UNIVERSIDADE FEDERAL DE OURO PRETO

DEPARTAMENTO DE MATEMÁTICA

Rebecca Galves Gutierres Toledo

Bases de Groebner

Ouro Preto, Brasil

2021

UNIVERSIDADE FEDERAL DE OURO PRETO

Rebecca Galves Gutierres Toledo

Bases de Groebner

Monografia submetida ao colegiado do Curso de Matemática da Universidade Federal de Ouro Preto como requisito parcial para a conclusão do curso de Licenciatura em Matemática.

Orientador: Prof. Dr. Edney Augusto Jesus de Oliveira

Universidade Federal de Ouro Preto – UFOP

Instituto de Ciências Exatas e Biológicas

Departamento de Matemática

Ouro Preto, Brasil

2021

SISBIN - SISTEMA DE BIBLIOTECAS E INFORMAÇÃO

T649b Toledo, Rebecca Galves Gutierres .
Bases de Groebner. [manuscrito] / Rebecca Galves Gutierres Toledo. - 2021.
59 f.

Orientador: Prof. Dr. Edney Augusto Jesus de Oliveira.
Monografia (Licenciatura). Universidade Federal de Ouro Preto. Instituto de Ciências Exatas e Biológicas. Graduação em Matemática .

1. Groebener, Base de . 2. Buchberger, Algoritmo de . 3. Polinômios . 4. Polinômios - Divisão. I. Oliveira, Edney Augusto Jesus de. II. Universidade Federal de Ouro Preto. III. Título.

CDU 510

Bibliotecário(a) Responsável: Celina Brasil Luiz - CRB6-1589

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E BIOLOGICAS
COLEGIADO DO CURSO DE LICENCIATURA EM MATEMATICA

FOLHA DE APROVAÇÃO

Rebecca Galves Gutierres Toledo

Bases de Groebner

Monografia apresentada ao Curso de Licenciatura em Matemática da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de licenciada em Matemática

Aprovada em 22 de abril de 2021

Membros da banca

Dr. Edney Augusto Jesus de Oliveira - Orientador - Universidade Federal de Ouro Preto
Dr. Juliano Soares Dias - Universidade Federal de Ouro Preto
Dr. Vinícius Vivaldino Pires de Almeida - Universidade Federal de Ouro Preto

Edney Augusto Jesus de Oliveira, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 07/05/2021

Documento assinado eletronicamente por **Edney Augusto Jesus de Oliveira**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 09/05/2021, às 16:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0168770** e o código CRC **EAEA5E51**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: (31)3559-1700 - www.ufop.br

Agradecimentos

Agradeço inicialmente a Deus, meu maior parceiro, por seu amor incondicional.

Em seguida gostaria de agradecer minha mãe, Rachel, por ser a mulher mais forte que eu conheço. Se eu pude escrever esse texto, é graças a ela. Obrigada por acreditar em mim e sempre lutar para que eu fosse uma pessoa melhor, tudo que sou e serei é por ela.

Sou grata também aos meus avós, Silvia e Luiz Antônio, por todo amor e carinho, vocês são a bondade e a poesia na minha vida. A minha madrinha, Priscilla, por me ensinar tanto e ser referencia em determinação. E a todos da minha família por sempre me apoiarem, principalmente em momentos importantes.

Tem uma pessoa que merece uma paragrafo neste agradecimento, meu amigo e orientador Edney. Por vezes eu pensei em desistir, mas ele sempre me apoiou e acreditou em mim. Esse texto tem muito dele, pois me inspirei na maneira que ele encarava a matemática. Por isso sou grata por todo o ensinamento e principalmente pela amizade que construímos junto ao texto, essa é uma conquista nossa.

E por último e não menos importante agradeço a minha família de coração, a Mais ou Menos República, por todo amor e consideração. Levarei vocês comigo por onde eu for.

"Não vos amoldeis às estruturas deste mundo,
mas transformai-vos pela renovação da mente,
a fim de distinguir qual é a vontade de Deus:
o que é bom, o que Lhe é agradável, o que é perfeito.
(Bíblia Sagrada, Romanos 12, 2)

Resumo

Neste trabalho apresentamos uma introdução à teoria das Bases de Groebner e como motivador, sua aplicação mais natural: o problema da pertinência de um polinômio a um ideal polinomial. Para isso, preparamos no texto a estrutura algébrica de anéis e de ideais, dando enfoque em conjuntos geradores para ideais e apresentando a definição de anéis Noetherianos. Em continuidade falamos dos anéis polinomiais em uma indeterminada para então estabelecer, via uma relação recorrência natural, os anéis de polinômios em um número finito de indeterminadas no qual exibimos o conceito de ordens monomiais, e ainda, no estudo de polinômios destacamos os algoritmos das divisões polinomiais em cada caso, visando algoritmos para obtenção dos quocientes e restos. Por fim estabelecemos a definição de Base de Groebner para um ideal polinomial, enunciamos e demonstramos um teste para a verificação de que um dado conjunto gerador é ou não Base de Groebner, o chamado *Critério de Buchberger*, e para quando o conjunto gerador não for uma Base de Groebner, exibimos e demonstramos um algoritmo que nos fornece uma tal base, o *Algoritmo de Buchberger*. Abordamos também importantes resultados que são essenciais para as referidas demonstrações, o Teorema da Base de Hilbert e o Lema de Dickson. Por fim, deixamos claro como é utilizado uma Base de Groebner para a resolução do problema da pertinência.

Palavras-chave: Divisão polinomial, bases de Groebner, Algoritmo de Buchberger.

Sumário

Introdução

Neste trabalho apresentamos uma introdução da teoria de Bases de Groebner e uma importante aplicação dela: como determinar a pertinência de um polinômio a um ideal polinomial. Vale destacar que o estudo de bases de Groebner é recente no meio matemático e foi desenvolvido inicialmente pelo matemático austríaco Bruno Buchberger em 1965, e foi assim denominada em homenagem ao seu orientador Wolfgang Groebner e ela possui diversas aplicações em álgebra comutativa, além da que exibiremos. Antes de apresentar o conceito de Bases de Groebner nós estudamos tópicos da teoria de anéis, em especial seus ideiais, uma vez que essa estrutura algébrica faz parte dos pré-requisitos básicos para se estudar as Bases de Groebner. Depois definimos os anéis polinomiais, em uma variável e em n indeterminadas, momento em que estudamos algumas de suas propriedades, principalmente as relacionadas às divisões polinomiais. Por fim definimos as Bases de Groebner e mostramos o algoritmo que de fato constrói uma Base de Grebner de um determinado ideal polinomial em n variáveis.

No primeiro capítulo apresentamos os conceitos básicos necessários para o desenvolvimento da monografia, como: anéis e seus ideais. No estudo de ideais, destacamos os conceitos de conjunto gerador e anéis Noetherianos. Usamos como base para nosso estudo os textos (GONÇALVES, 2017), (HEFEZ, 1993), (MONTEIRO, 1974), (IEZZI, 2005) e (VIDIGAL, 2005).

O segundo capítulo é voltado para o estudo de polinômios e está divido em duas partes: polinômios em uma indeterminada e polinômios em n indeterminadas. Como base para esse estudo, citamos o livro *Polinômios e Computação Algébrica* do Coutinho (COUTINHO, 2012). Observamos nesse estudo que o conjunto dos polinômios em uma indeterminada x_1 com coeficientes em um corpo K, é um anel comutativo com unidade denotado por $K[x_1]$ e que nele há um algoritmo de divisão que nos permite inferir diversas propriedades sobre ideais polinomiais. Em seguida definimos, de forma recursiva, o anel de polinômios em duas variáveis com coeficientes em $K[x_1]$ e com x_2 como indeterminada, sendo assim denotado por $K[x, y] := (K[x])[y]$, e a partir da extensão deste raciocínio obtemos o anel de polinômios em n indeterminadas. Observamos que no caso do estudo de polinômios em mais de uma indeterminada precisamos estabelecer uma espécie de ordem entre os monômios, as quais chamamos por ordens monomiais e com isso somos capazes de enunciar a versão do teorema de divisão polinomial em n indeterminadas. Uma divisão importante que desenvolvemos é a divisão de um polinômio por um conjunto finito de polinômios, esta será importante na hora de falar sobre pertinência de um polinômio a um ideal polinomial.

No terceiro capítulo apresentamos os resultados centrais deste trabalho e utilizamos como principais referências o livro (COUTINHO, 2012) e a dissertação (RAMOS, 2003), foram consultados também a monografia (MENDES, 2012). Neste capítulo definimos ideais monomiais e provamos que um ideal monomial sempre será finitamente gerado (e mais, gerado por monômios apenas), e com esse resultado em mãos, enunciamos e demonstramos o célebre *Teorema da Base de Hilbert*, o qual diz que todo ideal polinomial (com coeficientes em um corpo) será finitamente gerado. Para apresentarmos a definição de Base de Groebner para um ideal, precisamos estabelecer o ideal gerado pelos termos líderes de I, denotado por $\langle TL(I)\rangle$, e o ideal gerado pelos termos líderes dos polinômios que geram o ideal I, denotado por $\langle TL(g_1), TL(g_2), \ldots, TL(g_r)\rangle$. De imediato notamos que $\langle TL(g_1), TL(g_2), \ldots, TL(g_r)\rangle \subseteq \langle TL(I)\rangle$, e quando a igualdade for válida, dizemos que $\{g_1, g_2, \ldots, g_s\}$ é uma base de Groebner para o ideal I. Usamos de uma propriedade específica das bases de Groebner para resolver o problema da pertinência de um polinômio a um ideal polinomial. Uma parte importante deste capítulo é o Critério de Buchberger. Usamos tal critério para provar que o Algoritmo de Buchberger terá um fim e assim se torna válido, tal algoritmo nos proporciona achar uma base de Groebner de um determinado ideal a partir de um conjunto finito de geradores de I.

1 Anéis e ideais

Neste capítulo introduziremos o conceito de anéis e de ideais, os quais serão importantes para a formalização dos principais conceitos que necessitamos para introduzir a definição de Bases de Groebner: polinômios e do anel de polinômios.

Começamos pela definição de anel.

Definição 1. *Sejam A um conjunto não vazio e duas funções binárias $+ : A \times A \to A$ e $\cdot : A \times A \to A$ denominadas* adição *e* multiplicação*, respectivamente, dizemos que $(A, +, \cdot)$ é um* ***anel com unidade*** *se as operações $+$ e $\cdot$ satisfizerem as seguintes propriedades:*

i) (Associatividade da adição) Para todos a, b e $c \in A$, $(a + b) + c = a + (b + c)$;

ii) (Existência do elemento neutro da adição) Existe $\alpha \in A$, tal que $\forall a \in A$ tem-se $a + \alpha = \alpha + a = a$;

iii) (Existência do inverso aditivo) Para todos $a \in A$, $\exists\, b \in A$, tal que $a + b = b + a = a$;

iv) (Comutatividade da adição) Para todos $a, b \in A$, $a + b = b + a$;

v) (Associatividade da multiplicação) Para todos a, b e $c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

vi) (Existência do elemento neutro da multiplicação) Existe $e \in A$, tal que $\forall a \in A$ tem-se $a \cdot e = e \cdot a = a$;

vii) (Distributividade) Para todos a, b e $c \in A$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$;

Exemplo 1. *O conjunto dos números inteiros $\mathbb{Z}$, munido das operações usuais de adição e multiplicação, denotadas por $+$ e $\cdot$ respectivamente, constituem o anel dos inteiros $(\mathbb{Z}, +, \cdot)$. De modo similar, temos o anel dos racionais $(\mathbb{Q}, +, \cdot)$, o anel dos reais $(\mathbb{R}, +, \cdot)$ e o anel dos complexos $(\mathbb{C}, +, \cdot)$.*

Definição 2. *Dizemos que um anel A será comutativo se, para todo $a, b \in A$ a operação de multiplicação satisfizer a comutatividade, ou seja,*

$$a \cdot b = b \cdot a.$$

Com a intenção de simplificar a notação, sempre que as operações estiverem subentendidas, denotaremos o anel $(A, +, \cdot)$ simplesmente por A.

Exemplo 2. *O conjunto das matrizes $M_2(\mathbb{Z})$ não é um anel comutativo com as operações usuais de matrizes 2×2. De fato, basta observar que*

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Definição 3. *Sejam A um anel e $a \in A$ um elemento não nulo. Dizemos que a é um* ***divisor de zero*** *se existe $b \in A$ não nulo, tal que:*

$$a \cdot b = 0. \tag{1.1}$$

Definição 4. *Um anel A será dito ser um* ***domínio de integridade****, ou simplesmente* domínio*, se não possuir divisor de zero.*

Exemplo 3. *Os anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{R}$ são domínios de integridade. O anel $\mathbb{Z}_8$ não é um domínio pois $\overline{2} \cdot \overline{4} = \overline{0}$ e $\overline{2}, \overline{4} \neq \overline{0}$.*

A partir de agora todo anel será tomado como domínio de integridade.

