbb{Z}_6, \oplus, \odot)$, como definido acima, não o é, pois temos que $2 \odot 3 = 0$.

Exercício 1.4. *Mostre que* $(\mathbb{Z}_n, \oplus, \odot)$ *como definido anteriormente é um domínio se, e somente se,* n *é um número primo.*

Um domínio A é chamado **corpo** se todo elemento $a \in A \setminus \{0\}$ é invertível. Assim, os anéis $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são corpos, mas $\mathbb{Z}$ não o é.

Exercício 1.5. *Mostre que todo domínio que possui um número finito de elementos é um corpo. Conclua que $(\mathbb{Z}_n, \oplus, \odot)$ é corpo se, e somente se, n é um número primo. Calcule o inverso de todos os elementos não nulos do corpo $\mathbb{Z}_7$. Deduza um método para obter o inverso de qualquer elemento não nulo de $\mathbb{Z}_n$ com n um número primo.*

Exercício 1.6. *Seja $\mathbb{A}$ um domínio e considere o conjunto*

$$K = \left\{ \frac{p}{q};\ p, q \in \mathbb{A} \text{ com } q \neq 0 \right\}$$

cujos elementos estão sujeitos às relações:

1. $\frac{p_1}{q_1} = \frac{p_2}{q_2}$ *se, e somente se,* $p_1 q_2 = p_2 q_1$.

2. $\frac{p}{1} = p$, *isto é, identificamos* $\mathbb{A}$ *como subconjunto de* K.

Mostre que K é um corpo, chamado **corpo de frações** *do domínio $\mathbb{A}$, munido com as operações*

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 . q_2 + p_2 . q_1}{q_1 . q_2} \quad e \quad \frac{p_1}{q_1} \cdot \frac{p_2}{q_2} = \frac{p_1 . p_2}{q_1 . q_2}.$$

Exemplo 1.7. *O corpo de frações de $\mathbb{Z}$ é $\mathbb{Q}$.*

Dizemos que um elemento $a \in A \setminus \{0\}$ **divide** $b \in A$, ou equivalentemente, que b é **divisível** por a, que indicaremos $a \mid b$, se existe $c \in A$ tal que $b = ac$.

Observação 1.8. *Note que se A é um corpo, então temos que um elemento $a \neq 0$ divide qualquer outro elemento $b \in A$. De fato, como $a \neq 0$, existe $a^{-1} \in A$, assim $a^{-1}b \in A$ e portanto, temos que $b = 1.b = (aa^{-1})b = a(a^{-1}b)$.*

Se a divide b, então o elemento $c \in A$, tal que $b = ac$, quando não dado explicitamente, será denotado por $\frac{b}{a}$.

1.2 Anéis de Polinômios em uma indeterminada

Nesta seção abordaremos um anel particular: o anel de polinômios em uma indeterminada.

O leitor certamente já manteve um primeiro contato com polinômios em uma indeterminada e não encontrará obstáculos em aceitar como corretos os cálculos:

$$(3x^2 + 2x - 1) + (3x + 5) = 3x^2 + 5x + 4$$

$$(3x^2 + 2x - 1).(3x + 5) = 9x^3 + 21x^2 + 7x - 5.$$

Poderíamos simplesmente utilizar os conhecimentos prévios do leitor para o que necessitamos, mas optamos por uma apresentação mais rigorosa e precisa.

Seja $(A, +, \cdot)$ um anel e considere o conjunto

$$A[x] = \{a_n x^n + \ldots + a_1 x + a_0;\ n \in \mathbb{N} \text{ e } a_i \in A\}.$$

Um elemento de $A[x]$ é chamado um **polinômio na indeterminada** x **com coeficiente em** A.

Dizemos que $a_n x^n + \ldots + a_1 x + a_0, b_m x^m + \ldots + b_1 x + b_0 \in A[x]$ são iguais se, e somente se, $n = m$ e $a_i = b_i$ para todo $0 \leq i \leq n$.

Convencionando que $ax^0 = a$, temos que $A \subset A[x]$. Um polinômio é chamado de **constante** se ele pertence a A. Além disto, podemos munir $A[x]$ com operações que o tornam um anel e que estendem as operações do anel A. Para tanto, dados polinômios $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i \in A[x]$, definimos

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

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

No restante destas notas, vamos considerar apenas anéis comutativos com elemento unidade.

Exercício 1.9. *Sejam $(A, +, \cdot)$ um anel e o conjunto $A[x]$ munido com as operações acima definidas.*

1. *Mostre que $(A[x], +, \cdot)$ é um anel que é comutativo se A também o for.*
2. *Conclua que se A possui elemento unidade, então o mesmo ocorre com $A[x]$.*
3. *Mostre que $A[x]$ é um domínio sempre que A o for e que, neste caso, os únicos elementos invertíveis de $A[x]$ são os elementos invertíveis de A.*

A operação de multiplicação acima, nos assegura que $0x^i = 0$ para todo $i \in \mathbb{N}$. Deste modo, temos que

$$a_n x^n + \ldots + a_1 x + a_0 = 0x^r + \ldots + 0x^{n+1} + a_n x^n + \ldots + a_1 x + a_0$$

para qualquer $r > n$, ou seja, $a_i = 0$ para todo $i > n$, e assim, podemos redefinir a soma de elementos $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i \in A[x]$ como

$$f + g = \sum_{i=0}^{max\{n,m\}} c_i x^i \text{ com } c_i = a_i + b_i.$$

Dado um elemento $f = \sum_{i=0}^{n} a_i x^i \in A[x]$ não nulo, chamamos de **termo** de f a cada parcela $a_i x^i$ não nula, a_i é chamado **coeficiente** e x^i é chamado **monômio**. O monômio x^0 será denotado por 1. Além disto, indicaremos o conjunto de todos o monômios de f por $\mathbb{M}(f)$.

Definição 1.10. *Seja $f = \sum_{i=0}^{n} a_i x^i \in A[x]$ não nulo. Chamamos de* **grau de** *f e denotamos por $gr(f)$ o inteiro $max\{i;\ x^i \in \mathbb{M}(f)\}$. Vamos convencionar que $gr(0) = \infty$.*

O **termo líder** *de f é $tl(f) = a_n x^n$, $cl(f) = a_n$ é chamado de* **coeficiente líder** *e $ml(f) = x^n$ de* **monômio líder** *onde $n = gr(f)$.*

Um polinômio é dito **mônico** se seu coeficiente líder é 1. Note ainda que dado $f \in A[x]$ não nulo temos que $ml(f) = \frac{tl(f)}{cl(f)}$. Além disto, temos que $gr(f) = 0$ se, e somente se, $f \in A \setminus \{0\}$.

Exemplo 1.11. *Sejam* $f = 2x^2 + 4x + 2$ *e* $g = 3x^2 + 3 \in \mathbb{R}[x]$.

Temos que $f+g = 5x^2+4x+5$ *e* $fg = 6x^4+12x^3+12x^2+12x+6$ *possuem grau* 2 *e* 4 *respectivamente. No entanto, considerados como elementos de* $\mathbb{Z}_3[x]$ *temos que* $f + g = 2x^2 + x + 2$ *e* $fg = 0$ *possuem grau* 2 *e* ∞ *respectivamente, enquanto que tomados como elementos de* $\mathbb{Z}_5[x]$ *temos que* $f+g = 4x$ *e* $fg = x^4+2x^3+2x^2+2x+1$ *possuem grau* 1 *e* 4 *respectivamente.*

O exemplo acima nos instiga relacionar o grau de $f + g$ e fg com os graus dos polinômios f e g. Vejamos o que podemos concluir.

Dados $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{i=0}^{m} b_i x^i \in A[x]$, temos que

$$\mathbb{M}(f + g) \subseteq \mathbb{M}(f) \cup \mathbb{M}(g).$$

De fato, lembremos que os termos de $f + g$ são da forma $(a_j + b_j)x^j$ com $a_j + b_j \neq 0$ para todo $0 \leq j \leq max\{n, m\}$. Deste modo, todo monômio de $f + g$ é um monômio de f ou de g.

Segue assim que

$$\begin{aligned} gr(f + g) &= max\{i; x^i \in \mathbb{M}(f + g)\} \leq max\{i; x^i \in \mathbb{M}(f) \cup \mathbb{M}(g)\} \\ &= max\{max\{i; x^i \in \mathbb{M}(f)\}, max\{i; x^i \in \mathbb{M}(g)\}\} \\ &= max\{gr(f), gr(g)\}. \end{aligned}$$

Note que se $gr(f) \neq gr(g)$, então

$$max\{i; x^i \in \mathbb{M}(f + g)\} = max\{i; x^i \in \mathbb{M}(f) \cup \mathbb{M}(g)\}$$

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

Além disto, dados $f = \sum_{i=0}^{n} a_i x^i$ e $g = \sum_{i=0}^{m} b_i x^i$, temos que $gr(fg) = \infty$ se $fg = 0$. Por outro lado se $fg \neq 0, a_n \neq 0$ e $b_m \neq 0$, isto é, $gr(f) = n$ e $gr(g) = m$, então como $fg = \sum_{i=0}^{n+m} c_i x^i$ com $c_i = \sum_{j+k=i} a_j b_k$ temos que $gr(fg) \leq n + m = gr(f) + gr(g)$ com igualdade se $c_{n+m} = a_n b_m \neq 0$. Note que esta condição é satisfeita sempre que A é um domínio. No que segue vamos nos restringir a este caso, ou seja, consideramos A e consequentemente $A[x]$ domínios (veja Exercício 1.9). Neste caso, se convencionarmos que

$$\infty + i = \infty \text{ e } \infty + \infty = \infty$$

para todo $i \in \mathbb{N}$, então temos que

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

para quaisquer $f, g \in A[x]$.

1.2.1 Algoritmo da divisão em $\mathbb{K}[x]$

Nestas notas, o problema de decidir se um polinômio divide outro é a questão central de toda a teoria que abordaremos. Exploremos a noção de divisibilidade para elementos de $A[x]$ iniciando com o caso em que os polinômios envolvidos possuem apenas um termo não nulo.

Sabemos que em $A[x]$, um termo não nulo ax^i divide bx^j se, e somente se, existe $g \in A[x]$ tal que $bx^j = g \cdot ax^i$. Tal igualdade nos indica que $gr(g) = j - i$, ou seja, uma condição necessária para que $ax^i \mid bx^j$ é que $i \leq j$. Suponha que $bx^j = g.ax^i$ e $g = c_{j-i}x^{j-i} + \ldots + c_1x + c_0$, ou seja, $bx^j = c_{j-i}ax^j + \ldots + c_1ax + c_0a$, que consequentemente nos dá que $b = c_{j-i}a$, equivalentemente $a \mid b$ e $c_ka = 0$ para todo $0 \leq k < j - i$. Como A é um domínio e $a \neq 0$, devemos ter que $c_k = 0$ para todo $0 \leq k < j - i$. Assim, $ax^i \mid bx^j$ se, e somente se, $i \leq j$ e $a \mid b$.

Pela Observação 1.8, se A é um corpo, então a condição $a \mid b$ sempre é satisfeita para $a \neq 0$. Para nossos propósitos, a hipótese de A ser um corpo será suficiente para atingirmos os objetivos propostos. Seguindo a tendência de simplificarmos as notações, convencionaremos nestas notas que $\mathbb{K}$ denota um corpo. Desta forma em $\mathbb{K}[x]$ temos que ax^i divide bx^j se, e somente se, $i \leq j$ e neste caso, $\frac{bx^j}{ax^i} = ba^{-1}x^{j-i}$.

Um outro conhecimento que certamente faz parte da cultura matemática do leitor é o algoritmo da divisão em $\mathbb{K}[x]$, cuja descrição e justificativa apresentamos no teorema abaixo.

Teorema 1.12. (Algoritmo da Divisão) *Dado $g \in \mathbb{K}[x] \setminus \{0\}$, para qualquer $f \in \mathbb{K}[x]$ existem $q, r \in \mathbb{K}[x]$ unicamente determinados pelas condições*

$$f = qg + r, \text{ com } r = 0 \text{ ou } gr(r) < gr(g).$$

DEM: (*Existência:*) Se $f = 0$, então basta considerar $q = r = 0$ e teremos $f = 0 = 0.g + 0 = qg + r$ satisfazendo as condições do teorema.

Seja $f \neq 0$, vamos proceder a demonstração por indução sobre $gr(f)$.

Se $gr(f) < gr(g)$, então tomando $q = 0$ e $r = f$ temos $f = 0.g + f$ e obtemos o desejado.

Por outro lado, se $gr(f) \geq gr(g)$, então $tl(g)$ divide $tl(f)$ e assim,

$$tl(f) = \frac{tl(f)}{tl(g)} tl(g).$$

Se $f - \frac{tl(f)}{tl(g)} g = 0$, então tomando $q = \frac{tl(f)}{tl(g)}$ e $r = 0$ temos o desejado.

Se $f - \frac{tl(f)}{tl(g)} g \neq 0$, então

$$gr\left(f - \frac{tl(f)}{tl(g)} g\right) < gr(f)$$

e por hipótese de indução, existem polinômios $q_1, r_1 \in \mathbb{K}[x]$ tais que

$$f - \frac{tl(f)}{tl(g)} g = q_1 g + r_1,$$

com $r_1 = 0$ ou $gr(r_1) < gr(g)$. Assim,

$$f = \left(\frac{tl(f)}{tl(g)} + q_1\right) g + r_1.$$

Agora, tomando $q = \frac{tl(f)}{tl(g)} + q_1$ e $r_1 = r$ temos o almejado.

(*Unicidade:*) Suponha que existam $q_1, q_2, r_1, r_2 \in \mathbb{K}[x]$ tais que

$$f = q_1 g + r_1 \text{ e } f = q_2 g + r_2$$

com $r_i = 0$ ou $gr(r_i) < gr(g)$ para $i \in \{1, 2\}$, isto é, temos que $gr(g) > max\{gr(r_1), gr(r_2)\}$. Segue que

$$0 = f - f = (q_1 - q_2)g + (r_1 - r_2),$$

ou seja,

$$r_2 - r_1 = (q_1 - q_2)g.$$

Se $r_2 \neq r_1$, então

$$gr(g) > max\{gr(r_1), gr(r_2)\} \geq gr(r_2 - r_1) = gr((q_1 - q_2)g) \geq gr(g).$$

Um absurdo!

Assim, $r_2 = r_1$ e $0 = (q_1 - q_2)g$. Como $\mathbb{K}[x]$ é um domínio e $g \neq 0$, segue que $q_1 - q_2 = 0$ e obviamente $q_1 = q_2$, provando o teorema. ■

Os polinômios q e r, cuja existência e unicidade foram garantidos no teorema acima, são chamados, respectivamente de **quociente** e **resto** de f por g. Além disto, a demonstração do resultado anterior carrega a essência de um algoritmo computacional que permite obter q e r.

Por um algoritmo computacional entendemos uma sequência de passos dados explicitamente e descritos de modo claro que dependem de dados iniciais e após um número finito de etapas fornece o resultado desejado.

Reunindo as instruções dadas na demonstração do resultado acima temos:

ALGORITMO DA DIVISÃO PARA POLINÔMIOS EM $\mathbb{K}[x]$.

ENTRADA: $f, g \in \mathbb{K}[x]$ COM $g \neq 0$;
DEFINA $q := 0$ E $r := f$;
ENQUANTO $r \neq 0$ E $gr(r) \geq gr(g)$ FAÇA
$\quad q := q + \frac{tl(r)}{tl(g)}$;
$\quad r := r - \frac{tl(r)}{tl(g)}g$;
SAÍDA: q E r SATISFAZENDO $f = qg + r$
$\quad$ COM $r = 0$ OU $gr(r) < gr(g)$.

O símbolo ":=" nas instruções acima, que chamamos de *atribuição*, indica que devemos substituir o objeto à esquerda pelo que está à direita do símbolo. Deste modo, se $h := 2$, então $h := h + 1$ indica que h assume o valor 3.

Exemplo 1.13. *Apliquemos o algoritmo acima para obter o quociente e o resto da divisão de* $f = x^5 + x - 1$ *por* $g = 2x^2 + 1$ *em* $\mathbb{R}[x]$.

Inicialmente temos que $q = 0$ *e* $r = f = x^5 + x - 1$.

Passo 1*: Como* $r \neq 0$ *e* $5 = gr(r) > gr(g) = 2$ *fazemos*

$$q = 0 + \frac{x^5}{2x^2} = \frac{1}{2}x^3 \text{ e } r = x^5 + x - 1 - \frac{1}{2}x^3(2x^2 + 1) = -\frac{1}{2}x^3 + x - 1.$$

Passo 2*: Temos que* $r = -\frac{1}{2}x^3 + x - 1$ *e* $3 = gr(r) > gr(g) = 2$*, então*

$$q = \frac{1}{2}x^3 + \frac{-\frac{1}{2}x^3}{2x^2} = \frac{1}{2}x^3 - \frac{1}{4}x \text{ e } r = -\frac{1}{2}x^3 + x - 1 - \left(-\frac{1}{4}x\right)(2x^2+1) = \frac{5}{4}x - 1.$$

Passo 3*: Uma vez que* $r = \frac{5}{4}x - 1 \neq 0$*, mas* $1 = gr(r) < gr(g) = 2$*, o algoritmo finaliza fornecendo como quociente e resto*

$$q = \frac{1}{2}x^3 - \frac{1}{4}x \text{ e } r = \frac{5}{4}x - 1.$$

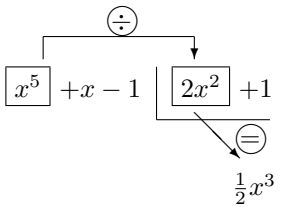
Em geral a aplicação do algoritmo da divisão é feita por meio de um dispositivo prático que facilita e simplifica sua utilização. Tal dispositivo consiste em alocar f, g, q e r como abaixo.

$$\begin{array}{l|l} f & g \\ \hline r & q \end{array}$$

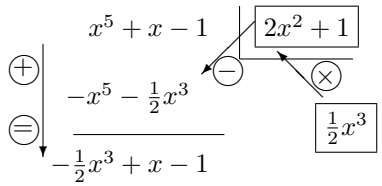
com f e g tendo seus termos ordenados segundo as potências decrescentes de seus monômios. No caso do exemplo considerado acima temos

$$\begin{array}{l|l} x^5 + x - 1 & 2x^2 + 1 \\ \hline \end{array}$$

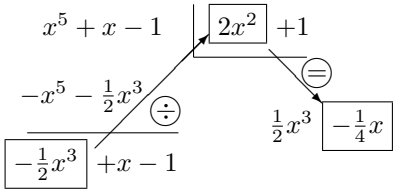
Na sequência procedemos a divisão do termo líder de f pelo termo líder de g, como indica o algoritmo, obtendo $\frac{1}{2}x^3$ que é alocado sob g como ilustrado abaixo.



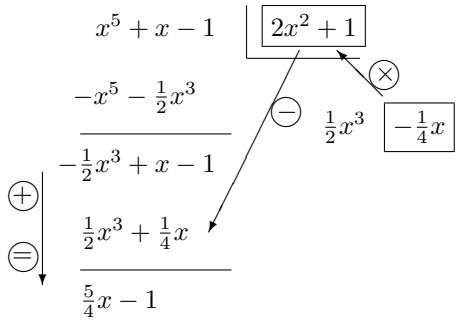
Agora multiplicamos $\frac{1}{2}x^3$ por g e subtraímos de f colocando o resultado da operação embaixo de f, como apresentamos a seguir.



Continuamos com o algoritmo, com $-\frac{1}{2}x^3 + x - 1$ assumindo o papel de f. Assim, temos



e repetimos o processo enquanto o último polinômio obtido à esquerda no dispositivo for não nulo e seu grau for maior ou igual ao grau do polinômio g.



Finalizando o processo obtemos:

$$
\begin{array}{r|l}
x^5 + x - 1 & 2x^2 + 1 \\
\cline{2-2}
-x^5 - \frac{1}{2}x^3 & \\
\cline{1-1}
-\frac{1}{2}x^3 + x - 1 & \boxed{\frac{1}{2}x^3 - \frac{1}{4}x} = q \\
\frac{1}{2}x^3 + \frac{1}{4}x & \\
\cline{1-1}
\boxed{\frac{5}{4}x - 1} = r &
\end{array}
$$

Exercício 1.14. *Sejam $f, g, q \in \mathbb{K}[x]$ tais que q é o quociente da divisão de f por g. Mostre que $gr(q) = gr(f) - gr(g)$.*

Exercício 1.15. *Determine $a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{R}$ de modo que o quociente e o resto da divisão de $x^5 + 2x^4 + 2x^3 + a_1x^2 + x + a_2$ por $a_3x^2 + a_4x + 2$ sejam respectivamente $x^3 + a_5x^2 - x - 3$ e $a_6x + 7$.*

Exercício 1.16. *Determine o quociente e o resto na divisão de f por g em cada caso.*

1. *$f = x^5 + 6x^4 - 10x^3 + 9x^2 - 24x + 5$ e $g = 3x^2 + 6x$ em $\mathbb{Q}[x]$.*
2. *$f = 2x^4 - 6\sqrt{2}x^3 + 9x^2 - 4x - 2$ e $g = \sqrt{2}x^2 - 3x + 1$ em $\mathbb{R}[x]$.*
3. *$f = ix^5 - (1 + i)x^4 + ix^3 - 2ix^2 - 1$ e $g = x^2 + ix + 1$ em $\mathbb{C}[x]$ ($i^2 = -1$).*
4. *$f = x^5 + 6x^4 + 6x^3 + 4x^2 + 4x + 4$ e $g = 4x^2 + 5x + 3$ em $\mathbb{Z}_7[x]$.*

Exercício 1.17. *Seja $n \in \mathbb{N}$ com $n > 0$. Encontre o quociente e o resto na divisão de $x^n - 1$ por $x - 1$.*

Um conceito intimamente ligado a polinômios em uma indeterminada é a noção de raiz que (re)lembramos abaixo.

Definição 1.18. *Seja $f = a_nx^n + \ldots + a_1x + a_0 \in \mathbb{K}[x]$. Um elemento $k \in \mathbb{K}$ é chamado de* **raiz** *de f, se $a_nk^n + \ldots + a_1k + a_0 = 0$.*

Obviamente um polinômio pode admitir mais de uma raiz, como é o caso de $x^2 - 5x + 6 \in \mathbb{Q}[x]$, cujas raízes são 2 e 3, bem como o polinômio nulo que admite qualquer elemento de $\mathbb{K}$ como raiz. Por outro lado, um polinômio pode não admitir raiz, como ocorre com $x^2 + 1 \in \mathbb{R}[x]$, embora possua raízes i e $-i$ se o considerarmos como elemento de $\mathbb{C}[x]$.

Nestas notas, não é nosso objetivo apresentar fórmulas, métodos ou algoritmos para o cálculo de raízes de polinômios em uma indeterminada em termos de seus coeficientes.

No entanto, não podemos deixar de explorar a relação íntima entre o algoritmo da divisão e raízes de polinômios, como expomos nos resultados abaixo.

Proposição 1.19. *Seja $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{K}[x]$. O resto da divisão de f por $x - k$ é $a_n k^n + \ldots + a_1 k + a_0 \in \mathbb{K}$.*

DEM: Aplicando o algoritmo da divisão para f e $x - k$, obtemos polinômios $q = b_{n-1}x^{n-1} + \ldots + b_1 x + b_0, r \in \mathbb{K}[x]$ com $r = 0$ ou então $gr(r) < gr(x - k) = 1$, o que implica que $r \in \mathbb{K}$. Além disto,

$$a_n x^n + \ldots + a_1 x + a_0 = q.(x-k) + r = (b_{n-1}x^{n-1} + \ldots + b_1 x + b_0).(x-k) + r.$$

Assim,

$$a_n k^n + \ldots + a_1 k + a_0 = (b_{n-1}k^{n-1} + \ldots + b_1 k + b_0).(k - k) + r,$$

ou seja,

$$r = a_n k^n + \ldots + a_1 k + a_0.$$

■

Exercício 1.20. *Calcule o resto de f por g nos casos abaixo, sem aplicar o algoritmo da divisão.*

1. $f = 3x^4 - 2x^3 - 5x^2 + 7x - 1$ *e* $g = x - 4$.
2. $f = x^n + x^{n-1} + \ldots + x + 1$ *e* $g = x - 1$.

Como consequência da proposição anterior temos o seguinte corolário.

Corolário 1.21. *Seja $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{K}[x]$. Temos que $k \in \mathbb{K}$ é raiz de f se, e somente se, f é divisível por $x - k$.*

DEM: Pela proposição anterior, o resto da divisão de f por $x-k$ é $a_n k^n + \ldots + a_1 k + a_0$. Por hipótese, k é raiz de f. Assim, temos $a_n k^n + \ldots + a_1 k + a_0 = 0$, isto é, f é divisível por $x - k$.

Reciprocamente, se f é divisível por $x - k$, então o resto da divisão é zero. Mas novamente, pela proposição anterior, temos que o resto é $a_n k^n + \ldots + a_1 k + a_0$, ou seja, $a_n k^n + \ldots + a_1 k + a_0 = 0$ e consequentemente k é raiz de f. ■

O próximo resultado nos dá um limitante para o número de raízes de um polinômio não nulo.

