UNIVERSIDADE FEDERAL DE SANTA CATARINA

SABRINA COELHO

# O ALGORITMO DA DIVISÃO PARA POLINÔMIOS EM VÁRIAS VARIÁVEIS

Blumenau

2018

**Sabrina Coelho**

# O ALGORITMO DA DIVISÃO PARA POLINÔMIOS EM VÁRIAS VARIÁVEIS

Trabalho de Conclusão de Curso submetido ao Curso de Licenciatura em Matemática da Universidade Federal de Santa Catarina para a obtenção do Grau de Licenciada em Matemática.

**Orientador**: Prof. Dr. Jorge Luiz Deolindo Silva

Blumenau

2018

Catalogação na fonte pela Biblioteca Universitária da Universidade Federal de Santa Catarina.

Arquivo compilado às 15:26h do dia 5 de dezembro de 2018.

Sabrina Coelho
O algoritmo da divisão para polinômios em várias variáveis : / Sabrina Coelho; Orientador, Prof. Dr. Jorge Luiz Deolindo Silva; , - Blumenau, 15:26, 5 de dezembro de 2018.
71 p.

Trabalho de Conclusão de Curso - Universidade Federal de Santa Catarina, Departamento de Matemática (MAT), Centro de Blumenau, Curso de Licenciatura em Matemática.

Inclui referências

1. Anel de polinômios em várias variáveis. 2. Ordem monomial. 3. Algoritmo da divisão. 4. Algoritmo da pseudo divisão. I. Prof. Dr. Jorge Luiz Deolindo Silva II. III. Curso de Licenciatura em Matemática IV. O algoritmo da divisão para polinômios em várias variáveis

CDU 02:141:005.7

Sabrina Coelho

**O ALGORITMO DA DIVISÃO PARA POLINÔMIOS EM VÁRIAS VARIÁVEIS**

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção do Título de Licenciada em Matemática, e aprovado em sua forma final pelo Curso de Licenciatura em Matemática do Departamento de Matemática (MAT), Centro de Blumenau da Universidade Federal de Santa Catarina.

Blumenau, 5 de dezembro de 2018.

---

**Prof. Dr. André Vanderlinde da Silva**
Coordenador do Curso de Licenciatura em Matemática

**Banca Examinadora:**

---

**Prof. Dr. Jorge Luiz Deolindo Silva**
Orientador
Universidade Federal de Santa Catarina – UFSC

---

**Prof. Dr. Felipe Vieira**
Universidade Federal de Santa Catarina – UFSC

---

**Prof. Dr. Renan Gambale Romano**
Universidade Federal de Santa Catarina – UFSC

*A todos aqueles que enxergam a beleza da matemática.*

## AGRADECIMENTOS

Ao meu orientador Prof Dr. Jorge Luiz Deolindo Silva por toda colaboração neste trabalho, por me incentivar a buscar novos conhecimentos e por acreditar em mim.

A meus pais que durante este período me incentivaram e me apoiaram em todos os momentos da graduação, assim como meu namorado, meus irmãos e minha avó.

Aos meus amigos, que durante este período tornaram-se pessoas essenciais em minha vida, com os quais compartilhei muitos momentos felizes e inesquecíveis.

A Universidade Federal de Santa Catarina por ter dado condições de que este trabalho assim como a graduação fosse possível. E por fim, a todo corpo docente da UFSC Blumenau que foram os responsáveis por me guiar neste caminho do conhecimento.

*"Tenho a impressão de ter sido uma criança brincando à beira-mar, divertindo-me em descobrir uma pedrinha mais lisa ou uma concha mais bonita que as outras, enquanto o imenso oceano da verdade continua misterioso diante de meus olhos"*

Isaac Newton

## RESUMO

Neste trabalho estudamos o anel de polinômios em várias variáveis e ordens monomiais. Mais especificamente, apresentamos os algoritmos da divisão e da pseudo divisão de polinômios em várias variáveis.



**Palavras-chaves**: Anel de polinômios em várias variáveis. Ordem monomial. Algoritmo da divisão. Algoritmo da pseudo divisão.

## ABSTRACT

In this work we study the polynomials ring in several variables and monomial orders. More specifically, we present the division and pseudo division algorithms for polynomials in several variables.



**Keywords**: Polynomials ring in several variables. Monomial order. Division algorithm. Pseudo division algorithm.

## SUMÁRIO


**1 INTRODUÇÃO . . . . . 17**

**2 ANEL . . . . . 19**
2.1 DEFINIÇÕES . . . . . 19
2.2 ANEL DE POLINÔMIOS . . . . . 25
**2.2.1 Algoritmo da divisão para o anel de polinômios . . 34**

**3 ANEL DE POLINÔMIOS EM VÁRIAS INDETERMINADAS . . . . . 39**
3.1 ORDENS MONOMIAIS . . . . . 42
**3.1.1 Algoritmo da divisão de polinômios em várias variáveis . . . . . 50**

**4 IDEAIS DO ANEL DE POLINÔMIOS EM VÁRIAS VARIÁVEIS . . . . . 57**
4.1 O ALGORITMO DA PSEUDO DIVISÃO . . . . 57
**4.1.1 Ideais em polinômios em várias variáveis . . . . . 65**

**5 CONSIDERAÇÕES FINAIS . . . . . 69**

**REFERÊNCIAS . . . . . 71**

# 1 INTRODUÇÃO

Este trabalho tem como objetivo estudar os algoritmos da divisão de polinômios em várias variáveis. Para isso estudamos o anel de polinômios $\mathbb{K}[x_1, \ldots, x_n]$ e ordens monomiais onde $\mathbb{K}$ é um corpo. Em geral, esse trabalho gira em torno da pergunta: "Quando um ou mais polinômios não nulos em $\mathbb{K}[x_1, \ldots, x_n]$ divide outro?". Com a resposta dessa pergunta e com um estudo mais avançado (não abordado neste trabalho), podemos determinar se um polinômio pertence ou não a um ideal do anel $\mathbb{K}[x_1, \ldots, x_n]$.

Inicialmente, baseado em [4],[1] e [2], o Capítulo 2 apresenta a teoria de anéis. Apresentamos alguns anéis especiais essenciais no decorrer do trabalho, como por exemplo, os anéis de integridade e corpos. Finalizamos o capítulo com o estudo do anel de polinômios e o algoritmo da divisão para polinômios em uma variável.

No Capítulo 3 os estudos focam-se em um tipo especial de anel, que é o anel de polinômios em várias variáveis. Estudamos ordens monomiais para que seja possível validar o algoritmo da divisão para polinômios em várias variáveis.

No Capítulo 4, apresenta-se o algoritmo da pseudo divisão, que é responsável por garantir uma maneira de dividir um polinômio por mais do que um quociente. Para entender a aplicabilidade do mesmo, no final do capítulo, comentamos brevemente a teoria de ideais e por meio desse algoritmo pode-se garantir se um polinômio $f$ pertence a um ideal gerado $\langle g_1, \ldots, g_s \rangle$, onde $g_1, \ldots g_s \in \mathbb{K}[x_1, \ldots, x_n]$.

É necessário que o leitor tenha conhecimentos básicos em álgebra abstrata (teoria de anéis e corpos), para que se tenha um bom entendimento do trabalho. Para a execução deste trabalho utilizou-se as referências [4],[1] e [2] para o conceito de anéis e corpos e [3] para o estudo de polinômios em várias variáveis e seus algoritmos.

# 2 ANÉIS

## 2.1 DEFINIÇÕES

Nesta seção apresentamos alguns conceitos das teorias de anéis e corpos que são essenciais para o estudo de anéis de polinômios, que serão abordados nos próximos capítulos.

**Definição 2.1.** Seja $\mathbb{A}$ um conjunto não vazio no qual estão definidas duas operações:

$$\begin{array}{rccc} + : & \mathbb{A}\times\mathbb{A} & \to \mathbb{A} & \qquad\qquad \times : \quad \mathbb{A}\times\mathbb{A} \quad \to \mathbb{A} \\ & (a,b) & \mapsto a+b & \qquad\qquad\quad\ (a,b) \quad \mapsto a\times b. \end{array}$$

Para que a terna $(\mathbb{A}, +, \times)$ seja um *anel*, é necessário que sejam válidas as seguintes propriedades:

i) A *associatividade* em relação a $+$, isto é,

$$a + (b + c) = (a + b) + c, \text{ para todos } a, b, c \in \mathbb{A}.$$

ii) A *comutatividade* em relação a $+$, ou seja,

$$a + b = b + a, \text{ para todos } a, b \in \mathbb{A}.$$

iii) Existe um *elemento neutro* em relação a $+$:

Para todo $a \in \mathbb{A}$, existe $0_{\mathbb{A}} \in \mathbb{A}$ tal que $a + 0_{\mathbb{A}} = 0_{\mathbb{A}} + a = a$.

iv) Existe *elemento oposto* em relação a $+$:

Para todo $a \in \mathbb{A}$, existe $b \in \mathbb{A}$ tal que, $a + b = b + a = 0_{\mathbb{A}}$.

Pode-se provar que para cada $a$, $b$ é único. Logo, denotaremos o elemento oposto de $a$ por $-a$.

v) A *associatividade* em relação a $\times$:

$$\text{Para todos } a, b, c \in \mathbb{A},\ a \times (b \times c) = (a \times b) \times c.$$

vi) A *distributividade*:

Para todo $a, b, c \in \mathbb{A}$

$$a \times (b + c) = (a \times b) + (a \times c)$$

$$(a + b) \times c = (a \times c) + (b \times c).$$

Às vezes por abuso de linguagem, dizemos simplesmente que $\mathbb{A}$ é um anel em vez de usar a terna $(\mathbb{A}, +, \times)$.

**Exemplo 2.1.1.** Veja alguns exemplos de anéis:

1. $(\mathbb{Z}, +, \cdot)$ com as operações usuais de soma e multiplicação é um anel.

2. $\mathbb{A} = \{n \in \mathbb{Z} : n = 2k, k \in \mathbb{Z}\}$ com as operações usuais de soma e multiplicação em $\mathbb{Z}$ é um anel. De fato, $\mathbb{A}$ é não vazio, pois $0 = 2 \cdot 0 \in \mathbb{A}$. Sejam $a, b, c \in \mathbb{A}$, então

$$a = 2 \cdot k_1, b = 2 \cdot k_2, c = 2 \cdot k_3 \text{ para } k_1, k_2, k_3 \in \mathbb{Z}.$$

i) Associatividade em relação a $+$:

$$\begin{aligned} a + (b + c) &= 2k_1 + (2k_2 + 2k_3) \\ &= 2k_1 + 2k_2 + 2k_3 \\ &= (2k_1 + 2k_2) + 2k_3 \\ &= (a + b) + c. \end{aligned}$$

ii) Comutatividade em relação a $+$:

$$a + b = 2k_1 + 2k_2 = 2k_2 + 2k_1 = b + a.$$

iii) Existência de elemento neutro em relação a $+$:
Note que $0_{\mathbb{A}}$ é o elemento neutro de $\mathbb{A}$, pois dado $a \in \mathbb{A}$, temos que

$$a + 0_{\mathbb{A}} = 2k_1 + 0_{\mathbb{A}} = 2k_1 = a.$$

iv) Elemento oposto de $a$ em $+$:

O elemento oposto de $a = 2k_1$ é $2(-k_1)$. Assim,

$$a + b = 2k_1 + 2(-k_1) = 2k_1 - 2k_1 = 0_{\mathbb{A}}.$$

Analogamente $b + a = 0_{\mathbb{A}}$

v) Associatividade em $\cdot$:

$$a \cdot (b \cdot c) = 2k_1 \cdot (2k_2 \cdot 2k_3) = (2k_1 \cdot 2k_2) \cdot 2k_3 = (a \cdot b) \cdot c.$$

vi) Distributividade em $\cdot$:

$$\begin{aligned} a \cdot (b + c) &= 2k_1 \cdot (2k_2 + 2k_3) \\ &= 2k_1 \cdot 2k_2 + 2k_1 \cdot 2k_3 \\ &= a \cdot b + a \cdot c. \end{aligned}$$

Analogamente para $(a + b) \cdot c = a \cdot c + b \cdot c$.

Portanto $(\mathbb{A}, +, \cdot)$ é um anel e denotamos por $\mathbb{A} = 2\mathbb{Z}$.

3. $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ com as operações usuais de soma e multiplicação são anéis.

4. O conjunto $\mathbb{M}_n(\mathbb{R})$ das matrizes com entradas reais com operações usuais de soma e multiplicação é um anel.