Exemplo 4. *Sejam A, B anéis, temos que o produto cartesiano $A \times B$ é também um anel. De fato, seja $C = A \times B$ e sendo $a, a' \in A$ e $b, b' \in B$, definimos as operações de adição e multiplicação de C coordenada-a-coordenada, ou seja, $(a, b) + (a', b') = (a + a', b + b')$ e $(a, b) \cdot (a', b') = (aa', bb')$.*

i) Sejam $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in C$ temos que,

$$\begin{aligned}[(a_1, b_1) + (a_2, b_2)] + (a_3, b_3) &= (a_1 + a_2, b_1 + b_2) + (a_3, b_3) \\ &= (a_1 + a_2 + a_3, b_1 + b_2 + b_3).\end{aligned}$$

Observe também que

$$\begin{aligned}(a_1, b_1) + [(a_2, b_2) + (a_3, b_3)] &= (a_1, b_1) + (a_2 + a_3, b_2 + b_3) \\ &= (a_1 + a_2 + a_3, b_1 + b_2 + b_3).\end{aligned}$$

Logo, a adição definida para C é associativa.

ii) Como A anel, existe $\alpha \in A$ tal que $a + \alpha = \alpha + a = a$, pra todo $a \in A$. Da mesma maneira existe $\beta \in B$, tal que $b + \beta = \beta + b = b$ para todo $b \in B$, então

$$(\alpha, \beta) + (a, b) = (\alpha + a, \beta + b) = (a, b)$$

e,

$$(a, b) + (\alpha, \beta) = (a + \alpha, b + \beta) = (a, b).$$

Logo existe um elemento neutro $(c, d) \in C$; em que $(c, d) = (\alpha, \beta)$

iii) Sabendo que A, B são anéis, temos que todo $a \in A$ possui um inverso aditivo c e todo $b \in B$ possui um inverso aditivo d. Portanto (c, d) é inverso aditivo de (a, b) uma vez que,

$$(a, b) + (c, d) = (a + c, b + d) = (\alpha, \alpha)$$

e,

$$(c, d) + (a, b) = (c + a, d + b) = (\alpha, \alpha)$$

iv) Sabendo que $a_1 + a_2 = a_2 + a_1$ em A (comutatividade da adição em A), e análogo em elementos de B, temos:

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2)\\ &= (a_2 + a_1, b_2 + b_1)\\ &= (a_2, b_2) + (a_1, b_1).\end{aligned}$$

Assim, provamos a comutatividade da adição em C.

v) Sejam $a_1, a_2, a_3 \in A$ e $b_1, b_2, b_3 \in B$ temos que,

$$\begin{aligned}[(a_1, b_1) \cdot (a_2, b_2)] \cdot (a_3, b_3) &= (a_1 \cdot a_2, b_1 \cdot b_2) \cdot (a_3, b_3)\\ &= (a_1 \cdot a_2 \cdot a_3, b_1 \cdot b_2 \cdot b_3).\end{aligned} \tag{1.2}$$

Mas também,

$$\begin{aligned}(a_1, b_1) \cdot [(a_2, b_2) \cdot (a_3, b_3)] &= (a_1, b_1) \cdot (a_2 \cdot a_3, b_2 \cdot b_3)\\ &= (a_1 \cdot a_2 \cdot a_3, b_1 \cdot b_2 \cdot b_3).\end{aligned}$$

Logo C é associativo pela multiplicação.

vi) Sejam $e_A \in A$ e $e_B \in B$ os elementos neutros multiplicativos de A e B, respectivamente. Então para todos $a \in A$ e $b \in B$ temos

$$(a, b)(e_A, e_B) = (a \cdot e_A, b \cdot e_B) = (a, b) \quad e \quad (e_A, e_B)(a, b) = (e_A \cdot a, e_B \cdot b) = (a, b).$$

Portanto $(e_A, e_B) \in C$ é um elemento neutro multiplicativo.

vii) Sejam $a_1, a_2, a_3 \in A$ e $b_1, b_2, b_3 \in B$.

$$\begin{aligned}(a_1, b_1) \cdot [(a_2, b_2) + (a_3, b_3)] = \;& (a_1, b_1) \cdot [(a_2 + a_3, b_2 + b_3] = (a_1 \cdot (a_2 + a_3), b_1 \cdot (b_2 + b_3))\\ =\;& (a_1 \cdot a_2 + a_1 \cdot a_3, b_1 \cdot b_2 + b_1 \cdot b_3)\\ =\;& (a_1 \cdot a_2, b_1 \cdot b_2) + (a_1 \cdot a_3, b_1 \cdot b_3)\\ =\;& (a_1, b_1) \cdot (a_2, b_2) + (a_1, b_1) \cdot (a_3, b_3).\end{aligned}$$

Logo, vale a regra da distributividade em C.

Assim, provamos que C é anel.

Corolário 1. *Para todo A anel, vale a lei do cancelamento na operação de soma, isto é,*

$$\forall a, b, c \in A,\ a + b = a + c \Rightarrow b = c.$$

Demonstração. Sejam A um anel, tal que $a, b, c \in A$ e

$$a + b = a + c.$$

Como $a \in A$, por definição existe $(-a) \in A$ tal que $(-a) + a = \alpha$, logo:

$$(-a) + a + b = (-a) + a + c \Rightarrow \alpha + b = \alpha + c \Rightarrow b = c.$$

□

Observamos que na definição de anel pede-se para cada elemento a existência do inverso aditivo, mas não é exigido uma propriedade análoga para a multiplicação. No entanto, isso não impede a existência de elementos do anel que possuam "inversos"multiplicativos, e isso motiva a seguinte definição.

Definição 5. *Sejam A um anel e $a \in A$ não nulo. Se existir $b \in A$ tal que $a \cdot b = e$, chamaremos b de **inverso multiplicativo** (ou simplesmente **inverso**) de a. Nesse caso, dizemos que a e b são elementos **invertíveis** de A.*

Note que os anéis $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ possuem a propriedade de que todo elemento não nulo é invertível. Com isso, podemos enunciar a seguinte definição:

Definição 6. *Se um anel A possui a propriedade de que todo elemento não nulo é invertível, dizemos que A é um **corpo**.*

É fácil notar que $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos, enquanto que $\mathbb{Z}$ não é um corpo, pois não existe $b \in \mathbb{Z}$ tal que $2 \cdot b = 1$.

Proposição 1. *Seja A um anel, são válidas as seguintes afirmações:*

(i) O elemento neutro aditivo de A é único.

(ii) Dado $a \in A$, existe um único elemento $b \in A$ inverso aditivo de A. Neste caso dizemos que b é um simétrico de a e o denotamos por $(-a)$.

(iii) Se um elemento $a \in A$ possuir inverso multiplicativo em A, então ele será único.

(iv) O elemento neutro multiplicativo de A é único.

Demonstração. Seja A anel, temos:

(i) Suponha que α, α' sejam elementos neutros aditivos de A. Daí temos,

$$\alpha = \alpha + \alpha' = \alpha',$$

em que na primeira igualdade acima utilizamos o fato de que α' é um neutro aditivo e na segunda utilizamos que α é o outro elemento neutro aditivo. Logo só existe um elemento neutro aditivo em A.

(ii) Seja $a \in A$ um elemento arbitrário e suponha que $(-a)$ e $(-a')$ sejam dois inversos aditivos seu. Logo,

$$(-a) + a = 0 = (-a') + a.$$

Aplicando a lei do cancelamento na igualdade acima (cancelando a em ambos os lados), obtemos

$$-a = -a'.$$

Mostramos então a unicidade do simétrico para cada elemento de A.

(iii) Suponha que $a \in A$ seja invertível e que $c,\ c' \in A$ sejam dois inversos de $a \in A$. Daí

$$c \cdot a \cdot c' = c \cdot (a \cdot c') = c \cdot e = c.$$

Ainda teremos,

$$c \cdot a \cdot c' = (c \cdot a) \cdot c' = e \cdot c' = c'.$$

Logo, $c = c'$, mostrando deste modo que só pode existir um inverso aditivo para cada elemento de A.

(iv) Suponha e e e' sejam elementos neutros multiplicativos de A. Daí,

$$e = e \cdot e' = e',$$

em que na primeira igualdade acima utilizamos o fato de que e' é uma identidade e na segunda utilizamos que e é uma identidade. Assim fica provada a unicidade do elemento neutro multiplicativo, se ele existir.

□

Demonstrada a unicidade do elemento neutro aditivo, vamos passar a representá-lo pelo algarismo 0, e o elemento neutro multiplicativo pelo algarismo 1.

Para aprimorar o texto usaremos a^{-1} como a notação do inverso multiplicativo do elemento $a \in A$, caso exista.

Exemplo 5. *Considere o conjunto das classes residuais de inteiros módulo n, o $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, em que $\overline{a} = \overline{b} \Leftrightarrow n|(a-b)$.*
Sobre esse conjunto defina as seguintes operações:

$$\begin{array}{rccc} + : & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & (\overline{a},\, \overline{b}) & \mapsto & \overline{a} + \overline{b} := \overline{a+b} \end{array} \quad e \quad \begin{array}{rccc} \cdot : & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & (\overline{a},\, \overline{b}) & \mapsto & \overline{a} \cdot \overline{b} := \overline{a \cdot b}. \end{array}$$

Vamos provar que $(\mathbb{Z}_n, +, \cdot)$ é um anel e o primeiro passo é verificar que as operações definidas estão bem definidas. Para tal, suponha $(\overline{a}, \overline{b}), (\overline{a_1}, \overline{b_1}) \in \mathbb{Z}_n \times \mathbb{Z}_n$, tais que $\overline{a} = \overline{a_1}$ e $\overline{b} = \overline{b_1}$.

Note que por definição, temos que $n|(a-a_1)$ *e* $n|(b-b_1)$*, donde vemos que existem* $x, y \in \mathbb{Z}$ *que satisfazem:*

$$a - a_1 = nx \quad e \quad b - b_1 = ny.$$

Somando essas duas equações temos:

$$(a+b) - (a_1+b_1) = (x+y)n,$$

isto significa que,

$$\overline{a+b} = \overline{a_1+b_1}.$$

Na multiplicação também temos que,

$$a \cdot b = (xn+a_1)(yn+b_1) = xyn^2 + xnb_1 + a_1yn + a_1b_1.$$

Sabendo que $a \cdot b = xyn^2 + xnb_1 + a_1yn + a_1b_1$*, se subtrairmos* a_1b_1 *de ambos os lados da equação teremos:*

$$ab - (a_1b_1) = xyn^2 + xnb_1 + a_1yn + (a_1b_1) - (a_1b_1) \Rightarrow ab - a_1b_1 = (xyn + xb_1 + a_1y)n.$$

Logo $n|(ab-a_1b_1)$*, e assim* $\overline{a \cdot b} = \overline{a_1 \cdot b_1}$*. Como a soma e a multiplicação de duas classes estão bem definidas, e dependem essencialmente da soma e multiplicação em* $\mathbb{Z}$*, respectivamente, as propriedades dessas operações necessárias para garantir que* $\mathbb{Z}_n$ *seja um anel são herdadas das propriedades das operações do anel* $\mathbb{Z}$*. Observe que o elemento neutro da soma de* $\mathbb{Z}_n$ *é a classe* $\overline{0}$*, que representa os múltiplos de* n *e o neutro multiplicativo é a classe* $\overline{1}$*.*

Uma importante propriedade dos anéis $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ é que se $a \cdot b = 0$ então ou $a = 0$ ou $b = 0$. No entanto, propriedade não é válida para todos os anéis, como por exemplo $\mathbb{Z}_4$:

$$\overline{2} \cdot \overline{2} = \overline{0},$$

com $\overline{2} \neq \overline{0}$.

Agora vamos estabelecer uma importante classe de funções relacionadas a anéis.

Definição 7. *Sejam* A *e* B *dois anéis. Uma função* $f : A \to B$ *é chamada* ***homomorfismo*** *de anéis se para todos* $a, b \in A$*, satisfizerem as condições abaixo:*

i) $f(a+b) = f(a) + f(b)$*;*

ii) $f(a \cdot b) = f(a) \cdot f(b)$*.*

Exemplo 6. *Sejam* A *e* B *anéis, com* $A = \mathbb{R}$ *e* $B = \mathbb{R} \times \mathbb{R}$ *(veja o exemplo 4). A função* $f : A \to B$*, dada por* $f(x) = (0, x)$ *é homomorfismo.*
De fato, sejam $x, y \in \mathbb{R}$*.*

i) Então $f(x+y) = (0, x+y) = (0,x) + (0,y) = f(x) + f(y)$,

ii) E também $f(x \cdot y) = (0, x \cdot y) = (0,x) \cdot (0,y) = f(x) \cdot f(y)$.

Logo f *é um homomorfismo de* A *em* B.

Definição 8. *Se* $f : A \to B$ *é um homomorfismo bijetor, dizemos* f *é um* ***isomorfismo*** *e que* A *e* B *são* ***isomorfos*** *e escreveremos* $A \cong B$. *Considerando o caso particular, em que* $A = B$, *chamamos* f *de* ***automorfismo***.

É importante ressaltar que se existir isomorfismo de anéis $f : A \to B$, então $f^{-1} : B \to A$ também é isomorfismo. E se A e B são isomorfos, os dois anéis são estruturalmente iguais do ponto de vista algébrico, ou seja, a diferença entre eles é basicamente a interpretação e a notação utilizada para os seus elementos.

Proposição 2. *Sejam* A, B *domínios de integridade e* $f : A \to B$ *um homomorfismo de anéis. São válidas:*

i) $f(0_A) = 0_B$;

ii) $f(1_A) = 0_B$ *ou* $f(1_A) = 1_B$;

iii) $f(-a) = -f(a), \forall\ a\ \in A$.

Demonstração. i) Podemos notar que:

$$f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A).$$

Sabendo que existe o inverso aditivo de $f(0_A)$ no anel B, que será denotado por $(-f(0_A))$. Vamos somar o inverso aditivo aos dois lados da igualdade acima, e então teremos:

$$f(0_A) + (-f(0_A)) = (f(0_A) + f(0_A)) + (-f(0_A)),$$

onde sabemos que somados os inversos dentro de um anel obtemos o elemento neutro do mesmo. Usando também da associatividade na primeira parte da igualdade temos,

$$0_B = f(0_A) + (f(0_A) + (-f(0_A)) \Rightarrow 0_B = f(0_A).$$

ii) Escrevendo $f(1_A) = a$, temos

$$a = f(1_A) = f(1_A \cdot 1_A) = f(1_A) \cdot f(1_A) = a \cdot a \Rightarrow a \cdot a - a = 0_B \Rightarrow a(a - 1_b) = 0_B.$$

Decorre deste modo que, como B é um domínio, $a = 0_B$ ou $a = 1_B$.

iii) Pelo item i) desta proposição temos que $f(0_A) = 0_B$. Com isso,

$$0_B = f(0_A) = f(a + (-a)) = f(a) + f(-a),$$

e somando o simétrico de $f(a)$, o $-f(a)$, a ambos os lados, vemos que

$$-f(a) = f(-a),$$

para todo $a \in A$.

□

1.1 Ideais

Nessa seção, trazemos uma ferramenta central para nossos estudos.

Definição 9. *Seja A um anel e I um subconjunto não vazio de A. Dizemos que I é um* ***ideal*** *de A, se:*

i) Para todo $a, b \in I$, então $a - b \in I$;

ii) Para todo $a, \in I$, e $b \in A$ então $a \cdot b \in I$.

Exemplo 7. *Seja A um anel qualquer. É imediato verificar que os subconjuntos $\{0\}$ e o próprio A são ideais. Tais ideais são usualmente chamados de* ***ideais triviais****.*

Exemplo 8. *Considere o anel $A = C[0,1]$ das funções contínuas $f : [0,1] \to \mathbb{R}$ munido das operações definidas ponto-a-ponto, ou seja, $\forall a \in [0,1]$:*

$$(f_1 + f_2)(a) = f_1(a) + f_2(a) \quad e \quad (f_1 \cdot f_2)(a) = f_1(a) \cdot f_2(a).$$

O elemento neutro aditivo do anel A é a função constante nula e o neutro multiplicativo é a função constante igual a 1.

Seja $b \in [0,1]$ fixado. Defina:

$$I_b = \{f \in A \,|\, f(b) = 0\}.$$

Então I_b é um ideal de A, pois:

i) Para todo $f, g \in I_b$, temos que $(f - g)(b) = f(b) - g(b) = 0 - 0 = 0$. Logo $f - g \in I_b$.

ii) Para todo $h \in A, g \in I_b$, Temos que $(h \cdot g)(b) = h(b) \cdot g(b) = h(b) \cdot 0 = 0$. Logo $h \cdot g \in I_b$.