Proposição 1.22. *Sejam $f \in \mathbb{K}[x]$ não nulo e $k_1, \ldots, k_n \in \mathbb{K}$ raízes distintas de f, então $(x - k_1) \cdot \ldots \cdot (x - k_n)$ divide f. Em particular, o número de raízes distintas de f é menor ou igual a $gr(f)$.*

DEM: Seja $f = a_m x^m + \ldots + a_1 x + a_0$. Como k_1 é raiz de f, segue do resultado anterior que $x - k_1$ divide f, ou seja,

$$f = q_1 \cdot (x - k_1),$$

com $q_1 = b_{m-1} x^{m-1} + \ldots + b_1 x + b_0 \in \mathbb{K}$.

Mas $k_2 \in \mathbb{K}$ também é raiz de f. Assim,

$$0 = a_m k_2^m + \ldots + a_1 k_2 + a_0 = (b_{m-1} k_2^{m-1} + \ldots + b_1 k_2 + b_0) \cdot (k_2 - k_1).$$

Como $\mathbb{K}$ é um corpo (em particular um domínio) e $k_2 \neq k_1$, devemos ter que $b_{m-1} k_2^{m-1} + \ldots + b_1 k_2 + b_0 = 0$, ou seja, k_2 é raiz de q_1. Deste modo, novamente pelo resultado anterior, temos que $x - k_2$ divide q_1, ou seja, $q_1 = q_2 \cdot (x - k_2)$ e assim,

$$f = q_2 \cdot (x - k_2) \cdot (x - k_1).$$

Repetindo o argumento para as demais raízes de f temos que

$$f = q_n \cdot (x - k_n) \cdot \ldots \cdot (x - k_1),$$

ou seja, $(x-k_n)\cdot\ldots\cdot(x-k_1)$ divide f. Além disto, da igualdade acima, temos que

$$gr(f) = gr(q_n) + n \geq n,$$

isto é, número de raízes distintas de f é menor ou igual a $gr(f)$. ■

Exercício 1.23. *Mostre que se $\alpha, \beta \in \mathbb{K}$ são distintos, então o resto da divisão de $f \in \mathbb{K}[x]$ por $(x-\alpha)\cdot(x-\beta)$é*

$$\left(\frac{f(\alpha)-f(\beta)}{\alpha-\beta}\right)x + \left(\frac{\alpha f(\beta)-\beta f(\alpha)}{\alpha-\beta}\right),$$

onde $f(\alpha)$ e $f(\beta)$ denotam respectivamente os restos da divisão de f por $x-\alpha$ e por $x-\beta$.

É muito comum não dar a devida importância à diferença entre os conceitos de polinômio e função polinomial. Esta última refere-se a uma função da forma

$$\begin{array}{rccl} p: & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & a_n x^n + \ldots + a_1 x + a_0, \end{array}$$

com $a_i \in \mathbb{K}$ para todo $i \in \mathbb{N}$. Apesar de muitas vezes indicarmos tal função por $p(x) = a_n x^n + \ldots + a_1 x + a_0$ quando o corpo $\mathbb{K}$ ficar subentendido, devemos tomar o cuidado para não a confundir com um polinômio. Sejamos mais claros.

Se denotarmos o conjunto de todas as funções polinomiais de $\mathbb{K}$ em $\mathbb{K}$ por $\mathcal{P}(\mathbb{K},\mathbb{K})$, então temos que a correspondência

$$\begin{array}{rccl} \varphi: & \mathbb{K}[x] & \to & \mathcal{P}(\mathbb{K},\mathbb{K}) \\ & a_n x^n + \ldots + a_1 x + a_0 & \mapsto & \begin{array}{rccl} p: & \mathbb{K} & \to & \mathbb{K} \\ & x & \mapsto & a_n x^n + \ldots + a_1 x + a_0, \end{array} \end{array} \tag{1.1}$$

está bem definida e é claramente sobrejetora.

No entanto, não temos necessariamente que φ é uma bijeção, ou seja, não podemos, em geral, identificar um polinômio com uma função polinomial. De fato, considere $\mathbb{K} = \mathbb{Z}_2$ e $x^2 + x \in \mathbb{Z}_2[x]$, claramente $x^2 + x$ não é o polinômio nulo, por outro lado a função

$$\begin{array}{rccl} p: & \mathbb{Z}_2 & \to & \mathbb{Z}_2 \\ & x & \mapsto & x^2 + x \end{array}$$

se anula em todo elemento de $\mathbb{Z}_2$, consequentemente, trata-se da função nula. Assim, $x^2 + x \neq 0$, mas $\varphi(x^2 + x) = \varphi(0)$, ou seja, φ não é injetora.

O fato de que a aplicação φ em (1.1) não ser uma bijeção é um comportamento que depende do corpo $\mathbb{K}$. De fato, temos o seguinte resultado:

Teorema 1.24. *Seja $\mathbb{K}$ um corpo infinito. A função $p : \mathbb{K} \to \mathbb{K}$ definida por $p(x) = a_n x^n + \ldots + a_1 x + a_0$ é nula se, e somente se, o polinômio $a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{K}[x]$ é nulo.*

Dem: Obviamente temos que se $a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{K}[x]$ é nulo, então a função $p : \mathbb{K} \to \mathbb{K}$ dada por $p(x) = a_n x^n + \ldots + a_1 x + a_0$ é nula.

Por outro lado, suponha que $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{K}[x]$ não seja nulo, então pela Proposição 1.22, o número de raízes distintas de f é menor ou igual a $gr(f) \leq n$. Como $\mathbb{K}$ é infinito, existe $k \in \mathbb{K}$ tal que $a_n k^n + \ldots + a_1 k + a_0 \neq 0$, ou seja, $p(k) \neq 0$, consequentemente $p : \mathbb{K} \to \mathbb{K}$ não é a função nula. ■

Nestas notas, sempre que $\mathbb{K}$ for um corpo infinito utilizaremos livremente a correspondência φ, apresentada em (1.1), entre o polinômio $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{K}[x]$ e a função polinomial que denotaremos por $f(x)$. Deste modo, o resto da divisão do polinômio $f = a_n x^n + \ldots + a_1 x + a_0$ por $x - k$ é $f(k) = a_n k^n + \ldots + a_1 k + a_0$, notação que foi utilizada previamente no Exercício 1.23.

Exercício 1.25. *Mostre que para todo $n \in \mathbb{N}$ maior que 1, existe um polinômio mônico $x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}_n[x]$ não nulo tal que a função polinomial*

$$\begin{array}{rccl} p: & \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & x & \mapsto & x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \end{array}$$

é a função nula.

Esperamos que esta breve (re)visão de conceitos e resultados sobre polinômios em uma indeterminada permita que o leitor não encontre maiores dificuldades no estudo dos objetos centrais destas notas que passamos a explorar na próxima seção.

1.3 Anéis de Polinômios em várias indeterminadas

No início da seção anterior abordamos o anel $A[y]$ com A um anel arbitrário e y uma indeterminada. Se considerarmos $A = \mathbb{K}[x]$, então temos o anel $\mathbb{K}[x][y]$ que é um domínio, uma vez que $\mathbb{K}[x]$ o é (veja Exercício 1.9). Os elementos de $\mathbb{K}[x][y]$ podem ser expressos na forma

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

com $f_i = \sum_{j=0}^{m_i} a_{ij} x^j \in \mathbb{K}[x]$, $n, m_i \in \mathbb{N}, a_{ij} \in \mathbb{K}$ para todo índice $i = 0, \ldots, n$.

Com tais notações e variações de índices, temos que

$$\begin{aligned}
\mathbb{K}[x][y] &= \{f_n y^n + f_{n-1} y^{n-1} + \ldots + f_1 y + f_0\} \\
&= \left\{ \left(\textstyle\sum_{j=0}^{m_n} a_{nj} x^j \right) y^n + \ldots + \left(\sum_{j=0}^{m_1} a_{1j} x^j \right) y + \left(\sum_{j=0}^{m_0} a_{0j} x^j \right) \right\} \\
&= \left\{ \left(\textstyle\sum_{l=0}^{n} a_{l m_k} y^l \right) x^{m_k} + \ldots + \left(\sum_{l=0}^{n} a_{l1} y^l \right) x + \left(\sum_{l=0}^{n} a_{l0} y^l \right) \right\} \\
&= \mathbb{K}[y][x]
\end{aligned}$$

com $m_k = max\{m_i;\ 0 \leq i \leq n\}$ e $a_{ij} = 0$ sempre que $j > m_i$.

Deste modo, indicaremos $\mathbb{K}[x][y]$ $(= \mathbb{K}[y][x])$ por $\mathbb{K}[x, y]$.

Analogamente introduzimos o domínio $\mathbb{K}[x_1, \ldots, x_n]$ que chamamos **anel de polinômios nas indeterminadas** $x_1, \ldots, x_n$ **com coeficientes no corpo** $\mathbb{K}$.

Um **termo** de $\mathbb{K}[x_1, \ldots, x_n]$ é um elemento da forma $a_\alpha \prod_{i=1}^n x_i^{\alpha_i}$ com $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $a_\alpha \in \mathbb{K}$ é chamado de **coeficiente** do termo e $\prod_{i=1}^n x_i^{\alpha_i}$ é denominado **monômio**. O **grau** (total) do monômio $\prod_{i=1}^n x_i^{\alpha_i}$ é dado por $gr(\prod_{i=1}^n x_i^{\alpha_i}) = \sum_{i=1}^n \alpha_i \in \mathbb{N}$.

Embora $\mathbb{K}[x_1, \ldots, x_n]$ seja um anel comutativo, seguiremos a convenção de expressar um monômio escrevendo (a partir da esquerda) as potências das variáveis segundo a ordem que aparecem na notação do anel a qual pertence. Assim, embora $x^3yz^2, yz^2x^3, z^2x^3y \in \mathbb{K}[x, y, z]$ sejam iguais, vamos adotar a representação x^3yz^2.

Analisando os elementos de $\mathbb{K}[x_1, \ldots, x_n]$, concluímos que um elemento não nulo $f \in \mathbb{K}[x_1, \ldots, x_n]$ é uma soma finita de termos, ou seja,

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

com $a_\alpha \in \mathbb{K}$ e $J \subset \mathbb{N}^n$ finito.

Dado $(k_1, \ldots, k_n) \in \mathbb{K}^n$ e $f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^n x_i^{\alpha_i} \in \mathbb{K}[x_1, \ldots, x_n]$ denotaremos $\sum_{\alpha \in J} a_\alpha \prod_{i=1}^n k_i^{\alpha_i} \in \mathbb{K}$ por $f(k_1, \ldots, k_n)$.

Seguindo as mesmas notações utilizadas para polinômios em uma indeterminada, dado $f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^n x_i^{\alpha_i} \in \mathbb{K}[x_1, \ldots, x_n]$, denotamos por

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

o conjunto de todos os monômios de f e chamamos

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

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

Algumas (poucas) vezes, sentiremos necessidade de considerar um polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ como um polinômio na indeterminada x_i com coeficientes no anel $\mathbb{K}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$. Neste caso, o **grau de f em x_i** é dado por

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

Do mesmo modo que no caso de polinômios em uma indeterminada, o leitor não encontrará dificuldades em constatar que

$$\boxed{gr(f+g) \leq max\{gr(f), gr(g)\}} \qquad \boxed{gr(fg) = gr(f) + gr(g)}$$

e $gr_{x_i}(f) \leq gr(f)$ para todos $f, g \in \mathbb{K}[x_1, \ldots, x_n]$.

Exercício 1.26. *Calcule $gr(f+g), gr(fg), gr_x(f+g), gr_y(f+g), gr_x(fg)$ e $gr_y(fg)$ nos casos abaixo.*

1. $f = 3x^3 + y^3$ *e* $g = -y^3 + x^3y$ *em* $\mathbb{R}[x, y]$.
2. $f = g = x$ *em* $\mathbb{R}[x, y]$.

Embora a adição e multiplicação de polinômios em $\mathbb{K}[x]$ sejam naturalmente estendidas para $\mathbb{K}[x_1, \ldots, x_n]$, o mesmo não se pode dizer da divisão.

Revisitando o algoritmo da divisão para polinômios em uma indeterminada, notamos que a primeira dificuldade consiste em definirmos o conceito de termo líder de polinômios em $\mathbb{K}[x_1, \ldots, x_n]$. Num primeiro momento poderíamos ser tentados a utilizar o conceito de grau (total) de modo similar ao que fizemos em $\mathbb{K}[x]$. No entanto, um pequeno instante de meditação nos leva a procurar um outro caminho, pois facilmente podemos exibir polinômios em mais de uma indeterminada que possuem vários monômios distintos com o mesmo grau (total). Por exemplo, o polinômio

$$x^2yz^2 + x^2y^2z + 3x^4y + 3x^3z^2 - y^4z + 2x^4z + 5x^2y^2z^2$$

tem vários termos de mesmo grau.

Temos assim que traçar uma outra estratégia para ordenar os termos de um polinômio em $\mathbb{K}[x_1, \ldots, x_n]$ que será abordada na subseção seguinte.

1.3.1 Ordens Monomiais

Uma vez que temos em mente a busca de uma generalização do algoritmo da divisão para polinômios em $\mathbb{K}[x_1, \ldots, x_n]$, façamos uma análise mais refinada sobre cada passo para que tentemos superar os obstáculos encontrados.

Como já comentamos, um primeiro conceito que necessitamos é o de termo líder de um elemento $f \in \mathbb{K}[x_1, \ldots, x_n]$. Este conceito por sua vez se baseia em como ordenamos os termos (ou monômios) de f. Como a resposta que procuramos deve se ajustar a qualquer elemento de $\mathbb{K}[x_1, \ldots, x_n]$, tal ordenação necessita se aplicar a qualquer monômio deste anel.

Definição 1.27. *O conjunto de todos os monômios de* $\mathbb{K}[x_1, \ldots, x_n]$ *será denotado por* $\mathbb{M}_n$*, ou seja,*

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

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

Não podemos resgatar todos os conceitos que utilizaremos neste livro, pois corremos o risco de criar um efeito cascata, de modo que a cada conceito relembrado, outros surgirão e, ao invés de avançarmos na direção de nosso objetivo, estaremos caminhando em direção oposta. No entanto, podemos nos dar o luxo de recordar alguns deles, como o próximo conceito.

Uma **relação de ordem**, ou uma ordenação, sobre um conjunto C (não vazio) é uma relação $\preceq$ satisfazendo:

1. $c \preceq c$ para todo $c \in C$ (propriedade reflexiva).
2. Se $c_1, c_2 \in C$ são tais que $c_1 \preceq c_2$ e $c_2 \preceq c_1$, então $c_1 = c_2$ (propriedade anti-simétrica).
3. Sejam $c_1, c_2, c_3 \in C$. Se $c_1 \preceq c_2$ e $c_2 \preceq c_3$, então $c_1 \preceq c_3$ (propriedade transitiva).

Se $c_1 \preceq c_2$, mas $c_1 \neq c_2$, então indicaremos $c_1 \prec c_2$.

Temos, por exemplo, que a relação dada por $\alpha \leq \beta$ (α é menor ou igual a β) sobre $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, bem como a relação $\alpha \mid \beta$ (α divide β) sobre $\mathbb{N}$ são relações de ordem. No entanto, a relação $\alpha \mid \beta$ sobre $\mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$ não é de ordem. De fato, $1 \mid -1$ e $-1 \mid 1$, mas $-1 \neq 1$, ou seja, a relação não é anti-simétrica.

Mais do que uma simples relação de ordem sobre $\mathbb{M}_n$, gostaríamos de poder relacionar quaisquer dois de seus elementos, isto é, desejamos que a relação de ordem seja *total*. Uma relação de ordem $\preceq$ sobre um conjunto C é **total** se para quaisquer $c_1, c_2 \in C$ temos que

$$c_1 \prec c_2, \quad c_2 \prec c_1 \quad \text{ou} \quad c_1 = c_2.$$

Note que a relação de ordem $\alpha \leq \beta$ é total sobre $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, enquanto a relação de ordem $\alpha \mid \beta$ não é total sobre $\mathbb{N}$ ou $\mathbb{Z}$.

Uma relação de ordem total $\preceq$ sobre $\mathbb{M}_n$ já seria suficiente para definirmos termo líder de um elemento $f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} \neq 0$. De fato, bastaria definirmos $ml(f) = max\{\prod_{i=1}^{n} x_i^{\alpha_i} \in \mathbb{M}(f)\}$, onde o máximo é tomado com respeito a ordem $\preceq$ fixada e considerar o termo líder de f como $a_\alpha \cdot ml(f)$.

No entanto, há outros pontos que merecem nossa atenção no algoritmo da divisão de um polinômio f por g em $\mathbb{K}[x]$. Digamos que $tl(f) = a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i}$ e $tl(g) = a_\beta \prod_{i=1}^{n} x_i^{\beta_i}$, devemos verificar se

$tl(g) \mid tl(f)$, isto é, se existe $m_1 = \prod_{i=1}^{n} x_i^{\gamma_i} \in \mathbb{M}_n$ e $a_\gamma \in \mathbb{K}$ tais que $tl(f) = a_\gamma \cdot m_1 \cdot tl(g)$, ou equivalentemente,

$$a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} = \left(a_\gamma \prod_{i=1}^{n} x_i^{\gamma_i} \right) \left(a_\beta \prod_{i=1}^{n} x_i^{\beta_i} \right) = a_\gamma a_\beta \prod_{i=1}^{n} x_i^{\gamma_i + \beta_i},$$

que ocorre se, e somente se, $\beta_i \leq \alpha_i$ para todo $i = 1, \ldots, n$, uma condição fácil de ser verificada. Em caso afirmativo, devemos calcular $f - \gamma \cdot m_1 \cdot g$ e repetir o argumento para o resultado obtido.

Lembremos que, no caso de polinômios em uma indeterminada, encontramos $gr(f - \gamma \cdot m_1 \cdot g) < gr(f)$, que pode ser reescrito, utilizando a noção de monômio líder, como $ml(f - \gamma \cdot m_1 \cdot g) \prec ml(f)$. Uma propriedade aparentemente simples, mas importante se esconde nestas condições, ou seja, nas expressões $tl(f) = \gamma \cdot m_1 \cdot tl(g)$ e $ml(f - \gamma \cdot m_1 \cdot g) \prec ml(f)$. De fato, a última condição, nos revela que se $m_2 \in \mathbb{M}(g)$ e $m_2 \prec ml(g)$, então temos $m_1 \cdot m_2 \prec m_1 \cdot ml(g) = ml(f)$, ou seja, uma ordem total sobre $\mathbb{M}_n$ deve ser *compatível com o produto*, dito de outro modo, se $m_1, m_2 \in \mathbb{M}_n$ são tais que $m_1 \preceq m_2$, então $m_1 \cdot m_3 \preceq m_2 \cdot m_3$ para todo $m_3 \in \mathbb{M}_n$.

Um último, mas não menos importante, aspecto do algoritmo da divisão reside na garantia de finalizarmos tal procedimento em um número finito de etapas, fato que também se assenta sobre a condição $ml(f - \gamma \cdot m_1 \cdot g) \prec ml(g)$ em cada etapa do algoritmo.

Tal condição pode ser traduzida, requisitando que a ordem total $\preceq$ sobre $\mathbb{M}_n$ seja uma *boa ordem*, isto é, que todo subconjunto não vazio de $\mathbb{M}_n$ admita um menor elemento com respeito à $\preceq$. Um exemplo de uma boa ordem em um contexto conhecido é a relação $\leq$ sobre $\mathbb{N}$.

No que segue, consideramos sobre $\mathbb{M}_n$ ordens que possuem as propriedades destacadas acima, para as quais reservamos uma designação própria dada na definição abaixo.

Definição 1.28. *Uma* **ordem monomial** $\preceq$ *sobre* $\mathbb{M}_n$ *é uma relação de ordem total que satisfaz:*

1. *se* $m_1, m_2 \in \mathbb{M}_n$ *são tais que* $m_1 \preceq m_2$*, então* $m_1 m_3 \preceq m_2 m_3$ *para todo* $m_3 \in \mathbb{M}_n$*.*

2. *Todo subconjunto não vazio de* $\mathbb{M}_n$ *admite um menor elemento com respeito à* $\preceq$*.*

O lema a seguir é na realidade uma reformulação da segunda condição na definição acima.

Lema 1.29. *Seja $\preceq$ uma ordem monomial em $\mathbb{K}[x_1, \ldots, x_n]$, então qualquer sequência decrescente (com respeito à $\preceq$) de monômios é finita.*

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

Exercício 1.30. *Seja $\mathbb{M}_1$, isto é, o conjunto de todos os monômios de $\mathbb{K}[x]$. Mostre que a ordem $\preceq$ dada por*

$$m_1 \preceq m_2 \text{ se, e somente se, } gr(m_1) \leq gr(m_2)$$

é a única ordem monomial sobre $\mathbb{M}_1$.

Vamos usar um pouco de nossa intuição e o fato de sabermos ordenar monômios em uma variável, como dado no exercício acima, para exibirmos uma ordem monomial em $\mathbb{K}[x_1, \ldots, x_n]$.

Dado um polinômio não nulo $f \in \mathbb{K}[x_1, \ldots, x_n]$ podemos, como vimos, considerá-lo como um polinômio em x_1 com coeficientes em $\mathbb{K}[x_2, \ldots, x_n]$. Agora por um argumento indutivo, ou seja, usando indução sobre o número de indeterminadas, podemos supor que saibamos ordenar os monômios em $\mathbb{K}[x_2, \ldots, x_n]$ de modo similar.

Apliquemos tal ideia ao polinômio $f = x^2yz^2 + x^2y^2z + 3x^4y + 3x^3z^2 - y^4z + 2x^4z + 5x^2y^2z^2$. Considerando $f \in \mathbb{K}[y, z][x]$ e ordenando pelo grau em x temos

$$f = (2z + 3y)x^4 + 3z^2x^3 + (yz^2 + y^2z + 5y^2z^2)x^2 - y^4z.$$

Agora considerando os coeficientes, que são elementos de $\mathbb{K}[y, z]$, como polinômios em y com coeficientes em $\mathbb{K}[z]$ e ordenando pelo grau em y e seus coeficientes pelo grau em z temos

$$f = (3y + 2z)x^4 + 3z^2x^3 + ((5z^2 + z)y^2 + z^2y)x^2 - zy^4,$$

ou ainda, efetuando as multiplicações indicadas e usando a convenção de representar um monômio listando suas potências em x, seguidas pelas potências em y e pelas potências em z, temos

$$f = 3x^4y + 2x^4z + 3x^3z^2 + 5x^2y^2z^2 + x^2y^2z + x^2yz^2 - y^4z.$$

Note que ao seguir tal estratégia, o que fizemos foi listar os termos do polinômio de modo que um monômio $x^{\alpha_1}y^{\beta_1}z^{\gamma_1}$ precede $x^{\alpha_2}y^{\beta_2}z^{\gamma_2}$ se, e somente se,

1. $\alpha_1 > \alpha_2$ ou
2. $\alpha_1 = \alpha_2$ e $\beta_1 > \beta_2$ ou
3. $\alpha_1 = \alpha_2,\ \beta_1 = \beta_2$ e $\gamma_1 > \gamma_2$.

Tal modo de ordenar os monômios é uma ordem monomial? Antes de responder tal pergunta, vamos formalizar o que fizemos para monômios $\mathbb{M}_n$.

Dados $\prod_{i=1}^n x_i^{\alpha_i}, \prod_{i=1}^n x_i^{\beta_i} \in \mathbb{M}_n$ distintos, diremos que

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

se, e somente se, existe $i \in \{1, \ldots, n\}$ tal que $\alpha_i < \beta_i$ e $\alpha_j = \beta_j$ para todo $j < i$, ou equivalentemente, a primeira coordenada não nula, a partir da esquerda, da n-upla $(\beta_1 - \alpha_1, \ldots, \beta_n - \alpha_n)$ é positiva.

Claramente $\preceq_L$ é uma relação reflexiva sobre $\mathbb{M}_n$.

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

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

temos que $\prod_{i=1}^n x_i^{\alpha_i} = \prod_{i=1}^n x_i^{\beta_i}$. De fato, se $\prod_{i=1}^n x_i^{\alpha_i} \neq \prod_{i=1}^n x_i^{\beta_i}$, então existe $k \in \{1, \ldots, n\}$ tal que $\alpha_k \neq \beta_k$ e seja i o menor tal índice. Caso $\alpha_i < \beta_i$, então não podemos ter $\prod_{i=1}^n x_i^{\beta_i} \preceq_L \prod_{i=1}^n x_i^{\alpha_i}$. Se $\beta_i < \alpha_i$, então não podemos ter $\prod_{i=1}^n x_i^{\alpha_i} \preceq_L \prod_{i=1}^n x_i^{\beta_i}$. Seguindo que $\prod_{i=1}^n x_i^{\alpha_i} = \prod_{i=1}^n x_i^{\beta_i}$ e que $\preceq_L$ é anti-simétrica.

Agora suponha que

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

Se ocorre igualdade em algum dos casos, então é fácil constatar que $\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\gamma_i}$.

Vamos admitir que nenhuma das igualdades ocorre. Deste modo, existem $i, k \in \{1, \ldots, n\}$ tais que

$$\alpha_i < \beta_i \text{ e } \alpha_j = \beta_j \text{ para todo } j < i \text{ e}$$

$$\beta_k < \gamma_k \text{ e } \beta_l = \gamma_l \text{ para todo } l < k.$$

Se $i = k$, então $\alpha_i < \gamma_i$ e $\alpha_j = \gamma_j$ para todo $j < i$.