5. Anel dos inteiros módulo $m$. Seja $m > 1$ um inteiro. Considere a relação $R$ definida sobre $\mathbb{Z}$ dada por

$$aRb \iff m|a - b \text{ para todos } a, b \in \mathbb{Z}.$$

Note que $R$ é uma relação de equivalência, isto é,

i) $aRa$ para todo $a \in \mathbb{Z}$ (reflexiva);

ii) Se $aRb$, então $bRa$ para todos $a, b \in \mathbb{Z}$ (simétrica);

iii) Se $aRb$ e $bRc$, então $aRc$ para todos $a, b, c \in \mathbb{Z}$ (transitiva).

Dado $a \in \mathbb{Z}$, a classe de equivalência de $a$ módulo $m$ é definida por

$$\bar{a} = \{x \in \mathbb{Z} \mid xRa\} = \{x \in \mathbb{Z} : m|\, x - a\}.$$

O conjunto de todas as classes de equivalência módulo $m$ é denotado por $\mathbb{Z}_m$ e pode-se mostrar que

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$

(veja [4]). Considere $\bar{a}$ e $\bar{b}$ dois elementos pertencentes a $\mathbb{Z}_m$. Definimos as operações $+$ e $\cdot$ em $\mathbb{Z}_m$ por

$$\bar{a} + \bar{b} = \overline{a+b}$$
$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

O $\mathbb{Z}_m$ com essas operações é um anel. Com efeito, veja que:

i) Dados $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$, temos

$$\begin{aligned} \bar{a} + (\bar{b} + \bar{c}) &= \bar{a} + \overline{b+c} \\ &= \overline{a+b+c} \\ &= \overline{a+b} + \bar{c} \\ &= (\bar{a} + \bar{b}) + \bar{c}. \end{aligned}$$

ii) Dados $\bar{a}, \bar{b} \in \mathbb{Z}_m$, segue que

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}.$$

iii) O $\bar{0}$ é o elemento neutro da adição, pois

$$\bar{a} + \bar{0} = \overline{a+0} = \bar{a} = \overline{0+a} = \bar{0} + \bar{a}.$$

iv) Dado $\bar{a} \in \mathbb{Z}_m$, $\overline{-a}$ é o elemento inverso de $\bar{a}$ em $\mathbb{Z}_m$, pois

$$\bar{a} + \overline{-a} = \overline{a + (-a)} = \bar{0} = \overline{-a + a} = \overline{-a} + \bar{a}.$$

v) Dados $\bar{a}, \bar{b}, \bar{c}$ em $\mathbb{Z}_m$, temos que

$$\bar{a} \cdot (\overline{b \cdot c}) = \bar{a} \cdot \overline{b \cdot c} = \overline{a \cdot b \cdot c} = \overline{a \cdot b} \cdot \bar{c} = (\bar{a} \cdot \bar{b}) \cdot \bar{c}.$$

vi) Dados $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$, temos

$$\begin{aligned} \bar{a} \cdot (\bar{b} + \bar{c}) &= \bar{a} \cdot \overline{b+c} \\ &= \overline{a \cdot (b+c)} \\ &= \overline{a \cdot b + a \cdot c} \\ &= \overline{a \cdot b} + \overline{a \cdot c} \\ &= \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}. \end{aligned}$$

Analogamente mostra-se que $(\bar{a} + \bar{b}) \cdot \bar{c} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c}$.

Portanto, $\mathbb{Z}_m$ é um anel.

**Definição 2.2.** Se além das 6 propriedades apresentadas na Definição 2.1 a terna $(\mathbb{A}, +, \times)$ satisfaz

$$a \times b = b \times a, \text{ para todos } a, b \in \mathbb{A},$$

o chamamos de *anel comutativo*.

**Exemplo 2.1.2.** O anel $\mathbb{Z}_m$ é comutativo, pois para todos $\bar{a}, \bar{b} \in \mathbb{Z}_m$,

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \cdot \bar{a}.$$

**Exemplo 2.1.3.** O anel das matrizes $\mathbb{M}_n(\mathbb{R})$ não é comutativo, pois dadas duas matrizes

$$\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \text{ e } \mathbf{B} = \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix}.$$

Temos que

$$\mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} 13 & 16 \\ 13 & 16 \end{pmatrix} \text{ e } \mathbf{B} \cdot \mathbf{A} = \begin{pmatrix} 7 & 14 \\ 11 & 22 \end{pmatrix}.$$

Portanto $A \cdot B \neq B \cdot A$.

**Definição 2.3.** Se no anel $(\mathbb{A}, +, \times)$ existe $1_{\mathbb{A}} \in \mathbb{A}$ tal que

$$x \times 1_{\mathbb{A}} = 1_{\mathbb{A}} \times x = x$$

para todo $x \in \mathbb{A}$, o chamamos de *anel com unidade*.

**Exemplo 2.1.4.** Vejamos que o anel $\mathbb{Z}_m$ é comutativo com unidade $\bar{1}$, pois para todo $\bar{a} \in \mathbb{Z}_m$,

$$\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a} = \overline{1 \cdot a} = \bar{1} \cdot \bar{a}.$$

**Definição 2.4.** Dizemos que um anel $(\mathbb{A}, +, \times)$ comutativo com unidade é um *anel de integridade* ou *domínio de integridade* se, para todos $a, b \in \mathbb{A}$ com $a \times b = 0_{\mathbb{A}}$, temos

$$a = 0_{\mathbb{A}} \text{ ou } b = 0_{\mathbb{A}}.$$

**Exemplo 2.1.5.** 1. $(\mathbb{Z},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$ com as operações usuais de soma e multiplicação são anéis de integridade.

2. $\mathbb{Z}_6$ não é um anel de integridade, pois

$$\bar{2} \neq \bar{0} \text{ e } \bar{3} \neq \bar{0}, \text{ mas } \bar{2} \cdot \bar{3} = \bar{6} = \bar{0}.$$

**Proposição 2.1.** *$\mathbb{Z}_m$, com $m > 1$ é anel de integridade se, e somente se, $m$ é primo.*

*Demonstração.* Suponha que $m$ não é primo, então existem inteiros $x$ e $y$ com $1 < x < m$ e $1 < y < m$, tais que $m = x \cdot y$. Note que $\bar{x} \neq 0$ e $\bar{y} \neq 0$, assim

$$\bar{x} \cdot \bar{y} = \overline{x \cdot y} = \bar{m} = \bar{0}.$$

Logo, $\mathbb{Z}_m$ não é anel de integridade. Por outro lado, suponha que $m$ é primo e que $\bar{a}, \bar{b} \in \mathbb{Z}_m$, tais que

$$\bar{a} \cdot \bar{b} = \bar{0} \Rightarrow \overline{a \cdot b} = \bar{0}.$$

Assim, $m|a \cdot b$. Como $m$ é primo, temos que $m|a$ ou $m|b$. Logo, $a = m \cdot k_1$ ou $b = m \cdot k_2$ com $k_1, k_2 \in \mathbb{Z}$. Assim

$$\bar{a} = \bar{0} \text{ ou } \bar{b} = \bar{0}.$$

Portanto, $\mathbb{Z}_m$ é anel de integridade. ■

**Definição 2.5.** Um anel $(\mathbb{A},+,\times)$ comutativo com unidade $1_{\mathbb{A}}$ é um *corpo* se, para cada elemento $0_{\mathbb{A}} \neq a \in \mathbb{A}$, existe um elemento $b \in \mathbb{A}$ tal que

$$a \times b = 1_{\mathbb{A}}.$$

Chamamos $b$ de *inverso* de $a$ e pode-se demonstrar que ele é único. Assim o denotaremos por $a^{-1}$.

**Exemplo 2.1.6.** i) $(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{C},+,\cdot)$ com as operações usuais de soma e multiplicação são corpos.

ii) $\mathbb{Z}_3$ é corpo, pois vejamos que

$$\bar{1} \cdot \bar{1} = \bar{1} \text{ e } \bar{2} \cdot \bar{2} = \bar{4} = \bar{1}.$$

iii) $\mathbb{Z}$ não é corpo. De fato, veja que dado $a \in \mathbb{Z}^*$, não existe inverso multiplicativo em $\mathbb{Z}$ tal que $a \cdot b = 1$.

iv) $\mathbb{Z}_4$ não é corpo, pois não existe nenhum elemento pertencente a $\mathbb{Z}_4$, de modo que $\bar{2} \cdot \bar{a} = \bar{1}$. Podemos ter essa garantia pela Proposição 2.1.

**Proposição 2.2.** *Se* $(\mathbb{A}, +, \times)$ *é corpo, então* $\mathbb{A}$ *é anel de integridade.*

*Demonstração.* Seja $\mathbb{A}$ um corpo, então em particular $\mathbb{A}$ é um anel comutativo com unidade. Suponha que para todo $a, b \in \mathbb{A}$, $a \cdot b = 0_{\mathbb{A}}$. Devemos separar em dois casos. O primeiro é quando $a = 0_{\mathbb{A}}$ e neste caso, nada temos a fazer. No segundo caso devemos então considerar $a \neq 0_{\mathbb{A}}$. Então se $a \neq 0_{\mathbb{A}}$, existe $a^{-1} \in \mathbb{A}$ tal que $a \times a^{-1} = 1_{\mathbb{A}}$. Assim,

$$\begin{aligned} a \times b &= 0_{\mathbb{A}} \\ &\Rightarrow a^{-1} \times a \times b = a^{-1} \times 0_{\mathbb{A}} \\ &\Rightarrow 1_{\mathbb{A}} \times b = 0_{\mathbb{A}} \\ &\Rightarrow b = 0_{\mathbb{A}}. \end{aligned}$$

Portanto, $\mathbb{A}$ é anel de integridade. ■

Note que a recíproca é falsa, pois $\mathbb{Z}$ é um anel de integridade mas, $\mathbb{Z}$ não é corpo.

## 2.2 ANEL DE POLINÔMIOS

Nesta seção vamos centrar os estudos em um exemplo especial de anel: o anel de polinômios. Vamos apresentar o algoritmo da divisão nesse anel que é base para compreender o algoritmo em polinômios em várias variáveis.

Seja $(\mathbb{A}, +, \times)$ um anel e vamos considerar o conjunto

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

Chamamos os elementos de $\mathbb{A}[x]$ de *polinômios*.

Dados dois elementos $f, g \in \mathbb{A}[x]$ tais que

$$f = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

e

$$g = b_m x^m + \cdots + b_2 x^2 + b_1 x + b_0$$

dizemos que eles são iguais se, e somente se, $n = m$ e $a_i = b_i$, para $0 \leq i \leq n$.

Queremos que $\mathbb{A}[x]$ tenha a estrutura de um anel. Para isso devemos definir duas operações em $\mathbb{A}[x]$ de modo que sejam satisfeitas as seis propriedades de anel da Definição 2.1. Considere a operação

$$\begin{array}{rccc} + : & \mathbb{A}[x] \times \mathbb{A}[x] & \to & \mathbb{A}[x] \\ & (f, g) & \mapsto & f + g \end{array}$$

em que

$$f + g = (a_s + b_s)x^s + \cdots + (a_1 + b_1)x + (a_0 + b_0),$$

onde definimos $a_i = 0 \; \forall i > n$ e $b_i = 0 \; \forall i > m$. Considere também a operação

$$\begin{array}{rccc} \cdot : & \mathbb{A}[x] \times \mathbb{A}[x] & \to & \mathbb{A}[x] \\ & (f, g) & \mapsto & f \cdot g \end{array}$$

onde

$$f \cdot g = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0,$$

em que

$$c_k = (a_k \times b_0) + (a_{k-1} \times b_1) + \cdots + (a_0 \times b_k),$$

para $k = 0, 1, \ldots, n + m$.

Dado um polinômio $f = a_n x^n + \cdots + a_1 x + a_0$ podemos assumir que $0x^i = 0_{\mathbb{A}}$ para todo $i > n$, ou seja,

$$a_n x^n + \cdots + a_1 x + a_0 = 0_{\mathbb{A}} x^r + \cdots + 0_{\mathbb{A}} x^{n+1} + a_n x^n + \cdots + a_1 x + a_0.$$

Assim, $a_i = 0_{\mathbb{A}}$ para todo $i > n$.

Denotaremos, para simplificar a notação, que $0_{\mathbb{A}} = 0$.