Teorema 1. *Seja I um ideal de $\mathbb{Z}$. Então existe $n \in \mathbb{Z}$ tal que $I = n\mathbb{Z}$.*

Demonstração: Se $I = \{0\}$, então $n = 0$ é o número procurado, pois é fácil notar que com essa condição o teorema é válido. Agora suponha então que $I \neq \{0\}$. Logo, existe $a \neq 0$ onde $a \in I$ e portanto, como $-1 \in \mathbb{Z}$ temos $(-1) \cdot a \in I$, que satisfaz a segunda condição estabelecida para os ideais, ou seja $-a, a \in I$. Definimos então:

$$I_+ = \{x \in I \ tal \ que \ x > 0\}.$$

Pelo que vimos acima, I_+ é um subconjunto não-vazio e limitado inferiormente de $\mathbb{Z}$. Assim, pelo Princípio da Boa Ordem, I_+ tem menor elemento, digamos d.

Vamos mostrar que $I = d\mathbb{Z}$. A inclusão $d\mathbb{Z} \subseteq I$ é imediata, visto que $d \in I$ e I é um ideal de $\mathbb{Z}$, agora provemos a outra inclusão. Para isso, seja $a \in I$. Pelo algoritmo da divisão em $\mathbb{Z}$ existem únicos q e r tais que:

$$a = q \cdot d + r, \ onde \ 0 \leq r < |d| = d.$$

E sabemos que $(a - q \cdot d) \in I$, já que I ideal, então se $r \neq 0$ vemos que,

$$r = a - q \cdot d \in I_+,$$

o que é um absurdo, pois d é o menor elemento de I_+ e $r < d$. Assim,

$$a = q \cdot d \in d\mathbb{Z},$$

e consequentemente, $I \subset d\mathbb{Z}$.

Definição 10. *Um ideal P de um anel A é um **ideal primo** se:*

i) $P \neq A$,

ii) Para todos $a, b \in A$, *se* $a \cdot b \in P$ *então ou* $a \in P$ *ou* $b \in P$.

Definição 11. *Seja A um anel. Um ideal J de A, com $J \neq A$ é dito ser um **ideal maximal** de A se sempre que existir I ideal de A com $J \subseteq I \subseteq A$, então $I = J$ ou $I = A$.*

Exemplo 9. *Os ideais $p\mathbb{Z}$, com p primo, são todos os ideais maximais de $\mathbb{Z}$.*
De fato, é fácil ver que para todo p primo temos $p\mathbb{Z} \neq \mathbb{Z}$. Pelo Teorema 1, todo ideal de $\mathbb{Z}$ é da forma $n\mathbb{Z}$, para algum $n \in \mathbb{Z}$. Suponha que $p\mathbb{Z} \subset n\mathbb{Z} \subset \mathbb{Z}$. Consequentemente,

$$p\mathbb{Z} \subseteq n\mathbb{Z} \Rightarrow p \in n\mathbb{Z} \Rightarrow p = n \cdot a, \ a \in \mathbb{Z}.$$

Como p é primo, temos que $n = 1$ ou $n = p$. Se $n = 1$, então $n\mathbb{Z} = 1 \cdot \mathbb{Z} = \mathbb{Z}$, e se $n = p$, temos $n\mathbb{Z} = p\mathbb{Z}$. Portanto, $p\mathbb{Z}$ com p primo é um ideal maximal de $\mathbb{Z}$.
Agora, suponha que $n\mathbb{Z}$ é um ideal maximal. Se n não for primo, então existem $n_1, n_2 \in \mathbb{Z}$ tais que $n = n_1 \cdot n_2$ com $1 < n_1, n_2 < n$. Disso vemos que:

$$n\mathbb{Z} \ = \ n_1 n_2 \mathbb{Z} \subset n_1\mathbb{Z} \subset \mathbb{Z} \ \Rightarrow \ n_1\mathbb{Z} = \mathbb{Z} \ \ ou \ \ n_1\mathbb{Z} = n\mathbb{Z}. \tag{1.3}$$

i) Se $n_1\mathbb{Z} = \mathbb{Z}$, e sabemos que $1 \in \mathbb{Z}$ teremos que $1 = n_1 k \Rightarrow n_1|1 \Rightarrow n_1 = 1$, absurdo;

ii) Se $n_1\mathbb{Z} = n\mathbb{Z}$, temos que $n_1 = n \cdot z$, com $z \in \mathbb{Z}$, donde $n|n_1$. Sabendo também que $n = n_1 \cdot n_2$ temos que $n_1|n$, o que implica que $n = n_1$, absurdo. Análogo para n_2.

Logo n deve ser primo.

Exemplo 10. *O ideal $4\mathbb{Z}$ de $\mathbb{Z}$ não é ideal primo. De fato, $6 \cdot 2 = 12 \in 4\mathbb{Z}$, mas nem 2 e nem 6 pertencem a $4\mathbb{Z}$.*

Exemplo 11. *O conjunto $\mathbb{Z}\times\{0\}$ é um ideal primo de $\mathbb{Z}\times\mathbb{Z}$. Se $(a,b)\cdot(c,d) \in \mathbb{Z}\times\{0\}$ então temos $bd = 0 \in \mathbb{Z}$. Isso implica que $b = 0$ e $(a,b) \in \mathbb{Z} \times \{0\}$ ou $d = 0$ e $(c,d) \in \mathbb{Z} \times \{0\}$.*

Definição 12. *Seja A um anel e $S \subset A$. Definimos o conjunto gerado por S como:*

$$\langle S\rangle = \left\{ \sum_{finito} a_i s_i \,\middle|\, a_i \in A,\ s_i \in S \right\}.$$

Agora vamos provar que o conjunto $\langle S\rangle$ é ideal.

i) Sejam p e q dois elementos de $\langle S\rangle$, então existem $a_1, \ldots, a_r, b_1, \ldots, b_m \in A$, tais que $p = a_1 s_1 + ... + a_r s_r$ e $q = b_1 s'_1 + ... + b_m s'_m$. Assim temos:

$$p - q = (a_1 s_1 + \ldots + a_m s_m + \ldots + a_r s_r) - (b_1 s'_1 + \ldots + b_m s'_m).$$

Destacando que $a_1 s_1 + \ldots + a_r s_r + (-b_1)s'_1 + \ldots (-b_m)s'_m$ é uma soma finita de elementos do tipo as com $a \in A$, $s \in S$. Temos que, $p - q \in \langle S\rangle$.

ii) Seja $p \in \langle S\rangle$ e $c \in A$, então temos,

$$p \cdot c = (a_1 s_1 + \ldots + a_r s_r) \cdot c = (ca_1)s_1 + \ldots + (ca_r)s_r;$$

com $s \in S$ e em que cada $ca_i \in A,\ i = 1, \ldots, r$, pois $c,\ a_i \in A$. Assim $(p \cdot c) \in \langle S\rangle$.

A notação $\langle S\rangle$ é usada para dizer ao público que tal conjunto é gerado por elementos de S, e assim, podemos escrever $\langle S\rangle = \langle s_1, s_2, \ldots, s_n \ldots\rangle$.

Um caso particular da Definição 12 é quando temos o conjunto S finito. Nesse caso, denominamos $\langle S\rangle$ como **ideal finitamente gerado**, e é comum escrevermos

$$\langle S\rangle = \langle s_1, s_2, \ldots, s_n\rangle .$$

Caso S for unitário, ou seja, $S = \{s\}$, então o ideal $\langle S\rangle = \langle s\rangle$ é dito ser **principal**.

Uma observação pertinente que podemos fazer é a seguinte: todo ideal I de um anel A sempre irá possuir um conjunto gerador, que é o próprio I tomado como conjunto.

Note que a situação menos complexa de se lidar é quando conseguimos obter um conjunto gerador finito, o que nem sempre é possível. Exemplos de ideais que não são finitamente gerados não são em geral tão simples de se imaginar em nível elementar, mas podemos citar (sem maiores detalhes) o ideal do anel de polinômios em infinitas indeterminadas $\{x_1, x_2, \ldots\}$ gerado por todas as indeterminadas.

Exemplo 12. *Pelo Teorema 1, temos que todo ideal I do anel $\mathbb{Z}$ é da forma $I = n\mathbb{Z}$, ou seja, I é gerado por n e desse modo concluímos que todo ideal de $\mathbb{Z}$ é um ideal principal.*

Definição 13. *Um anel A é dito Noetheriano se todo ideal $I \subset A$ for finitamente gerado.*

Pelo Exemplo 12 podemos concluir que o anel $\mathbb{Z}$ é Noetheriano, pois todos os seus ideais são principais, ou seja, finitamente gerados.

Exemplo 13. *Sejam K um corpo e $I \neq \{0\}$ um ideal de K. Como $I \neq \{0\}$, existe $x \in I$ não nulo, e por consequência, existe $x^{-1} \in K$ (o inverso multiplicativo de x). Pelas propriedades de ideal, temos*

$$1 = x \cdot x^{-1} \in I \;\Rightarrow\; K = \langle 1 \rangle \subset I \;\Rightarrow I = K.$$

Portanto os únicos ideais de um corpo K são os triviais, que são sabidamente finitamente gerados. Logo, todo corpo K é Noetheriano.

Seja $\mathcal{I} = \{I_j\}_{j\in\Gamma}$ uma família arbitrária de ideais de um anel A. Dizemos que os ideais da família $\mathcal{I}$ formam uma **Cadeia Ascendente de Ideais** em A se

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_j \subseteq \ldots \tag{1.4}$$

Lema 1. *Seja*

$$I_1 \subset I_2 \subset \ldots \subset I_j \subset \ldots$$

uma cadeia ascendente de ideais de A. Então $Y = \bigcup_{j\in\Gamma} I_j$ é um ideal de A.

Demonstração. Sejam $a, b \in Y$. Daí existem $m, n \in \mathbb{N}$, tais que $a \in I_m$ e $b \in I_n$. Sem perda de generalidade podemos supor que $m \leqslant n$, o que nos garante que

$$I_m \subseteq I_n.$$

Logo $a, b \in I_n \subset \bigcup_{j\in\Gamma} = Y$. Além disso, para todos $a \in Y$ e $r \in A$ temos que $ar \in I_n \subset \bigcup_{j\in\Gamma} = Y$. Portanto Y é um ideal. □

Diremos que a cadeia ascendente de ideais (1.4) é **estacionária** se existir algum $m \in \mathbb{N}$ para o qual $I_k = I_m$ para todo $k \geq m$.

Definição 14. *Dizemos que um anel A possui a propriedade de* ***Condição de Cadeias Ascendentes (cca)*** *se toda cadeia ascendente de ideais de A for estacionária.*

Proposição 3. *Seja A um anel. A é* Noetheriano *se, e somente se, A possui a propriedade (cca).*

Demonstração. Suponha A Noetheriano

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots \tag{1.5}$$

uma cadeia ascendente qualquer de ideais de A. Pelo Lema 1 temos que $Y = \bigcup_{n=1}^{\infty} I_n$ um ideal, e sendo um ideal de A temos que ele será finitamente gerado, ou seja, existem $x_1, \ldots, x_r \in A$ tais que:

$$Y = \langle x_1, \ldots x_r \rangle.$$

Sendo assim $x_k \in Y$, para todo $k = 1, \ldots, r$. Isso implica que para cada $k = 1, \ldots, r$, vai existir n que depende de k, denotado por n_k, tal que $x_k \in I_{n_k}$.

Como o conjunto dos n_k's é finito e $n_k \in \mathbb{N}$, percebemos que dentre $n_1, \ldots, n_r$ temos um maior elemento, digamos j' ($j' = max\{n_1, \ldots, n_r\}$). Com isso, vemos que

$$x_k \in I_{n_k} \subseteq I_{j'} \quad \forall k = 1, \ldots, r.$$

Portanto

$$Y = \langle x_1, x_2, \ldots, x_r \rangle \subseteq I_{j'} \subset \bigcup_{n=1}^{\infty} I_n = Y,$$

donde vemos que todas as inclusões acima devem ser obrigatoriamente igualdades. Deste modo, para todo $m > j'$ temos

$$I_{j'} \subseteq I_m \subset \bigcup_{n=1}^{\infty} I_n = I_{j'},$$

ou seja, para todo $m > j'$ tem-se que $I_{j'} = I_m$, e assim a cadeia ascendente de ideais dada em (1.5) é estacionária e A possui a propriedade (cca).

Agora suponha que A possua a propriedade (cca). Queremos provar que qualquer ideal de A é finitamente gerado. Suponha então I um ideal qualquer de A, gerado pelo conjunto S (que na pior das hipóteses pode ser o próprio I, como conjunto), isto é,

$$I = \langle S \rangle.$$

Se S for finito, provamos o que queríamos. Suponha que S seja infinito, isto é,

$$S = \{x_1, x_2, \ldots, x_n, \ldots\}.$$

Vamos criar uma cadeia ascendente de ideais gerados por elementos de S da seguinte forma:

$$I_1 = \langle x_1 \rangle \subset I_2 = \langle x_1, x_2 \rangle \subset \ldots \subset I_n = \langle x_1, x_2, \ldots, x_{n-1}, x_n \rangle \subset \ldots \tag{1.6}$$

Note que os ideais I_k foram construídos de modo que $x_k \in I_k$ para todo $x_k \in S$ e $I_k \subset I$. Além disso, (1.6) é cadeia ascendentes de ideais de A, e como toda cadeia ascendente de ideais de A deve ser estacionária, existe um $r \in \mathbb{N}$ tal que, para todo $m > r$, $I_m = I_r$. E daí vemos que para todo k,

$$x_k \in I_k \subseteq I_r;$$

ou seja, $S \subset I_r$ e por fim concluímos que

$$I \subset I_r \subset I,$$

ou seja, $I = I_r\langle x_1, \ldots, x_r \rangle$ e assim I finitamente gerado. □

2 Polinômios

O objetivo central deste capítulo será o de estabelecer de forma rigorosa o anel de polinômios, tanto em uma indeterminada, quanto em n indeterminadas, e além disso, observarmos diversas propriedades desses anéis.

Observamos que para generalizar o algoritmo de divisão polinomial de uma indeterminada para n indeterminadas, precisaremos generalizar o conceito de grau e de termo líder, e faremos isso apresentando o conceito de ordens monomiais.

Usamos como base para este capítulo os textos de (COUTINHO, 2012), (IEZZI, 2005) e (HEFEZ; VILLELA, 2012).

2.1 Polinômios em uma indeterminada

Seja A um anel comutativo com unidade e x um símbolo formal. Definimos um polinômio como uma expressão do tipo:

$$a_0x^0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n,$$

onde $n \in \mathbb{N} \cup \{0\}$ e $a_i \in A$, $i = 0, 1, 2, \ldots, n$. Note que a "soma" acima é definida formalmente, e ela pode ser denotada de maneira sucinta por

$$\sum_{i=0}^{n} a_ix^i,$$

sendo x um símbolo formal que podemos denominar como **indeterminada**, **incógnita** ou **variável**[1]. Já os elementos a_i, com $i = 1, 2, \ldots, n$, são os **coeficientes** do polinômio e i o índice do respectivo coeficiente. Bom, vale ressaltar que a indeterminada de um polinômio pode ser representada por outras letras minúsculas além do x, sendo as mais comuns x, y e z, e para representar o polinômio usamos f ou $f(x)$ quando quisermos destacar sobre qual incógnita ele se relaciona. Vamos denotar por $A[x]$ o conjunto de todos os polinômios cujos coeficientes forem elementos de um anel A.