Se $i < k$, então $\alpha_i < \beta_i = \gamma_i$ e $\alpha_j = \beta_j = \gamma_j$ para todo $j < i$.

Se $k < i$, então $\alpha_k = \beta_k < \gamma_k$ e $\alpha_l = \beta_l = \gamma_l$ para todo $l < k$.

Deste modo, qualquer uma das possibilidades permite concluir que $\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\gamma_i}$, ou seja, $\preceq_L$ é transitiva.

Temos assim, que $\preceq_L$ é uma relação de ordem sobre $\mathbb{M}_n$ e argumentos similares aos utilizados para garantir que tal relação é anti-simétrica, nos levam a concluir que a relação é uma ordem total.

Mostremos agora que $\preceq_L$ é compatível com o produto. Considere $\prod_{i=1}^{n} x_i^{\alpha_i}, \prod_{i=1}^{n} x_i^{\beta_i}, \prod_{i=1}^{n} x_i^{\gamma_i} \in \mathbb{M}_n$, com $\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\beta_i}$.

Se $\prod_{i=1}^{n} x_i^{\alpha_i} = \prod_{i=1}^{n} x_i^{\beta_i}$, então é óbvio que

$$(\prod_{i=1}^{n} x_i^{\gamma_i}) \cdot (\prod_{i=1}^{n} x_i^{\alpha_i}) \preceq_L (\prod_{i=1}^{n} x_i^{\gamma_i}) \cdot (\prod_{i=1}^{n} x_i^{\beta_i}).$$

Por outro lado, se $\prod_{i=1}^{n} x_i^{\alpha_i} \prec_L \prod_{i=1}^{n} x_i^{\beta_i}$, então existe um índice $k \in \{1, \ldots, n\}$ tal que $\alpha_k < \beta_k$ e $\alpha_j = \beta_j$ para todo $j < k$. Mas deste modo $\gamma_k + \alpha_k < \gamma_k + \beta_k$ e $\gamma_j + \alpha_j = \gamma_j + \beta_j$ para todo $j < k$, ou seja,

$$\left(\prod_{i=1}^{n} x_i^{\gamma_i}\right) \cdot \left(\prod_{i=1}^{n} x_i^{\alpha_i}\right) = \prod_{i=1}^{n} x_i^{\gamma_i+\alpha_i} \prec_L \prod_{i=1}^{n} x_i^{\gamma_i+\beta_i} = \left(\prod_{i=1}^{n} x_i^{\gamma_i}\right) \cdot \left(\prod_{i=1}^{n} x_i^{\beta_i}\right).$$

Para verificar que $\preceq_L$ é uma boa ordem, considere um subconjunto não vazio $S \subseteq \mathbb{M}_n$ e $S(1)$ o conjunto de todos os monômios $m \in S$ com a propriedade de que $gr_{x_1}(m) \leq gr_{x_1}(s)$ para todo $s \in S$. O conjunto

$S(1)$ é não vazio, uma vez que $\mathbb{N}$ é bem ordenado com respeito a ordem $\leq$ e o conjunto $\{gr_{x_1}(s);\ s \in S\} \subseteq \mathbb{N}$ não é vazio. Note que dado $m \in S(1)$, temos que $m \preceq_L s$ para todo $s \in S \setminus S(1)$.

Consideramos $S(2) = \{m \in S(1); gr_{x_2}(m) \leq gr_{x_2}(s),\ \forall\ s \in S(1)\}$ que também é não vazio, pois $\emptyset \neq \{gr_{x_2}(s);\ s \in S(1)\} \subseteq \mathbb{N}$. Temos que $gr_{x_1}(m_1) = gr_{x_1}(m_2)$ para todo $m_1, m_2 \in S(2)$ e dado $m \in S(2)$ tem-se que $m \preceq_L s$ para todo $s \in S \setminus S(2)$. Procedendo desta forma, temos que

$$S(n) = \{m \in S(n-1);\ gr_{x_n}(m) \leq gr_{x_n}(s) \text{ para todo } s \in S(n-1)\}$$

é não vazio e $gr_{x_i}(m_1) = gr_{x_i}(m_2)$ para todo $m_1, m_2 \in S(n)$ e qualquer $i = 1, \ldots, n-1$. Como $\emptyset \neq \{gr_{x_n}(s);\ s \in S(n)\} \subseteq \mathbb{N}$ e $\mathbb{N}$ é bem ordenado, segue que $\{gr_{x_n}(s);\ s \in S(n)\}$ admite um elemento mínimo α. Tomando $m \in S(n)$ tal que $gr_{x_n}(m) = \alpha$, temos que $m \preceq_L s$ para todo $s \in S$, ou seja, S admite um menor elemento.

Temos assim que $\preceq_L$ é uma ordem monomial sobre $\mathbb{M}_n$ que chamaremos **ordem lexicográfica**. Por comodidade e futuras referências, a apresentamos na definição abaixo.

Definição 1.31. (Ordem Lexicográfica $\preceq_L$) *Dados dois monômios $\prod_{i=1}^n x_i^{\alpha_i}, \prod_{i=1}^n x_i^{\beta_i} \in \mathbb{M}_n$, dizemos que*

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

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

A expressão *ordem lexicográfica* é usada para designar o modo que as palavras aparecem no dicionário. De um certo modo é justamente como estamos ordenando os monômios. Se, por exemplo, escrevermos os monômios x^2y^3z e $x^2y^2z^3$ como $xxyyyz$ e $xxyyzzz$, então $xxyyyz$ apareceria antes da "palavra" $xxyyzzz$ no dicionário. O que coincide com o modo de ordenarmos os monômios com respeito à ordem lexicográfica, ou seja, $x^2y^2z^3 \preceq_L x^2y^3z$.

Enquanto em $\mathbb{M}_1$ essencialmente temos apenas uma ordem monomial, em $\mathbb{M}_n$ tal fato está longe de ocorrer. Abaixo apresentamos outras ordens monomiais sobre $\mathbb{M}_n$ para as quais o leitor é convidado a justificar.

Definição 1.32. (Ordem Lexicográfica Graduada $\preceq_{LG}$) *Dados* $\prod_{i=1}^{n} x_i^{\alpha_i}, \prod_{i=1}^{n} x_i^{\beta_i} \in \mathbb{M}_n$*, dizemos que*

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

se:

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

Definição 1.33. (Ordem Lexicográfica Graduada Reversa $\preceq_{LGR}$) *Dados* $\prod_{i=1}^{n} x_i^{\alpha_i}, \prod_{i=1}^{n} x_i^{\beta_i} \in \mathbb{M}_n$*, dizemos que*

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

se:

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

Definição 1.34. (Ordem Ponderada $\preceq^{\rho}$) *Sejam* $\preceq$ *uma ordem monomial sobre* $\mathbb{M}_n$ *e* $\rho = (\rho_1, \ldots, \rho_n) \in \mathbb{N}^n$*. Dados dois monômios* $\prod_{i=1}^{n} x_i^{\alpha_i}, \prod_{i=1}^{n} x_i^{\beta_i} \in \mathbb{M}_n$*, dizemos que*

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

se:

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

Chamamos $\rho \in \mathbb{N}^n$ *de* **peso** *e o inteiro* $gr^{\rho}(\prod_{i=1}^{n} x_i^{\alpha_i}) = \sum_{i=1}^{n} \rho_i\alpha_i$ *de* **grau ponderado** *do monômio* $\prod_{i=1}^{n} x_i^{\alpha_i}$ *com respeito à* ρ.

Observe que se $\rho = (0, \ldots, 0)$*, então* $\preceq^{\rho}$ *coincide com* $\preceq$ *e tomando* $\rho = (1, \ldots, 1)$*, então* $\preceq_L^{\rho}$ *é a ordem lexicográfica graduada.*

Vejamos como as ordens monomiais acima atuam de modo distinto sobre um mesmo conjunto de monômios.

Exemplo 1.35. *Considerando as ordens monomiais definidas acima e os monômios* $xy^3z^3, xy^2z^4, x^2y^4z^2, x^4y, x^3y^2z^3 \in \mathbb{K}[x,y,z]$*, temos que:*

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

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

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

$$x^4y \preceq_L^{(1,2,3)} xy^3z^3 \preceq_L^{(1,2,3)} x^2y^4z^2 \preceq_L^{(1,2,3)} x^3y^2z^3 \preceq_L^{(1,2,3)} xy^2z^4.$$

Exercício 1.36. *Ordene os monômios de* $f = 2x^3y^2z - xy^2z^3 + 3x^3y^3z^2 + 5x^2y^3z^2 \in \mathbb{Q}[x,y,z]$ *com respeito às ordens monomiais* $\preceq_L, \preceq_{LG}, \preceq_{LGR}$ *e* $\preceq_L^{(2,1,6)}$ *.*

Exercício 1.37. *Mostre que se* $\preceq$ *é uma ordem monomial sobre* $\mathbb{M}_n$*, então* $1 \preceq m$ *para todo* $m \in \mathbb{M}_n$*.*

Exercício 1.38. *Considere a seguinte relação de ordem sobre* $\mathbb{M}_n$*:*
Dados $\prod_{i=1}^n x_i^{\alpha_i}, \prod_{i=1}^n x_i^{\beta_i} \in \mathbb{M}_n$*, dizemos que*

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

se existe $k \in \{1,\ldots,n\}$ *tal que* $\alpha_k > \beta_k$ *e* $\alpha_j = \beta_j$ *para todo* $j > k$*.*
Mostre que $\preceq_{LR}$ não *é uma ordem monomial sobre* $\mathbb{M}_n$*.*

Exercício 1.39. *Mostre que nenhuma ordem total sobre* $\mathbb{C}$ *compatível com a soma, ou seja,*

$$\text{se } z_1 \preceq z_2\text{, então } z_1 + z_3 \preceq z_2 + z_3 \text{ para todos } z_1, z_2, z_3 \in \mathbb{C}$$

satisfaz a propriedade

$$\text{se } z_1 \preceq z_2 \text{ e } 0 \prec z_3\text{, então } z_1 \cdot z_3 \preceq z_2 \cdot z_3.$$

(Sugestão: mostre que se existe uma ordem total $\preceq$ *com as propriedades acima, então* $z^2 \succeq 0$ *para todo* $z \in \mathbb{C}$*).*

1.3.2 Algoritmo da divisão em $\mathbb{K}[x_1, \ldots, x_n]$

Após as esplanações da seção anterior, temos todos os ingredientes para apresentar o algoritmo da divisão em $\mathbb{K}[x_1, \ldots, x_n]$.

O primeiro passo é dado na definição abaixo.

Definição 1.40. *Fixemos uma ordem monomial $\preceq$ sobre $\mathbb{M}_n$. Dado $f \in \mathbb{K}[x_1, \ldots, x_n] \setminus \{0\}$ chamamos $ml(f) = max_{\preceq}\mathbb{M}(f)$ de* **monômio líder de** *f.*

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

Exercício 1.41. *Calcule o termo líder de $f = 2x^3y^2z - xy^2z^3 + 3x^3y^3z^2 + 5x^2y^3z^2 \in \mathbb{Q}[x, y, z]$ com respeito às ordens monomiais $\preceq_L, \preceq_{LG}, \preceq_{LGR}$ e $\preceq_L^{(2,1,6)}$.*

Exercício 1.42. *Fixada uma ordem monomial $\preceq$ em $\mathbb{K}[x_1, \ldots, x_n]$ mostre que se $ml(g) \mid ml(f)$, então $ml(g) \preceq ml(f)$.*

Antes de apresentar o resultado que nos propomos, façamos uma rápida inspeção nos passos do algoritmo da divisão em $\mathbb{K}[x]$ tentando ajustar ao anel $\mathbb{K}[x_1, \ldots, x_n]$.

Dados $f, g \in \mathbb{K}[x]$ com $g \neq 0$, iniciamos o algoritmo da divisão ordenando os monômios de f e g segundo a ordem monomial $\preceq$ de $\mathbb{K}[x]$ dada pelo grau dos monômios. Em seguida, verificamos se $gr(f) \geq gr(g)$, isto é equivalente a dizer que $ml(g) \preceq ml(f)$, ou ainda, que $ml(g) \mid ml(f)$. Em caso negativo, finalizamos o algoritmo com $r = f$ e $q = 0$. Caso contrário, $\frac{tl(f)}{tl(g)}$ será um termo do quociente e o processo se repete com $f - \frac{tl(f)}{tl(g)}g$ tomando o lugar de f.

Note que, no caso de uma indeterminada, se $ml(g) \preceq ml(f)$ for falsa, ou seja, se $ml(f) \prec ml(g)$, então além de $ml(g)$ não dividir $ml(f)$, temos que $ml(g)$ não divide todos os monômios de f. Mas, no caso de várias indeterminadas isto pode não ocorrer, ou seja, mesmo que $ml(g) \nmid ml(f)$, pode ocorrer que outros monômios de f sejam divisíveis por $ml(g)$.

Por exemplo, se considerarmos a ordem lexicográfica graduada e $f = y^3 + x^2, g = x \in \mathbb{K}[x, y]$ temos que $ml(g) = x \nmid y^3 = ml(f)$ mas $ml(g) = x \mid x^2$. O que podemos dizer do quociente q e do resto r na divisão de f por g neste caso?

Imitando o critério de finalização do algoritmo da divisão para o caso de uma indeterminada, ou seja, repetir os passos até que encontremos $ml(g) \nmid ml(f)$, teríamos que $q = 0$ e $r = f = y^3 + x^2$. Mas seria este o resultado que nossa intuição matemática esperava?

A ideia básica da divisão de números naturais, apresentada à estudantes do ensino básico, consiste em extrair de um número (o dividendo) o maior múltiplo do divisor. Neste caso, as experiências remanescentes desta época de nossa instrução, nos levam a intuir que no exemplo acima, o mais aceitável seria considerar $f = y^3 + x^2 = x.g + y^3$, ou seja, $q = x$ e $r = y^3$.

Deste modo, simplesmente substituir a condição $gr(r) < gr(g)$ pela condição $ml(g) \nmid ml(r)$ não é a opção mais indicada, pois o que esperamos é que $ml(g) \nmid m$ para todo $m \in \mathbb{M}(r)$.

Teorema 1.43. (Algoritmo da Divisão em $\mathbb{K}[x_1, \ldots, x_n]$) *Fixada uma ordem monomial $\preceq$ e dado $g \in \mathbb{K}[x_1, \ldots, x_n] \setminus \{0\}$, para qualquer polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ existem $q, r \in \mathbb{K}[x_1, \ldots, x_n]$ unicamente determinados pelas condições*

$$f = qg + r, \text{ com } r = 0 \text{ ou } ml(g) \nmid m \text{ para todo } m \in \mathbb{M}(r).$$

Dem: (*Existência:*) Se $f = 0$, então $f = 0 = 0.g + 0 = q.g + r$, ou seja, $q = r = 0$ satisfazem as condições do teorema.

Sejam $f_0 = f \neq 0$ e o conjunto $S(f_0) = \{m \in \mathbb{M}(f);\ ml(g) \mid m\}$, se $S(f_0) = \emptyset$, então definimos $q = 0, r = f$ e temos o resultado.

Se $S(f_0) \neq \emptyset$, então tomamos $m_0 = max_{\preceq} S(f_0), a_0 \in \mathbb{K}$ o coeficiente de m_0 que ocorre em f e definimos $f_1 = f - \frac{a_0 m_0}{tl(g)} g$.

Agora consideramos o conjunto $S(f_1) = \{m \in \mathbb{M}(f_1);\ ml(g) \mid m\}$, se $S(f_1) = \emptyset$, então definimos $q = \frac{a_0 m_0}{tl(g)}, r = f_1$ e temos o resultado.

Se $S(f_1) \neq \emptyset$, então tomamos $m_1 = max_{\preceq} S(f_1), a_1 \in \mathbb{K}$ o coeficiente de m_1 que ocorre em f_1 e definimos $f_2 = f_1 - \frac{a_1 m_1}{tl(g)} g$. Note que $m_0 \succeq m_1$, uma vez que $\mathbb{M}(f_1) \subseteq \mathbb{M}(f) \cup \mathbb{M}(\frac{m_0}{tl(g)} g)$.

Repetindo o processo, definimos $S(f_i) = \{m \in \mathbb{M}(f_i);\ ml(g) \mid m\}$, $m_i = max_{\preceq} S(f_i)$ e $a_i \in \mathbb{K}$ o coeficiente de m_i que ocorre em f_i e obtemos uma sequência $m_0 \succeq m_1 \succeq m_2 \succeq \ldots$. Mas, pelo Lema 1.29, tal sequência deve ser finita, ou equivalentemente, existe $k \in \mathbb{N}$ tal que $S(f_k) = \{m \in \mathbb{M}(f_k);\ ml(g) \mid m\} = \emptyset$.

Pelo modo como definimos f_k, existe $q \in \mathbb{K}[x_1, \ldots, x_n]$ tal que $f_k = f - q \cdot g$ e se denotarmos $r = f_k$, teremos o resultado.

(*Unicidade:*) Suponha que existam $q_1, q_2, r_1, r_2 \in \mathbb{K}[x_1, \ldots, x_n]$ tais que

$$q_1 g + r_1 = f = q_2 g + r_2$$

com $r_i = 0$ ou $ml(g) \nmid m$ para todo $m \in \mathbb{M}(r_i)$ para $i \in \{1, 2\}$, isto é, $ml(g) \nmid m$ para todo $m \in \mathbb{M}(r_1) \cup \mathbb{M}(r_2) \supseteq \mathbb{M}(r_2 - r_1)$.

Segue que $0 = f - f = (q_1 - q_2)g + (r_1 - r_2)$, ou seja,

$$r_2 - r_1 = (q_1 - q_2)g.$$

Se $r_2 \neq r_1$, então

$$ml(g) \mid ml(r_2 - r_1) \in \mathbb{M}(r_2 - r_1).$$

Um absurdo!

Assim, $r_2 = r_1$ e $0 = (q_1 - q_2)g$. Sendo $\mathbb{K}[x_1, \ldots, x_n]$ um domínio e $g \neq 0$, segue que $q_1 - q_2 = 0$, ou seja, $q_1 = q_2$, provando o teorema. ■

Como no caso de uma indeterminada, chamaremos os polinômios q e r, tais que $f = q.g + r$ cuja existência e unicidade foi garantida pelo teorema anterior, respectivamente de **quociente** e **resto** da divisão de f por g.

Além disto, uma análise minuciosa da demonstração do teorema acima, indica que podemos encontrar o resto e o quociente da divisão de f por $g \neq 0$ em $\mathbb{K}[x_1, \ldots, x_n]$ seguindo as seguintes instruções:

ENTRADA: $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ COM $g \neq 0$;
DEFINA $q := 0, r := 0$ E $h = f$;
ENQUANTO $h \neq 0$ FAÇA
  SE $ml(g) \mid ml(h)$,
    ENTÃO
      $q := q + \frac{tl(h)}{tl(g)}$;
      $h := h - \frac{tl(h)}{tl(g)} g$;
    SENÃO
      $r := r + tl(h)$;
      $h := h - tl(h)$;
SAÍDA: q E r SATISFAZENDO $f = qg + r$ COM
  $r = 0$ OU $ml(g) \nmid m$ PARA TODO $m \in \mathbb{M}(r)$.

ALGORITMO DA DIVISÃO PARA POLINÔMIOS EM $\mathbb{K}[x_1, \ldots, x_n]$.

Exemplo 1.44. *Vamos utilizar o procedimento acima para encontrar o quociente e o resto da divisão de* $f = xy^4 + x^4 + x^3y + y^3$ *por* $g = y^3 + x^2$ *em* $\mathbb{Q}[x, y]$ *com respeito à ordem lexicográfica graduada.*

O procedimento inicia com $q = r = 0$ *e* $h = xy^4 + x^4 + x^3y + y^3$.

Passo 1*: Temos que* $h \neq 0$ *e* $ml(g) = y^3 \mid xy^4 = ml(h)$*, então fazemos*

$$q = q + \frac{tl(h)}{tl(g)} = 0 + \frac{xy^4}{y^3} = xy$$

e

$$h = h - \frac{tl(h)}{tl(g)} g = xy^4 + x^4 + x^3y + y^3 - \frac{xy^4}{y^3}(y^3 + x^2) = x^4 + y^3.$$

Passo 2*: Como* $h = x^4 + y^3 \neq 0$ *e* $ml(g) = y^3 \nmid x^4 = ml(h)$ *fazemos*

$$r = r + tl(h) = 0 + x^4 = x^4 \text{ e } h = h - tl(h) = x^4 + y^3 - x^4 = y^3.$$

Passo 3*: Uma vez que* $h = y^3 \neq 0$ *e* $ml(g) = y^3 \mid y^3 = ml(h)$*, obtemos*

$$q = q + \frac{tl(h)}{tl(g)} = xy + 1 \text{ e } h = h - \frac{tl(h)}{tl(g)} g = y^3 - 1.(y^3 + x^2) = -x^2.$$

Passo 4*: Temos que* $h = -x^2 \neq 0$ *e* $ml(g) = y^3 \nmid x^2 = ml(h)$*. Assim, fazemos*

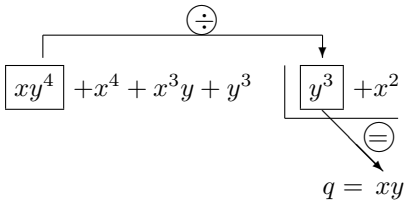
$$r = r + tl(h) = x^4 - x^2 \text{ e } h = h - tl(h) = -x^2 - (-x^2) = 0.$$

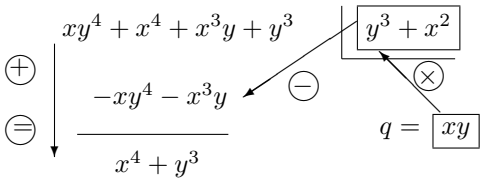
Passo 5*: Agora como* $h = 0$*, o algoritmo finaliza fornecendo como quociente e resto* $q = xy + 1$ *e* $r = x^4 - x^2$*, respectivamente.*

O mesmo dispositivo utilizado para obter rapidamente o quociente e o resto na divisão de polinômios em uma indeterminada pode ser usado para polinômios em $\mathbb{K}[x_1, \ldots, x_n]$, bastando lembrar de ordenar os monômios com respeito à ordem monomial fixada e deslocar um monômio sempre que este contribuir para o resto.

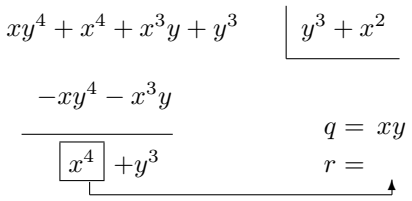
Para que fique mais claro o que dizemos, vamos ilustrar o uso do dispositivo utilizado, para os polinômios dados no exemplo acima.

No Passo 1, temos que $ml(g) = y^3 \mid xy^4 = ml(f)$ e $q = xy$. Multiplicando xy por g e subtraindo de f, obtemos:



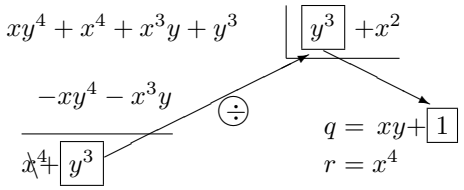


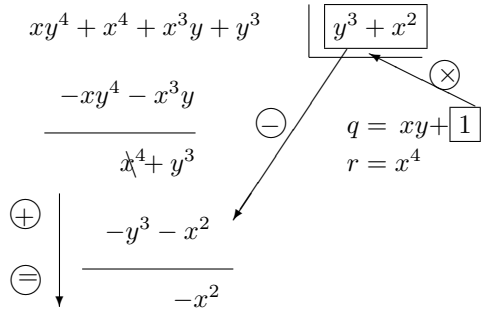
Prosseguindo com o algoritmo com $x^4 + y^3$ no papel de f, temos que $ml(g) = y^3 \nmid x^4$ e assim x^4 contribui para o resto r, que alocaremos, por comodidade, abaixo do quociente q.



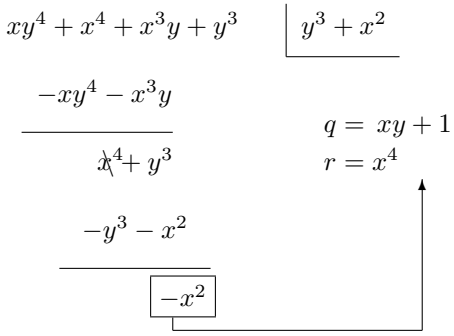
$$\begin{array}{l|l} xy^4+x^4+x^3y+y^3 & y^3+x^2 \\ \cline{2-2} -xy^4-x^3y & \\ \cline{1-1} \not{x}^4+y^3 & q=xy \\ & r=x^4 \end{array}$$

Agora y^3 assume o papel de f.





Uma vez que $ml(g) = y^3 \nmid x^2$, temos que $-x^2$ contribui para o resto r e o algoritmo finaliza.



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

Como o algoritmo da divisão utiliza várias vezes o conceito de termo líder e monômio líder é previsível que o quociente e o resto possam variar de acordo com a ordem monomial escolhida.