Vamos mostrar que o conjunto $\mathbb{A}[x]$ com as operações definidas acima é um anel. Considere $f, g$ e $h$ elementos de $\mathbb{A}[x]$, sendo

$$f = a_n x^n + \cdots + a_0$$
$$g = b_m x^m + \cdots + b_0$$
$$h = d_s x^s + \cdots + d_0.$$

i) Associatividade em relação a $+$:

Suponha, sem perda de generalidade que $n = m = s$. Os outros casos são análogos ao completar cada um dos polinômios com monômios da forma $0_{\mathbb{A}} x^i$.

$$\begin{aligned} f + (g + h) &= f + ((b_m + d_s)x^m + \cdots + (b_0 + d_0)) \\ &= (a_n + b_m + d_s)x^n + \cdots + (a_0 + b_0 + d_0) \\ &= ((a_n + b_m)x^n) + d_s x^n + \cdots + (a_0 + b_0) + d_0 \\ &= ((a_n + b_m)x^n + (a_0 + b_0)) + d_s x^n + \cdots + d_0 \\ &= (f + g) + h. \end{aligned}$$

ii) Comutatividade em relação a $+$:

$$\begin{aligned} f + g &= (a_n x^n + \cdots + a_0) + (0x^n + \cdots + 0x^{m+1} + \\ &\quad b_m x^m + \cdots + b_0) \\ &= (a_n + 0)x^n + \cdots + (a_m + b_m)x^m + \cdots + \\ &\quad (a_0 + b_0) \\ &= (0 + a_n)x^n + \cdots + (b_m + a_m)x^m + \cdots + \\ &\quad (b_0 + a_0) \\ &= (0x^n + \cdots + 0x^{m+1} + b_m x^m + \cdots + b_0) + \\ &\quad (a_n x^n + \cdots + a_0) \\ &= g + f. \end{aligned}$$

iii) Elemento neutro em relação a $+$:

Considere $0x^n + \cdots + 0 = 0_{\mathbb{A}[x]}$, o polinômio nulo $\in \mathbb{A}[x]$.

$$\begin{aligned} f + 0_{\mathbb{A}[x]} &= (a_n x^n + \cdots + a_0) + (0x^n + \cdots + 0) \\ &= (a_n + 0)x^n + \ldots + (a_0 + 0) \\ &= f. \end{aligned}$$

Analogamente para $0_{\mathbb{A}[x]} + f$. Logo, o polinômio nulo é o elemento neutro de $\mathbb{A}[x]$.

iv) Elemento oposto em relação a $+$ de $f \in \mathbb{A}[x]$:

Considere

$$-f = -a_n x^n + \cdots + (-a_0),$$

então

$$\begin{aligned} f + (-f) &= (a_n x^n + \ldots + a_0) + (-a_n)x^n - \ldots - a_0 \\ &= a_n x^n + \ldots + a_0 - a_n x^n - \ldots - a_0 \\ &= (a_n - a_n)x^n + \ldots + (a_0 - a_0) \\ &= 0_{\mathbb{A}[x]}. \end{aligned}$$

Analogamente para $(-f) + f = 0_{\mathbb{A}[x]}$.

v) Associatividade em relação a $\cdot$:

$$\begin{aligned} f \cdot (g \cdot h) &= f \cdot (c_{m+s} x^{m+s} + \cdots + c_1 x + c_0) \\ &= f \cdot (b_m \times d_s)x^{m+s} + \cdots + (b_1 \times d_0) \\ &\quad +(b_0 \times d_1) + b_0 \times d_0 \\ &= (a_n \times b_m \times d_s)x^{n+m+s} + \cdots + \\ &\quad +((a_1 \times b_0 \times d_0) + (a_0 \times b_1 \times d_0) \\ &\quad +(a_0 \times b_0 \times d_1))x + (a_0 \times b_0 \times c_0) \\ &= c_{n+m+s} x^{n+m+s} + \cdots + c_1 x + c_0 \end{aligned}$$

Por outro lado,

$$\begin{aligned} (f \cdot g) \cdot h &= (c_{n+m} x^{n+m} + \cdots + c_1 x + c_0) \cdot h \\ &= ((a_n \times b_m)x^{n+m} + \cdots + (a_1 \times b_0 + a_0 \times b_1) \\ &\quad +(a_0 \times b_0)) \cdot h \\ &= (a_n \times b_m \times d_s)x^{n+m+s} + \cdots + \\ &\quad +((a_1 \times b_0 \times d_0) + (a_0 \times b_1 \times d_0) \\ &\quad +(a_0 \times b_0 \times d_1))x + (a_0 \times b_0 \times c_0) \\ &= c_{n+m+s} x^{n+m+s} + \cdots + c_1 x + c_0 \end{aligned}$$

Assim,

$$f \cdot (g \cdot h) = (f \cdot g) \cdot h.$$

vi) Distributividade em relação a $\cdot$:
Suponha, sem perda de generalidade que $n > m = s$. Os outros casos são análogos ao completar cada um dos polinômios com monômios da forma $0_{\mathbb{A}}x^i$.

$$\begin{aligned}
f \cdot (g + h) &= f \cdot ((b_m + d_m)x^m + \cdots + (b_1 + d_1)x + \\
&\quad +(b_0 + d_0)) \\
&= (a_n \times (b_m + d_m))x^{n+m} + \cdots + \\
&\quad (a_1 \times (b_0 + d_0)) + a_0 \times (b_1 + d_1))x \\
&\quad +(a_0 \times (b_0 + d_0)) \\
&= (a_n \times b_m)x^{n+m} + (a_n \times d_m)x^{n+m} + \cdots + \\
&\quad (a_1 \times b_0 + a_0 \times b_1)x + (a_1 \times d_0 + a_0 \times d_1)x \\
&\quad +(a_0 \times b_0) + (a_0 \times d_0) \\
&= ((a_n \times b_m)x^{n+m} + \cdots + (a_1 \times b_0)x \\
&\quad +(a_0 \times b_0)) + ((a_n \times d_m)x^{n+m} + \cdots + \\
&\quad (a_0 \times d_1)x + (a_0 \times d_0)) \\
&= (f \cdot g) + (f \cdot h).
\end{aligned}$$

Portanto o conjunto $\mathbb{A}[x]$ com as operações definidas acima é um anel, chamado *anel de polinômios* sobre $\mathbb{A}$ em uma *indeterminada* $x$.

**Exemplo 2.2.1.** $\mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}[x]$, com as operações usuais de soma e multiplicação definidas anteriormente também são anéis de polinômios.

É importante ressaltar que os símbolos $x^1, x^2, \ldots, x^n$ não representam nenhum elemento do anel $\mathbb{A}[x]$. Eles servem como lugares "convenientes" para separar os elementos do anel.

Além disso, o anel $\mathbb{A}[x]$ tem características que dependem do anel $\mathbb{A}$. Os resultados a seguir garantem esse fato.

**Proposição 2.3.** *Se $(\mathbb{A}, +, \times)$ é um anel comutativo, então $\mathbb{A}[x]$ também o é.*

*Demonstração.* Considere $f = a_1 + \cdots + a_n x^n$ e $g = b_1 + \cdots + b_m x^m$ dois elementos do anel $\mathbb{A}[x]$. Assim

$$f \cdot g = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0,$$

onde

$$c_k = (a_k \times b_0) + (a_{k-1} \times b_1) + \cdots + (a_0 \times b_k),$$

para $k = 0, 1, \cdots, n+m$. Como $\mathbb{A}$ é comutativo, então

$$c_k = (b_0 \times a_k) + (b_1 \times a_{k-1}) + \cdots + (b_k \times a_0).$$

Desta forma,

$$f \cdot g = c_{m+n} x^{m+n} + ... + c_1 x + c_0 = g \cdot f.$$

Portanto $\mathbb{A}[x]$ é comutativo. ■

**Proposição 2.4.** *Se $(\mathbb{A}, +, \times)$ é um anel comutativo com unidade, então $\mathbb{A}[x]$ também o é.*

*Demonstração.* Sabendo que $(\mathbb{A}, +, \times)$ é um anel comutativo com unidade, considere $1_{\mathbb{A}}$ sendo a unidade de $\mathbb{A}$. Tome $g = 1_{\mathbb{A}}$ e $f$ um polinômio qualquer pertencente a $\mathbb{A}[x]$, assim temos que

$$\begin{aligned} f \cdot g &= (a_n x^n + \ldots + a_0) \cdot (0x^n + \ldots + 0x + 1_{\mathbb{A}}) \\ &= ((a_n \times 0) + \ldots + (a_n \times 1_{\mathbb{A}}))x^n + \ldots + \\ &\quad ((a_0 \times 0) + \ldots + (a_0 \times 1_{\mathbb{A}})) \\ &= a_n x^n + \ldots + a_0 \\ &= f. \end{aligned}$$

Pela Proposição 2.3 podemos garantir que $f \cdot g = g \cdot f$, pois $\mathbb{A}[x]$ é um anel comutativo. Portanto $\mathbb{A}[x]$ é um anel comutativo com unidade. ■

**Corolário 2.5.** *Se $(\mathbb{A}, +, \times)$ é anel de integridade, então $\mathbb{A}[x]$ também é anel de integridade.*

*Demonstração.* Considere $f, g$ dois elementos de $\mathbb{A}[x]$. Sabemos que $\mathbb{A}[x]$ é um anel comutativo. Suponha que $f \neq 0_{\mathbb{A}}$ e $g \neq 0_{\mathbb{A}}$. Então

existem $a_n, b_m \in \mathbb{A}$ com $a_n, b_m \neq 0_{\mathbb{A}}$, e $n, m$ os maiores possíveis. Como $\mathbb{A}$ é anel de integridade $a_n \times b_m \neq 0$. Logo,

$$f \cdot g = c_{n+m}x^{n+m} + \cdots + c_0.$$

Como $c_{n+m} = a_n \times b_m \neq 0_{\mathbb{A}}$, então

$$f \cdot g \neq 0.$$

Portanto $\mathbb{A}[x]$ é anel de integridade. ■

A partir das Proposições 2.3 e 2.4, no decorrer de nosso trabalho, vamos usar apenas anéis comutativos com unidade.

Agora vamos definir características próprias de cada polinômio de $\mathbb{A}[x]$.

**Definição 2.6.** Considere $f \in \mathbb{A}[x]$ da forma

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 x^0.$$

i) Chamaremos de *termo* cada parcela de $f$, desde que esta parcela seja não nula, isto é, $a_i x^i$ para todo $i = 1, \ldots, n$ com $a_i \neq 0$.

ii) O $a_i$ é chamada de *coeficiente*, para todo $i = 0, \ldots, n$.

iii) O $x^i$ é chamado de *monômio*, para todo $i = 0, \ldots, n$.

iv) O monômio $x^0$ denotaremos por 1.

v) O conjunto de todos os monômios de $f$ é indicado por $\mathbb{M}(f)$.

**Exemplo 2.2.2.** Considere o polinômio

$$f = 8x^4 + 3x^3 + 5x^2 + 2x + 1 \in \mathbb{R}[x].$$

Assim

1. Os *termos* de $f$ são $8x^4, 3x^3, 5x^2, 2x, 1$.
2. Os *coeficientes* de $f$ são $8, 3, 5, 2, 1$.

3. Os *monômios* de $f$ são $x^4, x^3, x^2, x^1, x^0$.
4. $\mathbb{M}(f) = \{x^4, x^3, x^2, x, 1\}$

**Definição 2.7.** Dado $f \in \mathbb{A}[x]$ da forma

$$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 x^0,$$

com $a_n \neq 0_{\mathbb{A}}$.

i) Chamamos de *grau de* $f$ e denotaremos por $\mathrm{gr}(f)$, o inteiro $max\{i, x^i \in \mathbb{M}(f)\}$.

ii) O *termo líder* de $f$ é $\mathrm{tl}(f) = a_n x^n$.

iii) $\mathrm{cl}(f) = a_n$ é chamado de *coeficiente líder*.

iv) $\mathrm{ml}(f) = x^n$ de *monômio líder* onde $n = \mathrm{gr}(f)$.

v) $\mathrm{gr}(f) = 0$ se, e somente se, $f \in \mathbb{A} \setminus \{0\}$.

*Observação* 1. i) Vamos convencionar que $\mathrm{gr}(0) = -\infty$.

ii) Um polinômio é dito *mônico* se seu coeficiente líder é $1_{\mathbb{A}}$.

iii) Para $f \in \mathbb{A}[x]$ não nulo, temos que $\mathrm{ml}(f) = \frac{\mathrm{tl}(f)}{\mathrm{cl}(f)}$.

**Exemplo 2.2.3.** Sejam $f = 5x^2 + 4x + 8$ e $g = 8x^2 + 9$ com $f, g \in \mathbb{R}[x]$, então

$$f + g = 13x^2 + 4x + 17 \text{ e}$$

$$f \cdot g = 40x^4 + 32x^3 + 109x^2 + 36x + 72.$$

Logo temos

i) $\mathrm{gr}(f) = 2$, $\mathrm{gr}(g) = 2$, $\mathrm{gr}(f+g) = 2$, $\mathrm{gr}(f \cdot g) = 4$;

ii) $\mathrm{tl}(f) = 5x^2$, $\mathrm{tl}(g) = 8x^2$, $\mathrm{tl}(f+g) = 13x^2$, $\mathrm{tl}(f \cdot g) = 40x^4$;

iii) $\mathrm{cl}(f) = 5$, $\mathrm{cl}(g) = 8$, $\mathrm{cl}(f+g) = 13$, $\mathrm{cl}(f \cdot g) = 40$;

iv) $\mathrm{ml}(f) = x^2$, $\mathrm{ml}(g) = x^2$, $\mathrm{ml}(f+g) = x^2$, $\mathrm{ml}(f \cdot g) = x^4$.

v) $\mathbb{M}(f) = \{x^2, x, 1\}$, $\mathbb{M}(g) = \{x^2, 1\}$, $\mathbb{M}(f+g) = \{x^2, x, 1\}$.