Vamos chamar de **polinômio nulo** aquele em que todos os coeficientes a_i, com $i \in \mathbb{N} \cup \{0\}$, são iguais a zero.

Exemplo 14. *Considerando em $K[x]$, os polinômios $f(x) = 5x^3 + 2x^2 + 3x + 1$ e $g(x) = 2x^4 + 6x^2 + 8$, temos que:*

i) os coeficientes de f são $a_0 = 1, a_1 = 3, a_2 = 2, a_3 = 5$.

[1] O termo variável aqui distingue do senso comum de uma variável em uma função, mas o seu uso não é equivocado, tendo em vista uma importante classe de funções, as polinomiais.

ii) os coeficientes de g são $a_0 = 8, a_1 = 0, a_2 = 6, a_3 = 0, a_4 = 2$.

Dentre o conjunto de polinômios há uma subclasse de polinômios especiais do tipo $a_n x^n$, os chamados **monômios**.

Definição 15. *Dado f, se n é o maior dos índices, tal que $a_n \neq 0$ dizemos que:*

i) $a_n x^n$ é chamado de termo líder, denotado por $TL(f)$,

ii) x^n é chamado de monômio líder, denotado por $ML(f)$,

iii) a_n é chamado de coeficiente líder, denotado por $CL(f)$,

iv) a_0 é chamado de termo independente.

Definição 16. *Definimos o **grau** de um polinômio não nulo f, denotado por $\partial(f)$, como sendo o expoente que acompanha a indeterminada do monômio líder, ou seja, se $ML(f) = x^n$, então $\partial(f) = n$.*

Observação 1. *O grau do polinômio nulo não está definido.*

Exemplo 15. *Considere o polinômio $f = 8x^2+3x+5$. Então o termo líder é $TL(f) = 8x^2$, o monômio líder é $ML(f) = x^2$, o coeficiente líder é $CL(f) = 8$ e o termo independente é 5. O grau deste polinômio é igual à $\partial(f) = 2$.*

Definição 17. *Dois polinômios f e g, da forma $f = a_n x^n + \ldots + a_1 x + a_0$ e $g = b_m x^m + \ldots + b_1 x + b_0$, são iguais se, e somente se $m = n$ e todos os coeficientes correspondentes são iguais, isto é,*

$$a_0 = b_0,\ a_1 = b_1,\ \ldots\ ,\ a_n = b_n.$$

Exemplo 16. *Para que os polinômios em $K[x]$ $f = ax^3+(b+c)x^2+cx+b$ e $g = 5x^3-2x+2$ sejam iguais, devemos ter que $a = 5$, $c = -2$ e $b = 2$.*

Observe que o polinômio $f = 2x^4 + 8x + 5$, pode também ser representado pelas seguintes expressões $f = 2x^4+0x^3+0x^2+8x+5$ ou $f = 0x^6+0x^5+2x^4+8x+5$. Esse tipo de raciocínio pode ser feito de forma geral, então suponha um polinômio que tenha grau n, ele pode ser escrito de modo que todos os monômios sejam explicitados (aqueles que anteriormente estavam omitidos agora aparecem com coeficiente zero), e esse raciocínio pode fazer que na representação desse polinômio, apareça monômios com grau maior do que o grau do próprio polinômio.

Essas representações são úteis para a apresentação da soma e multiplicação de polinômios que aparece a seguir, nos demais casos é pertinente usar de sua forma mais compacta.

Na soma de dois ou mais polinômios, obtemos um novo polinômio cujos coeficientes são precisamente a soma dos coeficientes correspondentes ao mesmo monômio x^i. Sendo assim, suponha $f = a_n x^n + \ldots + a_1 x + a_0$ e $g = b_m x^m + \ldots + b_1 x + b_0$ com $n \leq m$ então:

$$\begin{aligned} f + g = & \ (0 + b_m)x^m + \ldots + (a_n + b_n)x^n + \ldots + (a_1 + b_1)x + (a_0 + b_0) \\ = & \ \sum_{i=1}^{m} (a_i + b_i)x^i. \end{aligned}$$

Exemplo 17. *Sejam $f = 5x^3 + 4x^2 + 12$ e $g = 6x^2 + 3x + 8$. Conforme observamos acima, estes polinômios podem ser representados como $f = 5x^3 + 4x^2 + 0x + 12$ e $g = 0x^3 + 6x^2 + 3x + 8$. Sendo assim temos,*

$$\begin{aligned} f + g = & \ (5 + 0)x^3 + (4 + 6)x^2 + (0 + 3)x + (12 + 8) \\ = & \ 5x^3 + 10x^2 + 3x + 20. \end{aligned}$$

Sejam $f, g \in K[x]$ tais que $f = a_n x^n + \ldots + a_1 x + a_0$ e $g = b_m x^m + \ldots + b_1 x + b_0$ com $n \leq m$. O produto de f e g é definido por $f \cdot g = c_{m+n} x^{m+n} + \ldots + c_1 x^1 + c_0$, em que

$$c_i = \sum_{t=0}^{i} a_t b_{i-t}, \quad 0 \leq i \leq m + n.$$

Exemplo 18. *Sejam $f = x^3 + 4x^2 + 5$ e $g = 2x^3 + 5x^2 + 4$. Conforme observamos no início do capítulo, estes polinômios podem ser representados das seguintes formas: $f = x^3 + 4x^2 + 0x + 5$ e $g = 2x^3 + 5x^2 + 0x + 4$. Sendo assim temos,*

$$\begin{aligned} f \cdot g = & \ (x^3 + 4x^2 + 0x + 5) \cdot (2x^3 + 5x^2 + 0x + 4) \\ = & \ (1 \cdot 2)x^6 + (1 \cdot 5 + 4 \cdot 2)x^5 + (4 \cdot 5)x^4 + (1 \cdot 4 + 5 \cdot 2)x^3 + (4 \cdot 4 + 5 \cdot 5)x^2 + (5 \cdot 4) \\ = & \ 2x^6 + 13x^5 + 20x^4 + 14x^3 + 41x^2 + 20. \end{aligned}$$

Observe que, na prática, multiplicar dois polinômios é equivalente a fazer a distributividade de monômio a monômio.

Proposição 4. *Se f e g são não-nulos sobre um domínio de integridade, então fg é não-nulo e*

$$\partial(fg) = \partial(f) + \partial(g).$$

Demonstração. Sejam $f = a_n x^n + \ldots + a_1 x + a_0$ e $g = b_m x^m + \ldots + b_1 x + b_0$ tais que $f, g \in k[x]$, polinômios não nulos de grau n e m respectivamente. Denotemos por c_j, $j \in \mathbb{N}$, os coeficientes do produto fg. Sabemos que

$$c_j = a_j b_o + a_{j-1} b_1 + \ldots + a_1 b_{j-1} + a_0 b_j = \sum_{i=0}^{j} a_i b_{j-i}.$$

Para que tenhamos $j > n + m$, c_j será a soma dos termos do tipo $a_i b_{j-i}$ com $i = i + (j - i) > m + n$ dai devemos ter $j > m$ ou $j - i > m$. Como $\partial(f) = n$ e $\partial(g) = m$,

temos $a_i = 0$ para $i > n$, e $b_k = 0$ para $k > m$. Logo o produto $a_j b_{j-i} = 0$ para todo $j > n + m$. Por outro lado, $a_n b_m \neq 0$, o que implica $c_{n+m} \neq 0$. Assim, o menor natural k tal que $c_j \neq 0$, para todo $j > n + m$ é $k = n + m$. Logo

$$\partial(fg) = n + m = \partial(f) + \partial(g).$$

□

Enunciamos sem demonstração o seguinte resultado relacionado a estrutura algébrica do conjunto $A[x]$.

Teorema 2. *Seja A anel. O conjunto $A[x]$ munido das operações de adição e multiplicação descritos acima é um anel.*

A partir deste momento queremos que nossos coeficientes estejam em um corpo K, pois os inversos nos garante que sempre será possível dividir os tais coeficientes. Sendo assim, denotaremos o anel de polinômios daqui daqui em diante por $K[x]$.

Teorema 3 (Divisão Euclidiana para Polinômios)**.** *Sejam f e g polinômios em $K[x]$, com $g \neq 0$. Então existem polinômios q e r em $K[x]$ tais que*

$$f = qg + r$$

em que $r = 0$ ou que $\partial(r) < \partial(g)$.

A prova de tal teorema se encontra no livro (VIDIGAL, 2005, Teorema 8.10).

Corolário 2. *São únicos os polinômios q e r obtidos no teorema anterior.*

Demonstração. Suponha $f \in K[x]$ tal que

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

com

$$\partial(r_i) < \partial(g) \quad \text{ou} \quad r_i = 0 \quad \text{para} \quad i = 1, 2.$$

Subtraindo as duas expressões obtemos,

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

Se $r_2 - r_1 \neq 0$, então $\partial(r_2 - r_1) < \partial(g)$ e $q_1 - q_2 \neq 0$, já que $g \neq 0$. Mas então obtemos uma contradição, pois

$$\partial(g) > \partial(r_2 - r_1) = \partial((q_1 - q_2)g) \geq \partial(g).$$

Portanto, necessariamente, $r_2 - r_1 = 0$, o que implica $q_1 - q_2 = 0$ (pois $g \neq 0$), provando assim a unicidade. □

Sejam f, g dois polinômios em $K[x]$, dizemos que g é um **divisor** de f ou que f é **múltiplo** de g, se existe $q \in K[x]$ tal que $f = qg$.

Um caso especial a se analisar é quando f e g são não nulos e f é múltiplo de g, isto é $f = qg$. Esse caso implica que $\partial(f) \geq \partial(g)$, e a prova disso vem do seguinte fato: se $f = gq$, usando a Proposição 4 temos $\partial(f) = \partial(gq) = \partial(g) + \partial(q) \geq \partial(g)$.

Quando um polinômio é divisível por um monômio, de forma que r seja o polinômio nulo, podemos representar tal divisão como fração (generalizando a ideia de números racionais). Vejamos um exemplo.

Exemplo 19. *Sejam $f = 12x^3 + 16x^4 + 10x$ e $g = 4x$ dois polinômios em $\mathbb{R}[x]$. Observe que podemos escrever*

$$f = g \cdot \left(3x^2 + 4x^3 + \frac{5}{2}\right) + 0, \tag{2.1}$$

e como

$$q = 3x^2 + 4x^3 + \frac{5}{2} \quad e \quad r = 0$$

satisfazem as condições para quociente e resto do Teorema 3, temos que a igualdade dada em (2.1) é representação da divisão de f pelo monômio $4x$. E como o resto desta divisão é zero, temos que f é divisível pelo monômio $g = 4x$. Nesse caso é comum representarmos o quociente q em termos de uma "fração" (vale destacar que em geral $\frac{f}{g} \notin K[x]$ mesmo que $f, g \in K[x]$):

$$q = \frac{12x^3 + 16x^4 + 10x}{4x} = 3x^2 + 4x^3 + \frac{5}{2}.$$

O Corolário 2 traz a unicidade do quociente e do resto para a divisão de quaisquer polinômios f e $g \neq 0$ em $K[x]$, mas não nos dá um modo de obtê-los. Nesse sentido, iremos apresentar um algoritmo que nos permitirá obtê-los.

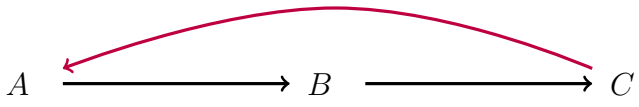
Sejam f, g polinômios. Vamos considerar inicialmente $r = 0$, $q = 0$.

Passo A: Teste se $TL(g)$ divide o $TL(f)$. Se o $TL(g)$ divide $TL(f)$ siga para o passo B, caso contrário pare o algoritmo.

Passo B: Faça $q := q + \dfrac{TL(f)}{TL(g)}$, $f := f - q \cdot g$. E vá para o passo C.

Passo C: Se $\partial(f) < \partial(g)$ pare o algoritmo e $r = f$, se $\partial(f) > \partial(g)$ volte ao passo A.

O algoritmo acima pode ser ilustrado pelo seguinte diagrama:



Esses passos formam o algoritmo de divisão polinomial, e quando no passo C o $\partial(f) < \partial(g)$ paramos o algoritmo e o polinômio r será o resto da divisão e o polinômio q o

quociente.

Exemplo 20. *Sejam* $f = 4x^3 - x^2 + 0x + 2$ *e* $g = x^2 + 1$. *A divisão de* f *por* g *é feita seguindo os passos acima:*

Observe que $TL(x^2 + 1)$ *divide* $4x^3$. *Sendo assim temos* $q = 0 + \frac{4x^3}{x^2} = 4x$ *e* $f = 4x^3 - x^2 + 0x + 2 - [4x \cdot (x^2 + 1)] = -x^2 - 4x + 2$. *Uma forma de representarmos essas informações é através da tradicional representação de divisão por chave:*

$$\begin{array}{r|l} f = 4x^3 - x^2 + 0x + 2 & g = x^2 + 1 \\ \cline{2-2} -4x \cdot (x^2 + 1) & 4x \\ \cline{1-1} f = -x^2 - 4x + 2 & \end{array}$$

Como o $gr(g) < gr(f)$ *e já que* $4x$ *divide* $-x^2$ *continuamos. Seguindo o passo C temos* $q = 4x + \frac{-x^2}{x^2} = -1$ *e* $f = -x^2 - 4x - [-1 \cdot (x^2 + 1)] = -x^2 - 1$

$$\begin{array}{r|l} f = 4x^3 - x^2 + 0x + 2 & g = x^2 + 1 \\ \cline{2-2} -4x \cdot (x^2 + 1) & 4x\text{-}1 \\ \cline{1-1} f = -x^2 - 4x + 2 & \\ +x^2 + 1 & \\ \cline{1-1} f = -4x + 3 & \end{array}$$

Como $gr(g) > gr(f)$ *paramos o algoritmo e concluímos que* $q = 4x-1$ *e* $r = -4x+3$.

2.2 Polinômios em n indeterminadas e Ordem Monomial

Nesta seção iremos apresentar o conjunto de polinômios em n indeterminadas, além de listarmos algumas de suas propriedades. Essa construção será feita de forma recursiva de modo que, a cada passo, possamos levar as propriedades de estrutura algébrica destes conjuntos para o próximo passo.

Inciamos definindo o anel de polinômios em duas indeterminadas x e y da seguinte forma: considere $A_1 = K[x]$ com K corpo e defina,

$$A_2 = A_1[y].$$

Decorre do Teorema 2 que A_1 é um anel e disto, pelo mesmo teorema, concluímos que $A_1[y]$ é um anel de polinômios com coeficientes em $A_1 = K[x]$ na indeterminada y.