Para ilustrar tal situação, aplicando novamente o algoritmo da divisão para $f = xy^4 + x^4 + x^3y + y^3$ e $g = y^3 + x^2$, fixando agora a ordem lexicográfica obtemos:

$$
\begin{array}{rl|l}
x^4 + x^3y + xy^4 + y^3 & & x^2 + y^3 \\
\cline{3-3}
-x^4 - x^2y^3 & & \boxed{q = x^2 + xy - y^3} \\
\cline{1-1}
x^3y - x^2y^3 + xy^4 + y^3 & & \boxed{r = y^6 + y^3} \\
-x^3y - xy^4 & & \\
\cline{1-1}
-x^2y^3 + y^3 & & \\
x^2y^3 + y^6 & & \\
\cline{1-1}
\cancel{y^6} + \cancel{y^3} & &
\end{array}
$$

Exercício 1.45. *Determine o quociente e o resto na divisão do polinômio* $f = x^4y + x^3y^3 + xy^4$ *por* $g = y^3 + xy$ *em* $\mathbb{R}[x, y]$ *com respeito à* $\preceq_L, \preceq_{LG}$ *e* $\preceq_L^{(1,2)}$.

Capítulo 2

Bases de Gröbner para ideais em $\mathbb{K}[x_1, \ldots, x_n]$

Muitas vezes, ao estudarmos uma estrutura algébrica como espaços vetoriais, grupos, anéis, corpos, etc., os elementos que estamos interessados formam uma subestrutura, ou seja, um subconjunto que mantém as propriedades operatórias, os quais denotamos por subespaços vetoriais, subgrupos, subanéis, subcorpos, etc. No caso de anéis, subconjuntos com uma outra particularidade despertam interesse, os quais são personagens principais destas notas.

2.1 Ideais

Iniciemos esta seção introduzindo o objeto algébrico que desempenhará papel central no que segue.

Definição 2.1. *Seja $(A, +, \cdot)$ um anel. Dizemos que um subconjunto não vazio $I \subseteq A$ é um* **ideal** *se:*

1. *$f + g \in I$ para quaisquer $f, g \in I$.*
2. *$h \cdot f \in I$ para todo $f \in I$ e todo $h \in A$.*

Observe que um ideal I é fechado para a adição, enquanto que o produto de um elemento qualquer do anel por um elemento de I

ainda é um elemento de I. Note ainda, que segue diretamente da definição acima, que $\{0\}$ e A são ideais de A, chamados de **ideais triviais**.

Exercício 2.2. *Seja $(A, +, \cdot)$ um anel. Mostre que:*

1. *$0 \in I$ para todo ideal I de A.*
2. *Se I é um ideal de A e um elemento invertível pertence a I, então $I = A$.*

Exercício 2.3. *Sejam I e J ideais de um anel A. Mostre que $I \cap J$ é ainda um ideal de A.*

Dado um subconjunto não vazio S de um anel $(A, +, \cdot)$, o conjunto

$$\langle S\rangle = \left\{ \sum_{i=1}^{n} h_i \cdot f_i;\ n \in \mathbb{N},\ f_i \in S \text{ e } h_i \in A \right\}$$

é um ideal de A.

De fato, sejam $a_1 = \sum_{i=1}^{n_1} h_i \cdot f_i, b_2 = \sum_{j=1}^{n_2} q_j \cdot g_j \in \langle S\rangle$, temos que

$$a_1 + a_2 = \sum_{i=1}^{n_1} h_i \cdot f_i + \sum_{j=1}^{n_2} q_j \cdot g_j = \sum_{k=1}^{n_1+n_2} h_k \cdot f_k \in \langle S\rangle,$$

com $h_{n_1+j} = q_j$ e $f_{n_1+j} = g_j$.

Além disto, se $h \in A$, então claramente temos que

$$h \cdot a_1 = h \sum_{i=1}^{n_1} h_i \cdot f_i = \sum_{i=1}^{n_1} (h \cdot h_i) \cdot f_i \in \langle S\rangle.$$

O ideal $\langle S\rangle$ é chamado **ideal gerado por** S, e no caso em que temos $S = \{f_1, \ldots, f_r\}$ indicaremos $\langle S\rangle$ por $\langle f_1, \ldots, f_r\rangle$. Um ideal é chamado **principal**, se ele pode ser gerado por um único elemento.

Uma vez que nosso ambiente é $\mathbb{K}[x_1, \ldots, x_n]$, vamos nos concentrar neste anel a partir deste ponto.

Exemplo 2.4. *Dado $\alpha \in \mathbb{K}$, o conjunto*

$$I = \{f \in \mathbb{K}[x]; f(\alpha) = 0\}$$

é um ideal de $\mathbb{K}[x]$, onde $f(\alpha) = a_n\alpha^n + \ldots + a_1\alpha + a_0 \in \mathbb{K}$ para $f \in \mathbb{K}[x]$.

De fato, dados quaisquer $f, g \in I$ e $h \in \mathbb{K}[x]$, temos que

$$(f+g)(\alpha) = f(\alpha) + g(\alpha) = 0 + 0 = 0,$$

$$(h \cdot f)(\alpha) = h(\alpha) \cdot f(\alpha) = h(\alpha) \cdot 0 = 0$$

ou seja, $f + g, h \cdot f \in I$.

Como $x - \alpha \in I$, temos

$$\langle x - \alpha \rangle = \{h \cdot (x - \alpha);\ h \in \mathbb{K}[x]\} \subseteq I.$$

Por outro lado, dado $f \in I$, temos que α é raiz do polinômio f, pois $f(\alpha) = 0$. Assim, pelo Corolário 1.21, temos que $x - \alpha$ divide f, ou seja, existe $h \in \mathbb{K}[x]$, tal que $f = h \cdot (x - \alpha)$, isto é, $f \in \langle x - \alpha \rangle$. Deste modo, $I \subseteq \langle x - \alpha \rangle$.

Portanto, temos que $I = \langle x - \alpha \rangle$. Em particular, I é principal.

Vejamos um exemplo de um ideal no anel de polinômios em mais de uma indeterminada.

Exemplo 2.5. *O conjunto*

$$I = \{f \in \mathbb{K}[x, y]; f(t^3, t^2) = 0\}$$

é um ideal não nulo de $\mathbb{K}[x, y]$.

A justificativa não reserva segredos e segue o que fizemos no exemplo anterior.

Vamos mostrar que $I = \langle x^2 - y^3 \rangle$.

Claramente se $f \in \langle x^2 - y^3 \rangle$, então $f = h \cdot (x^2 - y^3)$ para algum $h \in \mathbb{K}[x, y]$ e

$$f(t^3, t^2) = h(t^3, t^2) \cdot \left((t^3)^2 - (t^2)^3\right) = h(t^3, t^2) \cdot 0 = 0,$$

consequentemente, $f \in I$.

Por outro lado, se $f \in I$, então aplicando o algoritmo da divisão a f por $g = x^2 - y^3$ com respeito à ordem lexicográfica, existem únicos

$q, r \in \mathbb{K}[x, y]$, tais que $f = q \cdot g + r$ com $r = 0$ ou $ml(g) = x^2 \nmid m$ para todo $m \in \mathbb{M}(r)$.

Se $r \neq 0$, então a condição $x^2 \nmid m$ para todo $m \in \mathbb{M}(r)$, implica que $r = h_1 \cdot x + h_0$ com $h_0, h_1 \in \mathbb{K}[y]$ não simultaneamente nulos, ou seja, temos a igualdade $f = q \cdot (x^2 - y^3) + h_1 \cdot x + h_0$.

Como $f \in I$, temos que

$$0 = f(t^3, t^2) = q(t^3, t^2) \cdot \left((t^3)^2 - (t^2)^3\right) + h_1(t^2) \cdot t^3 + h_0(t^2),$$

ou ainda,

$$h_1(t^2) \cdot t^3 = -h_0(t^2).$$

Agora note que em $h_1(t^2)$ e $h_0(t^2)$ temos somente monômios de grau par (em t), ou seja, $gr_t(h_1(t^2)) = 2\alpha$ e $gr_t(h_0(t^2)) = 2\beta$ para algum $\alpha, \beta \in \mathbb{N}$. Mas, deste modo,

$$3 + 2\alpha = gr_t(h_1(t^2) \cdot t^3) = gr_t(h_0(t^2)) = 2\beta,$$

que é um absurdo. Assim, devemos ter $r = 0$ e $f = q \cdot (x^2 - y^3)$, ou seja, $f \in \langle x^2 - y^3 \rangle$.

Portanto, $I = \langle x^2 - y^3 \rangle$.

Uma pergunta natural, ao analisarmos o exemplo anterior é: como nos ocorreu o polinômio $x^2 - y^3$ e como sabíamos que se tratava do gerador do ideal?

Preferimos manter o suspense, dizendo apenas que os argumentos acima se tornarão obsoletos, serão simplificados e justificados se o leitor continuar atento a estas notas.

Os dois exemplos apresentados anteriormente, podem sugerir que todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ é principal, ou seja, pode ser gerado por um único elemento.

A proposição a seguir assegura que tal fato é uma certeza matemática em $\mathbb{K}[x]$.

Proposição 2.6. *Todo ideal I de $\mathbb{K}[x]$ é da forma $I = \langle g \rangle$ para algum $g \in \mathbb{K}[x]$.*

Dem: Se $I = \{0\}$, então naturalmente $I = \langle 0 \rangle$.

Se $I \neq \{0\}$, então tomemos $g \in I$ tal que $gr(g) \leq gr(f)$ para todo $f \in I$.

Como I é ideal e $g \in I$, temos que $h \cdot g \in I$ para todo $h \in \mathbb{K}[x]$, ou seja, $\langle g \rangle \subseteq I$.

Por outro lado, dado $f \in I$, o algoritmo da divisão aplicado a f e a g, garante a existência de $q, r \in \mathbb{K}[x]$ tais que $f = q \cdot g + r$ com $r = 0$ ou $gr(r) < gr(g)$. Como $f, g \in I$ e I é ideal, temos que $r = f - q \cdot g \in I$.

Se $r \neq 0$, então $gr(r) < gr(g)$ o que contraria a escolha de g. Resta-nos assim, concluir que $r = 0$ e $f = q \cdot g$, ou seja $f \in \langle g \rangle$ e $I \subseteq \langle g \rangle$.

Portanto, $I = \langle g \rangle$. ■

O resultado acima poderia ser mais uma indicação de que os ideais de $\mathbb{K}[x_1, \ldots, x_n]$ são sempre principais. Porém, o exemplo abaixo põe um ponto final nesta especulação.

Exemplo 2.7. *O ideal $I = \langle x, y \rangle \subset \mathbb{K}[x, y]$ não é principal.*

Suponha que $\langle x, y \rangle = \langle f \rangle$ para algum $f \in \mathbb{K}[x, y]$. Neste caso, deveriam existir $g, h, p, q \in \mathbb{K}[x, y]$ tais que

$$x = g \cdot f, \quad y = h \cdot f \quad e \quad f = p \cdot x + q \cdot y.$$

Assim, temos

$$1 = gr(g) + gr(f) \quad e \quad 1 = gr(h) + gr(f).$$

Tais equações e o fato de que $f \notin \mathbb{K}$, pois caso contrário teríamos $\langle x, y \rangle = \mathbb{K}[x, y]$, permitem concluir que $gr(f) = 1$, bem como ue $g = \beta_1, h = \beta_2 \in \mathbb{K} \setminus \{0\}$. Mas deste modo, devemos ter que $f = \alpha_1 x + \alpha_2 y$ com $\alpha_1, \alpha_2 \in \mathbb{K}$ e $\alpha_1 \neq 0$ ou $\alpha_2 \neq 0$.

Assim,

$$x = \beta_1(\alpha_1 x + \alpha_2 y) \quad e \quad y = \beta_2(\alpha_1 x + \alpha_2 y).$$

A primeira igualdade nos dá que $\beta_1 \alpha_1 = 1$ e $\beta_1 \alpha_2 = 0$, ou seja, $\alpha_2 = 0$, enquanto que a segunda igualdade acima $\alpha_1 = 0$. O que não pode ocorrer.

Como nenhum erro foi cometido em nossos argumentos, resta-nos concluir que a suposição de que existe $f \in \mathbb{K}[x, y]$ tal que $\langle f \rangle = \langle x, y \rangle$ é falsa, ou seja, $I = \langle x, y \rangle$ não pode ser principal.

Exercício 2.8. *Sejam $\beta_1, \ldots, \beta_n \in \mathbb{K}$. Mostre que:*

1. *o conjunto $I = \{f \in \mathbb{K}[x_1, \ldots, x_n];\ f(\beta_1, \ldots, \beta_n) = 0\}$ é ideal.*
2. *$I = \langle x_1 - \beta_1, \ldots, x_n - \beta_n \rangle$.*

O exercício anterior e os exemplos dados nos levam a formular a seguinte questão:

Problema 2.9. *Todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ é finitamente gerado?*

A resposta desta indagação é **sim**! Este resultado é conhecido como o *Teorema da Base de Hilbert* e é um dos primores da Álgebra Comutativa.

Na verdade, o Teorema da Base de Hilbert pode ser provado em um contexto mais geral, ele garante que se A é um anel em que todo ideal é finitamente gerado[1], então o mesmo se verifica para $A[x]$. Como em $\mathbb{K}[x_1]$ todo ideal é finitamente gerado, na verdade um ideal principal, conforme a Proposição 2.6, temos que todo ideal de $\mathbb{K}[x_1][x_2] = \mathbb{K}[x_1, x_2]$ também é finitamente gerado e por indução sobre o número de indeterminadas, temos que o mesmo se verifica para $\mathbb{K}[x_1, \ldots, x_n]$.

Vamos adiar a demonstração do Teorema da Base de Hilbert até a seção 2.3, porém vamos usá-lo livremente, ou seja, no que segue assumiremos que dado qualquer ideal I de $\mathbb{K}[x_1, \ldots, x_n]$, existam $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ tais que $I = \langle g_1, \ldots, g_s \rangle$.

Sem receio de cometermos exageros, o cerne destas notas e da teoria das Bases de Gröbner reside na busca de uma resposta para a seguinte questão:

Problema 2.10. *Dado um ideal $I = \langle g_1, \ldots, g_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ e um elemento $f \in \mathbb{K}[x_1, \ldots, x_n]$, como decidir se $f \in I$?*

Como subproduto da resposta da questão acima, temos um modo de decidir se dois ideais $I = \langle g_1, \ldots, g_s \rangle$ e $J = \langle f_1, \ldots, f_k \rangle$ do anel $\mathbb{K}[x_1, \ldots, x_n]$ são iguais. De fato, se $I = J$, então $g_i \in J$ e $f_j \in I$ para todo $i = 1, \ldots, s$ e todo $j = 1, \ldots, k$.

[1] Quando um anel possui esta propriedade, o chamamos de anel Noetheriano.

Reciprocamente, se $g_i \in J$ para todo $i = 1, \ldots, s$, então dado qualquer $g \in I$, temos $g = \sum_{j=1}^{s} h_j g_j \in J$ com $h_j \in \mathbb{K}[x_1, \ldots, x_n]$, ou seja, $I \subseteq J$. Analogamente, provamos que $J \subseteq I$ e portanto, $I = J$.

Note que a resposta afirmativa do Problema 2.10 consiste em garantirmos a existência de $h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$ tais que

$$f = h_1 \cdot g_1 + \ldots + h_s \cdot g_s.$$

Se I é um ideal principal, ou seja, se temos a existência de um polinômio $g \in \mathbb{K}[x_1, \ldots, x_n]$, tal que $I = \langle g \rangle$, então a afirmação $f \in I$ é equivalente a existência de $h \in \mathbb{K}[x_1, \ldots, x_n]$ tal que

$$f = h \cdot g,$$

que corresponde a garantir que o resto da divisão de f por g é zero. Algo que podemos verificar facilmente por meio do algoritmo da divisão.

Mas, e quanto ao caso de ideais que não são principais?

Antes de analisarmos o caso geral, vejamos um caso particular de ideais, os *ideais monomiais*, para os quais o problema da decisão de quando um elemento pertence ou não a um ideal tem uma solução fácil.

Definição 2.11. *Um ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ é chamado de* **ideal monomial***, se existe um conjunto de monômios que geram I.*

Vejamos alguns exemplos.

Exemplo 2.12. *O ideal $I = \langle x^3 + xy^4, y^2 \rangle \subseteq \mathbb{K}[x, y]$ é um ideal monomial.*

Basta observar que $I = \langle x^3, y^2 \rangle$. Claramente, $I \subseteq \langle x^3, y^2 \rangle$ e como temos $x^3 = (x^3 + xy^4) - xy^2 \cdot (y^2) \in I$, segue que $\langle x^3, y^2 \rangle \subseteq I$, donde segue que $I = \langle x^3, y^2 \rangle$.

Exemplo 2.13. *O ideal $I = \langle x + 1 \rangle \subset \mathbb{K}[x]$ não é ideal monomial.*

Se I fosse monomial, então existiria um conjunto $\{x^{i_1}, \ldots, x^{i_s}, \ldots\}$ de monômios que gerariam I. Neste caso, é fácil constatar que $I = \langle x^i \rangle$ com $i = min\{i_1, \ldots, i_s, \ldots\}$.

Além disto, se $\langle x + 1 \rangle = I = \langle x^i \rangle$, então existiriam $h, g \in \mathbb{K}[x]$ tais que

$$x + 1 = h \cdot x^i \quad e \quad x^i = g \cdot (x + 1).$$

Assim,

$$1 = gr(h) + i \quad e \quad i = gr(g) + 1,$$

ou seja, $1 = gr(h) + gr(g) + 1$. *Donde concluímos que* $gr(g) = 0$ *e* $gr(h) = 0$, *isto é,* $g = \alpha, h = \beta \in \mathbb{K} \setminus \{0\}$ *e* $i = 1$, *ou seja,* $x + 1 = \beta x$, *igualdade esta que não pode ocorrer. Portanto,* I *não pode ser um ideal monomial.*

Vamos fornecer uma resposta afirmativa ao Problema 2.9 quando o ideal é monomial.

Teorema 2.14. (Lema de Dickson) *Seja* I *um ideal monomial de* $\mathbb{K}[x_1, \ldots, x_n]$, *então existe um conjunto finito de monômios que geram* I.

Dem: Se $I = \{0\}$, então obviamente o conjunto $\{0\}$ gera I.

Vamos considerar que $I \neq \{0\}$ e provar o teorema usando indução sobre o número de indeterminadas.

O caso de uma indeterminada é imediato, uma vez que em $\mathbb{K}[x_1]$ todo ideal é principal, ou seja, $I = \langle f \rangle$ com $f \in \mathbb{K}[x_1]$. Dado um monômio $m \in I$ temos que $m = h \cdot f$ para algum $h \in \mathbb{K}[x_1]$. Pela igualdade de polinômios, segue que f deve ser um monômio.

Vamos supor que o teorema seja válido para ideais em anéis de polinômios com $n - 1$ indeterminadas.

Seja I um ideal monomial não nulo de $\mathbb{K}[x_1, \ldots, x_n]$ e escolha um monômio $f_1 = g_1 \cdot x_n^{\alpha_1} \in I$, onde $g_1 \in \mathbb{M}_{n-1}$ e $\alpha_1 \in \mathbb{N}$ é o menor possível.

Se $I = \langle f_1 \rangle$, então o teorema está demonstrado. Caso contrário, escolha um monômio $f_2 = g_2 \cdot x_n^{\alpha_2} \in I \setminus \langle f_1 \rangle$, onde $g_2 \in \mathbb{M}_{n-1}$ e α_2 é o menor possível. Note que obrigatoriamente temos que $\alpha_2 \geq \alpha_1$, pois caso contrário f_1 não teria sido escolhido de maneira a ter α_1 mínimo.

Se $I = \langle f_1, f_2 \rangle$, então provamos o teorema. Caso contrário continuamos com este procedimento.

Vamos supor que este procedimento continua indefinidamente, ou seja, que possamos obter uma sequência infinita de monômios $f_1, f_2, \ldots \in I$ tal que $f_i = g_i \cdot x_n^{\alpha_i} \in I \setminus \langle f_1, \ldots, f_{i-1} \rangle$ com $g_i \in \mathbb{M}_{n-1}$, $\alpha_i \in \mathbb{N}$ o menor possível e $\alpha_i \geq \alpha_{i-1}$ para todo $i > 1$.

Por hipótese de indução, temos que o ideal J de $\mathbb{K}[x_1, \ldots, x_{n-1}]$ gerado pelos monômios $g_1, g_2 \ldots \in \mathbb{M}_{n-1}$ é finitamente gerado, ou seja, existem monômios $m_1, \ldots, m_r \in \mathbb{M}_{n-1}$ tais que $J = \langle m_1, \ldots, m_r \rangle$.

Tome um monômio g_i como acima, temos que $g_i \in \langle m_1, \ldots, m_r \rangle$, ou seja, existe um monômio $p \in \mathbb{M}_{n-1}$ de modo que $g_i = p \cdot m_j$ para algum $j \in \{1, \ldots, r\}$. Por outro lado $m_j \in J$, então existe um monômio $q \in \mathbb{M}_{n-1}$ tal que $m_j = q \cdot g_k$ para algum g_k como descrito acima. Deste modo, temos que $g_i = p \cdot q \cdot g_k$.

Se $i = k$, então $p \cdot q = 1$, ou seja, $p = \alpha \in \mathbb{K} \setminus \{0\}$ e $g_i = \alpha \cdot m_j$. Como a sequência $g_1, g_2, \ldots \in \mathbb{M}_{n-1}$ é infinita, não podemos ter este caso indefinidamente, ou seja, existem índices $i \neq k$ tais que $g_k \mid g_i$, digamos $g_i = m \cdot g_k$ com $m \in \mathbb{M}_{n-1}$.

Sem perda de generalidade podemos supor $i > k$. Deste modo,

$$f_i = g_i \cdot x_n^{\alpha_i} = m \cdot g_k \cdot x_n^{\alpha_i - \alpha_k} \cdot x_n^{\alpha_k} = m \cdot x_n^{\alpha_i - \alpha_k} \cdot f_k$$

e $f_i \in \langle f_k \rangle \subset \langle f_1, \ldots, f_k \rangle$ contrariando o modo com que escolhemos f_i.

Segue assim, que existe um índice $s \in \mathbb{N}$ tal que $I = \langle f_1, \ldots, f_s \rangle$, ou seja, I é finitamente gerado por monômios. ■

Graças ao teorema acima, podemos considerar um conjunto finito de geradores para um ideal monomial e estamos aptos a formular um critério que permite decidir quando um elemento pertence ou não a um ideal monomial, respondendo ao Problema 2.10 para ideais monomiais.

Proposição 2.15. *Um polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ pertence a um ideal monomial $I = \langle m_1, \ldots, m_s \rangle$ se, e somente se, $m \in I$ para todo $m \in \mathbb{M}(f)$.*

Dem: Inicialmente, note que se $m \in I$ para todo $m \in \mathbb{M}(f)$, então é imediato que $f \in I$.

Por outro lado, suponha que $f \in I$, então temos $f = \sum_{i=1}^{s} g_i m_i$ com $g_i \in \mathbb{K}[x_1, \ldots, x_n]$. Agora, fixada uma ordem monomial sobre $\mathbb{M}_n$, temos que $ml(f) \in \bigcup_{i=1}^{s} \mathbb{M}(g_i m_i)$, ou seja, $ml(f) = r_j m_j$ onde $r_j \in \mathbb{M}(g_j)$ para algum $j = 1, \ldots, s$, que é equivalente a dizer que $ml(f) \in I$.

Como $f_1 = f - tl(f) \in I$, podemos repetir o raciocínio para f_1. Tal argumento permite concluir que $m \in I$ para todo $m \in \mathbb{M}(f)$. ■

O resultado acima nos dá um modo de decidir facilmente se um elemento $f \in \mathbb{K}[x_1, \ldots, x_n]$ pertence a um ideal monomial I. Para tanto, consideramos um conjunto finito de geradores $\{m_1, \ldots, m_s\}$ de I e verificamos se cada monônio de f pertence ao ideal I, e isto ocorre se, e somente se, cada monômio é divisível por um dos monômios geradores de I. De fato, seja m um monômio e um ideal I monomial $I = \langle m_1, \ldots, m_s \rangle$. Se $m \in I$, então como vimos na demonstração da proposição anterior temos que $m = r_j m_j$ onde r_j é um monômio e m_j é um dos geradores do ideal I.

Exemplo 2.16. *Os polinômios* $f = 6x^4 + 4xy^2 - 3x^3y$ *e* $g = 2x^4 + 5xy^2 - 8x^2y$ *pertencem ao ideal* $I = \langle x^3 + xy^4, y^2 \rangle$*?*

Como vimos no Exemplo 2.12, I *é um ideal monomial, a saber,* $I = \langle x^3, y^2 \rangle$*.*

Uma vez que $x^4, xy^2, x^3y \in I$ *e* $x^2y \notin I$*, segue que* $f \in I$ *e* $g \notin I$*.*

O primeiro passo para respondermos ao Problema 2.10, merece uma seção própria que introduzimos a seguir.