**Exemplo 2.2.4.** Tome $f = 2x^2 + 3x + 6$ e $g = 4x^4 + 4x + 8$ com $f, g \in \mathbb{R}[x]$. Vamos calcular $f + g$.

$$\begin{aligned} f + g &= (2x^2 + 3x + 6) + (4x^4 + 4x + 8) \\ &= 4x^4 + 2x^2 + 7x + 14. \end{aligned}$$

Assim,

$$\mathbb{M}(f+g) = \{x^4, x^2, x, 1\}, \mathbb{M}(f) = \{x^2, x, 1\} \text{ e } \mathbb{M}(g) = \{x^4, x, 1\}.$$

O exemplo da soma de polinômios visto acima, nos leva a indagar se

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

Com efeito, basta lembrar que ao tomarmos $f$ um polinômio de $\text{gr}(f) = n$ e $g$ um polinômio de $\text{gr}(g) = m$, então os termos de $f + g$ são escritos da forma $(a_j + b_j)x^j$, com $a_j + b_j \neq 0_{\mathbb{A}}$ para todo $0 \leq j \leq max\{n, m\}$. Assim todo monômio de $f + g$ é um monômio de $f$ ou de $g$.

Além disso, temos que

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

Veja que, se $\text{gr}(f) \neq \text{gr}(g)$, então

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

Neste caso, temos que $\text{gr}(f+g) = max\{\text{gr}(f), \text{gr}(g)\}$. Agora, se $f \cdot g = 0_{\mathbb{A}}$, temos que $\text{gr}(f \cdot g) = -\infty$, como mencionado na Observação 1 e, com certeza, $\text{gr(f} \cdot \text{g)} \leq \text{gr}(f) + \text{gr}(g)$.

Se $f \cdot g \neq 0$ com $a_n \neq 0_{\mathbb{A}}, b_m \neq 0_{\mathbb{A}}$, como

$$f \cdot g = c_{n+m}x^{n+m} + \ldots + c_1 x + c_0$$

temos que $\text{gr}(f \cdot g) \leq n + m = \text{gr}(f) + \text{gr}(g)$, com a igualdade acontecendo se $c_{n+m} = a_n \times b_m \neq 0_{\mathbb{A}}$. Note que esta condição será satisfeita sempre que $\mathbb{A}$ for um anel de integridade.

Desta forma, a partir de agora vamos nos restringir a este caso, onde $\mathbb{A}$ e consequentemente $\mathbb{A}[x]$ são anéis de integridade. Portanto, para todos $f, g \in \mathbb{A}[x]$, temos que

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

$$\text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g).$$

**Exemplo 2.2.5.** Tome $f = 2x^2+4x+2$, $g = 3x^2+3 \in \mathbb{R}[x]$. Vamos calcular $f \cdot g$.

$$\begin{aligned} f \cdot g &= (2x^2 + 4x + 2) \cdot (3x^2 + 3) \\ &= 6x^4 + 12x^3 + 12x^2 + 12x + 6. \end{aligned}$$

Logo, $\text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g)$.

### 2.2.1 Algoritmo da divisão para o anel de polinômios

A partir de agora iremos tomar o anel $\mathbb{A}$ como sendo um corpo $\mathbb{K}$ onde as operações serão dadas por $+$ e $\cdot$ respectivamente. Agora toda a teoria que é estudada daqui em diante gira em torno de uma pergunta: quando um polinômio não nulo de $\mathbb{K}[x]$ divide outro?

Vamos iniciar nossos estudos para elementos de $\mathbb{K}[x]$, no caso em que os polinômios envolvidos, tenham apenas um termo não nulo.

Em $\mathbb{K}[x]$, um termo não nulo $ax^i$ divide $bx^j$, se e somente se, existe $g \in \mathbb{K}[x]$ tal que $bx^j = g \cdot ax^i$. Essa igualdade nos indica que $\text{gr}(g) = j - i$, ou seja, é condição necessária para que $ax^i | bx^j$, que $i \leq j$.

Se $bx^j = g \cdot ax^i$ e $g = c_{j-i}x^{j-i} + \cdots + c_0$, então

$$bx^j = c_{j-i}ax^j + \cdots + c_1ax^{i+1} + c_0ax^j$$

que por consequência nos indica que $b = c_{j-i}a$, equivalente $a|b$ e $c_k a = 0$ para $0 \leq k < j - i$. Como $\mathbb{K}$ é um domínio e $a \neq 0$, temos $c_k = 0$ para todo $0 \leq k < j - i$. Logo $ax^i | bx^j$ se, e somente se, $i \leq j$ e $a|b$. Como $\mathbb{K}$ é um corpo, então temos que $a|b$ sempre que $a \neq 0$.

Logo em $\mathbb{K}[x]$ temos que, $ax^i$ divide $bx^j$ se, e somente se, $i \leq j$ e neste caso,

$$\frac{bx^j}{ax^i} = ba^{-1}x^{(j-i)}.$$

Utilizando este fato, agora veremos o algoritmo da divisão para quaisquer polinômios em uma variável. Este algoritmo é bastante conhecido e é de grande importância para o estudo dos próximos algoritmos.

**Teorema 2.6.** *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*

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

*Demonstração.* (Existência.) Se $\mathrm{gr}(f) < \mathrm{gr}(g)$, então tomando $q = 0$ e $r = f$ temos $f = 0 \cdot g + f$ satisfazendo as condições do teorema. Por outro lado, se $\mathrm{gr}(f) \geq \mathrm{gr}(g)$, então procedemos a prova por indução sobre $\mathrm{gr}(f)$. Vamos assumir que o resultado é válido para qualquer polinômio com o grau menor que o $\mathrm{gr}(f)$. Como $\mathrm{gr}(f) \geq \mathrm{gr}(g)$ temos que $\mathrm{tl}(g)$ divide $\mathrm{tl}(f)$ e assim,

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

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

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

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

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

com $\mathrm{gr}(r_1) < \mathrm{gr}(g)$. Assim,

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

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

Para provar a 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 $\text{gr}(r_i) < \text{gr}(g)$ para $i \in \{1, 2\}$, isto é,

$$\text{gr}(g) > max\{\text{gr}(r_1), \text{gr}(r_2)\}.$$

Segue que $0_{\mathbb{A}} = f - f = (q_1 - q_2)g + (r_1 - r_2)$, ou seja,

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

Se $r_2 \neq r_1$, então como $\mathbb{K}[x]$ é um domínio e $g \neq 0$, segue que $q_1 \neq q_2$ e

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

Um absurdo! Assim, $r_2 = r_1$ e obviamente $q_2 = q_1$. ■

**Exemplo 2.2.6.** Tome

$$f = x^4 + x^3 - 7x^2 + 9x - 1 \text{ e } g = x^2 + 3x - 2 \text{ em } \mathbb{R}[x],$$

vamos aplicar o algoritmo na divisão de $f = x^4 + x^3 - 7x^2 + 9x - 1$ por $g = x^2 + 3x - 2$.

| | | | | | $x^2 + 3x - 2$ |
|---|---|---|---|---|---|
| $\cancel{x^4}$ | $+x^3$ | $-7x^2$ | $+9x$ | $-1$ | $q = x^2 - 2x + 1$ |
| $-\cancel{x^4}$ | $-3x^3$ | $+2x^2$ | | | |
| | $-\cancel{2x^3}$ | $-5x^2$ | $+9x$ | $-1$ | |
| | $+\cancel{2x^3}$ | $+6x^2$ | $-4x$ | | |
| | | $\cancel{x^2}$ | $+5x$ | $-1$ | |
| | | $-\cancel{x^2}$ | $-3x$ | $+2$ | |
| | | | $r = 2x$ | $+1$ | |

Então $f = q \cdot g + r$, ou seja,

$$f = (x^2 - 2x + 1) \cdot (x^2 + 3x - 2) + (2x + 1).$$

**Exemplo 2.2.7.** Tome

$$f = x^4 + x^2 + x \text{ e } g = x^2 - x + 1 \text{ em } \mathbb{R}[x],$$

vamos aplicar o algoritmo na divisão de $f = x^4 + x^2 + x$ por $g = x^2 - x + 1$.

$$\begin{array}{lll|l}
\cancel{x^4} & \cancel{+x^2} & +x & x^2 - x + 1 \\
\cancel{-x^4} & +x^3 & \cancel{-x^2} & \hline
 & \cancel{+x^3} & \cancel{+x} & q = x^2 + x + 1 \\
 & \cancel{-x^3} & +x^2 \quad \cancel{-x} & \\
 & & \cancel{x^2} & \\
 & & \cancel{-x^2} \quad +x \quad -1 & \\
 & & r = x \quad -1 &
\end{array}$$

Assim, $f = q \cdot g + r$, ou seja

$$f = (x^2 + x + 1) \cdot (x^2 - x + 1) + (x - 1).$$

**Exemplo 2.2.8.** Considere $f = \bar{3}x^3 + \bar{2}x^2 + \bar{5}x$ e $g = \bar{2}x$ em $\mathbb{Z}_7[x]$ Vamos aplicar o algoritmo na divisão de $f = \bar{3}x^3 + \bar{2}x^2 + \bar{5}x$ por $g = \bar{2}x$.

$$\begin{array}{lll|l}
\cancel{\bar{3}x^3} & +\bar{2}x^2 & +\bar{5}x & \bar{2}x \\
\cancel{-\bar{3}x^3} & & & \hline
 & \cancel{+\bar{2}x^2} & +\bar{5}x & q = \bar{5}x^2 + \bar{1}x + \bar{6} \\
 & \cancel{-\bar{2}x^2} & & \\
 & & \cancel{\bar{5}x} & \\
 & & \cancel{-\bar{5}x} & \\
 & & 0 &
\end{array}$$

Pelo algoritmo da divisão em $\mathbb{K}[x]$, $f$ pode ser reescrito sendo

$$f = (\bar{5}x^2 + \bar{1}x + \bar{6}) \cdot (\bar{2}x) + \bar{0}.$$

# 3 ANEL DE POLINÔMIOS EM VÁRIAS INDETERMINADAS

Nesta capítulo apresentamos o anel de polinômios em várias variáveis e vamos estudar ordens monomiais que é o passo mais importante para que possamos realizar o algoritmo da divisão em várias variáveis.

Começamos esta seção definindo o anel de polinômios em várias variáveis. Anteriormente estávamos considerando $\mathbb{K}[x]$, onde os polinômios tinham uma indeterminada em $x$. Como $\mathbb{K}[x]$ é um anel de integridade, temos que o anel $\mathbb{K}[x][y]$ também é. Expressamos os elementos de $\mathbb{K}[x][y]$ da forma

$$f_n y^n + f_{n-1} y^{n-1} + \cdots + f_1 y + f_0 \tag{3.1}$$

com

$$f_i = \sum_{j=0}^{m_i} a_{ij} x^j \in \mathbb{K}[x], n, m_i \in \mathbb{N} \text{ e } a_{ij} \in \mathbb{K}.$$

para todo $i = 0, \ldots, n$.
Vejamos que $g = f_n y^n + f_{n-1} y^{n-1} + \cdots + f_1 y + f_0 \in \mathbb{K}[x][y]$, como em (3.1), podemos escrever

$$\begin{aligned} g &= \left(\sum_{j=0}^{m_n} a_{nj} x^j\right) y^n + \cdots + \left(\sum_{j=0}^{m_1} a_{1j} x^j\right) y + \left(\sum_{j=0}^{m_0} a_{0j} x^j\right) \\ &= \left(\sum_{l=0}^{n} a_{lm_k} y^l\right) x^{m_k} + \cdots + \left(\sum_{l=0}^{n} a_{l1_k} y^l\right) x + \left(\sum_{l=0}^{n} a_{l0_k} y^l\right) \end{aligned}$$

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

$$\mathbb{K}[x][y] \subseteq \mathbb{K}[y][x].$$

Do mesmo modo, mostramos que

$$\mathbb{K}[y][x] \subseteq \mathbb{K}[x][y]].$$

Assim,

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

Vamos denotar $\mathbb{K}[x][y] = \mathbb{K}[y][x]$ por $\mathbb{K}[x, y]$. Para facilitar a notação dos elementos $g \in \mathbb{K}[x, y]$ podemos escrever

$$g = \sum_{(\alpha_1,\alpha_2)\in J} a_{(\alpha_1,\alpha_2)} x^{\alpha_1} y^{\alpha_2}.$$

com $J$ um conjunto finito em $\mathbb{N}^2$ e $a_{(\alpha_1,\alpha_2)} \in \mathbb{K}$. Procedendo da mesma forma que antes podemos construir o anel de integridade $\mathbb{K}[x_1, \ldots, x_n]$ nas indeterminadas $x_1, \ldots, x_n$. Com esta mesma nomenclatura, $\mathbb{K}[x_1, \ldots, x_n]$ é chamado de *anel de polinômio nas indeterminadas* $x_1, \ldots, x_n$ *com coeficientes no corpo* $\mathbb{K}$.