Um elemento típico de A_2 é da forma

$$f = f_0(x) + f_1(x)y + f_2(x)y^2 + \cdots + f_n(x)y^n,$$

com $f_i(x) \in A_1$. Olhando mais atentamente para uma dessas parcelas, observamos o seguinte:

$$f_i(x)y^i = \left(\sum_{j=0}^{m_j} a_j x^j\right) y^i = \sum_{j=0}^{m_j} a_j x^j y^i.$$

A justificativa para a última igualdade acima é que cada termo do polinômio $f_i(x)$ é também um polinômio em A_1, ou seja, um coeficiente válido no anel $A_1[y]$, onde sabemos valer a distributiva do produto em relação a adição, vale ressaltar também, que pelo mesmo motivo temos a comutatividade da multiplicação entre as indeterminadas x e y. Deste modo percebemos que f na verdade pode ser escrito como uma soma (finita) de expressões do tipo

$$a_{i,j}x^i y^j,$$

em que $a_{i,j} \in K$. Com isso em mente, ao invés de dizer que f além de ser um polinômio na indeterminada y com coeficientes no anel de polinômios na indeterminada x e coeficientes em K, podemos simplesmente dizer que f é um polinômio nas indeterminadas x e y com coeficientes em K, e sob essa nova visão, iremos usar a seguinte notação:

$$A_2 = A_1[y] = K[x,\, y].$$

Esse conjunto $K[x, y]$ é chamado de anel de polinômios nas (duas) indeterminadas x e y com coeficientes em K. Para anéis de polinômios em duas ou até três indeterminadas é comum o uso das letras x, y e z para representar as incógnitas, mas a partir de 4 indeterminadas, se torna interessante o uso de índices para representar todas as incógnitas, como por exemplo

$$x_1,\, x_2,\, x_3,\, x_4, \quad \text{ou} \quad y_1,\, y_2,\, \ldots,\, y_{18},\, y_{19},$$

para representar o conjunto de incógnitas de anéis de polinômios em 4 e 19 indeterminadas, respectivamente.

Recursivamente, definimos o anel de polinômios em n indeterminadas como o anel de polinômios na indeterminada x_n com coeficientes no anel de polinômios em $n-1$ indeterminadas, denotado por $A_{n-1} = K[x_1, x_2, \ldots, x_{n-1}]$, isto é,

$$K[x_1, x_2, \ldots, x_n] = A_{n-1}[x_n].$$

Um polinômio típico desse anel será uma combinação linear finita sobre K de polinômios especiais do tipo,

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}, \quad \alpha_i \in \mathbb{N} \cup \{0\}.$$

Estes serão chamados de monômios em n indeterminadas.

Quando trabalhamos com um polinômio em uma indeterminada, mesmo que sem perceber, usamos uma ordenação de seus monômios, baseada em seus respectivos graus

(ora ordenação crescente desse grau, ora decrescente desses graus), o que em geral facilita os cálculos das operações usuais. No entanto, quando trabalhamos com polinômios em várias variáveis, considerando apenas os graus dos monômios é insuficiente uma vez que existem mais de um monômio com mesmo grau, por exemplo x^2 e xy. Por esse motivo precisamos estabelecer meios de ordenar esses monômios de uma forma completa, e neste capítulo vamos estudar alguns exemplos de tais estratégias.

Para facilitar a notação podemos associar de forma biunívoca o monômio $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ com o vetor $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in (\mathbb{N} \cup \{0\})^n$. Quando é conhecido α é comum denotarmos o $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ por x^α. Por exemplo, ao trabalhar com $A[x_1, x_2, x_3]$, podemos representar o monômio $x_1^1x_2^0x_3^0$ por x^α com $\alpha = (1, 0, 0)$.

Essa notação é útil pois concorda com soma de potências quando multiplicamos polinômios em n indeterminadas. Dessa forma, sendo $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ e $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$, temos:

$$\begin{aligned} x^{\alpha+\beta} &= x_1^{\alpha_1+\beta_1}x_2^{\alpha_2+\beta_2}\cdots x_n^{\alpha_n+\beta_n} = \left(x_1^{\alpha_1}x_1^{\beta_1}\right)\cdot\left(x_2^{\alpha_2}x_2^{\beta_2}\right)\cdots\left(x_n^{\alpha_n}x_n^{\beta_n}\right) \\ &= (x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n})\cdot\left(x_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}\right) \\ &= x^\alpha x^\beta. \end{aligned}$$

Definição 18. *Definimos **multigrau** de um monômio em n indeterminadas como sendo $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, tal que $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ seja o nosso monômio. E o **grau** de um monômio de n indeterminadas sendo a soma dos expoentes de cada indeterminada, ou seja $|\alpha| = \alpha_1 + \alpha_2 + \ldots + \alpha_n$. Seja m um monômio que pertence a $K[x_1, \ldots, x_n]$ denotamos, respectivamente, o multigrau e o grau por multigrau(m) e $\partial(m)$.*

Definição 19. *Uma **ordenação monomial** sobre $K[x_1, \ldots, x_n]$ é qualquer relação $>$ sobre o conjunto dos monômios $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ em que $\alpha_i \in \mathbb{N}$ com $i = 1, \ldots n$, que satisfaz:*

i) $>$ é uma ordenação total sobre o conjunto dos monômios, ou seja, para quaisquer dois monômios x^α e x^β, em que α, $\beta \in (\mathbb{N} \cup \{0\})^n$, uma das três alternativas devem ocorrer:

$$x^\alpha = x^\beta \quad ou \quad x^\alpha > x^\beta \quad ou \quad x^\beta > x^\alpha.$$

ii) Se $x^\alpha > x^\beta$, então

$$x^{\alpha+\gamma} = x^\alpha \cdot x^\gamma > x^\beta \cdot x^\gamma = x^{\beta+\gamma}.$$

iii) No conjunto dos monômios, munido da relação $>$, vale o princípio da boa-ordenação. Isto significa que todo subconjunto não vazio de $K[x_1, \ldots, x_n]$, contendo somente monômios, tem um menor elemento com relação a $>$.

Note que estabelecer uma ordem monomial em um anel em n indeterminadas é equivalente a estabelecer uma ordem no conjunto dos multigraus $(\mathbb{N} \cup \{0\})^n$, e por

esse motivo, iremos fazer o abuso notacional de usarmos a mesma notação em ambos os conjuntos, ou seja,

$$x^{\alpha} > x^{\beta} \Longleftrightarrow \alpha > \beta.$$

Agora que temos tal notação esclarecida vamos mostrar algumas ordenações monomiais válidas, destacando a que iremos usar daqui para frente.

Definição 20 (Ordem Lexicográfica)**.** *Sejam os monômios x^{α} e x^{β} com $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ e $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$. Nós dizemos que:*

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} >_{lex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n},$$

se existir $i \in \{1, 2, \ldots, n\}$ tal que $\alpha_i > \beta_i$ e $\alpha_j = \beta_j$ para todo $j > i$.

Note que pela ordem lexicográfica, a ordenação das indeterminadas $x_1, x_2, \ldots, x_n$ é $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$. De fato, basta notar que ao identificarmos

$$x_1 = x_1^1 x_2^0 \cdots x_n^0, \; x_2 = x_1^0 x_2^1, \cdots x_n^0, \quad \ldots, \quad x_n = x_1^0 x_2^0 \cdots x_n^1,$$

é imediato verificar que

$$(1, 0, \ldots, 0) >_{lex} (0, 1, \ldots, 0) >_{lex} \cdots >_{lex} (0, 0, \ldots, 1).$$

É importante frisar que na ordem lexicográfica, independente do grau total, uma indeterminada é maior que qualquer monômio envolvendo indeterminadas menores; por exemplo, em $A[x, y, z]$, usando a ordem lexicográfica $x >_{lex} y >_{lex} z$, temos $x >_{lex} y^4 z^7$.

Definição 21 (Ordem Lexicográfica Graduada)**.** *Sejam $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ e $x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$, dizemos que:*

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} >_{grlex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n},$$

i) se $\partial\left(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}\right) > \partial\left(x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}\right)$, ou

ii) se $\partial\left(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}\right) = \partial\left(x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}\right)$ e $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} >_{lex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$.

Exemplo 21. *Sejam $x^1 y^2 z^4$ e $x^1 y^1 z^5$ temos $x^1 y^2 z^4 >_{grlex} x^1 y^1 z^5$ já que $\partial\left(x^1 y^2 z^4\right) = \partial\left(x^1 y^1 z^5\right)$ e $x^1 y^2 z^4 >_{lex} x^1 y^1 z^5$.*

Definição 22 (Ordem Lexicográfica Graduada Reversa)**.** *Sejam $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ e $x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$, dizemos que:*

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} >_{grevlex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n},$$

i) se $\partial\left(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}\right) > \partial\left(x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}\right)$, ou

ii) se $\partial\left(x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}\right) = \partial\left(x_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}\right)$ *e existe* $i \in \{1, 2, \ldots, n\}$*, tal que* $\alpha_i < \beta_i$ *e* $\alpha_j = \beta_j$ *para todo* $j > i$*.*

Exemplo 22. *Sejam* $x^1y^5z^2$ *e* $x^4y^1z^3$*. Temos que* $x^1y^5z^2 >_{grevlex} x^4y^1z^3$*, pois* $\partial\left(x^1y^5z^2\right) = \partial\left(x^4y^1z^3\right) = 8$ *e* $1 < 4$*.*

Exemplo 23. *Seja* $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ *um polinômio em* $K[x, y, z]$*. Então podemos reescrevê-lo, ordenando seus termos, das seguintes formas:*

i) Na ***ordenação lexicográfica****, temos que:*

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2 \quad ou, \quad f = 4z^2 + 4xy^2z + 7x^2z^2 - 5x^3.$$

ii) Já na ***ordenação lexicográfica graduada****:*

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2 \quad ou, \quad f = 4z^2 - 5x^3 + 4x^2zy + 7x^2z^2.$$

iii) Por fim, usando a ***ordenação lexicográfica graduada reversa*** *temos que:*

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2 \quad ou, \quad f = 4z^2 - 5x^3 + 7x^2z^2 + 4xy^2z.$$

Apesar de um polinômio poder ser representado de diversas formas como vimos no exemplo anterior, fixado um tipo de ordenação, o polinômio só terá uma maneira de ser escrito de forma crescente e uma de forma decrescente. A ordem monomial que escolhemos para trabalhar daqui em diante é a **ordem monomial lexicográfica graduada reversa**.

De modo análogo ao que definimos para polinômios em uma indeterminada, podemos estabelecer que dado $f \in K[x_1, \ldots, x_n]$, e sendo a_nx^α o termo do polinômio em que $a_n \neq 0$ e x^α é o maior monômio que aparece, de acordo com a ordem monomial usada, diremos que a_nx^α é o termo líder de f, denotado por $\mathrm{TL}(f)$, x^α o monômio líder, denotado por $\mathrm{ML}(f)$, a_n o coeficiente líder, denotado por $\mathrm{CL}(f)$ e a_0 é o termo independente de f. Neste ponto estamos hábeis a definir **multigrau** e **grau** de um polinômio $f \in K[x_1, \ldots, x_n]$ não nulo de maneira bem natural:

- $multigrau(f) = multigrau\,(ML(f))$;
- $\partial(f) = \partial\,(ML(f))$.

Lema 2. *Sejam* $f, g \in K[x_1, \ldots, x_n]$ *polinômios não nulos. Então:*

i) $multigrau(fg) = multigrau(f) + multigrau(g)$.

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

Ainda se $multigrau(f) \neq multigrau(g)$*, temos então,*

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

Demonstração. i) Sejam f, g polinômios em $K[x_1, x_2, \ldots, x_n]$, tais que

$$f = \sum_{i=1}^{n} a_i x^{\alpha_i} \quad \text{e} \quad g = \sum_{j=1}^{m} b_j x^{\beta_j}$$

aos quais, $a_i, b_j \in K$ e $\alpha_i, \beta_j \in (\mathbb{N} \cup \{0\})^n$, para $1 \leq i \leq n$ e $1 \leq j \leq m$. Seja $>$ uma ordenação monomial qualquer, de forma que podemos, sem perda de generalidade, supor:

$$\alpha_1 < \alpha_2 < \ldots < \alpha_n \quad \text{e} \quad \beta_1 < \beta_2 < \ldots < \beta_m,$$

e assim $multigrau(f) = \alpha_n$ e $multigrau(g) = \beta_m$. Observe que:

$$fg = \left(\sum_{i=1}^{n} a_i x^{\alpha_i}\right) \cdot \left(\sum_{j=1}^{m} b_j x^{\beta_j}\right) = \sum_{i=1}^{n} \sum_{j=i}^{m} a_i b_j x^{\alpha_i + \beta_j}.$$

Observe ainda que,

$$\alpha_n > \alpha_i, \ \forall\ 1 \leq i \leq (n-1), \quad \text{e} \quad \beta_m > \beta_j, \ \forall\ 1 \leq j \leq (m-1),$$

e da definição de ordenação monomial temos

$$\alpha_n + \beta_j > \alpha_i + \beta_j, \ \forall\ 1 \leq i \leq (n-1) \quad \text{e} \quad 1 \leq j \leq m.$$

Da mesma forma, temos que

$$\alpha_i + \beta_m > \alpha_i + \beta_j, \ \forall\ 1 \leq i \leq n \quad \text{e} \quad 1 \leq j \leq (m-1),$$

e portanto,

$$\alpha_n + \beta_m > \alpha_i + \beta_j, \ \forall\ 1 \leq i \leq (n-1) \text{ e } \ 1 \leq j \leq (m-1).$$

Desta forma $\alpha_n + \beta_m$ é o multigrau de fg.

ii) Sejam f e g definidos como no item acima e tais que $f + g \neq 0$, de forma que $multigrau(f+g)$ está definido.

Suponhamos inicialmente que $multigrau(f) \neq multigrau(g)$. Temos daí que $\alpha_n > \alpha_i$ para $1 \leq i \leq (n-1)$ e $\beta_m > \beta_j$ para $1 \leq j \leq (m-1)$. Como $\alpha_n \neq \beta_m$, o $multigrau(f+g)$ será o maior entre os dois, ou seja,

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

Se no entanto tivermos que $multigrau(f) = multigrau(g)$, então temos duas possibilidades:

(a) Se $TL(f) = -TL(g)$: Neste caso os termos líderes se cancelam, deixando apenas termos menores que $x^{\alpha_n} = x^{\beta_m}$ e temos que $multigrau(f+g) < \alpha_n = \beta_m$ e portanto

$$multigrau(f+g) < max\{multigrau(f), multigrau(g)\}.$$

(b) Se $TL(f) \neq -TL(g)$: Neste caso não há cancelamento entre os termos líderes e temos que

$$TL(f+g) = (a_1 + b_1)x^{\alpha_n} = (a_1 + b_1)x^{\beta_m},$$

e portanto,

$$multigrau(f+g) = \alpha_n = \beta_m = max\{multigrau(f), multigrau(g)\}.$$

□

Estabelecida a ordenação dos monômios de um polinômio, vamos estender as operações com os polinômios em $K[x_1]$ para os polinômios em $K[x_1, \ldots, x_n]$.