2.2 O Algoritmo da divisão revisitado

Como vimos, dado um ideal $I = \langle g_1, \ldots, g_s \rangle$ e um elemento f de $\mathbb{K}[x_1, \ldots, x_n]$, afirmar que $f \in I$ é equivalente a garantir a existência de $q_1, \ldots, q_s \in \mathbb{K}[x_1, \ldots, x_n]$ tais que

$$f = q_1 \cdot g_1 + \ldots + q_s \cdot g_s.$$

Na seção anterior, analisamos situações particulares que correspondem ao caso em que temos $s = 1$, ou seja, o ideal I é principal e o caso em que g_i é um monômio para todo $i = 1, \ldots, s$. Resta agora o caso geral para a qual a equaçao anterior é o ponto de partida.

A equação acima pode ser livremente (e tendenciosamente) interpretada como sendo obtida pela divisão de f por $g_1, \ldots, g_s$, onde $q_1, \ldots, q_s$ correspondem a quocientes e o resto é nulo.

Divisão de um polinômio f por vários polinômios $g_1, \ldots, g_s$? Como poderíamos realizar tal procedimento?

A ideia, mais intuitiva que nos ocorre, é tentar aplicar o algoritmo da divisão que conhecemos e apresentamos no Teorema 1.43 para f e g_1 enquanto possível, entre outras coisas, isto implica em fixar uma ordem monomial. Antes de alocar um termo ao resto, ou seja, um termo que não é divisível por $tl(g_1)$, tentamos proceder a divisão por $tl(g_2)$, em caso de impossibilidade, passamos para g_3 e assim sucessivamente. Deste modo, um termo contribuirá para o resto apenas se este não for divisível por $tl(g_i)$ para todo $i = 1, \ldots, s$.

Note que tal processo pressupõe uma prioridade entre os elementos do conjunto $\{g_1, \ldots, g_s\}$.

Ao que tudo indica, parece que tal processo funciona. Em verdade, temos o seguinte resultado.

Teorema 2.17. (Algoritmo da Pseudo-Divisão) *Fixada uma ordem monomial $\preceq$ e dados $f, g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ com $g_i \neq 0$ para todo $i = 1, \ldots, s$, existem polinômios $q_1, \ldots, q_s, r \in \mathbb{K}[x_1, \ldots, x_n]$ tais que*

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

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

Dem: Vamos demonstrar o teorema apresentando e justificando um procedimento que fornece o resultado esperado.

Considere o seguinte algoritmo:

ENTRADA: $f, g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ COM $g_i \neq 0$
PARA TODO $i = 1, \ldots, s$;
DEFINA $q_1 := \ldots := q_s := r := 0$ E $h := f$;
ENQUANTO $h \neq 0$ FAÇA
SE EXISTE $i \in \{1, \ldots, s\}$ TAL QUE $ml(g_i) \mid ml(h)$
ENTÃO
ESCOLHA O MENOR TAL ÍNDICE i E FAÇA
$q_i := q_i + \frac{tl(h)}{tl(g_i)}$;
$h := h - \frac{tl(h)}{tl(g_i)} g_i$;
SENÃO
$r := r + tl(h)$;
$h := h - tl(h)$;
SAÍDA: $q_1, \ldots, q_s$ E r TAIS QUE $f = \sum_{j=1}^{s} q_j g_j + r$
E $ml(g_i) \nmid m$ PARA TODO $m \in \mathbb{M}(r)$
E TODO $i = 1, \ldots, s$.

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

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

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

Pelo Lema 1.29, toda sequência decrescente de monômios é finita, ou seja, em algum momento obteremos $h = 0$ e consequentemente o algoritmo finaliza.

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

Note que em cada passo executado no algoritmo temos a igualdade $f = \sum_{j=1}^{s} q_j g_j + r + h$. De fato, iniciamos com $h = f, r = 0$ e $q_i = 0$ para todo $i = 1, \ldots, s$, assim a afirmação inicia verdadeira.

Se existe $i \in \{1, \ldots, s\}$ tal que $ml(g_i) \mid ml(h)$, então redefinimos

q_i por $q_i + \frac{tl(h)}{tl(g_i)}$ e h por $h - \frac{tl(h)}{tl(g_i)}g_i$ e temos

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

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

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

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

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

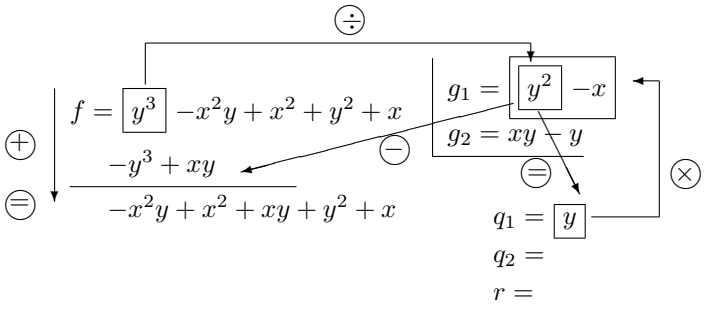
Como nos Teoremas 1.12 e 1.43, podemos utilizar um dispositivo prático para efetuar os passos do algoritmo contido na demonstração do teorema anterior. A única modificação, com relação ao caso tratado no Teorema 1.43, que faremos é de permitir acrescentar mais do que um divisor e consequentemente obter um "quociente" para cada um deles. Deste modo o dispositivo terá a seguinte configuração:

$$\begin{array}{rl|l} & & g_1 \\ f & & \vdots \\ & & g_s \\ \hline & & q_1 \\ 0 & & \vdots \\ & & q_s \\ & & r \end{array}$$

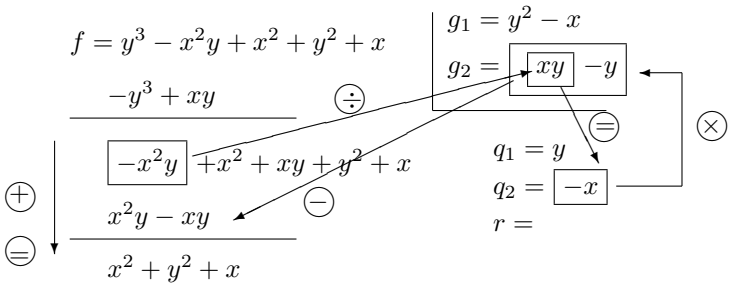
Pela segurança obtida na aplicação do algoritmo da divisão de um polinômio por outro, acreditamos que podemos seguir diretamente para a apresentação de um exemplo utilizando o dispositivo acima.

Vamos encontrar polinômios q_1, q_2 e r satisfazendo as condições do teorema anterior para $f = y^3 - x^2y + x^2 + y^2 + x, g_1 = y^2 - x$, $g_2 = xy - y \in \mathbb{R}[x, y]$ com respeito à ordem lexicográfica graduada, aplicando o algoritmo contido em sua demonstração, que passaremos a nos referir simplesmente como **Algoritmo da Pseudo-Divisão**.

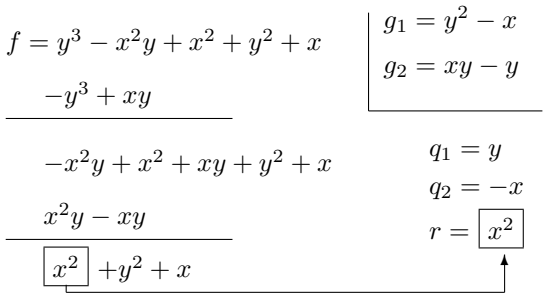
Seguindo as instruções temos que $ml(g_1) \mid ml(f)$, assim:



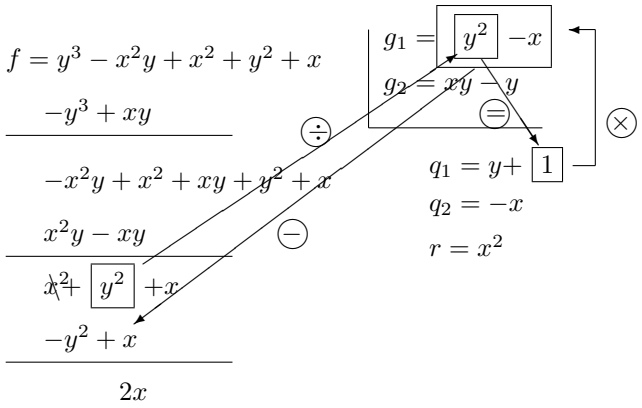
Como $ml(g_1) = y^2 \nmid x^2y = ml(-x^2y + x^2 + xy + y^2 + x)$, mas temos $ml(g_2) = xy \mid x^2y$, procedemos a divisão usando g_2:



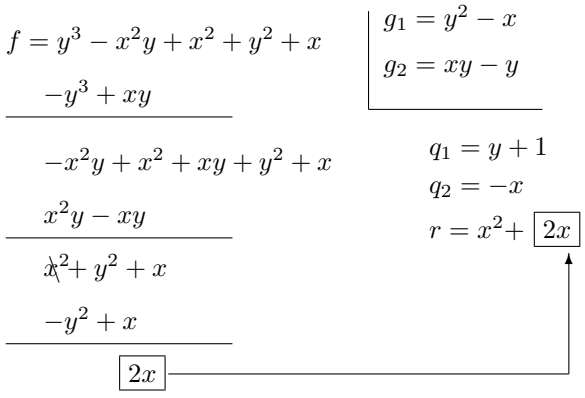
Temos $ml(g_1) = y^2 \nmid x^2 = ml(x^2 + y^2 + x)$ e $ml(g_2) = xy \mid x^2$, desta forma o termo x^2 contribui para o resto.



Agora continuamos o procedimento, dividindo $y^2 + x$ por g_1 e g_2.



Uma vez que $ml(g_1) = y^2 \nmid x = ml(2x)$ e $ml(g_2) = xy \nmid x$, temos que $2x$ contribui para o resto e o algoritmo finaliza com os polinômios $q_1 = y + 1, q_2 = -x$ e $r = x^2 + 2x$.



$$\begin{array}{l|l} f = y^3 - x^2y + x^2 + y^2 + x & g_1 = y^2 - x \\ \quad -y^3 + xy & g_2 = xy - y \\ \hline \quad -x^2y + x^2 + xy + y^2 + x & \\ \quad x^2y - xy & \\ \hline \quad \cancel{x^2} + y^2 + x & \\ \quad -y^2 + x & \\ \hline \quad 2x & \end{array} \qquad \begin{array}{l} q_1 = y + 1 \\ q_2 = -x \\ r = x^2 + 2x \end{array}$$

Note que há uma sutil diferença entre o teorema acima e os Teoremas 1.12 e 1.43 para a qual o leitor deve atentar: não anunciamos unicidade dos polinômios $q_1, \ldots, q_s$ e r! Tal fato não foi um descuido, uma vez que não podemos garantir que isto ocorra, como fica evidente no próximo exemplo.

Exemplo 2.18. *Fixemos a ordem lexicográfica graduada. Aplicando o algoritmo contido na demonstração do teorema anterior para os polinômios $f = xy^2 - x, g_1 = y^2 - x, g_2 = xy - y \in \mathbb{K}[x, y]$ e para estes mesmos polinômios trocando a prioridade entre $y^2 - x$ e $xy - y$, ou seja, considerando $g_1 = xy - y$ e $g_2 = y^2 - x$, obtemos respectivamente:*

$$\begin{array}{l|l} f = xy^2 - x & g_1 = y^2 - x \\ \underline{-xy^2 + x^2} & g_2 = xy - y \\ \cancel{x^2} - \cancel{x} & \end{array} \qquad \begin{array}{l} q_1 = x \\ q_2 = 0 \\ r = x^2 - x \end{array}$$

$$\begin{array}{l|l} f = xy^2 - x & g_1 = xy - y \\ \underline{-xy^2 + y^2} & g_2 = y^2 - x \\ y^2 - x & \\ \underline{-y^2 + x} & \\ 0 & \end{array} \qquad \begin{array}{l} q_1 = y \\ q_2 = 1 \\ r = 0 \end{array}$$

Exercício 2.19. *Aplique o algoritmo da pseudo-divisão a f e $g_1, \ldots, g_s$ para escrever $f = \sum_{i=1}^{s} q_i g_i + r$.*

1. *$f = y^3 + x^2 + xy, g_1 = y^2 + x$ e $g_2 = xy + 1$ com respeito à ordem lexicográfica graduada.*

2. $f = y^3 + x^2 + xy, g_1 = y^2 + x$ *e* $g_2 = xy + 1$ *com respeito à ordem lexicográfica.*

3. $f = y^3 + x^2 + xy, g_1 = xy + 1$ *e* $g_2 = y^2 + x$ *com respeito à ordem lexicográfica.*

4. $f = x^2 + y^2 + z^2, g_1 = y, g_2 = y + z$ *e* $g_3 = z + 1$ *com respeito à ordem lexicográfica graduada.*

O exemplo acima ilustra que, se ao aplicarmos o algoritmo da pseudo-divisão obtemos $r = 0$, então $f = \sum_{i=1}^{s} q_i g_i$, o que indica que $f \in \langle g_1, \ldots, g_s \rangle$, mas a recíproca não é verdadeira, ou seja, se temos $f = \sum_{i=1}^{s} q_i g_i + r$ com $r \neq 0$, então não podemos afirmar que tenhamos $f \notin \langle g_1, \ldots, g_s \rangle$.

Poderíamos ser tentados a acreditar que para verificar se f pertence ao ideal $\langle g_1, \ldots, g_s \rangle$, bastaria aplicar o algoritmo da pseudo-divisão para todas as enumerações possíveis dos elementos $g_1, \ldots, g_s$, ou seja, para $s!$ maneiras, o que é um número monstruosamente grande a medida que s aumenta.

Mesmo se aceitássemos o árduo trabalho, ainda assim, não teríamos garantia de uma conclusão para o problema, como vemos no exemplo a seguir.

Exemplo 2.20. *Podemos afirmar que o polinômio* $f = x^2y^4 - x^2$ *pertence ao ideal* $I = \langle y^2 - x, xy - y \rangle$*?*

Fixando a ordem lexicográfica graduada e aplicando o algoritmo da pseudo-divisão para $f, g_1 = y^2 - x$ *e* $g_2 = xy - y$*, bem como para* $f, g_1 = xy - y$ *e* $g_2 = y^2 - x$*, obtemos respectivamente*

$$\begin{array}{l|l} f = x^2y^4 - x^2 & g_1 = y^2 - x \\ -x^2y^4 + x^3y^2 & g_2 = xy - y \\ \hline x^3y^2 - x^2 & q_1 = x^2y^2 + x^3 \\ -x^3y^2 + x^4 & q_2 = 0 \\ \hline \cancel{x^4} - \cancel{x^2} & r = x^4 - x^2 \end{array}$$

$$\begin{array}{l|l} f = x^2y^4 - x^2 & g_1 = xy - y \\ -x^2y^4 + xy^4 & g_2 = y^2 - x \\ \hline xy^4 - x^2 & q_1 = xy^3 + y^3 + y \\ -xy^4 + y^4 & q_2 = y^2 + 1 \\ \hline y^4 - x^2 & r = -x^2 + x \\ -y^4 + xy^2 & \\ \hline xy^2 - x^2 & \\ -xy^2 + y^2 & \\ \hline -\cancel{x^2} + y^2 & \\ -y^2 + x & \\ \hline \cancel{x} & \end{array}$$

Ou seja, para todas as enumerações dos elementos do conjunto $G = \{xy - y, y^2 - x\}$*, a redução de* f *por* G *não é zero. No entanto, temos que* $f = (x^2y^2 + x) \cdot (y^2 - x) + (x^2y + xy) \cdot (xy - y)$*, isto é,* $f \in \langle xy - y, y^2 - x \rangle$*.*

O exemplo anterior alerta para o fato de que o algoritmo da pseudo-divisão, mesmo que aplicado para todas as enumerações possíveis do conjunto $\{g_1, \ldots, g_s\}$ não é um modo eficaz para verificar se um elemento f pertence ao ideal $I = \langle g_1, \ldots, g_s \rangle$.

Como dissemos no final da seção anterior tal algoritmo é o primeiro passo na direção de uma estratégia efetiva. Chegou o momento de introduzirmos os conceitos que nos conduzirão na busca desta estratégia.

2.3 Bases de Gröbner

Constatamos, na seção anterior, que o problema de decidir se um polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ pertence ou não a um ideal I é uma questão não trivial, que respondemos apenas para o caso em que I é um ideal principal ou monomial. Nesta seção apresentaremos as noções básicas da teoria de Bases de Gröbner, que permite respondermos completamente tal questão.

Um dos grandes estudiosos desta questão foi o matemático alemão Gröbner. Dentre suas principais contribuições neste assunto, está um argumento que garante que todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ admite conjuntos finitos de geradores "especiais" chamados posteriormente de Bases de Gröbner, os quais possibilitam facilmente decidir se um elemento pertence ou não ao ideal dado. No entanto, apesar de apresentar uma prova da existência de tais geradores e comprovar sua existência em um número considerável de exemplos não dispunha de um método sistemático para computá-los. Coube a um de seus alunos, Bruno Buchberger, na sua tese de doutorado em 1967, depois de aproximadamente 15 anos da descoberta de tais conjuntos de geradores, formular um algoritmo para obter os mesmos.

Muitas vezes, o assunto de uma tese de doutorado, em matemática, pode ser tão profundo e específico que é necessário vários conceitos, definições e resultados para que possamos desfrutar dos avanços que

o trabalho apresenta. A tese de Bruno Buchberger é uma rara e preciosa exceção a este padrão, contém ideias simples e principalmente procedimentos que podem ser implementados, tornando o método eficaz e poderoso.

Os resultados obtidos por Buchberger não tiveram de imediato uma repercussão como se imagina. Apenas uma década após a divulgação de seus resultados, aplicações nas mais variadas áreas colocaram o método em evidência, principalmente pela surpreendente simplicidade e genialidade.

Definição 2.21. *Sejam $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal e $\preceq$ uma ordem monomial fixada. Um subconjunto não vazio e finito G de I é uma* **Base de Gröbner** *para I, com respeito à $\preceq$, se para todo $f \in I$ existe $g \in G$ de modo que $ml(g) \mid ml(f)$.*

Vamos aproveitar situações abordadas anteriormente para apresentar alguns exemplos.

Exemplo 2.22. *Dado um ideal principal $I = \langle g \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$, então $G = \{g\}$ é uma Base de Gröbner para I com respeito a qualquer ordem monomial.*

Exemplo 2.23. *Se $I = \langle m_1, \ldots, m_r \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$ é um ideal monomial, então segue da Proposição 2.15 que $G = \{m_1, \ldots, m_r\}$ é uma Base de Gröbner para I com respeito a qualquer ordem monomial.*

Para que não criemos a falsa imagem de que todo conjunto de geradores de um ideal é uma Base de Gröbner, apresentamos o seguinte exemplo.

Exemplo 2.24. *Considere o ideal $I = \langle y^2 - x, xy - y \rangle \subseteq \mathbb{K}[x, y]$, então $G = \{y^2 - x, xy - y\}$ não é uma Base de Gröbner para I com respeito à ordem lexicográrica graduada.*

De fato, temos que $x^2 - x = (-x+1)(y^2 - x) + y(xy - y) \in I$, mas considerando a ordem lexicográfica graduada temos $ml(x^2 - x) = x^2$ não é divisível pelos monômios líderes dos elementos de G.

A propriedade de um conjunto ser uma Base de Gröbner não é uma propriedade intrínseca, ou seja, não depende apenas do conjunto, mas depende também da ordem monomial considerada.

Exemplo 2.25. *Analisemos o ideal* $I = \langle x+y^2, y^2\rangle \subset \mathbb{K}[x,y]$. *Temos que* $G = \{x+y^2, y^2\}$ *não é uma Base de Gröbner para* I, *com respeito à ordem lexicográfica graduada, pois* $x = (y^2+x)-y^2 \in I$, *no entanto temos que* $ml(y^2+x) = ml(y^2) = y^2 \nmid x$.

No entanto, G *é uma Base de Gröbner para* I *com respeito à ordem lexicográfica. De fato, dado* $f \in I$ *não nulo, então existem* $p, q \in \mathbb{K}[x,y]$ *tais que*

$$f = p \cdot (x + y^2) + q \cdot y^2 = p \cdot x + (p+q) \cdot y^2.$$

Assim, $ml(f) \in \mathbb{M}(p \cdot x) \cup \mathbb{M}((p+q) \cdot y^2)$.

Se $ml(f) \in \mathbb{M}(p \cdot x)$, *então* $ml(f) = ml(p) \cdot x$ *e obtemos que* $ml(x + y^2) = x \mid ml(f)$. *Por outro lado, se* $ml(f) \in \mathbb{M}((p+q) \cdot y^2)$, *então temos que* $ml(f) = ml(p+q) \cdot y^2$ *e* $ml(y^2) = y^2 \mid ml(f)$.

Portanto, $G = \{x + y^2, y^2\}$ *é uma Base de Gröbner para* I *com respeito à ordem lexicográfica.*

Muitas vezes, uma propriedade pode ser expressa de várias maneiras equivalentes, o que pode auxiliar a sua verificação, pois dependendo da situação particular pode-se tornar mais fácil analisar uma situação em detrimento de outra. O teorema a seguir, nos dá outras caracterizações para uma Base de Gröbner de um ideal.

Teorema 2.26. *Fixe uma ordem monomial* $\preceq$. *Dados* I *um ideal não nulo de* $\mathbb{K}[x_1, \ldots, x_n]$ *e* $G = \{g_1, \ldots, g_s\} \subset I$, *então são equivalentes:*

1. G *é uma Base de Gröbner para o ideal* I *com respeito à ordem monomial* $\preceq$.

2. $\langle ml(I)\rangle = \langle ml(G)\rangle$, *onde* $ml(I)$ *e* $ml(G)$ *indicam o conjunto dos monômios líderes de todos os elementos de* I *e* G *respectivamente.*

3. $f \in I$ *se, e somente se, o resto da pseudo-divisão de* f *pelos elementos de* G *é zero.*

4. $f \in I$ *se, e somente se, podemos escrever* $f = \sum_{i=1}^{s} q_i \cdot g_i$ *tal que* $ml(f) = \max_{1 \le i \le s}\{ml(q_i)ml(g_i)\}$.

DEM: 1) $\Rightarrow$ 2). Como $G \subset I$, certamente $ml(G) \subset ml(I)$ e consequentemente $\langle ml(G)\rangle \subseteq \langle ml(I)\rangle$.

Por outro lado, seja $m \in ml(I)$, então existe $f \in I$, tal que $ml(f) = m$. Como G é Base de Gröbner para I, existe $g_i \in G$ tal que $ml(g_i) \mid m$, ou seja, existe um monômio $m_i \in \mathbb{M}_n$ de tal modo que $m = m_i \cdot ml(g_i)$, ou seja, $m \in \langle ml(G)\rangle$ e $ml(I) \subseteq \langle ml(G)\rangle$. Deste modo, dado $h \in \langle ml(I)\rangle$ existem polinômios $h_1, \ldots, h_k$ em $\mathbb{K}[x_1, \ldots, x_n]$ e $f_1, \ldots, f_k \in I$ tais que

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

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

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

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

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

com $r = 0$ ou $ml(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$. Assim, temos que $r = f - \sum_{i=1}^{s} q_i \cdot g_i \in I$.

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

3) $\Rightarrow$ 4). Esta implicação segue imediatamente do algoritmo da pseudo-divisão (Teorema 2.17).

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

Uma nota digna de menção é que, se G é uma Base de Gröbner para um ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, então, pelo teorema anterior (item 4), G é também um conjunto de geradores para I.

No Exemplo 2.18 tivemos oportunidade de constatar que o resto da pseudo-divisão de um polinômio f por $g_1, \ldots, g_s$ em $\mathbb{K}[x_1, \ldots, x_n]$ pode variar conforme a prioridade dada para os elementos $g_1, \ldots, g_s$, este é um fato que não ocorre para Base de Gröbner, como fica claro no resultado abaixo.

Corolário 2.27. *Se $G = \{g_1, \ldots, g_s\}$ é uma Base de Gröbner para um ideal I com respeito à uma ordem monomial, então o resto da pseudo-divisão de um elemento $f \in \mathbb{K}[x_1, \ldots, x_n]$ pelos elementos de G é único (não importando a enumeração de seus elementos).*

DEM: Consideremos r_1 e r_2 restos da pseudo-divisão de um polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ pelos elementos de G enumerados de alguma forma.

Assim, existem polinômios $p_1, \ldots, p_s, q_1, \ldots, q_s \in \mathbb{K}[x_1, \ldots, x_n]$ tais que $f - \sum_{i=1}^{s} q_i \cdot g_i = r_1$ e $f - \sum_{i=1}^{s} p_i \cdot g_i = r_2$. Deste modo, temos que

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

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

Note que o teorema anterior, nos dá uma solução para a Pergunta 2.10 apresentada na primeira seção deste capítulo. De fato, se G é uma Base de Gröbner para o ideal I, para determinar se um elemento $f \in \mathbb{K}[x_1, \ldots, x_n]$ pertence ou não a I, basta computar o resto da pseudo-divisão de f pelos elementos de G, ou ainda, verificar se existe $g \in G$ tal que $ml(g) \mid ml(f)$. Isto explica porque, não casualmente, conseguimos responder à questão para o caso em que o ideal I é principal ou gerado por um número finito de monômios, tínhamos em nossas mãos uma Base de Gröbner, como constatamos nos Exemplos 2.22 e 2.23.

Desta forma, para nosso objetivo *basta* computar uma Base de Gröbner para o ideal I dado. Tudo estaria concluído se não tivéssemos

passado sob alguns pontos fundamentais. Todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ possui uma Base de Gröbner? Em caso afirmativo, como obter uma delas?