Analisando os elementos de $\mathbb{K}[x_1, \ldots, x_n]$, podemos concluir que um polinômio $f$ não nulo em $\mathbb{K}[x_1, \ldots, x_n]$ é uma soma finita de termos, a qual pode ser escrita da forma

$$f = \sum_{\alpha\in J} a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i}, \tag{3.2}$$

com $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n, a_\alpha \in \mathbb{K}$ e $J \subset \mathbb{N}^n$ finito. Assim podemos definir de maneira mais clara algumas propriedades dos polinômios de $\mathbb{K}[x_1, \ldots, x_n]$.

**Definição 3.1.** 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 $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. O elemento $a_\alpha \in \mathbb{K}$ do termo é chamado de *coeficiente do termo* e $\prod_{i=1}^{n} x_i^{\alpha_i}$ é denominado *monômio*. Chamamos de *grau(total)* do monômio $\prod_{i=1}^{n} x_i^{\alpha_i}$ o número natural dado por $\mathrm{gr}(\prod_{i=1}^{n} x_i^{\alpha_i}) = \sum_{i=1}^{n} \alpha_i$.

Mesmo nos restringindo ao caso em que $\mathbb{K}[x_1, \ldots, x_n]$ é um anel comutativo, vamos convencionar que escreveremos as potências das variáveis de um monômio da esquerda para direita, respeitando a ordem que aparece na notação do anel a qual este polinômio pertence, isto é, mesmo que $x^5yz^4, yz^4x^5, z^4yx^5 \in \mathbb{K}[x, y, z]$, vamos usar a notação $x^5yz^4$.

Sejam $(k_1, \ldots, k_n) \in \mathbb{K}^n$ e $f \in \mathbb{K}[x_1, \ldots, x_n]$ com

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

Denotaremos por $f(k_1, \ldots, k_n)$ o elemento

$$\sum_{\alpha \in J} a_\alpha \prod_{i=1}^{n} k_i^{\alpha_i} \in \mathbb{K}.$$

Se $f \in \mathbb{K}[x_1, \ldots, x_n]$ é não nulo, vamos denotar 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 chamaremos

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

o *grau total* de $f$.

Como no caso de polinômios em uma indeterminada, se constata igualmente que

$$\mathrm{gr}(f+g) \leq max\{\mathrm{gr}(f), \mathrm{gr}(g)\} \text{ e } \mathrm{gr}(f \cdot g) = \mathrm{gr}(f) + \mathrm{gr}(g).$$

**Exemplo 3.0.1.** Considere os polinômios $f = 2x^2y + 2y^2 + x$ e $g = 3x^3 + x^2y + 2$ em $\mathbb{R}[x, y]$. Vamos calcular $\mathrm{gr}(f+g)$ e $\mathrm{gr}(f \cdot g)$

$$\begin{aligned} f + g &= (2x^2y + 2y^2 + x) + (3x^3 + x^2y + 2) \\ &= (3x^3 + 3x^2y + 2y^2 + x + 2). \end{aligned}$$

Assim

$$\begin{aligned} \mathrm{gr}(f+g) &\leq max\{\mathrm{gr}(f), \mathrm{gr}(g)\} \\ &\leq \{3, 3\} \\ &= 3. \end{aligned}$$

$$\begin{aligned} f \cdot g &= (2x^2y + 2y^2 + x) \cdot (3x^3 + x^2y + 2) \\ &= (6x^5y + 2x^4y^2 + 4x^2y + 6x^3y^2 + 2x^2y^3 + \\ &\quad + 4y^2 + 3x^4 + x^3y + 2x) \\ &= (6x^5y + 3x^4 + 2x^4y^2 + 6x^3y^2 + x^3y + \\ &\quad 2x^2y^3 + 4x^2y + 2x + 4y^2. \end{aligned}$$

Logo,

$$\begin{aligned} \mathrm{gr}(f \cdot g) &= \mathrm{gr}(f) + \mathrm{gr}(g) \\ &= 3 + 3 \\ &= 6. \end{aligned}$$

Da mesma forma que em polinômios de uma variável, podemos afirmar que $\text{gr}(f \cdot g) = \text{gr}(f) + \text{gr}(g)$ somente quando estamos trabalhando com anéis de integridade.

## 3.1 ORDENS MONOMIAIS

Sabendo que nosso objetivo é apresentar o algoritmo da divisão em $\mathbb{K}[x_1, \ldots, x_n]$, devemos analisar cada passo do algoritmo para que possamos resolver todos os obstáculos que podem ser encontrados.

Como no algoritmo da divisão em $\mathbb{K}[x]$ o primeiro conceito que precisamos é determinar o que é o termo líder de um polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$. O termo líder é necessário para que possamos ordenar o polinômio, sabendo qual monômio de $f$ é maior para que seja possível efetuar o algoritmo. Além disso, é preciso que o conceito de termo líder, sirva para qualquer polinômio pertencente a $\mathbb{K}[x_1, \ldots, x_n]$, ou seja, para todos os monômios deste anel, deve valer esta ordenação.

**Definição 3.2.** 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 $x_1^0 \cdot \cdots \cdot x_n^0$ será denotado por 1.

Podemos nos perguntar, porque não utilizar o conceito de grau total do mesmo modo que utilizamos em $\mathbb{K}[x]$ para ordenar monômios. Vamos analisar o polinômio abaixo:

$$x^2yz^2 + x^2y^2z + 3x^4y + 3x^3y^2 - y^4z + 2x^4z. \tag{3.3}$$

Utilizando o conceito de grau total de $\mathbb{K}[x]$ percebemos que todos os monômios tem o mesmo grau. Por conta de problemas deste tipo, é necessário estudarmos ordens monomiais para decidir quem é o termo líder de um polinômio em $\mathbb{K}[x_1, \ldots, x_n]$.

Para iniciar nossos estudos precisamos revisar o conceito de relação de ordem.

**Definição 3.3.** 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 $c_1 \prec c_2$.

Uma relação de ordem sobre o conjunto $C$ é *total* quando para todos $c_1, c_2 \in C$,

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

Queremos definir uma relação de ordem sobre $\mathbb{M}_n$ que seja total, pois com ela teremos bem definido o conceito de termo líder de um elemento

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

De fato, podemos definir

$$\mathrm{ml}(f) = max \left\{ \prod_{i}^{n} x_i^{\alpha_i} \right\} \in \mathbb{M}(f)$$

onde o máximo é tomado com respeito à ordem $\preceq$ fixada e considerar o *termo líder* de $f$ como $a_\alpha \cdot \mathrm{ml}(f)$, isto é, $\mathrm{tl}(f) = a_\alpha \, \mathrm{ml}(f)$. Mas, precisamos nos atentar a outros pontos que existem na divisão de um polinômio $f$ por $g$ em $\mathbb{K}[x]$.

Considerando

$$\mathrm{tl}(f) = a_\alpha \prod_{i=1}^{n} x_i^{\alpha_i} \text{ e } \mathrm{tl}(g) = a_\beta \prod_{i=1}^{n} x_i^{\beta_i}$$

devemos verificar se $\mathrm{tl}(g) | \, \mathrm{tl}(f)$, 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

$$\mathrm{tl}(f) = a_\gamma \cdot m_1 \cdot \mathrm{tl}(g),$$

ou equivalentemente,

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

Isso ocorre se, e somente se, $\beta_i \leq \alpha_i$ para todo $i = 1, \ldots, n$. Nos casos que isso ocorre, devemos calcular $f - a_\gamma \cdot m_1 \cdot g$ e repetir o argumento para o resultado que se obter. Devemos lembrar que no caso de polinômios em $\mathbb{K}[x]$, encontramos

$$\mathrm{gr}(f - a_\gamma \cdot m_1 \cdot g) < \mathrm{gr}(f),$$

que podemos reescrever utilizando a noção de monômio líder, como

$$\mathrm{ml}(f - a_\gamma \cdot m_1 \cdot g) \prec \mathrm{ml}(f).$$

Devemos nos atentar a uma propriedade que aparentemente é simples, mas muito importante, que se esconde nessas condições, ou seja, nas expressões

$$\mathrm{tl}(f) = a_\gamma \cdot m_1 \cdot \mathrm{tl}(g) \text{ e } \mathrm{ml}(f - a_\gamma \cdot m_1 \cdot g) \prec \mathrm{ml}(f).$$

De fato, a última condição nos mostra que se

$$m_2 \in \mathbb{M}(g) \text{ e } m_2 \prec \mathrm{ml}(g), \text{ então } m_1 \cdot m_2 \prec m_1 \cdot ml(g) = \mathrm{ml}(f),$$

ou seja, uma ordem total sobre $\mathbb{M}_n$ deve ser compatível com o produto. Em outras palavras, se $m_1, m_2 \in \mathbb{M}_n$ são tais que $m_1 \preceq m_2$, então

$$m_1 \cdot m_3 \preceq m_2 \cdot m_3 \; \forall \; m_3 \in \mathbb{M}_n.$$

Um dos últimos, mas não menos importante, aspecto do algoritmo da divisão, é garantir que ele seja feito em um número finito de passos, devemos ter essa garantia para conseguirmos finalizá-lo. Esta etapa está condicionada à condição

$$\mathrm{ml}(f - a_\gamma \cdot m_1 \cdot g) \prec \mathrm{ml}(f)$$

em cada etapa do algoritmo, que pode ser representada de outro modo, se requisitarmos que a ordem total $\preceq$ sobre $\mathbb{M}_n$ seja uma boa

ordem, isto é, que todo subconjunto não vazio de $\mathbb{M}_n$ possua um menor elemento com respeito à $\preceq$. Portanto o algoritmo tem que parar.

Vamos considerar sobre $\mathbb{M}_n$ ordens que possuem as propriedades que destacamos acima.

**Definição 3.4.** Uma *ordem monomial* $\preceq$ sobre $\mathbb{M}_n$ é uma relação de ordem total que satisfaz:

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

**Lema 3.1.** *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.*

*Demonstração.* Seja $m_1 \succeq m_2 \succeq m_3 \succeq \ldots$ uma sequência decrescente de elementos de $\mathbb{M}_n$, então $S = \{m_1, m_2, m_3 \ldots\} \neq 0$ admite um menor elemento com respeito à $\preceq$, ou seja, a sequência é finita. ■

Já sabemos como ordenar monômios em uma variável, vamos tentar ordenar monômios em $\mathbb{K}[x_1, \ldots, x_n]$ usando a mesma ideia. Considere um polinômio não nulo $f \in \mathbb{K}[x_1, \ldots, x_n]$ podemos considerá-lo como um polinômio em $x_1$ com coeficientes em $\mathbb{K}[x_2, \ldots, x_n]$. Vamos usar um argumento indutivo sobre o número de indeterminadas e tentar ordenar os monômios em $\mathbb{K}[x_1, \ldots, x_n]$ do mesmo modo. Considere por exemplo o polinômio

$$f = x^2y^3z^2 + x^2y^2z^4 + 3x^4yz^5 + 3x^3y^2 - y^4z + 2x^4z + x^32y^2z.$$

Considerando que nosso polinômio $f \in \mathbb{K}[x, y, z]$, vamos ordená-lo de modo que consideramos os coeficientes em $\mathbb{K}[y, z]$ ordenados pelo grau em $x$.

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

Agora consideramos os coeficientes que são elementos em $\mathbb{K}[y,z]$, como polinômios em $y$ com coeficientes em $\mathbb{K}[z]$. Vamos ordená-lo considerando os coeficientes em $\mathbb{K}[z]$ e com o grau em $y$.

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

Vamos fazer as multiplicações indicadas acima, e usando a indicação de ordenar monômios listando suas potências em $x$, seguido por $y$ e por fim em $z$ vamos obter

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

Perceba que ao terminar esses passos, o que fizemos foi ordenar os monômios de tal modo que

$$x^{\alpha_1}y^{\alpha_2}z^{\alpha_3}$$

preceda

$$x^{\beta_1}y^{\beta_2}z^{\beta_3},$$

Assim

$$x^{\alpha_1}y^{\alpha_2}z^{\alpha_3} \preceq x^{\beta_1}y^{\beta_2}z^{\beta_3},$$

e isso acontece, se e somente se,

i) $\alpha_1 < \beta_2$ ou

ii) $\alpha_1 = \beta_1$ e $\alpha_2 < \beta_2$ ou

iii) $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$ e $\alpha_3 < \beta_3$.