Quando falamos em operações com polinômios em n indeterminadas, precisamos entender como elas funcionam no caso especial, que é quando trabalhamos com monômios, e posteriormente estendemos tais operações para polinômios quaisquer fazendo uso da propriedade distributiva.

Para somar dois monômios que pertencem a $K[x_1, \ldots, x_n]$, primeiro devemos verificar o multigrau destes monômios. Se os multigraus forem iguais somamos os coeficientes destes e mantemos as indeterminadas e seus expoentes, mas se os multigraus forem diferentes, mantemos a soma indicada e dessa forma passamos a ter um polinômio com dois termos distintos, por exemplo, $x + y$ é a melhor representação para a soma dos monômios x e y.

Desta forma, quando somamos dois polinômios seguimos os passos acima. Caso os polinômios em que estamos somando tenham termos com mesmo multigrau, somamos os coeficientes de tais termos e geramos um termo de mesmo multigrau para o polinômio resultado. Já para os termos que não possuem multigrau em comum, basta repetir este termo no polinômio resultado que ele se tornará um termo do mesmo.

Exemplo 24. *Sejam f, g polinômios em $K[x, y, z]$, tais que $f = 3x^2y + y + 5z$ e $g = 2xy + 4y - z$. O polinômio resultado da soma $f + g$ é dado por*

$$f + g = 3x^2y + 2xy + (1+4)y + (5-1)z = 3x^2y + 2xy + 5y + 4z.$$

Já ao multiplicarmos dois monômios geramos um novo monômio ao qual o coeficiente é formado pelo produto dos coeficientes dos outros dois polinômios e o multigrau das indeterminadas é formado pela soma dos multigraus dos monômios envolvidos na multiplicação.

Sendo assim, quando multiplicamos dois polinômios em $K[x_1, \ldots, x_n]$ fazemos a distributiva de termo a termo, similar ao feito em $K[x]$, e depois efetuamos a soma dos termos que possuem mesmo multigrau.

Exemplo 25. *Sejam f, g polinômios em $K[x, y, z]$, tais que $f = 3x^2y + y + 5z$ e $g = 2xy + 4y - z$. O polinômio resultado da multiplicação fg é dado por*

$$\begin{aligned} fg = & \ (3x^2y + y + 5z)(2xy + 4y - z) \\ = & \ 6x^3y^2 - 3x^2yz + 12x^2y^2 + 10xyz + 2xy^2 + 20yz - yz + 4y^2 - 5z^2 \\ = & \ 6x^3y^2 - 3x^2yz + 12x^2y^2 + 10xyz + 2xy^2 + 19yz + 4y^2 - 5z^2. \end{aligned}$$

O nosso próximo objetivo será estudar o conceito de divisão de polinômios em n indeterminadas, e para tal, é natural intuirmos que basta usarmos o que sabemos sobre divisão em uma indeterminada e aplicarmos diretamente. No entanto esse raciocínio simplório nos conduzirá a um problema, e para percebermos isso, consideremos a divisão de x^2 por xy. Uma aplicação direta do Corolário 1 nos diz que devemos ter únicos q e r polinômios tais que

$$x^2 = q \cdot xy + r,$$

com $r = 0$ ou $r < xy$ (note que usamos a ordem monomial ao invés da simples ordem dos graus). No entanto é fácil verificar que não existe um polinômio não nulo q em $K[x_1, \ldots, x_n]$ tal que

$$x^2 = q \cdot xy + r \quad r < xy.$$

Contudo, ainda sim conseguimos escrever x^2 em função de xy da seguinte forma,

$$x^2 = 0 \cdot (xy) + x^2,$$

em primeira instância esta representação pode parecer desnecessária, mas ao usar o polinômio nulo no lugar de q assemelhamos a equação ao teorema de divisão polinomial, mas note que nesse caso, o "candidato" a resto da divisão não satisfaz a condição de ser menor que o divisor (pois $xy < x^2$).

Para avançarmos um pouco mais, vamos deixar de lado por ora a condição exigida para o resto da divisão, e vamos tentar dividir dois polinômios em 3 indeterminadas. Sejam $f = x^5 + y^2 + yz$ e $g = x^4y$ tais que $f, g \in K[x, y, z]$. Para dividir f por g seguimos a ideia da divisão em $K[x]$ e vamos dividir termo a termo de f.

- x^5**:** Perceba que não existe q não nulo tal que

$$x^5 = q \cdot xy^4.$$

- y^2 **e** yz**:** Analogamente, não existe q_1 e q_2 não nulos tais que,

$$y^2 = q_1 \cdot x^4y \quad \text{e} \quad yz = q_2 \cdot x^4y,$$

de tal forma que chegamos a conclusão que g não divide nenhum termo de f. Donde concluímos que g não divide o primeiro termo de f. Da mesma forma que fizemos com os monômios no paragrafo anterior, podemos representar f em relação à divisão por g da seguinte maneira,

$$f = 0 \cdot g + f,$$

no qual seguindo a terminologia do Teorema 3, o quociente da divisão é zero e o resto o próprio f.

Para fixar as ideias, vamos considerar outro exemplo: Vamos tentar dividir $f = x^5 + 3x^2y + z$ por $g = xy$, e seguindo o exemplo anterior vamos dividir termo a termo de f.

- x^5: Note que não existe q não nulo tal que,

$$x^5 = q_1 \cdot xy.$$

- $3x^2y$: Já para este monômio existe $q_2 = 3x$ tal que,

$$3x^2y = q_2 \cdot xy.$$

- z: É fácil ver que para este termo também não existe q_3 não nulo tal que,

$$z = q_3 \cdot xy,$$

dessa forma podemos concluir que g divide somente um termo de f, e seguindo o raciocínio que construímos até agora temos,

$$f = (3x)g + (x^5 + z).$$

Daqui tiramos que diferente da divisão com polinômios em uma indeterminada, o fato de um monômio do dividendo, considerado maior pela ordenação, não ser divisível pelo termo líder do divisor, não garante que os outros também não serão.

Perceba que sempre que um termo do polinômio dividendo não for divisível, automaticamente ele entra como um termo do polinômio resto. E essas ideias nos conduzem ao seguinte resultado:

Teorema 4 (Divisão de polinômios em n indeterminadas)**.** *Sejam f e g polinômios em $K[x_1, \ldots, x_n]$ com $g \neq 0$. Então existem polinômios q e r em $K[x_1, \ldots, x_n]$ tais que*

$$f = qg + r,$$

onde r é composto pelos termos de f que não são divisíveis por g.

A demonstração deste teorema pode ser descrita em forma de um algoritmo que, além de garantir a validade do teorema, nos fornece um meio efetivo de obter o quociente e o resto da divisão. Passamos agora a descrever tal algoritmo

Sejam f e g dois polinômios em n indeterminadas e consideremos inicialmente $r = 0$, $q = 0$.

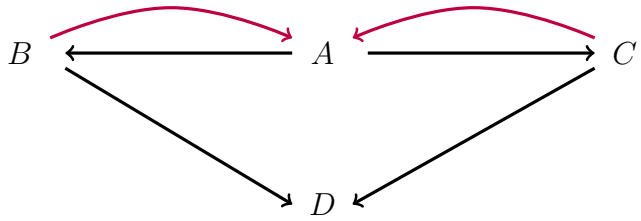
Passo A: Teste se $TL(g)$ divide o $TL(f)$. Se o $TL(g)$ divide $TL(f)$ siga para o passo B. Se o $TL(g)$ não divide $TL(f)$ siga para o passo C.

Passo B: Faça $q := q + \dfrac{TL(f)}{TL(g)}$, $f := f - q \cdot g$. Se $f = 0$ vá para o passo D e caso contrário volte ao passo A.

Passo C: Faça $r := r + TL(f)$ e $f := f - TL(f)$. Se $f = 0$ vá para o passo D e caso contrário volte ao passo A.

Passo D: Imprima q como quociente e r como resto da divisão de f (original) por g.

Este diagrama descreve o funcionamento do algoritmo acima:



E assim que $f = 0$ finalizamos o algoritmo obtendo q como quociente e r como resto da divisão, em que nenhum termo de r é divisível pelo $TL(g)$.

Exemplo 26. *Sejam* $f = 12x^3y^3 + 16x^4y + 10xy$ *e* $g = 4xy + x$. *Vamos efetuar a divisão entre esses dois polinômios usando os passos do algoritmo:*

i) Como $TL(g) = 4xy$ *divide* $TL(f) = 12x^3y^3$, *seguimos para o próximo passo B onde* $q = 0 + \dfrac{12x^3y^3}{4xy} = 3x^2y^2$ *e* $f = 12x^3y^3 + 16x^4y + 10xy - [3x^2y^2 \cdot (4xy + x)] = 16x^4y - 3x^3y^2 + 10xy \neq 0$ *e voltamos ao passo A.*

$$\begin{array}{l|l} 12x^3y^3 + 16x^4y + 10xy & 4xy + x \\ \cline{2-2} -12x^3y^3 - 3x^3y^2 & 3x^2y^2 \\ \cline{1-1} 16x^4y - 3x^3y^2 + 10xy & \end{array}$$

A partir de agora vamos omitir algumas operações para tornar mais rápido o desenvolvimento da divisão.

ii) Como $4xy$ *divide* $16x^4y$ *seguimos para o passo B e fazemos* $q = 3x^2y^2 + 4x^3$ *e* $f = x^4 - 3x^3y^2 + 10xy \neq 0$ *e voltamos ao passo A.*

$$\begin{array}{l|l} 12x^3y^3+16x^4y+10xy & 4xy+x \\ \hline -12x^3y^3-3x^3y^2 & 3x^2y^2+4x^3 \\ \hline 16x^4y-3x^3y^2+10xy & \\ -16x^4y-4x^4 & \\ \hline -4x^4-3x^3y^2+10xy & \end{array}$$

iii) Como $4xy$ *não divide* $-4x^4$ *seguimos para o passo C e fazemos* $r = 0 + 4x^4$ *e* $f = -3x^3y^2 + 10xy \neq 0$ *e voltamos ao passo A.*

iv) Como $4xy$ *divide* $-3x^3y^2$ *seguimos para o passo B e fazemos* $q = 3x^2y^2 + 4x^3 - \dfrac{3x^2y}{4} +$ *e* $f = \dfrac{3x^3y}{4} + 10xy \neq 0$ *e voltamos ao passo A.*

$$\begin{array}{l|l} 12x^3y^3+16x^4y+10xy & 4xy+x \\ \hline -12x^3y^3-3x^3y^2 & 3x^2y^2+4x^3-\dfrac{3x^2y}{4} \\ \hline 16x^4y-3x^3y^2+10xy & \\ -16x^4y-4x^4 & \\ \hline -3x^3y^2+10xy & \\ 3x^3y^2+\dfrac{3x^3y}{4} & \\ \hline \dfrac{3x^3y}{4}+10xy & \end{array}$$

v) Como $4xy$ *divide* $\dfrac{-3x^3y}{4}$ *seguimos para o passo B e fazemos* $q = 3x^2y^2 + 4x^3 - \dfrac{3x^2y}{4} + \dfrac{3x^2}{16}$ *e* $f = -\dfrac{3x^3}{16} + 10xy \neq 0$ *e voltamos ao passo A.*

$$\begin{array}{l|l} 12x^3y^3+16x^4y+10xy & 4xy+x \\ \hline -12x^3y^3-3x^3y^2 & 3x^2y^2+4x^3-\dfrac{3x^2y}{4}+\dfrac{3x^2}{16} \\ \hline 16x^4y-3x^3y^2+10xy & \\ -16x^4y-4x^4 & \\ \hline -4x^4-3x^3y^2+10xy & \\ 3x^3y^2+\dfrac{3x^3y}{4} & \\ \hline \dfrac{3x^3y}{4}+10xy & \\ -\dfrac{3x^3y}{4}-\dfrac{3x^3}{16} & \\ \hline -\dfrac{3x^3}{16}+10xy & \end{array}$$

vi) Como $4xy$ *não divide* $-\dfrac{3x^3}{16}$ *vamos para o passo C e fazemos* $r = -4x^4 - \dfrac{3x^3}{16}$ *e* $f = 10xy \neq 0$ *e voltamos ao passo A.*

vii) Como $4xy$ *divide* $10xy$ *seguimos para o passo B e fazemos* $q = 3x^2y^2 + 4x^3 - \frac{3x^2y}{4} + \frac{3x^2}{16} + \frac{5}{2}$ *e* $f = \frac{5x}{2} \neq 0$ *e voltamos ao passo A.*

$$
\begin{array}{l|l}
12x^3y^3 + 16x^4y + 10xy & 4xy + x \\
\hline
-12x^3y^3 - 3x^3y^2 & 3x^2y^2 + 4x^3 - \frac{3x^2y}{4} + \frac{3x^2}{16} + \frac{5}{2} \\
\hline
16x^4y - 3x^3y^2 + 10xy & \\
-16x^4y - 4x^4 & \\
\hline
x^4 - 3x^3y^2 + 10xy & \\
3x^3y^2 + \frac{3x^3y}{4} & \\
\hline
\frac{3x^3y}{4} + 10xy & \\
-\frac{3x^3y}{4} - \frac{3x^3}{16} & \\
\hline
10xy & \\
-10xy - \frac{5x}{2} & \\
\hline
-\frac{5x}{2} &
\end{array}
$$

viii) Como $4xy$ *não divide* $-\frac{5x}{2}$ *vamos para o passo C e fazemos* $r = -4x^4 - \frac{3x^3}{16} - \frac{5x}{2}$, $f = 0$ *e vamos para o passo D, momento em que o algoritmo é finalizado.*

Sendo assim finalizamos a divisão entre esses polinômios com $q = 3x^2y^2 + 4x^3 - \frac{3x^2y}{4} + \frac{3x^2}{16} + \frac{5}{2}$ *e* $r = x^4 - \frac{3x^3}{16} - \frac{5x}{2}$.

Agora vamos estudar uma divisão sucessiva com mais de um divisor, e nesse sentido, o que temos é uma generalização da divisão anterior que segue do teorema a seguir.

Teorema 5. *Sejam* $f, g_1, \ldots, g_s$ *polinômios e* $>$ *uma ordem monomial do anel* $K[x, \ldots, x_n]$. *Então existem polinômios* $q_1, \ldots, q_s$ *tais que*

$$f = q_1g_1 + q_2g_2 + \ldots + q_sg_s + r,$$

em que $r = 0$ *ou nenhum termo de* r *é divisível por nenhum* $TL(g_i)$, *com* $i = 1, 2, \ldots, s$ *e* $TL(f) = max\{TL(g_1q_1), \ldots, TL(q_sg_s), TL(r)\}$.