Na sequência, vamos responder a primeira destas perguntas. Já sabemos que ideais principais e ideais monomiais admitem Base de Gröbner, a saber, o próprio conjunto gerador do ideal.

Proposição 2.28. *Todo ideal não nulo I de $\mathbb{K}[x_1, \ldots, x_n]$, possui uma Base de Gröbner com respeito à uma ordem monomial fixada.*

DEM: Seja $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal não nulo e considere o ideal monomial $J = \langle ml(I) \rangle$.

Pelo Teorema 2.14 temos a garantia da existência de um número finito de monômios $m_1, \ldots, m_s \in J$ tais que $J = \langle m_1, \ldots, m_s \rangle$.

Agora escolha elementos $f_1, \ldots, f_s \in I$ tais que $ml(f_i) = m_i$ para todo $i = 1, \ldots, s$. Afirmamos que $G = \{f_1, \ldots, f_s\}$ é uma Base de Gröbner para I. De fato, dado $f \in I$ temos que $ml(f) \in ml(I) \subseteq J$. Assim, existe $i = 1, \ldots, s$ tal que $m_i = ml(f_i) \mid ml(f)$ e por definição temos que $G = \{f_1, \ldots, f_s\}$ é uma Base de Gröbner para I. ■

Mais do que garantir a existência de uma Base de Gröbner para qualquer ideal não nulo I de $\mathbb{K}[x_1, \ldots, x_n]$, o resultado anterior nos dá uma resposta a questão 2.9, ou seja, uma demonstração para o Teorema da Base de Hilbert, que como comentamos, é uma das pérolas da Álgebra Comutativa. Embora enunciemos tal resultado como um corolário do resultado anterior, relembramos que o Teorema da Base de Hilbert é mais abrangente do que o caso apresentado aqui para anéis de polinômios.

Corolário 2.29. (Teorema da Base de Hilbert) *Se I é um ideal de $\mathbb{K}[x_1, \ldots, x_n]$, então I é finitamente gerado.*

DEM: Se $I = \{0\}$, então $\{0\}$ é um conjunto gerador para I. Por outro lado, se $I \neq \{0\}$, então a proposição anterior nos assegura que I admite uma Base de Gröbner com respeito a uma ordem monomial fixada, mas como observamos logo após o Teorema 2.26, uma Base de Gröbner é um conjunto finito de geradores para I. ■

Como uma importante consequência destacamos:

Corolário 2.30. *Sejam $I_i \subseteq \mathbb{K}[x_1, \ldots, x_n]$ com $i \in \mathbb{N}$ ideais tais que $I_i \subseteq I_{i+1}$ para todo $i \in \mathbb{N}$, então existe $m \in \mathbb{N}$ de modo que $I_m = I_{m+j}$ para todo $j \in \mathbb{N}$.*

DEM: Inicialmente note que $I = \bigcup_{i \in \mathbb{N}} I_i \subseteq \mathbb{K}[x_1, \ldots, x_n]$ é um ideal (Exercício), seguindo do Teorema da Base de Hilbert acima que existem $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$ tais que $I = \langle f_1, \ldots, f_r \rangle$.

Para cada $k = 1, \ldots, r$ temos que $f_k \in I_{i_k}$ para algum $i_k \in \mathbb{N}$. Tomando $m = max\{i_1, \ldots, i_r\}$, segue do fato de que $I_i \subseteq I_{i+1}$ que $f_1, \ldots, f_r \in I_m$ e $I \subseteq I_m \subseteq I_{m+1} \subseteq \ldots \subseteq I$. Portanto, temos que $I_m = I_{m+j}$ para todo $j \in \mathbb{N}$. ■

Note que a demonstração do corolário acima utiliza apenas o fato de que todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ é finitamente gerado (Teorema da Base de Hilbert).

O leitor deve ter percebido a ausência de exercícios nesta seção, justamente a que trata do assunto central destas notas. Questões interessantes e computáveis envolveriam necessariamente o cálculo de uma Base de Gröbner para um dado ideal, para o qual até o momento não dispomos de um procedimento para sua obtenção.

Para saciar nossa curiosidade, resta agora tomar conhecimento do método, idealizado por Bruno Buchberger, que permite, a partir de um conjunto finito de geradores de um ideal, encontrar uma Base de Gröbner com respeito a uma ordem monomial fixada. Este é o assunto da próxima seção deste capítulo.

2.4 Algoritmo de Buchberger

Como comentamos no início deste capítulo, os conceitos por trás do método obtido por Buchberger são simples. Vamos introduzir os ingredientes para o procedimento que permitirá obter uma Base de Gröbner a partir de um conjunto finito de geradores de um ideal de $\mathbb{K}[x_1, \ldots, x_n]$.

Definição 2.31. *O* **mínimo múltiplo comum**, *ou simplesmente* MMC, *de dois monômios* $\prod_{i=1}^{n} x_i^{\alpha_i}, \prod_{i=1}^{n} x_i^{\beta_i} \in \mathbb{M}_n$ *é o monômio*

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

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

É realmente fácil constatar que dados $m_1, m_2 \in \mathbb{M}_n$ temos que:

$$m_1 \mid MMC(m_1, m_2), \quad m_2 \mid MMC(m_1, m_2)$$

e se $m_1 \mid m_2$, então $MMC(m_1, m_2) = m_2$.

Exercício 2.32. *Para qualquer ordem monomial* $\preceq$, *mostre que:*

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

para quaisquer $f, g \in \mathbb{K}[x_1, \ldots, x_n] \setminus \{0\}$.

A ideia fundamental do algoritmo que apresentaremos encontra-se no conceito de S-polinômio que apresentamos abaixo.

Definição 2.33. *Fixada uma ordem monomial em* $\mathbb{M}_n$ *e dados elementos* $f, g \in \mathbb{K}[x_1, \ldots, x_n] \setminus \{0\}$, *o* **$S$-polinômio** *ou* **$S$-processo** *de* f *e* g, *que denotamos* $S(f, g)$ *é o polinômio*

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

Exemplo 2.34. *Fixemos a ordem lexicográfica graduada. O* S*-polinômio de* $f = y^2 - x$ *e* $g = xy - y$ *é*

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

Exercício 2.35. *Para qualquer ordem monomial* $\preceq$, *mostre que:*

1. $S(f, g) = -S(g, f)$ *para quaisquer* $f, g \in \mathbb{K}[x_1, \ldots, x_n] \setminus \{0\}$.

2. *Se* $m_1, m_2 \in \mathbb{M}_n$, *então* $S(m_1, m_2) = 0$.

3. *Para quaisquer polinômios* $f, g \in \mathbb{K}[x_1, \ldots, x_n] \setminus \{0\}$ *temos* $ml(S(f,g)) \prec ml\left(MMC(ml(f), ml(g))\frac{f}{tl(f)}\right) = MMC(ml(f), ml(g))$.

Agora estamos aptos a apresentar o resultado crucial para um algoritmo que nos fornece uma Base de Gröbner. Tal resultado, nos dá uma outra caracterização de uma Base de Gröbner via S-polinômios.

Proposição 2.36. *Fixada uma ordem monomial* $\preceq$ *sobre* $\mathbb{M}_n$, *temos que um conjunto* $G = \{g_1, \ldots, g_s\} \subset \mathbb{K}[x_1, \ldots, x_n]$ *é uma Base de Gröbner para o ideal* $I = \langle g_1, \ldots, g_s \rangle$ *com respeito a* $\preceq$ *se, e somente se, o resto da pseudo-divisão de todo* S*-polinômio* $S(g_i, g_j)$ *pelos elementos de* G *é nulo.*

DEM: Se G é uma Base de Gröbner para I, então como todo S-polinômio $S(g_i, g_j)$ de elementos de G é um elemento de I, segue do Teorema 2.26 que o resto da pseudo-divisão de $S(g_i, g_j)$ pelos elementos de G é nulo.

Para a recíproca, vamos supor que o resto da pseudo-divisão de qualquer S-polinômio $S(g_i, g_j)$ pelos elementos de G seja nulo. *Basta* mostrarmos que para todo elemento $f \in I$ existe $g_k \in G$, tal que $ml(g_k) \mid ml(f)$.

Para tanto, dentre todas as representações de f na forma

$$f = \sum_{i=1}^{s} q_i \cdot g_i, \tag{2.1}$$

com $q_1, \ldots, q_s \in \mathbb{K}[x_1, \ldots, x_n]$ tome aquelas para os quais o monômio $m = \max_{1 \leq i \leq s}\{ml(q_i \cdot g_i)\}$ seja o mínino possível e, dentre estas, escolha uma representação de modo que $H = \{j;\ ml(q_j \cdot g_j) = m\}$ tenha o menor número de elementos.

Podemos ter duas situações:

Caso 1: $m = ml(f)$. Neste caso, existe um elemento $g_i \in G$ tal que $ml(g_i) \mid ml(f)$ e G é, por definição, uma Base de Gröbner para I.

Caso 2: $ml(f) \prec m$. Como $ml(f) = ml\left(\sum_{i=1}^{s} q_i \cdot g_i\right)$ devemos ter $\#H \geq 2$, ou seja, existem ao menos duas parcelas na representação

(2.1) com monômios líderes iguais a m. Sem perda de generalidade podemos supor que

$$tl(q_1 \cdot g_1) = -tl(q_2 \cdot g_2). \tag{2.2}$$

Temos que

$$q_1 \cdot g_1 + q_2 \cdot g_2 = tl(q_1) \cdot g_1 + tl(q_2) \cdot g_2 + (q_1 - tl(q_1)) \cdot g_1 + (q_2 - tl(q_2)) \cdot g_2. \tag{2.3}$$

Note que $ml((q_1 - tl(q_1)) \cdot g_1) \prec m$ e $ml((q_2 - tl(q_2)) \cdot g_2) \prec m$. Além disto,

$$\begin{aligned} tl(q_1) \cdot g_1 + tl(q_2) \cdot g_2 &= tl(q_1 \cdot g_1) \cdot \left(\tfrac{tl(q_1) \cdot g_1}{tl(q_1 \cdot g_1)} + \tfrac{tl(q_2) \cdot g_2}{tl(q_1 \cdot g_1)} \right) \\ &\overset{(2.2)}{=} tl(q_1 \cdot g_1) \cdot \left(\tfrac{tl(q_1) \cdot g_1}{tl(q_1 \cdot g_1)} - \tfrac{tl(q_2) \cdot g_2}{tl(q_2 \cdot g_2)} \right) \\ &= tl(q_1 \cdot g_1) \cdot \left(\tfrac{g_1}{tl(g_1)} - \tfrac{g_2}{tl(g_2)} \right) \\ &= \tfrac{tl(q_1 \cdot g_1)}{MMC(ml(g_1), ml(g_2))} S(g_1, g_2). \end{aligned} \tag{2.4}$$

Por hipótese, ao aplicarmos o algoritmo da pseudo-divisão ao S-polinômio $S(g_1, g_2)$ pelos elementos de G, obtemos resto nulo, ou seja, encontramos polinômios $h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$ tais que

$$S(g_1, g_2) = \sum_{i=1}^{s} h_i \cdot g_i, \tag{2.5}$$

e $ml(S(g_1, g_2)) = ml(h_j \cdot g_j)$ para um único índice $j \in \{1, \ldots, s\}$.

Pelo Exercício 2.35, item 3, temos

$$ml(S(g_1, g_2)) \prec ml\left(MMC(ml(g_1), ml(g_2)) \frac{g_1}{tl(g_1)} \right)$$

e assim,

$$\begin{aligned} ml\left(\tfrac{tl(q_1 \cdot g_1)}{MMC(ml(g_1), ml(g_2))} S(g_1, g_2) \right) &= \tfrac{ml(q_1 \cdot g_1)}{MMC(ml(g_1), ml(g_2))} ml(S(g_1, g_2)) \\ &\prec ml(q_1 \cdot g_1) = m. \end{aligned}$$

Substituindo (2.5) em (2.4), e este por sua vez em (2.3), obtemos uma nova representação para f, a saber

$$f = \frac{tl(q_1 \cdot g_1)}{MMC(ml(g_1), ml(g_2))} \sum_{i=1}^{s} h_i \cdot g_i + (q_1 - tl(q_1)) \cdot g_1 + (q_2 - tl(q_2)) \cdot g_2 + \sum_{i=3}^{s} q_i \cdot g_i \tag{2.6}$$

Agora observe que nesta nova representação para f, as únicas parcelas que podem ter monômio líder igual a m estão em $\sum_{i=3}^{s} q_i \cdot g_i$.

Se não houver uma tal parcela, então a representação (2.1) foi mal escolhida, pois (2.6) contraria a minimalidade de m.

Se por outro lado, existe uma parcela em $\sum_{i=3}^{s} q_i \cdot g_i$ com monômio líder m, então a representação (2.1) não é uma que possui $\sharp H$ mínimo[2].

Qualquer uma destas possibilidades nos levam a uma contradição, permitindo concluir que apenas o Caso 1 pode ocorrer, ou seja, existe $g_i \in G$ tal que $ml(g_i) \mid ml(f)$ e portanto G é uma Base de Gröbner para o ideal I. ■

A demonstração rebuscada do resultado acima pode obscurecer a ferramenta poderosa que temos em mãos.

Antes de apresentar o algoritmo formulado por Buchberger, façamos algumas observações sobre as ideias contidas nesse procedimento.

O ponto central, que é ao mesmo tempo, simples e genial, é partir de um conjunto finito de geradores F de um ideal não nulo I de $\mathbb{K}[x_1, \ldots, x_n]$ e acrescentar elementos de I tais que o seus monômios líderes não são divisíveis pelos monômios líderes dos elementos do conjunto de geradores, a saber, acrescentamos o resto da pseudo-divisão dos S-polinômios dos geradores do ideal por F, sempre que tal resto for não nulo. Deste modo, obtemos um novo conjunto de geradores de I para o qual aplicamos novamente o procedimento.

Como veremos abaixo, este processo é finito, o que o torna um algoritmo e passível de implementação. Mais ainda, o conjunto de geradores obtido após a aplicação deste processo é uma Base de Gröbner para o ideal gerado por F.

Teorema 2.37. (Algoritmo de Buchberger) *Fixada uma ordem monomial e dado* $\{g_1, \ldots, g_s\} \subset \mathbb{K}[x_1, \ldots, x_n]$*, podemos obter uma*

[2]O símbolo $\sharp$ indica número de elementos.

Base de Gröbner G para o ideal $I = \langle g_1, \ldots, g_s \rangle$ aplicando o seguinte algoritmo:

ALGORITMO DE BUCHBERGER

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

DEM: Se em algum momento a condicional "SE" dada nos procedimentos acima for negativa, então pela proposição anterior, G_i é uma Base de Gröbner para o ideal gerado por G_i e consequentemente para I, uma vez que todos os S-polinômios dos elementos de G_i deixam resto nulo na pseudo-divisão por G_i.

Resta mostrarmos que a referida negativa ocorre após um número finito de passos.

Suponha que o procedimento acima nunca finalize. Neste caso, teríamos uma sequência infinita de conjuntos

$$G_1 \subsetneq G_2 \subsetneq \cdots \subsetneq G_i \subsetneq \cdots,$$

onde G_{i+1} é obtido a partir de G_i pela adjunção de um elemento $r \neq 0$ tal que $ml(g) \nmid ml(r)$ para todo $g \in G_i$.

Deste modo, teríamos uma sequência infinita de ideais monomiais

$$\langle ml(G_1) \rangle \subsetneq \langle ml(G_2) \rangle \subsetneq \cdots \subsetneq \langle ml(G_i) \rangle \subsetneq \cdots.$$

No entanto, isto não pode ocorrer, pois como vimos no Teorema 2.14, todo ideal monomial de $\mathbb{K}[x_1, \ldots, x_n]$ é finitamente gerado. ■

Não nos preocuparemos com a questão de otimização do algoritmo acima, no entanto algumas observações merecem destaque. Por exemplo, é claro que se o S-polinômio $S(f,g)$ tem resto nulo na pseudo-divisão por um conjunto de polinômios, então $h \cdot S(f,g)$ também o terá para qualquer $h \in \mathbb{K}[x_1, \ldots, x_n]$, em particular, isto nos diz que analisando o S-polinômio $S(f,g)$ não temos que nos preocupar com o S-polinômio $S(g,f)$.

Além disto, observe que se um S-polinômio fornece resto não nulo r na pseudo-divisão por um conjunto G_i, então, no passo seguinte do algoritmo de Buchberger, este mesmo S-polinômio terá resto nulo na pseudo-divisão pelo conjunto G_{i+1} uma vez que $G_{i+1} = G_i \cup \{r\}$.

Estas observações embora imediatas permitem diminuir nossos esforços na aplicação do algoritmo.

É o momento de apresentarmos um exemplo da aplicação do algoritmo acima. Dentre todas as escolhas que nos ocorre, nenhuma parece ser melhor do que retomar o Exemplo 2.24, onde apresentamos um conjunto de geradores de um ideal que não é uma Base de Gröbner.

Exemplo 2.38. *Fixemos a ordem lexicográfica graduada. Como vimos no Exemplo 2.24, o conjunto* $\{f = y^2 - x, g = xy - y\}$ *não é uma Base de Gröbner para o ideal* $I = \langle f, g \rangle$*. Vamos aplicar o algoritmo de Buchberger, a fim de obter uma tal base.*

Passo 1: *Consideramos* $G_1 = \{f, g\}$*. Como vimos no Exemplo 2.34,* $S(f,g) = -x^2 + y^2$*, cujo resto da pseudo-divisão pelos elementos de* G_1 *é* $h = -x^2 + x$*.*

Passo 2: *Agora consideramos* $G_2 = \{f, g, h\}$*. Os S-polinômios que merecem análise são* $S(f,h) = y^4 - x^3$ *e* $S(g,h) = y^3 - xy$*, lembre-se que pelo comentário acima, não necessitamos nos atentar à* $S(f,g)$ *neste passo.*

Como $S(f,h) = (y^2+1) \cdot f + y \cdot g + (x+1) \cdot h$ *e* $S(g,h) = y \cdot f$*, ou seja, o resto da divisão por* G_2 *é nulo, temos que* $G = G_2 = \{y^2 - x, xy - y, -x^2 + x\}$ *é uma Base de Gröbner para* I*.*

Recomendamos a resolução do exercício abaixo, uma vez que o utilizaremos em outras passagens destas notas.

Exercício 2.39. *Calcule uma Base de Gröbner para os seguintes ideais, utilizando a ordem lexicográfica e a ordem lexicográfica graduada.*

1. $\langle x^4 + y^5, x^4 + y^5 + 1\rangle \subset \mathbb{C}[x, y]$.
2. $\langle x^2 + y^2 + z^2 - 4, x^2 + 2y^2 - 5, xy - 1\rangle \subset \mathbb{C}[x, y, z]$.
3. $\langle x^4-3y^3+z^2-1, x^4+y^4-2z-2, y^4+3y^3-z^2-2z+1\rangle \subset \mathbb{C}[x, y, z]$.
4. $\langle x^2 + 2y^2 - y - 2z, x^2 - 8y^2 + 10z, x^2 - 7yz\rangle \subset \mathbb{C}[x, y, z]$.
5. $\langle x^2 + y^2 + z^2 - 2x, -yz - x, x - y + 2z\rangle \subset \mathbb{C}[x, y, z]$.
6. $\langle x + y - z - 2, x - y + z, 2x + 2y - 2z - 2\rangle \subset \mathbb{C}[x, y, z]$.

O leitor deve ter observado que nos referimos sempre a *uma* Base de Gröbner, o que sugere que um ideal pode admitir várias Bases de Gröbner. Isto é evidente ao observarmos que se acrescentarmos um elemento qualquer do ideal à uma Base de Gröbner, continuamos com uma Base de Gröbner.

Isto sugere que podemos ter elementos redundantes em uma Base de Gröbner, ou seja, elementos que podemos desconsiderar de modo ainda a continuar com uma tal base. A proposição abaixo indica como proceder tal mecanismo.

Proposição 2.40. *Seja $G = \{g_1, \ldots, g_s\}$ uma Base de Gröbner para um ideal I com respeito à uma ordem monomial fixada. Se temos $ml(g_i) \mid ml(g_j)$ para $i, j \in \{1, \ldots, s\}$ com $i \neq j$, então $H = G \setminus \{g_j\}$ é ainda uma Base de Gröbner para I.*

Dem: Seja $f \in I$. Como G é uma Base de Gröbner para I, existe $g_k \in G$ tal que $ml(g_k) \mid ml(f)$. Se $g_k \neq g_j$, então $g_k \in H$. Por outro lado, se $g_k = g_j$, então como $ml(g_i) \mid ml(g_j) = ml(g_k)$ e $ml(g_k) \mid ml(f)$ temos que $ml(g_i) \mid ml(f)$ e $g_i \in H$. Portanto, de qualquer modo, dado $f \in I$ existe $g \in H$ tal que $ml(g) \mid ml(f)$, indicando assim, que H é uma Base de Gröbner para I. ■

O resultado anterior clama por uma definição.

Definição 2.41. *Seja G uma Base de Gröbner para um ideal I com respeito à uma ordem monomial. Dizemos que G é uma* **Base de Gröbner Mínima** *para I, se temos $ml(g_i) \nmid ml(g_j)$ para todos $g_i, g_j \in G$ com $g_i \neq g_j$.*

Um fato que decorre facilmente, é que duas Bases de Gröbner mínimas G e H de um ideal I, com respeito à uma mesma ordem monomial, possuem o mesmo número de elementos. De fato, para cada $g \in G$ temos $f, h \in H$ tais que $ml(f) \mid ml(g)$ e $ml(g) \mid ml(h)$, ou seja, $ml(f) \mid ml(h)$. Como H é Base de Gröbner mínima, segue que $f = h$ e $ml(g) = ml(f)$, o que estabelece uma bijeção entre os elementos de G e H.

Mesmo possuindo o mesmo número de elementos, não podemos garantir a unicidade de uma Base de Gröbner mínima para um ideal com respeito à uma ordem monomial fixada. Isto é facilmente verificado no próximo exemplo.

Exemplo 2.42. *Como tivemos a oportunidade de verificar no Exemplo 2.38, o conjunto* $G = \{y^2 - x, xy - y, -x^2 + x\}$ *é uma Base de Gröbner para o ideal* $I = \langle y^2 - x, xy - y\rangle$ *com respeito à ordem lexicográfica graduada.*

Substituindo $-x^2 + x$ *por* $-x^2 + y^2 = (-x^2 + x) + (y^2 - x) \in I$, *temos que* $H = \{y^2 - x, xy - y, -x^2 + y^2\}$ *é também uma Base de Gröbner para* I.

É imediato verificar que ambas são mínimas e que $G \neq H$.

Exercício 2.43. *Encontre uma Base de Gröbner mínima a partir de cada uma das Bases de Gröbner obtidas no Exercício 2.39.*

Podemos no entanto, refinar um pouco mais nossas exigências sobre Bases de Gröbner.

Definição 2.44. *Uma Base de Gröbner Mínima* G *para um ideal* I *é chamada de* **Base de Gröbner Reduzida**, *com respeito à uma ordem monomial, se os elementos de* G *são mônicos e para qualquer* $g_i \in G$, $ml(g_j) \nmid m$ *para todo* $m \in \mathbb{M}(g_i)$ *com* $i \neq j$ *e para todo* $m \in \mathbb{M}(g_j) \setminus \{ml(g_j)\}$.

Todo ideal não nulo admite uma Base de Gröbner reduzida?

Em caso afirmativo, como obter uma tal base?

Podemos garantir que uma Base de Gröbner reduzida para um ideal é única?

Responderemos a todas estas questões de uma só vez por meio do seguinte resultado.

Proposição 2.45. *Fixada uma ordem monomial e dado um ideal $I = \langle g_1, \ldots, g_s \rangle$ não nulo de $\mathbb{K}[x_1, \ldots, x_n]$, existe uma única Base de Gröbner reduzida.*

DEM: **(Existência)** Tomemos uma Base de Gröbner mínima G para o ideal I, cuja existência é garantida pela Proposição 2.40. Trocando cada elemento $g \in G$ por $\frac{g}{cl(g)}$, continuamos com uma Base de Gröbner mínima cujos elementos são mônicos.

Agora para cada $g \in G$ considere o resto r_g da pseudo-divisão de $g - ml(g)$ pelos elementos de G. Note que $g - ml(g) = \sum_{i=1}^{s} q_i \cdot g_i + r_g$ e $ml(g) + r_g = g - \sum_{i=1}^{s} q_i \cdot g_i \in I$. Deste modo, temos que o conjunto $H = \{ml(g) + r_g;\ g \in G\}$ é uma Base de Gröbner reduzida de I.

(Unicidade) Tomemos G e H duas Bases de Gröbner reduzidas para o ideal I com respeito à ordem monomial fixada, em particular, Bases de Gröbner mínimas. Assim, G e H possuem o mesmo número de elementos.