Para que possamos utilizar a ordenação acima como uma ordem monomial devemos estender o algoritmo para monômios $\mathbb{M}_n$ e, além disso, garantir que tal ordem seja uma relação de ordem total. Considere

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

distintos, diremos que

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

se, e somente se, existe $i \in \{1, \cdots, n\}$ tal que

$$\alpha_i < \beta_i \text{ e } \alpha_j = \beta_j$$

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.

Veja que $\preceq_L$ tem a propriedade reflexiva sobre $\mathbb{M}_n$. Além disso, dados

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

tais que

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

Então

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

De fato, se

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

então existe $k \in \{1, \cdots, n\}$ tal que $\alpha_k \neq \beta_k$ e sendo $j$ o menor índice. Caso $\alpha_j < \beta_j$, então não podemos ter

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

Se $\beta_j < \alpha_j$, então não podemos ter

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

Assim

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

ou seja, $\preceq_L$ é anti-simétrica. Agora suponha que

$$\prod_{i=1}^{n} x_i^{\alpha_i} \preceq_L \prod_{i=1}^{n} x_i^{\beta_i} \text{ e } \prod_{i=1}^{n} x_i^{\beta_i} \preceq_L \prod_{i=1}^{n} x_i^{\gamma_i}. \tag{3.4}$$

Se em algum dos casos ocorrer a igualdade, é fácil verificar que

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

Assumindo que nenhuma igualdade ocorra em (3.4). existem $i, k \in \{1, \ldots, n\}$ tais que

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

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 $l < k$. Assim, qualquer uma destas possibilidades nos permite concluir que

$$\prod_{i=1}^{n} x_i^{\alpha i} \preceq_L \prod_{i=1}^{n} x_i^{\gamma_i},$$

logo, $\preceq_L$ é transitiva. Usando argumentos similares, podemos garantir que $\preceq_L$ é uma relação de ordem total sobre $\mathbb{M}_n$. Tal ordem é chamada de *lexicográfica*. Nesta ordem lexicográfica usamos a mesma ordem do dicionário, ou seja, determinamos o termo líder pela posição da variável. Por exemplo

$$x^3 y^{1000} z \preceq_L x^4.$$

Veja que o termo $x^4$ pode ser descrito como $xxxx$, e o termo $x^3 y^{1000} z$ é descrito como $xxxyyy \cdots yyz$. Note que por maior que seja o valor do expoente da variável $y$, ela não tem importância desde que o valor da variável $x$ do outro polinômio seja maior. Sendo mais formal podemos resumir a ordem lexicográfica na seguinte definição.

**Definição 3.5. (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 $j < i$.

Da mesma forma que antes podemos criar outras ordens monomiais. Por exemplo a ordem *Lexicográfica graduada*, o primeiro olhar que devemos ter sobre um polinômio é sobre o grau total de cada termo. Caso o grau total de todos os termos forem iguais, recorremos à ordem lexicográfica acima e seguiremos ordenando pela ordem do dicionário. Considerando o polinômio abaixo,

$$x^4 \preceq_{LG} x^3y^{1000}z.$$

Veja que agora o valor da variável $x$ não importa, tendo em vista que o grau total do monômio $x^3y^{1000}z$ é 1004, enquanto por outro lado o monômio $x^4$ tem o seu grau total sendo 4. Desta maneira podemos verificar que $1004 > 4$. Logo

$$x^4 \preceq_{LG} x^3y^{1000}z.$$

Sendo mais formal ela é definida da forma a seguir.

**Definição 3.6. (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:

i) $\text{gr}(\prod_{i=1}^n x_i^{\alpha_i}) < \text{gr}(\prod_{i=1}^n x_i^{\beta_i})$ ou

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

**Exemplo 3.1.1.** Sejam os monômios

$$x^3yz, x^4y^4, y^4z^2, x^8, x^5y^2z^4, x^2y^3z^2 \in \mathbb{K}[x, y, z].$$

Vamos fazer ordenação considerando as ordens monomiais definidas acima.

$$y^4z^2 \preceq_L x^2y^3z^2 \preceq_L x^3yz \preceq_L x^4y^4 \preceq_L x^5y^2z^4 \preceq_L x^8.$$

$$x^3yz \preceq_{LG} y^4z^2 \preceq_{LG} x^2y^3z^2 \preceq_{LG} x^4y^4 \preceq_{LG} x^8 \preceq_{LG} x^5y^2z^4.$$

**Exemplo 3.1.2.** Considere os monômios

$$\bar{2}x^4y^5\bar{3}z^7, x^7y^5z^2, \bar{8}xy^{11}z^8, \bar{3}y^2z^3, \bar{7}z^3 \in \mathbb{Z}_9[x].$$

Vamos fazer a ordenação considerando as ordens monomiais definidas acima.

$$\bar{7}z^3 \preceq_L \bar{3}y^2z^3 \preceq_L \bar{8}xy^{11}z^8 \preceq_L \bar{2}x^4y^5\bar{3}z^7 \preceq_L x^7y^5z^2.$$

$$\bar{7}z^3 \preceq_{LG} \bar{3}y^2z^3 \preceq_{LG} x^7y^5z^2 \preceq_{LG} \bar{2}x^4y^5\bar{3}z^7 \preceq_{LG} \bar{8}xy^{11}z^8.$$

**Exemplo 3.1.3.** Considere os monômios

$$x^2y^{80}z, x^5yz, xyz^{70}, x^{40}y^{20}z^{30}, xy^3, z^8 \in \mathbb{R}[x].$$

Vamos fazer a ordenação considerando as ordens monomiais definidas acima.

$$z^8 \preceq_L xyz^{70} \preceq_L xy^3 \preceq_L x^2y^{80}z \preceq_L x^5yz \preceq_L x^{40}y^{20}z^{30}.$$

$$xy^3 \preceq_{LG} x^5yz \preceq_{LG} z^8 \preceq_{LG} xyz^{70} \preceq_{LG} x^2y^{80}z \preceq_{LG} x^{40}y^{20}z^{30}.$$

### 3.1.1 Algoritmo da divisão de polinômios em várias variáveis

**Teorema 3.2.** ***(Algoritmo da divisão em*** $\mathbb{K}[x_1, \ldots, x_n]$*)* *Fixada uma ordem monomial* $\preceq$ *e dado* $g \in \mathbb{K}[x_1, \ldots, x_n]\backslash\{0\}$*, 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.*

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

*Demonstração.* (Existência.) Se $f = 0$, então

$$f = 0 = 0 \cdot g + 0 = q \cdot g + r$$

ou seja, $q = r = 0$, satisfazem as condições do teorema. Sejam $f_0 = f \neq 0$ e o conjunto $S(f_0) = \{m \in \mathbb{M}(f); \mathrm{ml}(g)|m\}$ 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

$$f_1 = f - \frac{a_0 m_0}{\mathrm{tl}(g)} g.$$

Agora consideramos o conjunto $S(f_1) = \{m \in \mathbb{M}(f_1); \mathrm{ml}(g)|m\}$, se $S(f_1) = \emptyset$, então definimos

$$q = \frac{a_0 m_0}{\mathrm{tl}(g)}, r = f_1$$

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

$$f_2 = f_1 - \frac{a_1 m_1}{\mathrm{tl}(g)} g.$$

Note que $m_0 \succeq m_1$, uma vez que

$$\mathbb{M}(f_1) \subseteq \mathbb{M}(f) \cup \mathbb{M}\left(\frac{m_0}{\mathrm{tl}(g)} g\right).$$

Repetindo o processo, definimos $S(f_i) = \{m \in \mathbb{M}(f_i); \mathrm{ml}(g)|m\}, m_i = max_{\preceq} S(f_i), a_i \in \mathbb{K}$ o coeficiente de $m_i$ que ocorre em $f_i$ e obtemos uma sequência

$$m_0 \succeq m_1 \succeq m_2 \succeq \cdots .$$

Mas, pelo Lema 3.1, tal sequência deve ser finita, ou equivalentemente, existe $k \in \mathbb{N}$ tal, existe $k \in \mathbb{N}$ tal que

$$S(f_k) = \{m \in \mathbb{M}(f_k); \mathrm{ml}(g)|m\} = \emptyset.$$

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 $\mathrm{ml}(g) \nmid m$ para todo $m \in \mathbb{M}(r_i)$ e $i \in \{1, 2\}$, isto é, $\mathrm{ml}(g) \nmid m$ 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

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

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 $q_1 - q_2 = 0$, isto é, $q_1 = q_2$, o que prova o teorema. ■

**Exemplo 3.1.4.** Considere os polinômios

$$f = xy^4 + x^4 + x^3y + y^3, g = y^3 + x^2 \in \mathbb{R}[x, y].$$

Vamos ordenar seguindo as ordens monomiais vistas anteriormente e depois efetuar o algoritmo da divisão em $\mathbb{R}[xy]$.

Primeiramente ordenamos os polinômios na ordem lexicográfica em seguida fazemos a divisão de $f = x^4 + x^3y + xy^4 + y^3$ por $g = x^2 + y^3$.

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

Portanto, pelo algoritmo da divisão em $\mathbb{K}[x_1, \ldots, x_n]$ temos que

$$f = q \cdot g + r$$

$$f = (x^2 + xy - y^3) \cdot (x^2 + y^3) + (y^6 + y^3).$$

Ordenando os polinômios na ordem lexicográfica graduada, temos

$$f = xy^4 + x^4 + x^3y + y^3, g = y^3 + x^2$$

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

Portanto, pelo algoritmo da divisão em $\mathbb{K}[x_1, \ldots, x_n]$ temos que

$$f = q \cdot g + r$$

$$f = (xy + 1) \cdot (y^3 + x^2) + (x^4 - x^2).$$

**Exemplo 3.1.5.** Considere os polinômios $f = 4xy + y^3 + 2x^2 + 2yz$ e $g = x + y + z$ em $\mathbb{R}[x, y, z]$.

Vamos ordená-los na ordem lexicográfica e aplicar o algoritmo na divisão de $f$ por $g$.

$$\begin{array}{l|l}
\cancel{2x^2} \cancel{+4xy} + y^3 + 2yz & x + y + z \\
\cancel{-2x^2} \cancel{-2xy} - 2xz & \hline
\hline
\cancel{2xy} - 2xz + y^3 \cancel{+2yz} & r = y^3 - 2y^2 + 2yz + 2z^2 \\
\cancel{-2xy} - 2y^2 \cancel{-2yz} & \\
\hline
\cancel{-2xz} + y^3 - 2y^2 & \\
\cancel{+2xz} + 2yz + 2z^2 & \\
\hline
y^3 - 2y^2 + 2yz + 2z^2 &
\end{array}$$

Portanto, $f$ pode ser reescrito sendo $f = q \cdot g + r$

$$f = (2x + 2y - 2z) \cdot (x + y + z) + (y^3 - 2y^2 + 2yz + 2z^2).$$

**Exemplo 3.1.6.** Considere os polinômios $f = y^5 + x^4 + 2xy + x^3$ e $g = x^2 + y \in \mathbb{R}[x, y]$.

Vamos ordená-los primeiramente com a ordem lexicográfica e fazer a divisão de $f$ por $g$.

$$\begin{array}{llll|l}
\cancel{x^4} & +x^3 & +2xy & +y^5 & x^2 + y \\
\cancel{-x^4} & -x^2y & & & \hline
\hline
 & \cancel{x^3} & -x^2y & +2xy \quad +y^5 & q = x^2 + x - y \\
 & \cancel{-x^3} & -xy & & \\
\hline
 & & \cancel{-x^2y} & +xy \quad +y^5 & r = xy + y^5 + y^2 \\
 & & \cancel{+x^2y} & +y^2 & \\
\hline
 & & & xy \quad \cancel{+y^5} \quad \cancel{+y^2} &
\end{array}$$

Lembre que $f$ pode ser reescrito sendo $f = q \cdot g + r$

$$f = (x^2 + x - y) \cdot (x^2 + y) + (xy + y^5 + y^2).$$

Agora vamos ordenar os polinômios $f$ e $g$ na ordem lexicográfica graduada e calcular a divisão de $f = y^5+x^4+x^3+2xy$ por $g = x^2+y$.