Com algumas alterações do algoritmo anterior, este abaixo, além de provar o teorema da divisão de um polinômio por s polinômios em n indeterminadas, também nos dá uma maneira de encontrar $q_1, q_2, \ldots, q_s, r$ que satisfazem as condições necessárias do Teorema 5. Sejam f e $G = \{g_1, g_2, \ldots, g_s\}$, tal que $f, g_i \in K[x_1, \ldots, x_n]$, com $i \in \{1, \ldots, s\}$.

Passo *A*: Defina $f_j = f$, e considere $r_1 = 0$ e $q_i, p_i = 0$ tal que $i \in \{1, \ldots, s\}$ e $j = 1$.

Passo B_i**:** Teste se $TL(g_i)$ divide $TL(f_j)$, se $TL(g_i)$ divide $TL(f_j)$ vá para o **passo** C_i. Caso contrário vá para o **passo** D_i

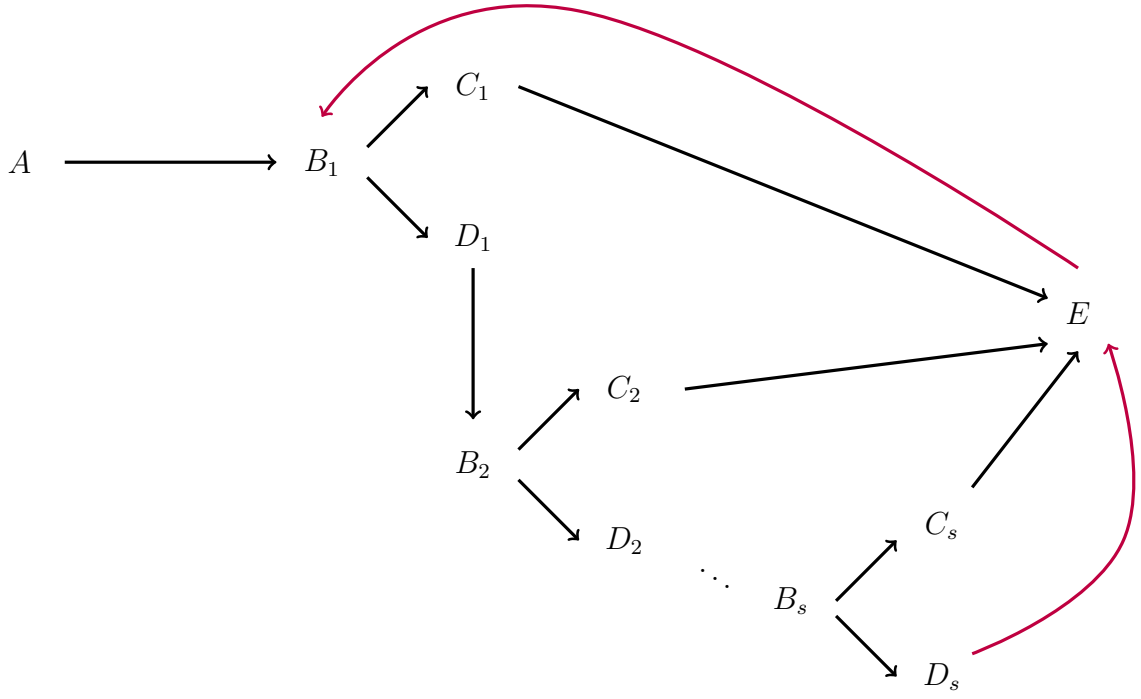
Passo C_i**:** Faça $q_i := \dfrac{TL(f_j)}{TL(g_i)}$, $p_i := p_i + q_i$ e $f_{j+1} := f_j - q_i \cdot g_i$. Vá para o **passo** E.

Passo D_i**:** Faça $i := i + 1$ e vá para o **passo** B_i.

...

Passo D_s**:** Se $TL(g_s)$ não divide $TL(f_j)$. Faça $f_{j+1} = f_j - TL(f_j)$, $r_{j+1} := r_j + TL(f_j)$, $i = 1$ e vá para o **passo** E.

Passo E**:** Se $f_{j+1} \neq 0$ continue o algoritmo e volte ao
passo B_1, mas se $f_{j+1} = 0$ pare e imprima o conjunto $P = \{p_i\}$ com $i = 1, \ldots, s$ como o conjunto quociente da divisão e o polinômio r_j o resto.



Assim, quando o algoritmo parar, o conjunto $P = \{p_i\}$ com $i = 1, \ldots, s$ é o conjunto quociente da divisão e o polinômio r_j o resto. E por esse algoritmo anterior temos

$$f = g_1 \cdot p_1 + g_2 \cdot p_2 + \ldots + g_s \cdot p_s + r_j,$$

em que cada termo de r_j é não divisível pelos $TL(g_i)$ (vide passo D_s). Note que se $r_j = 0$, temos que f é formado por uma combinação linear dos polinômios g_i, com $i = 1, 2, \ldots, s$. E com isso concluímos a existência dos polinômios $q_1, \ldots, q_s$ e r que satisfazem o enunciado do Teorema 5

Exemplo 27. *Vamos dividir o polinômio* $f = x^3y^2 + y^4 + x^3 + xy^2 + y + 1$ *pelo subconjunto* $G = (g_1, g_2)$ *onde* $g_1 = xy^2 + x$ *e* $g_2 = x^2y + y$*, temos:*

$$\begin{array}{l|l|l} x^3y^2+y^4+x^3+xy^2+y+1 & xy^2+x & \text{Resto:} \\ f=y^4+xy^2+y+1 & x^2y+y & r=y^4 \\ \cline{2-2} f=xy^2+y+1 & p_1=x^2+1 & \\ f=-x+y+1 & p_2=0 & r=y^4-x+y+1 \end{array}$$

Agora, note que xy^2 divide x^3y^2 pois $x^3y^2=(x^2)(xy^2)$ e portanto seguindo o algoritmo temos $p_1=x^2$ e $f=y^4+xy^2+y+1$. Como nem xy^2 e nem x^2y dividem y^4 pelo passo D_2 temos $r=y^4$ e $f=xy^2+y+1$. Perceba que xy^2 divide o novo $TL(f)$, pois $xy^2=1(xy^2)$ logo $p_1=x^2+1$ e $f=-x+y+1$. Note que nessa fase da divisão nenhum termo de f é divisível por nenhum $TL(g_i)$ com $i=1,2$, portanto fazemos $r=y^4-x+y+1$ e $f=0$ e assim finalizamos o algoritmo. Deste tiramos que $p_1=x^2+1, p_2=0$ e $r=y^4-x+y+1$ e sendo assim podemos escrever f como:

$$f=p_1g_1+p_2g_2+r.$$

Contudo, se alterarmos os polinômios divisores, obteremos resultados diferentes.Neste próximo exemplo vamos omitir os passos escritos de modo a só apresentar a diferença de resultados.

Exemplo 28. *Vamos dividir o polinômio $f=x^3y^2+y^4+x^3+xy^2+y+1$ pelo subconjunto $G=\{g_2,g_1\}$ onde $g_1=xy^2+x$ e $g_2=x^2y+y$, temos:*

$$\begin{array}{l|l|l} x^3y^2+y^4+x^3+xy^2+y+1 & x^2y+y & \text{Resto:} \\ f=y^4+x^3+y+1 & xy^2+x & \\ \cline{2-2} & a_1=xy & r=y^4+x^3+y+1 \\ & a_2=0 & \end{array}$$

Como podemos ver, a ordem dos divisores pode alterar o resultado, e nesse sentido passaremos a denotar o conjunto de divisores G por s-uplas ao invés da notação usual de conjuntos, para indicar (e reforçar) que estamos usando uma ordem específica dos divisores. Por exemplo, a notação para o conjunto de divisores da divisão em que dividimos por g_1, g_2, $\ldots$, g_s nessa ordem será

$$G=(g_1,\, g_2,\, \ldots,\, g_s)\,.$$

Definição 23. *Escreveremos $\overline{f}^G$ para o resto da divisão de f pela s-upla ordenada G.*

Exemplo 29. *Dados $f=x^3y^2+x^3$ e $g_1=xy^2+x$ e $g_2=x^2y+y$, vamos determinar $\overline{f}^{G_1}$ e $\overline{f}^{G_2}$ em que $G_1=(g_2,\, g_1)$ e $G_2=(g_1,\, g_2)$. Observe que dividir f por G_1 temos a seguinte situação:*

$$\begin{array}{r|ll} x^3y^2 + x^3 & x^2y + y & \text{Resto:} \\ xy^2 + x^3 & xy^2 + x & \\ \hline x^3 + x & q_1 = xy & \\ & q_2 = 1 & r = x^3 + x \end{array}$$

E como nem $TL(g_2)$ nem o $TL(g_1)$ dividem quaisquer temor de $x^3 + x$, encerramos nossa divisão com $\overline{f}^{G_1} = r = x^3 + x$ que é diferente de zero. Contudo, ao trocar a ordem dos g_i e dividir f por G_2, temos a seguinte situação:

$$\begin{array}{r|ll} x^3y^2 + x^3 & xy^2 + x & \text{Resto:} \\ & x^2y + y & r = 0 \\ \hline & q_1 = x^2 & \\ & q_2 = 0 & \end{array}$$

Daqui tiramos que o resto da divisão é igual a zero.

Uma consequência do exemplo acima é a seguinte: considere $I = \langle g_1, \ , g_2 \rangle$ um ideal de $K[x, y]$. Após determinar que $\overline{f}^{G_1} = x^3 + x$ poderíamos achar que

$$f \notin I,$$

e perceba que tal suposição é razoável uma vez que nenhum termo de $\overline{f}^{G_1} = x^3 + x$ é divisível pelos termos líderes dos geradores de I. No entanto, ao termos efetuado a segunda divisão, percebemos rapidamente que essa conclusão está errada, uma vez que $\overline{f}^{G_2} = 0$, ou seja,

$$f = x^2 \cdot (xy^2 + x) + 0 \cdot (x^2y + y) = x^2 \cdot g_1 + 0 \cdot g_2 \in \langle g_1, \ , g_2 \rangle = I.$$

Isso nos leva a concluir que se desejamos saber se $f \in I$, então devemos fazer todas as divisões de f pelas diferentes ordenações dos elementos de um conjunto gerador finito de I. Apesar de válida essa conclusão, ela pode ser consideravelmente custosa, uma vez que se tivermos s geradores, o número total de ordenações desses geradores é $s!$. Veremos no próximo capítulo condições e estratégia para que não tenhamos que fazer essa quantidade enorme de divisões.

3 Bases de Groebner

Neste capítulo vamos apresentar as Bases de Groebner e uma propriedade importante que possibilita resolver o problema citado no final do capitulo anterior. Aqui também será apresentado ao leitor o algoritmo que possibilita achar uma Base de Groebner dado um conjunto gerador de um ideal e o critério de parada de tal algoritmo, o que possibilita afirmarmos que toda Base de Groebner é finita.

Definição 24. *Um ideal $I \subset K[x_1, \ldots, x_n]$ é um **ideal monomial** se existe um subconjunto $A \subset \mathbb{Z}^n_{\geq 0}$ tal que para $h_\alpha \in K[x_1, \ldots, x_n]$, I consiste em todos os polinômios que são somas finitas da forma:*

$$\sum_{\alpha \in A} h_\alpha x^\alpha.$$

Neste caso, escrevemos $I = \langle x^\alpha : \alpha \in A \rangle$.

Lema 3. *Seja $I = \langle x^\alpha : \alpha \in A \rangle$ um ideal monomial. Então um monômio x^β pertence a I se, e somente se, x^β é divisível por x^α para algum $\alpha \in A$.*

Demonstração. Defina o conjunto $\mathcal{A}$ como o conjunto de todos os monômios em cujos respectivos multigraus pertençam a A. Com isso, se x^β pertence a I, então podemos escrever:

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha_i}, \text{ com } h_i \in K[x_1, \ldots, x_n], \text{ e } \quad x^{\alpha_i} \in \mathcal{A}.$$

A igualdade acima pode ser reinterpretada do seguinte modo: como a divisão do polinômio x^β (que é em particular um monômio) pelo conjunto $\mathcal{A}_s = \{x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_s}\}$ no qual obtemos como conjunto quociente $\{h_1, \ldots, h_s\}$ e resto $r = 0$.

Note que o algoritmo de divisão dado para a dedução do Teorema 5 nos diz que o processo de divisão é feito termo a termo do dividendo, no qual testamos se ele é divisível por cada divisor e em caso positivo, obtemos o respectivo quociente, em caso negativo, ele é remetido ao resto.

Agora, como estamos em um caso em que o resto é zero e o dividendo só possui um termo, o monômio x^β, concluímos que ele deve ser divisível por algum dos divisores presentes em $\mathcal{A}_s$, pois caso contrário $r \neq 0$.

De forma recíproca, se x^β é um múltiplo de x^α, para $\alpha \in A$, então $x^\beta \in I$ pela definição de ideal. □

Note que x^β é um múltiplo de x^α quando $x^\beta = x^\alpha \cdot x^\gamma$ para algum $\gamma \in \mathbb{Z}^n_{\geq 0}$, o que é equivalente a dizer que $\beta = \alpha + \gamma$. E daqui tiramos que o conjunto

$$\alpha + \mathbb{Z}^n_{\geq 0} = \{\alpha + \gamma : \gamma \in \mathbb{Z}^n_{\geq 0}\},$$

é formado pelos expoentes de todos os monômios que são divisíveis por x^α.

O próximo lema relaciona a pertinência de um polinômio f a um ideal monomial com seus monômios.

Lema 4. *Seja I um ideal monomial, e seja $f \in K[x_1, \ldots, x_n]$. Então são equivalentes:*

i) $f \in I$;

ii) Todo termo de f pertence a I;

iii) f é uma combinação linear de monômios de I.