Para cada $g \in G$, existe $h \in H$ tal que $ml(g) = ml(h)$, cuja existência é garantida pelo comentário que segue a Definição 2.41. Se tivéssemos $g \neq h$, então $g - h \in I \setminus \{0\}$. Mas deste modo, teríamos que $m = ml(g-h) \neq ml(g) = ml(h)$. Como $g - h \in I \setminus \{0\}$ existiriam elementos de G e H com monômios líderes iguais que dividiriam o monômio $m \in \mathbb{M}(g) \cup \mathbb{M}(h)$, mas isto não pode ocorrer, pois G e H são Bases de Gröbner reduzidas. Seguindo que $g = h$, e consequentemente, $G = H$. ■

Exemplo 2.46. *O Exemplo 2.42 nos garante que o conjunto dado por $\{y^2 - x, xy - y, -x^2 + x\}$ é uma Base de Gröbner mínima para $I = \langle y^2 - x, xy - y \rangle$ com respeito à ordem lexicográfica graduada. Aplicando o método descrito na demonstração da proposição anterior, temos que $G = \{y^2 - x, xy - y, x^2 - x\}$ é a Base de Gröbner reduzida para I.*

Exercício 2.47. *Encontre a Base de Gröbner reduzida para cada ideal dado no Exercício 2.39, a partir de uma Base de Gröbner mínima obtida no Exercício 2.43.*

2.4.1 Implementações

O algoritmo de Buchberger não reserva dificuldades para implementação em *softwares* de manipulação algébrica. A maioria dos aplicativos que manipulam polinômios contém alguma rotina que calcula uma Base de Gröbner para um ideal.

Citemos alguns dos sistemas mais difundidos.

CoCoA (*Computations in Commutative Algebra*) *software* gratuito e disponível em *http://cocoa.dima.unige.it*.

Maple cujo *site* oficial *http://www.maplesoft.com* é um *software* comercial.

Mathematica programa computacional algébrico comercial cujo *site* oficial é *http://www.wolfram.com*.

Singular disponível em *http://www.singular.uni-kl.de* gratuitamente.

Algumas das aplicações mais interessantes e não triviais das Bases de Gröbner envolvem ideais com um número relativamente grande de geradores em muitas variáveis o que pode tornar a aplicação do algoritmo de Buchberger uma tarefa árdua e nada estimulante sem uso de um sistema computacional. Deste modo, não mais indicaremos os passos intermediários, como cálculo de S-processos e pseudo-divisões, apresentando apenas a Base de Gröbner do ideal manipulado, para as quais utilizamos, na maioria das vezes, um sistema computacional algébrico.

Capítulo 3

Aplicações

Bases de Gröbner para ideais de $\mathbb{K}[x_1, \ldots, x_n]$ reservam interessantes aplicações nos mais variados ramos da matemática.

Não é uma tarefa fácil selecionar que aplicações abordar nestas notas. Optamos por três delas que aparentemente sugerem áreas distintas da matemática: estudar sistemas de equações polinomiais (um problema algébrico), como decidir se um mapa pode ser colorido utilizando apenas três cores (um problema de origem topológica) e como validar construções realizadas com Origami (um problema cujas raízes são geométricas).

O leitor sentirá diferença da abordagem feita nos capítulos anteriores e este. Enquanto nos anteriores nosso objetivo era apresentar com detalhes e rigor os resultados para construir uma base sólida da teoria, neste capítulo objetivamos as aplicações.

3.1 Sistemas de Equações Polinomiais

Uma das aplicações mais poderosas e conhecidas das Bases de Gröbner, encontra-se no estudo de sistemas de equações polinomiais, ou seja, sistemas da forma

$$f_1 = \cdots = f_m = 0, \tag{3.1}$$

onde $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ para $i = 1, \ldots, m$.

Para facilitar nossas considerações e fazer uso de algumas poderosas ferramentas de Geometria Algébrica, a partir deste ponto vamos considerar $\mathbb{K} = \mathbb{C}$. Na verdade, poderíamos considerar um *corpo algebricamente fechado*[1] qualquer.

Por "estudar" um sistema como (3.1), entendemos poder decidir se o sistema admite solução(ões). Caso o sistema possua solução(ões) gostaríamos de avaliar o número delas e em caso de um número finito determinar todas elas.

Embora o conceito de solução do sistema (3.1) é bem intuitivo, sejamos mais rigorosos.

Dado $f = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} \in \mathbb{C}[x_1, \ldots, x_n]$ dizemos que um elemento $(z_1, \ldots, z_n) \in \mathbb{C}^n$ é uma **solução** de $f = 0$, se

$$f(z_1, \ldots, z_n) = \sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} z_i^{\alpha_i} = 0.$$

Uma **solução para o sistema** (3.1) é uma solução de $f_i = 0$ para todo $i = 1, \ldots, m$.

O primeiro resultado que apresentaremos é o único destas notas que não vamos demonstrar completamente. Uma demonstração provocaria um desvio de nossa rota e atrasaríamos a aplicação propriamente dita das Bases de Gröbner que temos em mente.

Teorema 3.1. (Teorema dos Zeros de Hilbert-Versão Fraca) *O sistema (3.1) admite solução se, e somente se,*

$$1 \notin \langle f_1, \ldots, f_m \rangle.$$

Dem: Inicialmente note que as soluções do sistema (3.1) são soluções de qualquer elemento $f \in \langle f_1, \ldots, f_m \rangle$.

De fato, se $f \in \langle f_1, \ldots, f_m \rangle$, então $f = h_1 \cdot f_1 + \ldots + h_m \cdot f_m$ com $h_1, \ldots, h_m \in \mathbb{C}[x_1, \ldots, x_n]$. Agora, se $(z_1, \ldots, z_n) \in \mathbb{C}^n$ é solução do

[1] Dizemos que um corpo $\mathbb{K}$ é **algebricamente fechado**, se todo $f \in \mathbb{K}[x]$, se expressa como produto de fatores lineares, isto é, $f = \alpha \cdot (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k)$, com $\alpha, \alpha_1, \ldots, \alpha_k \in \mathbb{K}$.

sistema, então

$$f(z_1,\ldots,z_n)=\sum_{i=1}^{m}h_i(z_1,\ldots,z_n)f_i(z_1,\ldots,z_n)=0.$$

Deste modo, se $1\in\langle f_1,\ldots,f_m\rangle$, então o sistema considerado não admite solução.

Para a recíproca veja Teorema 1 do Capítulo 4 de [S]. ■

O resultado anterior determina um modo de verificar se um sistema $f_1=\ldots=f_m=0$ com $f_1,\ldots,f_m\in\mathbb{C}[x_1,\ldots,x_n]$ possui ou não solução utilizando a teoria apresentada no capítulo anterior, pois como vimos no Teorema 2.26, basta calcular uma Base de Gröbner G para o ideal $\langle f_1,\ldots,f_m\rangle$ e utilizar o algoritmo da pseudo-divisão para verificar se o resto de 1 por G é nulo ou não.

Uma variante do teorema anterior que nos auxiliará, é a que apresentamos em seguida.

Teorema 3.2. (Teorema dos Zeros de Hilbert-Versão Forte) *Sejam $f,f_1,\ldots,f_m\in\mathbb{C}[x_1,\ldots,x_n]\setminus\{0\}$. A equação $f=0$ admite todas as soluções do sistema $f_1=\cdots=f_m=0$ se, e somente se, existe $s\in\mathbb{N}\setminus\{0\}$ tal que $f^s\in\langle f_1,\ldots,f_m\rangle$.*

Dem: Claramente, se $f^s\in\langle f_1,\ldots,f_m\rangle$ para algum $s\in\mathbb{N}\setminus\{0\}$, então toda solução do sistema $f_1=\cdots=f_m=0$ é também uma solução de $f^s=0$ e consequentemente, da equação $f=0$.

Para a recíproca, considere uma indeterminada auxiliar y e tome o ideal $J=\langle f_1,\ldots,f_m,g\rangle\subset\mathbb{C}[x_1,\ldots,x_n,y]$, com $g=1-yf$. Vamos mostrar que $1\in J$.

Se $(z_1,\ldots,z_n,z)\in\mathbb{C}^{n+1}$ é uma solução de $f_1=\cdots=f_m=g=0$, então temos $h(z_1,\ldots,z_n)=0$ para todo elemento $h\in I$ e assim $0=g(z_1,\ldots,z_n,z)=1-zf(z_1,\ldots,z_n)=1$, um absurdo!

Assim, o sistema $f_1=\cdots=f_m=g=0$ não admite solução e, pelo teorema anterior, temos que $1\in J=\langle f_1,\ldots,f_m,g\rangle$, ou seja, existem $h,h_1,\ldots,h_m\in\mathbb{C}[x_1,\ldots,x_n,y]$, tais que

$$1=hg+\sum_{i=1}^{m}h_if_i=h\cdot(1-y\cdot f)+\sum_{i=1}^{m}h_i\cdot f_i.$$

Substituindo y por $\frac{1}{f}$ na equação acima temos

$$1 = \sum_{i=1}^{m} h_i \left(x_1, \ldots, x_n, \frac{1}{f} \right) \cdot f_i(x_1, \ldots, x_n).$$

Podemos eliminar os denominadores da última expressão multiplicando por uma potência f^s conveniente, donde obtemos polinômios $g_1, \ldots, g_m \in \mathbb{C}[x_1, \ldots, x_n]$ tais que $f^s = \sum_{i=1}^{m} g_i \cdot f_i \in I$. ■

Extraindo o essencial do teorema anterior, temos:

Corolário 3.3. *Sejam f um polinômio e $I = \langle f_1, \ldots, f_m \rangle$ um ideal de $\mathbb{C}[x_1, \ldots, x_n]$. A equação $f = 0$ admite todas as soluções do sistema $f_1 = \cdots = f_m = 0$ se, e somente se,*

$$1 \in \langle f_1, \ldots, f_m, 1 - yf \rangle \subseteq \mathbb{C}[x_1, \ldots, x_n, y].$$

DEM: Segue diretamente dos argumentos contidos na demonstração do teorema anterior. ■

Antes de continuarmos as considerações sobre um sistema polinomial qualquer, vejamos um exemplo que retrata uma situação particular, um sistema linear.

Exemplo 3.4. *Considere o sistema*

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

Tomando o ideal $I = \langle 2x+y+z+1, 3x-y+2z+1, -x+y-z \rangle$ e calculando uma Base de Gröbner G com respeito à ordem lexicográfica temos

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

e facilmente verificamos que $1 \notin I$*, ou seja, o sistema admite solução.*

Além disto, note que uma Base de Gröbner mínima para o ideal I *é dada por* $\{2x+y+z+1, 5y-z+1, -2z+2\}$ *e a Base de Gröbner reduzida é* $\{x+1, y, z-1\}$*.*

O exemplo anterior chama a atenção para um fato curioso: a Base de Gröbner mínima para o ideal gerado pelas equações do sistema, nos forneceu um novo sistema escalonado e que claramente é equivalente, isto é, possui as mesmas soluções do sistema original. Além disto, a Base de Gröbner reduzida nos presenteou com um sistema, equivalente ao original, cuja solução não poderia ser mais fácil de ser obtida, a saber $x = -1, y = 0$ e $z = 1$.

Na verdade, nas entrelinhas do que se esconde neste exemplo reside um modo de obter as soluções de um sistema como (3.1).

O teorema abaixo evidencia e esclarece os detalhes ocultos no exemplo anterior.

Teorema 3.5. *Sejam* $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$*. O sistema de equações* $f_1 = \cdots = f_m = 0$ *admite um número finito de soluções se, e somente se, ao considerarmos* $I = \langle f_1, \ldots, f_m \rangle$*, com respeito à ordem lexicográfica,* $x_i^{\gamma_i} \in ml(I)$ *para algum* $\gamma_i \in \mathbb{N} \setminus \{0\}$ *e todo* $i = 1, \ldots, n$*.*

Dem: Se o sistema $f_1 = \cdots = f_m = 0$ admite um número $k > 0$ de soluções

$$(z_{11}, \ldots, z_{n1}), \ldots, (z_{1k}, \ldots, z_{nk}) \in \mathbb{C}^n,$$

então os possíveis valores para as i-ésimas coordenadas das soluções, satisfazem $h_i = \prod_{j=1}^{\alpha_i}(x_i - z_{ij}) = x_i^{\alpha_i} + \cdots + a_{i1}x + a_{i0} \in \mathbb{C}[x_i]$ com $0 < \alpha_i \leq k$. Como as soluções do sistema $f_1 = \cdots = f_m = 0$ são soluções de $h_i = 0$, pelo Corolário 3.3 existe $\beta_i \in \mathbb{N} \setminus \{0\}$ tal que $h_i^{\beta_i} \in \langle f_1, \ldots, f_m \rangle$ e consequentemente $ml(h_i^{\beta_i}) = x_i^{\alpha_i \beta_i} \in ml(I)$ para todo $i = 1, \ldots, n$.

Para a recíproca, lembremos que com respeito à ordem lexicográfica temos $x_n \prec_L x_{n-1} \prec_L \ldots \prec_L x_2 \prec_L x_1$.

Por hipótese, existe $\gamma_i \in \mathbb{N}$ de modo que $x_i^{\gamma_i} \in ml(I)$ para todo $i = 1, \ldots, n$, então temos $g_n \in I$, tal que $ml(g_n) = x_n^{\gamma_n}$, além disto, a ordem lexicográfica nos garante que $g_n \in \mathbb{C}[x_n]$ e o número de soluções de $g_n = 0$ é limitado por $gr_{x_n}(g_n) = \gamma_n$.

Como $x_{n-1}^{\gamma_{n-1}} \in ml(I)$, temos um elemento $g_{n-1} \in I$ tal que $ml(g_{n-1}) = x_{n-1}^{\gamma_{n-1}}$. Como estamos considerando a ordem lexicográfica segue que $g_{n-1} \in \mathbb{C}[x_{n-1}, x_n]$.

Para cada solução $z_n \in \mathbb{C}$ de $g_n = 0$, temos um número finito de soluções para $g_{n-1}(x_{n-1}, z_n)$, a saber, limitado por $gr_{x_{n-1}}(g_{n-1}) = \gamma_{n-1}$. Deste modo, o número de soluções de $g_n = g_{n-1} = 0$ é finito e limitado por $\gamma_{n-1} \cdot \gamma_n$.

Procedendo deste modo, podemos garantir a existência de polinômios $g_1, \ldots, g_n \in I$ com $g_i \in \mathbb{C}[x_i, \ldots, x_n]$ e $ml(g_i) = x_i^{\gamma_i}$ para todo $i = 1, \ldots, n$ cujo número de soluções de $g_1 = \ldots = g_n = 0$ é finito e limitado por $\gamma_1 \cdot \ldots \cdot \gamma_n$.

Agora, como $g_i \in I$, ou seja, $g_i = \sum_{j=1}^{m} q_j f_j$ com $q_j \in \mathbb{C}[x_1, \ldots, x_n]$, temos que todas as soluções de $f_1 = \cdots = f_m = 0$ são também soluções de $g_1 = \cdots = g_n = 0$. Como este último sistema admite apenas um número finito de soluções, o mesmo acontece com o sistema original. ■

Observe que o teorema anterior, mais do que uma condição necessária e suficiente para que um sistema de equações polinomiais admita um número finito de soluções, nos fornece um modo de encontrar tais soluções, basta para tanto, tomar uma Base de Gröbner mínima ou reduzida para o ideal gerado pelos polinômios que define o sistema.

Analisando o método descrito na demonstração do resultado acima, vemos que no caso de um sistema de equações lineares, o processo da eliminação Gaussiana que efetuamos normalmente, corresponde ao processo de redução dos S-polinômios obtidos pelas equações que definem o sistema. Ou seja, o método descrito na demonstração do resultado anterior pode ser considerado como uma generalização da Eliminação Gaussiana.

Vejamos um exemplo do estudo de um sistema de equações polinomiais não lineares.

Exemplo 3.6. *Vamos encontrar as soluções, caso existam e sejam em um número finito, do sistema de equações polinomiais*

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

Ao computarmos uma Base de Gröbner mínima para o ideal I dado por $\langle x^2+y^2+z^2-4, x^2+2y^2-5, xz-1\rangle$ com respeito à ordem lexicográfica, obtemos

$$G = \{x + 2z^3 - 3z, y^2 - z^2 - 1, 2z^4 - 3z^2 + 1\}.$$

Constatamos que $1 \notin I$, ou seja, o sistema admite solução e, uma vez que $x, y^2, z^4 \in ml(I)$, o último teorema garante que o sistema dado tem um número de soluções menor ou igual a

$$gr_x(x^2 + 2z^3 - 3z) \cdot gr_y(y^2 - z^2 - 1) \cdot gr_z(2z^4 - 3z^2 + 1) = 8.$$

Além disto, podemos obter todas as soluções. De fato, a equação $2z^4 - 3z^2 + 1 = 0$ admite como solução ± 1 e $\pm\frac{\sqrt{2}}{2}$.

Substituindo cada uma das possibilidades em $x + 2z^3 - 3z = 0$ e $y^2 - z^2 - 1 = 0$, temos que as soluções do sistema são:

$$\left\{\left(1, \pm\sqrt{2}, 1\right), \left(-1, \pm\sqrt{2}, -1\right), \left(\sqrt{2}, \pm\frac{\sqrt{6}}{2}, \frac{\sqrt{2}}{2}\right), \left(-\sqrt{2}, \pm\frac{\sqrt{6}}{2}, -\frac{\sqrt{2}}{2}\right)\right\}.$$

Exercício 3.7. *Estude os sistemas polinomiais abaixo.*
Caso possuam um número finito de solução, determine-as.

1. $\langle x^4-3y^3+z^2-1, x^4+y^4-2z-2, y^4+3y^3-z^2-2z+1\rangle \in \mathbb{C}[x,y,z]$.
2. $\langle x^2 + 2y^2 - y - 2z, x^2 - 8y^2 + 10z, x^2 - 7yz\rangle \in \mathbb{C}[x,y,z]$.
3. $\langle x^2 + y^2 + z^2 - 2x, -yz - x, x - y + 2z\rangle \in \mathbb{C}[x,y,z]$.

3.2 Coloração de Mapas

Tome ou, mais radicalmente, desenhe um mapa com regiões bem delimitadas. Qual o número mínimo de cores necessárias para colorir o mapa de forma que regiões vizinhas[2] não recebam uma mesma cor?

Esta questão foi levantada pela primeira vez em 1852 por Francis Guthrie, enquanto coloria um mapa da Inglaterra. Guthrie conjecturou que o número mínimo de cores necessárias para colorir *qualquer* mapa seria quatro. Tal conjectura ficou conhecida como o *Problema das quatro cores.*

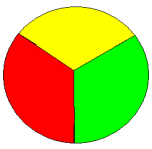
[2]Regiões que se tocam em apenas um ponto não são consideradas vizinhas.

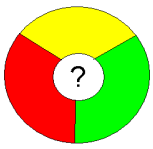
A primeira *demonstração* para este fato foi dada em 1976 por Kenneth Appel e Wolfgang Haken e se baseia na redução a um número finito de situações a serem testadas. Para se ter uma ideia, o número de situações era tão grande que foram necessárias mais de mil horas de uso de computadores de alta velocidade. Tal fato causou polêmica, uma vez que os cálculos envolvidos são impossíveis de serem verificados humanamente.

Em 1994, no Congresso Internacional de Matemática, em Zurique, Paul D. Seymour, Neil Robertson, Daniel P. Sanders e Robin Thomas apresentaram uma demonstração simplificada para o Teorema das Quatro Cores, reduzindo a quantidade de cálculos para um nível tolerável. No entanto, ainda não conseguiram dispensar o uso de computador, fato que continua a despertar o interesse de muitos.

O problema das quatro cores pode ser reformulado em termos de grafos. No entanto, não será esta nossa abordagem. Na verdade, estaremos interessados em um problema derivado do Teorema das Quatro Cores.

Uma vez que todo mapa pode ser colorido com quatro cores e é imediato decidir se um mapa pode ser colorido com duas cores, basta não termos regiões com uma tríplice fronteira, a questão que se põe é de como decidir se um mapa pode ser colorido utilizando apenas 3 cores? Em caso afirmativo, como proceder a coloração?





Para apresentar uma solução para este problema, que chamaremos de **Problema das Três Cores**, vamos "algebrizar" tal questão, ou seja, vamos expressar por meio de um sistema de equações polinomiais todas as informações necessárias para caracterizar a situação observada no mapa dado.

Para modelagem do problema iremos utilizar alguns resultados sobre números complexos, mais especificamente, sobre raízes da unidade, que para comodidade do leitor reunimos na subseção a seguir.

3.2.1 Raízes da Unidade

Vamos recordar alguns fatos e resultados sobre números complexos os quais utilizaremos em nossa abordagem na subseção seguinte.

O Teorema Fundamental da Álgebra assegura que todo polinômio $p \in \mathbb{C}[x]$ admite $gr(p)$ raízes. Deste modo, o polinômio $p = x^n - 1$ admite n raízes que chamamos de **raízes n-ésimas da unidade**.

As raízes n-ésimas da unidade são todas distintas e são precisamente os elementos do conjunto

$$U_n = \left\{ cos\left(\frac{2k\pi}{n}\right) + i \cdot sen\left(\frac{2k\pi}{n}\right); k = 0, \ldots, n-1 \right\}.$$

O número complexo

$$\omega = cos\left(\frac{2\pi}{n}\right) + i \cdot sen\left(\frac{2\pi}{n}\right)$$

é chamado uma **raiz primitiva n-ésima da unidade** e temos que

$$\omega^k = cos\left(\frac{2k\pi}{n}\right) + i \cdot sen\left(\frac{2k\pi}{n}\right),$$

ou seja, as raízes n-ésimas da unidade são $\{\omega^k; k = 0, \ldots, n-1\}$.

Exercício 3.8. *Sejam $1, \omega$ e ω^2 as raízes cúbicas da unidade, isto é, as raízes do polinômio $p = x^3 - 1$. Mostre que as únicas soluções da equação $y_1 + y_2 + y_3 = 0$ tais que $y_i \in U_3 = \{1, \omega, \omega^2\}$ são aquelas para as quais y_1, y_2 e y_3 assumem valores todos distintos.*

3.2.2 O Problema das Três Cores

Vejamos agora com modelar o problema das três cores.

Inicialmente, indicaremos cada uma das cores a serem usadas por uma raiz cúbica da unidade, usando as notações da seção anterior, as três cores serão interpretadas como $1, \omega$ e ω^2.

Cada uma das regiões será representada por uma indeterminada. Assim, se o mapa consiste de n regiões, o anel de polinômios considerado será $\mathbb{C}[x_1, \ldots, x_n]$.

Note que, podemos expressar o fato de que cada região pode ser colorida por uma das cores, isto é, $1, \omega$ ou ω^2, indicando que a resposta para o problema, encontra-se entre as soluções do sistema

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

Ainda devemos "equacionar" a restrição de que duas regiões vizinhas x_i e x_j não podem ser coloridas com uma mesma cor. Isto pode ser feito observando que $x_i^3 = x_j^3$, ou ainda,

$$x_i^3 - x_j^3 = (x_i - x_j) \cdot (x_i^2 + x_i x_j + x_j^2) = 0.$$

Como $x_i - x_j$ não deve ser nulo, pois isto indicaria que as regiões x_i e x_j receberiam a mesma cor, devemos ter $x_i^2 + x_i x_j + x_j^2 = 0$.

Agora estamos aptos a resolver o problema. De fato, para decidir se um mapa M de n regiões pode ser colorido com três cores, de modo que regiões adjacentes recebam cores distintas, basta estudar o sistema

$$\begin{cases} x_i^3 - 1 = 0 \\ x_j^2 + x_j x_k + x_k^2 = 0 \end{cases} \tag{3.2}$$

onde $i = 1, \ldots, n$, x_j e x_k percorrem todas as regiões que possuem fronteira comum.

Como vimos, no Teorema 3.1, o problema tem solução se $1 \notin I$, onde I é o ideal gerado pelos polinômios envolvidos no sistema (3.2).

Para ilustrar o descrito acima, verifiquemos se é possível colorir a região nordeste do território brasileiro, usando apenas três cores.

Para tanto, vamos utilizar a seguinte associação:

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

Figura 3.1: Região Nordeste do Brasil.

Observando as regiões no mapa, o sistema a ser estudado é

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

com $i = 1, \ldots, 9$ e $(j,k) \in \{(1,2),(2,3),(2,6),(2,9),(3,4),(3,5),(3,6),(4,5),(5,6),(6,7),(6,9),(7,8),(7,9),(8,9)\}$.

O próximo passo é aplicar o algoritmo de Buchbeger para o ideal I gerado pelos polinômios envolvidos no sistema anterior com respeito à ordem lexicográfica.

Calculando a Base de Gröbner reduzida para o ideal I gerado pelos polinômios envolvidos no sistema anterior com respeito a ordem lexicográfica, obtemos:

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

Podemos constatar facilmente que $1 \notin I$ e o Teorema 3.1 garante que o sistema admite solução, ou seja, o mapa pode ser colorido com 3 cores sem que duas regiões adjacentes admitam a mesma cor.

Além disto, a Base de Gröbner G nos indica como colorir o mapa a partir das soluções do sistema. Para tanto, temos agora que fazer

o caminho contrário ao que realizamos ao modelar algebricamente o problema, ou seja, devemos interpretar o que cada polinômio de G representa.