$$\begin{array}{llll|l}
\cancel{y^5} & \cancel{+x^4} & +x^3 & +2xy & x^2+y \\
\cancel{-x^4} & -x^2y & & & \hline
x^3 & -x^2y & +2xy & & q = x^2+x-y \\
\cancel{-x^3} & -xy & & & r = y^5+xy+y^2 \\
\hline
 & \cancel{-x^2y} & +xy & & \\
 & \cancel{+x^2y} & +y^2 & & \\
\hline
 & & \cancel{xy} & \cancel{+y^2} &
\end{array}$$

$f$ pode ser escrito como $f = q \cdot g + r$

$$f = (x^2+x-y)\cdot(x^2+y) + (y^5+xy+y^2).$$

**Exemplo 3.1.7.** Considere os polinômio $f = \bar{5}x^4\bar{3}y + \bar{7}y^5 + \bar{5}x + \bar{3}x^5$ e $g = \bar{2}x + \bar{3}y$ em $\mathbb{Z}_7[x]$. Vamos ordená-los usando a ordem lexicográfica e fazer a divisão de $f = \bar{3}x^5 + \bar{5}x^4\bar{3}y + \bar{5}x + \bar{7}y^5$ por $g = \bar{2}x + \bar{3}y$.

$$\begin{array}{llll|l}
\cancel{\bar{3}x^5} & \cancel{+\bar{5}x^4\bar{3}y} & +\bar{5}x & +\bar{7}y^5 & \bar{2}x+\bar{3}y. \\
\cancel{-\bar{3}x^5} & \cancel{-\bar{5}x^4\bar{3}y} & & & \hline
\bar{5}x & +\bar{7}y^5 & & & q = \bar{5}x^4+\bar{6} \\
\cancel{-\bar{5}x} & +\bar{4}y & & & r = \bar{7}y^5+\bar{4}y \\
\hline
 & \cancel{\bar{7}y^5} & \cancel{+\bar{4}y} & &
\end{array}$$

Veja que $f$ pode ser reescrita sendo

$$f = (\bar{5}x^4+\bar{6})\cdot(\bar{2}x+\bar{3}y) + (\bar{7}y^5+\bar{4}y).$$

Agora vamos ordenar os polinômios $f = \bar{5}x^4\bar{3}y + \bar{7}y^5 + \bar{5}x + \bar{3}x^5$ e $g = \bar{2}x + \bar{3}y \in \mathbb{Z}_7[x]$ usando a ordem lexicográfica graduada, e fazer a divisão de $f$ por $g$.

$$f = \bar{3}x^5 + \bar{5}x^4\bar{3}y + \bar{7}y^5 + \bar{5}x \;\; g = \bar{2}x + \bar{3}y.$$

$$\begin{array}{llll|l}
\cancel{\bar{3}x^5} & +\bar{7}y^5 & \cancel{+\bar{5}x^4\bar{3}y} & +\bar{5}x & \bar{2}x+\bar{3}y. \\
\cancel{-\bar{3}x^5} & \cancel{-\bar{5}x^4\bar{3}y} & & & \hline
 & \cancel{+\bar{7}y^5} & \cancel{+\bar{5}x} & & q = \bar{5}x^4+\bar{6} \\
 & \cancel{-\bar{5}x} & +\bar{4}y & & r = \bar{7}y^5+\bar{4}y \\
\hline
 & \cancel{+\bar{4}y} & & &
\end{array}$$

Veja que $f$ pode ser reescrita sendo

$$f = (\bar{5}x^4 + \bar{6}) \cdot (\bar{2}x + \bar{3}y) + (\bar{7}y^5 + \bar{4}y).$$

# 4 IDEAIS DO ANEL DE POLINÔMIOS EM VÁRIAS VARIÁVEIS

Neste capítulo apresentamos o algoritmo da pseudo divisão para polinômios em $\mathbb{K}[x_1, \ldots, x_n]$. Para mostrar sua aplicabilidade apresentamos brevemente a teoria de ideais em $\mathbb{K}[x_1, \ldots, x_n]$.

## 4.1 O ALGORITMO DA PSEUDO DIVISÃO

O algoritmo da pseudo divisão nos permite dividir um polinômio $f$ por $s$ quocientes $g_1, \ldots, g_s$. Essa possibilidade é a maior diferença entre este algoritmo e o algoritmo apresentado no capítulo anterior.

**Teorema 4.1.** *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 $\mathrm{ml}(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$, para todo $i = 1, \ldots, s$.*

*Demonstração.* Para fazer a demonstração desse teorema, vamos usar um algoritmo, e justificar o porque podemos usá-lo, então considere o algoritmo abaixo:

**ENTRADA:** $f, g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_s]$ 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 $\mathrm{ml}(g_i) \mid \mathrm{ml}(h)$

então escolha o menor índice $i$ e faça

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

$$h := h - \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)} g_1.$$

Caso contrário

$$r := r + \mathrm{tl}(h);$$

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

**SAÍDA:** $q_1, \ldots, q_s \in \mathbb{K}[x_1, \ldots, x_n]$ tais que $f = \sum_{j=1}^{s} q_j g_j + r$, $\mathrm{ml}(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$ e todo $i = 1, \ldots, s$.

A primeira observação que podemos fazer sobre o algoritmo acima, é que ele sempre nos fornece uma resposta independente do valor dado a $h$, assim, independente do valor de entrada em um número finito de passos teremos uma saída. Podemos ter essa garantia, pois sempre vamos redefinir $h$ de modo que seu monômio líder $m_i$ vai sempre satisfaz $m_i \prec m_{i-1}$, sendo que $m_{i-1}$ é o monômio líder de $h$ no passo anterior.

De fato, se existe $i \in \{1, \ldots, s\}$ tal que

$$\mathrm{ml}(g_i) \mid \mathrm{ml}(h),$$

então temos obrigatoriamente que $\mathrm{ml}(h) \succ \mathrm{ml}(h - \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)} g_i)$. Caso contrário temos que $ml(h) \succ \mathrm{ml}(h - \mathrm{tl}(h))$.

Como vimos anteriormente no Lema 3.1, sabemos que toda sequência decrescente de monômios é finita, portanto em algum momento teremos $h = 0$, como consequência o algoritmo se finaliza.

Para entender o porque o algoritmo acima dos dá uma resposta adequada, devemos perceber que em cada passo do algoritmo temos a igualdade

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

Para confirmar, iniciaremos com $h = f, r = 0$ e $q_i = 0$ para todo $i = 1, \ldots, s$, e note que assim a afirmação é verdadeira.

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

$$q_i \text{ por } q_i + \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)} \text{ e } h \text{ por } \frac{\mathrm{tl}(h)}{\mathrm{tl}(g_i)} g_i$$

e assim teremos

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

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

Caso contrário, iremos redefinir $r$ por $r + \mathrm{tl}(h)$, $h$ por $h - \mathrm{tl}(h)$ e assim teremos

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

Assim, a equação

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

se verifica em todos os passos do procedimento feito. Como o algoritmo se finaliza com $h = 0$, após um número finito de etapas teremos

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

Perceba que com todas as instruções do procedimento visto acima, é fácil ver que $\mathrm{ml}(g_i) \nmid m$ para todo $m \in \mathbb{M}(r)$ e todo $j = 1, \ldots, s$, e isso prova o teorema. ■

**Exemplo 4.1.1.** Considere os polinômios

$$f = xy^3 + y^2 + x^2 + y^3,\ g_1 = x + y,\ g_2 = xy - x \in \mathbb{R}[x, y].$$

Primeiramente vamos ordenar os monômios seguindo a ordem lexicográfica, em seguida efetuaremos a divisão de $f$ por $g_1$ e $g_2$ respectivamente.

$$f = x^2 + xy^3 + y^3 + y^2, g_1 = x + y, g_2 = xy - x.$$

Chamando $f = h_1$, perceba que $\mathrm{ml}(g_1) \mid \mathrm{ml}(h_1)$, assim

$$\begin{array}{llll|l} \cancel{x^2} & +xy^3 & +y^3 & +y^2 & x+y \\ & & & & xy-x \\ \hline \cancel{-x^2} & -xy & & & q_1 = x \\ \hline \multicolumn{4}{c}{h_2 = xy^3 \quad -xy \quad +y^3 \quad +y^2} & \end{array}$$

O $\mathrm{ml}(g_1)$ continua dividindo $\mathrm{ml}(h_2)$, então

$$\begin{array}{llllll|l}
\cancel{x^2} & +xy^3 & +y^3 & +y^2 & & & x+y \\
 & & & & & & xy-x \\
\cancel{-x^2} & -xy & & & & & \hline q_1 = x+y^3 \\
\hline
 & \cancel{xy^3} & -xy & +y^3 & +y^2 & & \\
 & \cancel{-xy^3} & -y^4 & & & & \\
\hline
 & & h_3 = -xy & -y^4 & +y^3 & +y^2 &
\end{array}$$

Ainda conseguimos fazer a divisão do $\mathrm{ml}(h_3)$ pelo $\mathrm{ml}(g_1)$

$$\begin{array}{llllll|l}
\cancel{x^2} & +xy^3 & +y^3 & +y^2 & & & x+y \\
 & & & & & & xy-x \\
\cancel{-x^2} & -xy & & & & & \hline q_1 = x+y^3-y \\
\hline
 & \cancel{xy^3} & -xy & +y^3 & +y^2 & & \\
 & \cancel{-xy^3} & -y^4 & & & & \\
\hline
 & & \cancel{-xy} & -y^4 & +y^3 & +y^2 & \\
 & & \cancel{+xy} & +y^2 & & & \\
\hline
 & & & h_4 = -y^4 & +y^3 & +2y^2 &
\end{array}$$

Perceba que $\mathrm{ml}(g_1) \nmid m$, e $\mathrm{ml}(g_2) \nmid m$, onde $m \in \mathbb{M}(h_4)$. Então $-y^4 + y^3 + 2y^2$ vai contribuir para o nosso resto.

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

Logo, pelo teorema da pseudo divisão, podemos reescrever $f$ sendo

$$f = q_1 g_1 + q_2 g_2 + r$$

$$f = ((x+y)\cdot(x+y^3-y)) + ((xy-x)\cdot(0)) + (-y^4+y^3+2y^2).$$

Agora vamos inverter a ordem dos divisores, ou seja, vamos dividir

$f$ por $g_2$ e $g_1$ respectivamente.

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

Veja que $f$ pode ser reescrito sendo

$$f = q_1 g_1 + q_2 g_2 + r$$

$$f = ((y^2+y)\cdot(xy-x)) + ((x)\cdot(x+y)) + (y^3+y^2).$$

Vamos realizar a divisão de $f$ por $g_1$ e $g_2$ respectivamente, usando a ordem lexicográfica graduada. Ordenando nossos monômios na ordem lexicográfica graduada temos:

$$f = xy^3 + y^3 + x^2 + y^2, g_1 = x+y, g_2 = xy-x.$$

Iremos dividir $f$ por $g_1$ e $g_2$ respectivamente.

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

Assim, $f$ pode ser reescrito sendo

$$f = ((y^3+x-y)\cdot(x+y)) + (0\cdot(xy-x)) + (-y^4+y^3+2y^2).$$

Agora, vamos dividir $f$ por $g_2$ e $g_1$ respectivamente.

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

O polinômio $f$ pode ser reescrito como:

$$f = q_1 g_1 + q_2 g_2 + r$$

$$f = ((y^2+y)\cdot(xy-x)) + ((x)\cdot(x+y)) + (y^3+y^2)$$

Note que, pelo Exemplo 4.1.1 vimos claramente que $f$ pode ser reescrito de diferentes maneiras usando o algoritmo da pseudo divisão. Perceba que uma das maiores diferenças deste algoritmo para os algoritmos demonstrados em 2.6 e 3.2, além de possibilitar a divisão por $n$ divisores, é que neste algoritmo não podemos garantir a unicidade dos quocientes e nem do resto. Vejamos outro exemplo.