A equação $x_9^3 - 1 = 0$, indica que podemos escolher qualquer cor para x_9, digamos a cor c_1. Como vimos, $x_8^2 + x_8x_9 + x_9^2 = 0$ é interpretada como o fato de que a cor de x_8 não pode ser a mesma que x_9 assume. Assim, atribuímos à x_8 a cor c_2. Uma vez que a equação $x_7+x_8+x_9 = 0$ deve admitir soluções entre as raízes cúbicas complexas da unidade, o Exercício 3.8, indica que x_7, x_8 e x_9 devem assumir valores distintos, ou seja, x_7 deve ser colorida com uma cor distinta das cores utilizadas para x_8 e x_9. O mesmo se pode dizer das equações $x_5 + x_8 + x_9 = 0$ e $x_2 + x_8 + x_9 = 0$. Assim, reservamos a cor c_3 para x_7, x_5 e x_2.

As equações $x_6 - x_8 = 0$ e $x_4 - x_8 = 0$ correspondem a informação de que x_6 e x_4 assumem a mesma cor de x_8, isto é, c_2. Do mesmo modo que a equação $x_3 - x_9 = 0$ indica que devemos associar à x_3 a mesma cor dada a x_9. Analisemos agora a equação

$$0 = x_1^2 - x_1x_8 - x_1x_9 + x_8x_9 = (x_1 - x_8) \cdot (x_1 - x_9).$$

Note que temos as possibilidades: $x_1 - x_8 = 0$ ou $x_1 - x_9 = 0$. Portanto, atribuímos à x_1 a mesma cor de x_8 ou a cor usada em x_9.

Resumindo os dados oriundos da interpretação das equações obtidas pelos elementos de G temos duas situações:

Situação 1:

Cor	Região
c_1	x_1, x_3, x_9
c_2	x_4, x_6, x_8
c_3	x_2, x_5, x_7

Situação 2:

Cor	Região
c_1	x_3, x_9
c_2	x_1, x_4, x_6, x_8
c_3	x_2, x_5, x_7

Devemos observar que as duas situações acima para colorir o mapa da região nordeste do Brasil, são precisamente os únicos modos de fazê-lo, a menos de permutação das três cores.

Exercício 3.9. *Decida se o mapa da América do Sul pode ser colorido com apenas três cores. Em caso afirmativo, encontre os modos distintos de proceder tal coloração.*

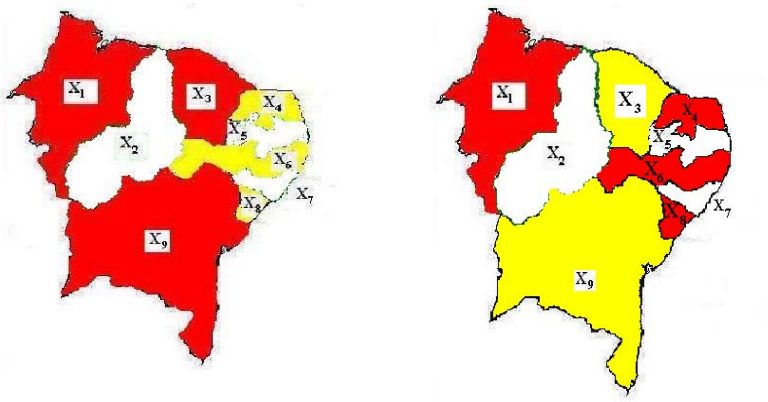


Figura 3.2: Situações 1 e 2.

3.3 Validação de Origamis

Nas seções anteriores apresentamos algumas aplicações voltadas à álgebra e a topologia. Iremos agora apresentar uma interessante forma de utilizarmos as Bases de Gröbner para a validação matemática de Origamis.

A palavra **Origami** se deriva das palavras japonesas *Oru* que significa *dobrar* e de *Kami* cujo significado é *papel*.

O Origami nada mais é do que a arte de fazer dobras em uma peça de papel, onde não é permitido realizar cortes ou colagens.

Mais do que um simples entretenimento, por trás do Origami encontramos muitas aplicações, para se ter uma ideia, o problema do Origami rígido, que consiste em substituir o papel por metal, é de grande utilidade e tem sido estudado e usado para levar ao espaço grelhas de painéis solares para satélites.

Hoje, a arte do Origami, tem tomado várias direções e os artistas cada vez mais utilizam livremente sua criatividade para construir suas peças. No entanto, o Origami clássico segue determinadas regras ou operações básicas que são chamadas de *Axiomas de Huzita* que são

realizadas sobre um papel de formato obrigatoriamente quadrado.

Os Axiomas de Huzita são:

1. Dados dois pontos A e B, podemos realizar uma dobra através deles.

2. Dados dois pontos A e B, podemos fazer uma dobra sobrepondo um dos pontos ao outro.

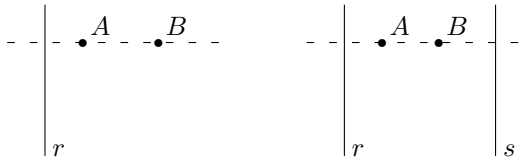
3. Dadas duas linhas[3] r e s, podemos fazer uma dobra sobrepondo as duas linhas.

4. Dados um ponto A e uma linha r, podemos realizar uma dobra que é perpendicular a r e passa por A.

5. Dados dois pontos A e B e uma linha r, podemos fazer uma dobra passando por B tal que a dobra sobrepõe A e r, ou essa dobra é impossível.

6. Dados dois pontos A e B e duas linhas s e r, podemos realizar uma dobra sobrepondo A a s e B a r, ou essa dobra é impossível.

Note que os Axiomas 5 e 6 têm limitações geométricas, ou seja, nem sempre podem ser aplicados a quaisquer configurações de pontos e linhas. Por exemplo, se a reta determinada por A e B é perpendicular a reta r com A entre B e r, então não se pode aplicar as operações descritas nos Axiomas 5 e 6.



Além de criar figuras de animais, flores e outros objetos para distração e deleite de muitos, um dos interesses que o Origami tem despertado nos matemáticos é a possibilidade de realizar certas construções que ferramentas clássicas como régua (sem graduação) e compasso não permitem.

[3]Uma linha é o vinco no papel que obtemos ao realizarmos uma dobra e desdobrarmos.

É um capítulo particularmente interessante, o estudo dos três problemas clássicos da Geometria Grega que envolvem construções com régua e compasso:

1. **(Quadratura do círculo)** Como construir um quadrado com área igual a de um círculo dado?
2. **(Trisecção do ângulo)** Como dividir um ângulo dado em três partes de mesma medida?
3. **(Duplicação do cubo)** Como construir um cubo com o dobro do volume de um cubo dado?

Estes problemas impulsionaram o desenvolvimento da Teoria de Grupos e culminaram com os célebres trabalhos do jovem e precoce Galois. Os resultados contidos em seus estudos permitiram garantir a impossibilidade das construções requisitadas nos 3 problemas clássicos.

No entanto, os axiomas de Huzita permitem realizar construções que vão além das possíveis com régua e compasso. Dentre tais construções encontramos uma que resolve o Problema da Duplicação do Cubo.

Vejamos o que está por trás deste problema. Se o cubo dado tem aresta de medida α, então seu volume é α^3. O cubo a ser construído deve ter volume $2\alpha^3$, ou seja, deve ter aresta de comprimento $\alpha\sqrt[3]{2}$.

Dados dois segmentos, por meio de régua e compasso, podemos construir um segmento com comprimento igual ao produto e ao quociente dos comprimentos dos dois segmentos. Como α é dado, o problema estará resolvido se pudermos construir um segmento de comprimento $\sqrt[3]{2}$.

Na figura a seguir apresentamos como realizar a construção de $\sqrt[3]{2}$ utilizando os Axiomas de Huzita.

Vamos identificar os axiomas utilizados nas construções realizadas:

Passo 1: Sobrepomos as retas AC e BD (Axioma 3) e determinamos o ponto P em AB.

Passo 2: Desdobramos.

Passo 3: Realizamos uma dobra sobrepondo C a P (Axioma 2) o que determina o ponto E em BD e o ponto K em CA.

Passo 4: Fazemos uma dobra que é perpendicular a reta BD passando por E (Axioma 4) determinando o ponto F na reta AC.

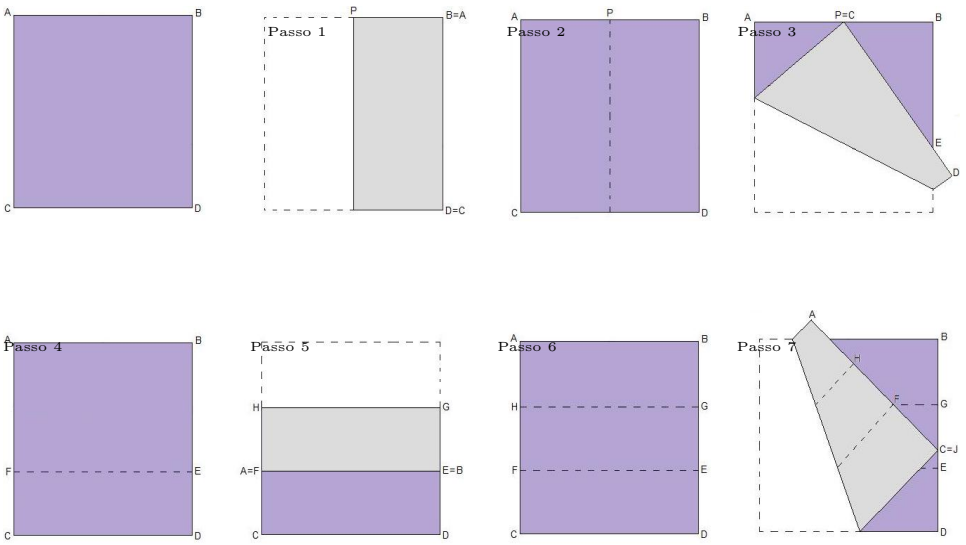


Figura 3.3: Construção de $\sqrt[3]{2}$ via Origami.

Passo 5**:** Sobrepomos as retas AB e FE (Axioma 3) que nos dá os pontos G em BD e H em AB.

Passo 6**:** Desdobramos.

Passo 7: Realizamos uma dobra sobrepondo F a reta HG e C a reta BD, determinando o ponto J.

Deste modo, temos que

$$\overline{BJ} = \overline{JD} \cdot \sqrt[3]{2}.$$

Há uma questão que não podemos deixar de levantar: o que garante que a construção realizada realmente nos fornece o resultado e não uma aproximação grosseira? Não estamos aqui questionando a

acuidade visual, nem a falta de precisão ao realizar as dobras. Digamos que estamos em uma situação *ideal*, ou seja, não temos problemas e erros de natureza física. Como validar o resultado obtido pelas dobras realizadas?

A ideia é, como no caso da coloração de mapas, modelar o problema de modo a traduzir as operações realizadas no Origami e os objetos envolvidos em termos de um sistema de equações polinomiais $h_1 = \ldots = h_m = 0$. O mesmo é feito com o resultado que suspeitamos ser verdadeiro, ou seja, expressamos sob a forma $t_1 = \ldots = t_r = 0$.

Para tanto, vamos fazer uso da Geometria Analítica, uma vez que esta permite "equacionar" os objetos geométricos envolvidos, bem como suas propriedades. Uma vez obtidas as equações, consideramos o ideal I dado por $\langle h_1, \ldots, h_m \rangle$.

Para verificar que a construção realizada através do Origami é verdadeira e garantir que a mesma é válida para qualquer situação, basta verificarmos se todas as soluções do sistema $h_1 = \ldots = h_m = 0$ são também soluções de $t_1 = \ldots = t_r = 0$. Isto por sua vez pode ser verificado invocando o Teorema dos Zeros de Hilbert (Versão Forte) 3.2, ou ainda, o Corolário 3.3, isto é, basta verificarmos se 1 pertence a $\langle h_1, \ldots, h_m, 1 - y \cdot t_j \rangle$ para todo $j \in \{1, \ldots, r\}$.

Vamos aplicar o descrito acima no exemplo dado da construção de $\sqrt[3]{2}$ via Origami.

Para facilitar as expressões, sem perda de generalidade, podemos atribuir um sistema de coordenadas cartesianas ao quadrado $ABDC$ de modo que $C = (0,0), D = (1,0), A = (0,1)$ e $B = (1,1)$.

Os Passos 1 e 2, nos dão que as coordenadas de P são $\left(\frac{1}{2}, 1\right)$.

O Passo 3 determina os pontos $E = (1, a)$ e $K = (0, k)$, tais que

$$d(C,K) = d(K,P) \quad \text{e} \quad KP \perp PE,$$

que nos dão respectivamente

$$k = \sqrt{\left(\frac{1}{2}\right)^2 + (1-k)^2} \;\Rightarrow\; k = \frac{5}{8}$$

$$\left(\frac{1}{2}, 1-k\right) \cdot \left(1 - \frac{1}{2}, a - 1\right) = 0 \;\Rightarrow\; a = \frac{1}{3},$$

ou seja, os Passos $1, 2, 3$ e 4 permitem dividir um segmento (no caso BD) em três partes iguais.

Nos Passos 5 e 6, obtemos os pontos $G = \left(1, \frac{2}{3}\right)$ e $H = \left(0, \frac{2}{3}\right)$.

Finalmente, chegamos ao último passo, que é crucial para nossa conclusão. O fato de justapor o ponto C em BD originando o ponto $J = (1, j)$ e o ponto F em HG obtendo o ponto $M = \left(m, \frac{2}{3}\right)$, pode ser modelado pelas condições:

$$d(C, F) = d(J, M), \quad C\widehat{F}M \equiv F\widehat{M}J \quad \text{e} \quad CJ \backslash\backslash FM.$$

Denotando por α e β a medida de $C\widehat{F}M$ e $F\widehat{M}J$ respectivamente, temos que $\alpha = \beta$ é equivalente a

$$cos(\alpha) = cos(\beta) \Leftrightarrow \frac{\overrightarrow{FC} \cdot \overrightarrow{MF}}{|\overrightarrow{FC}| \cdot |\overrightarrow{MF}|} = \frac{\overrightarrow{MF} \cdot \overrightarrow{MJ}}{|\overrightarrow{MF}| \cdot |\overrightarrow{MJ}|},$$

ou em termos polinomiais, por meio de relações conhecidas da Geometria Analítica,

$$\begin{cases} (1-m)^2 + \left(j - \frac{2}{3}\right)^2 - \frac{1}{9} = 0 \\ -\frac{1}{9} + m \cdot (1-m) + \frac{1}{3} \cdot j \cdot \left(j - \frac{2}{3}\right) = 0 \\ j \cdot m + \frac{2}{3} = 0. \end{cases} \tag{3.3}$$

A afirmação que queremos verificar é $\overline{BJ} = \overline{JD} \cdot \sqrt[3]{2}$ que pode ser expressa por

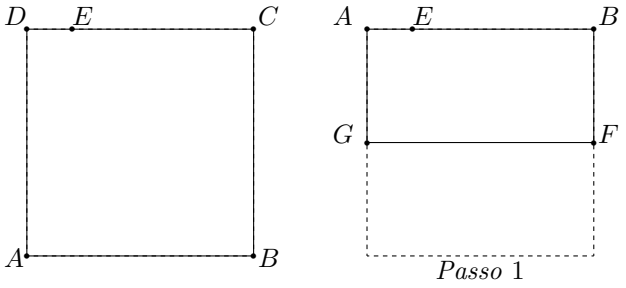
$$(1-j)^3 = 2j^3, \quad \text{ou seja,} \quad (1-j)^3 - 2j^3 = 0.$$

Como comentamos, para validar a construção devemos verificar se todas as soluções do sistema 3.3 são soluções de $(1-j)^3 - 2j^3 = 0$, que é equivalente a verificar se $1 \in I$ onde

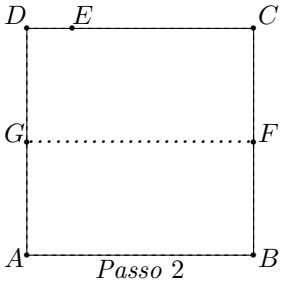
$$I = \langle (1-m)^2 + \left(j - \frac{2}{3}\right)^2 - \frac{1}{9}, -\frac{1}{9} + m \cdot (1-m) + \frac{1}{3} \cdot j \cdot \left(j - \frac{2}{3}\right),$$
$$j \cdot m + \frac{2}{3}, 1 - y \cdot ((1-j)^3 - 2j^3) \rangle.$$

o que é constatado ao calcularmos a Base de Gröbner reduzida para o ideal I com respeito à ordem lexicográfica. Portanto, realmente a construção nos dá um modo de obter $\sqrt[3]{2}$ e o problema da duplicação do cubo pode ser resolvido por meio de Origami.

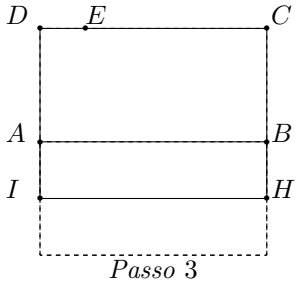
Exercício 3.10. *Mostre que na sequência de passos a seguir, o ângulo $K\widehat{A}B$ tem medida igual a um terço da medida do ângulo $E\widehat{A}B$ para qualquer posição do ponto E sobre o segmento CD, provando assim que o problema da trisecção do ângulo pode ser resolvido por meio de Origami.*



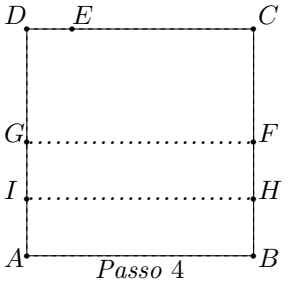
Passo 1



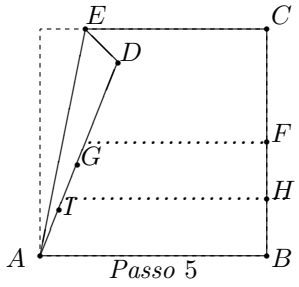
Passo 2



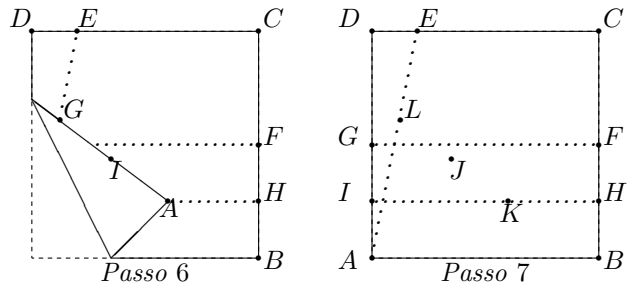
Passo 3



Passo 4



Passo 5



Abaixo identificamos os axiomas utilizados nas construções realizadas:

Passo 1**:** *Sobrepomos as retas AB e DC (Axioma* 3*), determinando o ponto G em AD e o ponto F em BC.*

Passo 2**:** *Desdobramos.*

Passo 3**:** *Realizamos uma dobra sobrepondo AB a GF, de acordo com o Axioma* 3*, o que determina o ponto I em AD e o ponto H em BC.*

Passo 4**:** *Desdobramos.*

Passo 5**:** *Procedemos uma dobra sobre os pontos A e E, ou seja, utilizamos o Axioma* 1*.*

Passo 6**:** *Realizamos uma dobra sobrepondo A a reta IH e G a reta AE, determinando os pontos K em IH e L em AE (Axioma* 6*).*

Passo 7**:** *Desdobramos e obtemos que*

$K\widehat{A}B$ *tem medida igual a um terço da medida de* $E\widehat{A}B$*.*

Bibliografia

[A] Alperin, R. C., *A Mathematical Theory of Origami Constructions and Numbers*. New York Journal of Mathematics, 6, 119-133, (2000).

[AL] Adams, W and Loustaunau, P., *An Introduction to Gröbner Basis*, AMS, Providence RI (1994).

[B] Buchberger, B., *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*. Aequationes mathematicae 4\3, 374-383 (1970). (Tradução em: Buchberger, B. and Winkler, F. (eds.), *Gröbner Basis and Applications*. London Mathematical Society Lecture Notes Series, Vol. 251, Cambridge University Press, 535-545, (1998)).

[BI] Buchberger, B. and Ida, T., *Origami Theorem Proving*, SFB Scientific Computing Technical Report 2003, 23-Oct, Johannes Kepler University RISC, (2003).

[C] Coutinho, S. C., *Demonstração Automática de Teoremas*, Notas de minicurso da I Bienal da Sociedade Brasileira de Matemática, Icex-UFMG (2002).

[CLO1] Cox, D; Little, J. and O'Shea, D., *Ideals, Varieties and Algorithms*, 2nd edition, Springer-Verlag, New York, (1996).

[CLO2] Cox, D; Little, J. and O'Shea, D., *Using Algebraic Geometry*, Springer-Verlag, New York, (1997).

[CV] Costa, A. V. e Vainsencher, I., *Bases de Gröbner: Resolvendo Equações Polinomiais*, Atas da XIII Escola de Álgebra Vol. 1, pag. 111-184, IMECC-UNICAMP (1994).

[Fr] Fröberg, R., *An Introduction to Gröbner Basis*, Pure and Applied Mathematics. A Wiley-Interscience Series of Texts, Monographs, and Tracts (1997).

[GP] Greuel, G.-M. and Pfister, G., *A Singular Introduction to Commutative Algebra*. Second Edition. Springer, (2007).

[H] Huzita, H., *Axiomatic Development of Origami Geometry*, Proceedings of the First International Meeting of Origami Science and Technology, 143-158, (1989).

[JM] Jacquemard, A. e Martins, R. M., *Solução de Sistemas Algébricos e Aplicações em Teoria de Singularidades*. Matemática Universitária 47, 31-39, (2009).

[KR] Kreuzer, M. and Robbiano, L., *Computational Commutative Algebra 1*, Springer-Verlag, New York, (2000).

[S] Soares, M. G., *Cálculo em uma Variável Complexa*, Coleção Matemática Universitária, SBM, (1999).

[Va] Vainsencher, I., *Introdução às Curvas Algébricas Planas*. Segunda edição. Coleção Matemática Universitária. IMPA (2005).

Índice

S-polinômio, 60
n-ésimas da unidade, raízes, 78

algebricamente fechado, corpo, 71
Algoritmo de Buchberger, 63
anel, 2
anel de polinômios, 18
axiomas de Huzita, 82

Base de Gröbner, 54
Base de Gröbner Mínima, 66
Base de Gröbner Reduzida, 67
Base de Hilbert, Teorema da, 58
binária, operação, 1
boa ordem, 22
Buchberger, Algoritmo de, 63

círculo, quadratura do, 84
CoCoA, 69
coeficiente, 6, 18
coeficiente líder, 6, 29
Coloração, problema da, 76, 77
comum, mínimo múltiplo, 60
comutativo, anel, 2
constante, polinômio, 5
corpo, 3
    de frações, 4
corpo algebricamente fechado, 71
cubo, duplicação do, 84

Dickson, Lema de, 43
divisão, quociente e resto, 10, 31
divisibilidade, 4
domínio de integridade, 3
duplicação do cubo, 84

elemento invertível e unidade, 2
elemento neutro, 2
elemento, simétrico de um, 2

fechado, corpo algebricamente, 71
frações, corpo de, 4

Gröbner Mínima, Base de, 66
Gröbner Reduzida, Base de, 67
Gröbner, Base de, 54
graduada reversa, ordem lex., 27
graduada, ordem lexicográfica, 27
grau, 6
grau (total), 18, 19
grau em x_i, 19
grau ponderado, 27

Hilbert, Teo. dos Zeros, 71, 72
Hilbert, Teorema da base, 58
Huzita, axiomas de, 82

ideais triviais, 37
ideal, 36

ideal monomial, 42
ideal principal, 37
igualdade de polinômios, 5
integridade, domínio de, 3
invertível, elemento, 2

líder, coeficiente, 6, 29
líder, monômio e termo, 6, 29
Lema de Dickson, 43
lexicográfica graduada reversa, 27
lexicográfica graduada, ordem, 27
lexicográfica, ordem, 26

Mínima, Base de Gröbner, 66
mínimo múltiplo comum, 60
mônico, polinômio, 6
Maple, 69
Mathematica, 69
MMC, 60
monômio, 6, 18
monômio líder, 6, 29
monomial, ideal, 42
monomial, ordem, 22

neutro, elemento, 2

operação binária, 1
oposto de um elemento, 2
ordem lex. graduada reversa, 27
ordem lexicográfica, 26
ordem lexicográfica graduada, 27
ordem monomial, 22
ordem ponderada, 27
ordem total, 21
ordem, boa, 22
ordem, relação de, 21
origami, 82

peso, 27
polinômio, 5
polinômio constante, 5
polinômio mônico, 6
polinômio, raiz, 13
polinômios, anel de, 18
ponderada, ordem, 27
primitiva da unidade, raiz, 78
principal, ideal, 37
Problema da coloração, 76, 77
pseudo-divisão, 46

quadratura do círculo, 84
Quatro cores, problema das, 76
quociente da divisão, 10, 31

raízes n-ésimas da unidade, 78
raiz de polinômio, 13
Reduzida, Base de Gröbner, 67
relação de ordem, 21
resto da divisão, 10, 31
reversa, ordem lex. graduada, 27

simétrico de um elemento, 2
Singular, 69

Teo. dos Zeros de Hilbert, 71, 72
Teorema da Base de Hilbert, 58
Teorema das Quatro Cores, 76
termo, 6, 18
termo líder, 6, 29
total, grau, 18
total, ordem, 21
Três cores, problema das, 77
trisecção do ângulo, 84
triviais, ideais, 37

unidade, elemento, 2
unidade, raízes n-ésimas, 78

Zeros de Hilbert, Teo. dos, 71, 72