**Exemplo 4.1.2.** Considere os polinômios

$$f = x^2 - x^2y - xy^2 + y^4 + xy + y^2 + x, g_1 = y^2 - x, g_2 = xy - y \in \mathbb{R}[x,y].$$

Primeiramente vamos ordenar os monômios seguindo a ordem lexicográfica, em seguida efetuaremos a divisão de $f$ por $g_1$ e $g_2$ respectivamente. Seja

$$f = -x^2y + x^2 - xy^2 + xy + x + y^4, g_1 = x - y^2, g_2 = xy - y.$$

$$
\begin{array}{l|c}
-x^2y + x^2 - xy^2 + xy + x + y^4 & x - y^2 \\
 & xy - y \\
\hline
+x^2 - xy^3 & q_1 = -xy + x - y^3 + y + 1 \\
\hline
x^2 - xy^3 - xy^2 + xy + x + y^4 & q_2 = 0 \\
-x^2 + xy^2 & r = -y^5 + y^4 + y^3 + y^2 \\
\hline
-xy^3 + xy + x + y^4 & \\
+xy^3 - y^5 & \\
\hline
xy + x - y^5 + y^4 & \\
-xy + y^3 & \\
\hline
x - y^5 + y^4 + y^3 & \\
-x + y^2 & \\
\hline
-y^5 + y^4 + y^3 + y^2 &
\end{array}
$$

Logo, $f$ pode ser reescrito como

$$f = ((x - xy + 1 - y^3 + y) \cdot (x - y^2)) + (0 \cdot (xy - y)) + (-y^5 + y^4 + y^3 + 2y^2).$$

Agora, vamos inverter os divisores, ou seja vamos dividir $f$ por $g_2$ e $g_1$ respectivamente.

$$
\begin{array}{llllllll|c}
-x^2y & +x^2 & -xy^2 & +xy & +x & +y^4 & +y^2 & & xy - y \\
 & & & & & & & & x - y^2 \\
\hline
+x^2y & -xy & & & & & & & q_1 = -x \\
\hline
 & +x^2 & -xy^2 & +x & +y^4 & +y^2 & & & q_2 = x + 1 \\
 & -x^2 & +xy^2 & & & & & & r = y^4 + 2y^2 \\
\hline
 & & x & +y^4 & +y^2 & & & & \\
 & & -x & +y^2 & & & & & \\
\hline
 & & & & y^4 & +2y^2 & & &
\end{array}
$$

Assim, $f$ pode ser reescrito sendo

$$f = ((-x) \cdot (xy - y)) + ((x + 1) \cdot (x - y^2)) + (y^4 + 2y^2).$$

Note que ao inverter a ordem dos divisores, o nosso resultado também foi alterado, agora vamos usar a ordem lexicográfica graduada e ver o que acontece com o nosso resultado. Seja

$$f = y^4 - x^2y - xy^2 + x^2 + xy + y^2 + x, g_1 = -y^2 + x, g_2 = xy - y,$$

vamos efetuar a divisão de $f$ por $g_1$ e $g_2$ respectivamente.

$$\begin{array}{lllllll|l}
\cancel{y^4} & -x^2y & \cancel{-xy^2} & +x^2 & +xy & +y^2 & +x & -y^2+x \\
 & & & & & & & xy-y \\
\cancel{-y^4} & \cancel{+xy^2} & & & & & & \hline q_1 = -y^2-1 \\
\cline{1-7}
 & \cancel{-x^2y} & +x^2 & \cancel{+xy} & +y^2 & +x & & q_2 = -x \\
 & \cancel{+x^2y} & \cancel{-xy} & & & & & r = x^2+2x \\
\cline{2-6}
 & & \cancel{x^2} & \cancel{+y^2} & +x & & & \\
 & & \cancel{-y^2} & +x & & & & \\
\cline{3-5}
 & & & 2x & & & &
\end{array}$$

Então, $f$ pode ser reescrito sendo

$$f = ((-y^2-1)\cdot(-y^2+x)) + ((-x)\cdot(xy-y)) + (x^2+2x).$$

Agora, vamos alterar as ordens dos divisores ou seja, vamos dividir $f$ por $g_2$ e $g_1$ respectivamente.

$$\begin{array}{lllllll|l}
\cancel{y^4} & -x^2y & \cancel{-xy^2} & +x^2 & +xy & +y^2+x & & xy-y \\
 & & & & & & & -y^2+x \\
\cancel{-y^4} & \cancel{+xy^2} & & & & & & \hline q_1 = -x \\
\cline{1-6}
 & \cancel{-x^2y} & +x^2 & \cancel{+xy} & +y^2 & +x & & q_2 = -y^2-1 \\
 & \cancel{+x^2y} & \cancel{-xy} & & & & & r = x^2+2x \\
\cline{2-5}
 & & \cancel{x^2} & \cancel{+y^2} & +x & & & \\
 & & \cancel{-y^2} & +x & & & & \\
\cline{3-4}
 & & & 2x & & & &
\end{array}$$

Logo, $f$ pode ser reescrito sendo

$$f = ((-x)\cdot(xy-y)) + ((-y^2-1)\cdot(-y^2+x)) + (x^2+2x).$$

Perceba que nada se alterou quando foram invertido os divisores usando a ordem lexicográfica graduada.

**Exemplo 4.1.3.** Considere os polinômios

$$f = x^2+xy+x^2y-xz, g_1 = y+xy, g_2 = -z+x \in \mathbb{R}[x,y,z].$$

Vamos ordenar os polinômios na ordem lexicográfica graduada e

fazer a divisão de $f$ por $g_1$ e $g_2$, respectivamente.

$$\begin{array}{llll|l} \cancel{x^2y} & +x^2 & \cancel{+xy} & -xz & xy+y \\ & & & & x-z \\ \hline \cancel{-x^2y} & \cancel{-xy} & & & q_1 = x \\ \hline & \cancel{x^2} & \cancel{-xz} & & q_2 = x \\ & \cancel{-x^2} & \cancel{+xz} & & r = 0 \\ \hline & & 0 & & \end{array}$$

Assim, $f$ pode ser reescrito sendo

$$f = ((x) \cdot (xy + y)) + ((x) \cdot (x - z)) + 0.$$

Agora usando a mesma ordem vamos dividir $f$ por $g_2$ e $g_1$ respectivamente

$$\begin{array}{l|c} \cancel{x^2y} + x^2 + xy - xz & x - z \\ & xy + y \\ \hline \cancel{-x^2y} + xyz & q_1 = xy + x + y + yz \\ \hline \cancel{x^2} + xy + xyz \cancel{-xz} & q_2 = 0 \\ \cancel{-x^2} \cancel{+xz} & r = yz^2 + yz \\ \hline \cancel{xy} + xyz & \\ \cancel{-xy} + yz & \\ \hline \cancel{xyz} + yz & \\ \cancel{-xyz} + yz^2 & \\ \hline \cancel{yz^2} \cancel{+yz} & \end{array}$$

Então, $f$ pode ser reescrito sendo

$$f = ((xy + x + y + yz) \cdot (x - z)) + (0 \cdot (xy + y)) + yz^2 + yz.$$

### 4.1.1 Ideais em polinômios em várias variáveis

O algoritmo da pseudo divisão é aplicado na teoria de ideais em anel de polinômios em várias variáveis. Para tanto, daremos uma breve introdução desta teoria para que possamos entender sua aplicabilidade.

**Definição 4.1.** Seja $(\mathbb{A}, +, \times)$ um anel. Dizemos que um subconjunto não vazio $I \subseteq \mathbb{A}$ é um *ideal* se:

i) $f - g \in I$ para quaisquer $f, g \in I$.

ii) $h \times f \in I$ para todo $f \in I$ e todo $h \in \mathbb{A}$.

Perceba que um ideal $I$ é fechado para subtração, enquanto a regra para a multiplicação é mais exigente, pois o produto de um elemento qualquer do anel $\mathbb{A}$ por um de $I$ deve ainda ser um elemento de $I$. Isso se deve ao fato de que a teoria de ideais "enxuga" todo um conjunto o fazendo ser reescrito por um único gerador.

**Proposição 4.2.** *Seja $\mathbb{A}$ um anel e $I$ um ideal de $\mathbb{A}$, então*

*i)* $0_{\mathbb{A}} \in I$,

*ii) Se um elemento invertível de $\mathbb{A}$ pertence a $I$, então $I = \mathbb{A}$.*

*Demonstração.* i) Considere $f \in I$, assim $f - f = 0_{\mathbb{A}}$. Logo, $0_{\mathbb{A}} \in I$.

ii) Suponha que exista $i \in \mathbb{A}$ um elemento invertível tal que $i \in I$. Considere $a \in \mathbb{A}$, logo

$$a = a \times 1_{\mathbb{A}} = a \times i^{-1} \times i.$$

Note que $a \times i^{-1} \in \mathbb{A}$ e $i \in I$, pois $I$ é um ideal de $\mathbb{A}$. Portanto, $\mathbb{A} = I$.

■

Considere $\mathbb{A}$ um anel e sejam $a_1, \ldots, a_n \in \mathbb{A}$. O conjunto

$$\langle a_1, \ldots, a_n \rangle = \{a_1 q_1 + \cdots + a_n q_n \mid q_1, \ldots, q_n \in \mathbb{A}\}$$

é um ideal de $\mathbb{A}$, chamado de *ideal gerado por* $a_1, \ldots, a_n$.

De fato, considere $I = \langle a_1, \ldots, a_n \rangle$ e $f, g \in I$. Assim, existem $q_1, \ldots, q_n \in \mathbb{A}$ tais que

$$f = q_1 a_1 + \cdots + q_n a_n$$

e existem $h_1, \ldots, h_n \in \mathbb{A}$ tais que

$$g = h_1 a_1 + \cdots + h_n g_n.$$

Logo,

$$f - g = (q_1 - h_1)a_1 + \cdots + (q_n - h_n)a_n,$$

e como $h_i - q_i \in \mathbb{A}$ para todo $i = 1, \ldots, n$, segue que $f - g \in I$.

Agora dado $h \in \mathbb{A}$, temos

$$h \cdot g = (hq_1)a_1 + \cdots + (hq_n)a_n,$$

como $hq_i \in \mathbb{A}$ para todo $i = 1, \ldots, n$, então $h \cdot g \in I$. Portanto $\langle a_1, \ldots, a_n \rangle$ é um ideal de $\mathbb{A}$.

Apresentados esses conceitos de ideais em um anel $\mathbb{A}$, vamos considerar agora que o anel $\mathbb{A}$ é o anel de polinômios em várias variáveis $\mathbb{K}[x_1, ..., x_n]$ e o ideal $\langle g_1, \ldots, g_s \rangle$ gerado pelos polinômios $g_i \in \mathbb{K}[x_1, ..., x_n]$. Queremos saber se dado $f \in \mathbb{K}[x_1, ..., x_n]$ ele pertence ao ideal $\langle g_1, \ldots, g_s \rangle$, isto é, existem $q_1, \ldots, q_s \in K[x_1, ..., x_n]$ tais que

$$f = q_1 g_1 + \cdots + q_s g_s.$$

O algoritmo da pseudo divisão pode nos ajudar com esse fato, desde que, o resto da pseudo divisão de $f$ por $g_1, \ldots, g_s$ seja zero.

Observe no Exemplo 4.1.3 que se aplicarmos o algoritmo da pseudo divisão de $f$ por $g_1 = xy + y$ e $g_2 = x - z$ nesta ordem, obtemos $r = 0$, com isso podemos garantir que

$$f \in \langle xy + y, x - z \rangle = \langle g_1, g_2 \rangle.$$

No entanto, se aplicarmos o algoritmo de $f$ por $g_2$ e $g_1$ invertendo a ordem dos quocientes, obtemos $r \neq 0$ e assim não se pode garantir que

$$f \notin \langle x - z, xy + y \rangle$$

utilizando o algoritmo, mas sabemos que $f \in \langle xy + y, x - z \rangle$.

# 5 CONSIDERAÇÕES FINAIS

Esta monografia possibilitou conhecer os conceitos de anel de polinômios em várias variáveis, ordens monomiais e os seus algoritmos de divisão de polinômios que não são abordados nas disciplinas da graduação em Licenciatura em Matemática, além de responder a principal pergunta: "quando um ou mais polinômios não nulos divide outro?".

Além disso, em teoria de ideais em $\mathbb{K}[x_1, ..., x_n]$, o algoritmo da pseudo divisão não pode ser usado, em geral, para verificar se um dado $f \in \mathbb{K}[x_1, ..., x_n]$ pertence ou não a um ideal gerado por $G = \{g_1, \ldots, g_s\}$. Para acabar com esse problema é necessário estudar os conceitos de *bases de Gröbner* e determinar um conjunto gerador $J = \{h_1, \ldots, h_k\}$ de $G$ que independente da ordem de escolha dos quocientes $h_i s$, no algoritmo da pseudo divisão, o resto não vai se alterar. Neste caso, $\{h_1, \ldots, h_k\}$ é chamado de base de Gröbner do ideal gerado por $G$. Assim ao aplicar o algoritmo da pseudo divisão de $f \in \mathbb{K}[x_1, ..., x_n]$ por $h_1, \ldots, h_k$, então $r = 0$ se, e somente se, $f \in \langle G \rangle$.

Portanto, esse trabalho serve como referência para se iniciar um estudo sobre as bases de Gröbner.

## REFERÊNCIAS


[1] GONÇALVES. A. *Introdução à álgebra*. IMPA, 1979.

[2] HEFEZ. A. *Curso de Algebra, vol. 1*. Coleção Matemática Universitária, IMPA/CNPq, RJ, 1993.

[3] HERNANDES. M. E. *Um primeiro contato com as bases de Gröbner*. IMPA, 2011.

[4] DOMINGUES. H. H. E IEZZI G. *Álgebra moderna*. Atual Editora, São Paulo, 1982.