Demonstração. As implicações $i) \Rightarrow ii) \Rightarrow iii)$ são triviais. Já a implicação $i) \Rightarrow iii)$ vem de que se $f \in I$ implica que $f = \sum_{i=1}^{s} h_i x^\alpha$, onde $h_i \in K[x_1, x_2, \ldots, x_n]$. Se abrirmos este somatório fica nítida a combinação linear dos monômios de I. □

Lema 5. *Dois ideais monomiais são iguais se, e somente se, eles contém os mesmos monômios.*

Demonstração. Sejam I e J dois ideais monomiais. Dado $f \in I$, temos que

$$f = \sum_{i=0}^{s} a_i x^{\alpha_i}, \quad \text{com} \quad a_i \in K.$$

Pelo Lema 4, todos os termos de f pertencem a I, ou seja, $a_i x^{\alpha_i} \in I$ para todo $i = 1, \ldots, s$. Como $a_i \in K$ e I ideal, temos que

$$x^{\alpha_i} = a_i^{-1}(a_i x^{\alpha_i}) \in I.$$

Por hipótese, todo monômio de I está em J, e daí $x^{\alpha_i} \in J$ para todo i, e como J é um ideal concluímos que

$$f = \sum_{i=0}^{s} a_i x^{\alpha_i} \in J,$$

ou seja, $I \subset J$. A outra inclusão é análoga, donde verificamos que $I = J$. □

Lema 6 (Lema de Dickson)**.** *Um ideal monomial, $I = \langle x^\alpha : \alpha \in A \rangle$ contido em $K[x_1, \ldots, x_n]$ pode ser descrito na forma $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, com $\alpha_1, \ldots, \alpha_s \in A$. Em particular I tem uma base finita.*

Demonstração. Vamos provar por indução sobre n, onde n é o número de indeterminadas em $K[x_1, x_2, \ldots, x_n]$. Se $n = 1$, então $I = \langle x_1^\alpha : \alpha \in A \rangle$ tal que $A \subset \mathbb{N} \cup \{0\}$. Seja β o menor elemento de $A \subset \mathbb{N} \cup \{0\}$, então $\beta \leq \alpha$, para todo $\alpha \in A$, portanto x_1^β divide todos os outros geradores x_1^α. Logo $I = \left\langle x_1^\beta \right\rangle$.

Agora assumimos $n > 1$ e que o teorema seja válido para $n-1$ indeterminadas. Escrevemos as indeterminadas como $x_1, \ldots, x_{n-1}, y$, assim os monômios em $K[x_1, \ldots, x_{n-1}, y]$ podem ser escritos como $x^\alpha y^m$, com $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ e $m \in \mathbb{Z}_{\geq 0}$.

Suponha que $I \subset K[x_1, \ldots, x_{n-1}, y]$ é um ideal monomial. Para encontrar geradores para I, seja J um ideal em $K[x_1, \ldots, x_{n-1}]$ gerado pelos monômios x^α tais que $x^\alpha y^m \in I$ para algum $m \geq 0$. Desde que J é um ideal monomial em $K[x_1, \ldots, x_{n-1}]$, nossa hipótese indutiva implica que um número finito de x^α geram J, digamos $J = \langle x_1^\alpha, \ldots, x_2^\alpha \rangle$. O ideal J pode ser entendido como a "projeção" de I em $K[x_1, \ldots, x_{n-1}]$.

Para cada i entre 1 e s, a definição de J nos diz que $x^{\alpha_i} y^{m_i} \in I$ para algum $m_i \geq 0$. Seja $m = maior(m_i)$, então, para cada k tal que $0 < k < m-1$, considere o ideal $J_k \subset K[x_1, \ldots, x_{n-1}]$ gerado pelos monômios x^β tais que $x^{\beta_i} y^k \in I$. Pode-se pensar em J_k como uma "fatia" de I gerada por monômios contendo y^k. Usando nossa hipótese indutiva novamente, J_k tem um conjunto finito de monômios geradores, digamos $J_k = \left\langle x^{\alpha_{k(1)}}, \ldots, x^{\alpha^{k(s_k)}} \right\rangle$.

Sendo assim, vamos afirmar que I é gerado pelos monômio descritos abaixo:

$$\begin{aligned} J: &\quad x^{\alpha_1} y^m, \ldots, x^{\alpha_s} y^m, \\ J_0: &\quad x^{\alpha_{0(1)}}, \ldots, x^{\alpha_{0(s_0)}}, \\ J_1: &\quad x^{\alpha_{1(1)}} y, \ldots, x^{\alpha_{1(s_1)}} y, \\ &\vdots \\ J_{m-1}: &\quad x^{\alpha_{m-1(1)}} y^{m-1}, \ldots, x^{\alpha_{m-1(s_{m-1})}} y^{m-1}. \end{aligned}$$

Primeiro note que todo monômio em I é divisível por alguém da lista. Para ver o porquê, seja $x^\alpha y^p \in I$. Temos então:

(i) Se $p \geq m$, então $x^\alpha y^p$ é divisível por algum $x^{\alpha_i} y^m$ pela construção de J.

(ii) Se $p \leq m-1$, então $x^\alpha y^p$ é divisível por algum $x^{\alpha_{p(j)}} y^p$ pela construção de J_p.

Segue do Lema 3 que os monômios acima geram um ideal contendo os mesmos monômios tal como I, e pelo Lema 5, isso implica que os ideais são iguais, e nossa afirmação está provada.

Para completar a prova do teorema, precisamos mostrar que um conjunto finito de geradores pode ser escolhido a partir de um dado conjunto de geradores (possivelmente infinito) do ideal. Se retornarmos à situação anterior para escrever as variáveis como $x_1, \ldots, x_n$, então nosso ideal monomial é $J = \langle x^\alpha : \alpha \in A \rangle$ que está contido em $K[x_1, \ldots, x_n]$.

Queremos mostrar que I é gerado por um número finito de monômios x^α, onde $\alpha \in A$. Pelo parágrafo anterior, sabemos que $J = \left\langle x^{\beta_1}, \ldots, x^{\beta_s} \right\rangle$ para alguns monômios x^{β_i} que pertencem a I. Note que, desde que $x^{\beta_i} \in I = \langle x^\alpha : \alpha \in A \rangle$, o Lema 3 nos diz que

cada x^{β_i} é divisível por x^{α_i} para algum $\alpha_i \in A$ e, portanto

$$x^{\beta_i} = h_i x^{\alpha_i}, \quad \text{onde} \quad h_i \in K[x_1, \ldots, x_n] \quad \text{para} \quad i = 1, 2, \ldots, s.$$

Dado $f \in I$, podemos escrever

$$f = \sum_{i=1}^{s} a_i x^{\beta_i} = \sum_{i=1}^{s} (a_i h_i) x^{\beta_i} \quad \text{onde} \quad a_i h_i \in k[x_1, \ldots, x_n]$$

e, portanto $f \in \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$.

Daí, $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$. Isto completa a demonstração. □

Pelo Lema de Dickson temos que todo ideal monomial tem uma base geradora finita contendo somente monômios. Isso facilita verificar a pertinência de um polinômio f a I com $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, pois a pertinência será confirmada se, somente se, o resto da divisão de f por $x^{\alpha_1}, \ldots, x^{\alpha_s}$, em alguma ordem, for zero.

No próximo lema, iremos apresentar sem demonstração, uma consequência da definição de ordenação total sobre $\mathbb{Z}_{\geq 0}^n$ quando incluímos uma propriedade adicional.

Lema 7. *Seja $>$ uma relação sobre $\mathbb{Z}_{\geq 0}^n$ satisfazendo:*

i) $>$ é uma ordenação total sobre $\mathbb{Z}_{\geq 0}^n$.

ii) Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}_{\geq 0}^n$, então $\alpha + \gamma > \beta + \gamma$.

Então $>$ é uma boa-ordenação se, e somente se, $\alpha \geq 0$ para todo $\alpha \in \mathbb{Z}_{\geq 0}^n$.

Definição 25. *Seja $I \in K[x_1, \cdots, x_n]$ um ideal não nulo. Denotamos por $TL(I)$ o conjunto formado pelos termos líderes dos elementos de I. De modo que,*

$$TL(I) = \{a_\alpha x^\alpha : \exists\, f \in I \, com TL(f) = a_\alpha x^\alpha\}.$$

Denotamos por $\langle TL(I) \rangle$ o ideal gerado pelos termos líderes dos elementos de I.

Seja I um ideal de $K[x_1, \ldots, x_n]$ finito, tal que $I = \langle f_1, f_2, \cdots, f_s \rangle$. Por definição temos que, $TL(f_i)$ pertence à $TL(I)$ que está contido em $\langle TL(I) \rangle$, portanto $\langle TL(f_i) \rangle \subset \langle TL(I) \rangle$, implicando em $\langle TL(f_1), TL(f_2), \cdots, TL(f_s) \rangle \subset \langle TL(I) \rangle$. Mas se, por exemplo, $I = \left\langle x^2 + y, x^2 - 1 \right\rangle$,

$$y + 1 = (x^2 + y) - (x^2 - 1) \in I \Rightarrow y = TL(y + 1) \in \langle TL(I) \rangle .$$

Por outro lado, $\left\langle (TL(x^2 + y)), (TL(x^2 - 1)) \right\rangle = \left\langle (x^2, x^2) \right\rangle = \left\langle (x^2) \right\rangle \not\ni y$. Sendo assim podemos afirmar que nem sempre $\langle TL(f_1), TL(f_2), \cdots, TL(f_s) \rangle$ e $\langle TL(I) \rangle$ são iguais.

Proposição 5. *Seja $I \subset K[x_1, \cdots, x_n]$ um ideal:*

i) O conjunto $\langle TL(I)\rangle$ é um ideal monomial.

ii) Existem $g_1, g_2, \cdots, g_s \in I$ tais que $\langle TL(I)\rangle = \langle TL(g_1), TL(g_2), \cdots, TL(g_s)\rangle$.

Demonstração.

i) Considere o ideal gerado por todos os monômios líderes dos elementos presentes em $I-\{0\}$, $\langle ML(g) : g \in I - \{0\}\rangle$. Como os monômios líderes e os termos líderes de $I-\{0\}$ se diferem por uma constante não nula, concluímos que $\langle ML(g) : g \in I - \{0\}\rangle = \langle TL(g) : g \in I - \{0\}\rangle = \langle TL(I)\rangle$. Logo, $\langle TL(I)\rangle$ é um ideal monomial.

ii) Como foi provado acima $\langle TL(I)\rangle$ é gerado por monômios, e pelo Lema de Dickson temos que existe um conjunto de elementos finitos $g_1, g_2, \cdots, g_s \in I$ tais que $\langle TL(I)\rangle = \langle ML(g_1), ML(g_2), \cdots, ML(g_s)\rangle$. E como dito anteriormente, $ML(g)$ e o $TL(g)$ só se diferem em uma constante não nula, podemos concluir,

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

□

Com a proposição acima, temos ferramentas suficientes para demonstrar um teorema de suma importância na existência das bases de Groebner, este é chamado de **Teorema das Bases de Hilbert**.

Teorema 6 (Bases de Hilbert)**.** *Todo ideal $I \subset K[x_1, x_2, \ldots, x_n]$ tem um conjunto finito de geradores. Sendo assim, $I = \langle g_1, g_2, \ldots, g_s\rangle$ para alguns $g_1, g_2, \ldots, g_s \in I$.*

Demonstração. Se $I = \{0\}$, não temos nada a provar. Já que o conjunto gerador será $\{0\}$.

Se I é um ideal não nulo, temos pela proposição anterior que, existem $g_1, g_2, \ldots, g_s \in I$ tais que $\langle TL(I)\rangle = \langle TL(g_1), TL(g_2), \ldots, TL(g_s)\rangle$. Queremos mostrar que $\langle I\rangle = \langle g_1, g_2, \ldots, g_s\rangle$.

Como cada $g_i \in I$, o conjunto $\langle g_1, g_2, \ldots, g_s\rangle \subset I$.

Agora considere $f \in I$ um polinômio qualquer, e $G = (g_1, g_2, \ldots, g_s)$. Suponha então que o resto da divisão de f por G seja diferente de zero, e pelo algoritmo de divisão polinomial temos a seguinte equação,

$$f = a_1 g_1 + \ldots + a_s g_s + r.$$

De forma que nenhum termo de r é divisível por algum $TL(g_1), TL(g_2), \ldots, TL(g_s)$. Isolando r ao lado direito da equação teremos:

$$r = f - a_1 g_1 - \ldots - a_s g_s \in I.$$

Como $r \in I$, suponha $r \neq 0$. Sendo assim

$$TL(r) \in \langle TL(I) \rangle = \langle TL(g_1), TL(g_2), \ldots, TL(g_s) \rangle ,$$

e pelo Lema 6, segue que $TL(r)$ deve ser divisível por algum $TL(g_i)$, o que contradiz o fato de r ser o resto de $\overline{f}^G$. Portanto,

$$f = a_1 g_1 + \ldots + a_s g_s \in \langle g_1, g_2, \ldots, g_s \rangle ,$$

e daí concluímos que $I \subset \langle g_1, g_2, \ldots, g_s \rangle$. □

Este conjunto gerador finito assume o papel principal do nosso estudo como definimos a seguir.

Definição 26. *Seja $I \subset K[x_1, \ldots, x_n]$ um ideal. Dizemos que $G = (g_1, \ldots, g_r) \subset I$ é uma* base de Groebner *para I, se:*

$$\langle (TL(g_1)), \ldots, (TL(g_r)) \rangle = \langle TL(I) \rangle .$$

Exemplo 30. *Seja I um ideal de $K[x, y]$ em que $I = \langle g_1, g_2, g_3 \rangle$ ao qual, $g_1 = x^5, g_2 = xy + y$ e $g_3 = y$. Temos que $G = \{g_1, g_2, g_3\}$ é uma base de Groebner de I. Adiante, no Exemplo 33, com mais ferramentas vamos provar tal afirmação.*

Corolário 3. *Fixada uma ordem monomial, então todo ideal $I \subset K[x_1, x_2, \ldots, x_n]$ não nulo tem uma base de Groebner. Temos ainda que qualquer base de Groebner de I é um conjunto gerador de I.*

Demonstração. Dado um ideal $\in K[x_1, \ldots, x_n]$ não nulo, o conjunto $G = (g_1, \ldots, g_s)$, construído na demonstração do Teorema da Base de Hilbert, é uma base de Groebner por definição.

Agora para mostrar que qualquer base de Groebner de um ideal I também é um conjunto gerador de I basta observar que se $\langle TL(I) \rangle = \langle (TL(g_1)), \ldots, (TL(g_r)) \rangle$, então pelo mesmo argumento anterior $I = \langle g_1, g_2, \ldots, g_s \rangle$. □

Adiante vamos apresentar a propriedade mais importante para o nosso questionamento principal do texto. Antes de definirmos as bases de Groebner percebemos que, ao fazer a divisão de um polinômio f por um conjunto G gerador de um ideal I, podemos obter restos diferentes se trocarmos a ordem dos polinômios de G na divisão. Mas agora, tal propriedade mostra que quando esse conjunto gerador G é uma base de Groebner não importa a ordem dos polinômios divisores, o resto sempre será o mesmo.

Proposição 6. *Seja $G = (g_1, \ldots, g_s)$ uma base de Groebner para o ideal I tal que $I \subset K[x_1, \ldots, x_n]$ e seja $f \in K[x_1, \ldots, x_n]$. Então existe um único $r \in K[x_1, \ldots, x_n]$ com as seguintes propriedades:*

i) Nenhum termo de r é dividível por nenhum dos $TL(g_1), TL(g_2), \ldots, TL(g_s)$.

ii) Existe $h \in I$ tal que $f = h + r$.

Demonstração. Pelo algoritmo da divisão temos $f = a_1g_1 + a_2g_2 + \ldots + a_sg_s + r$, no qual r satisfaz (i). E se $h = a_1g_1 + a_2g_2 + \ldots + a_sg_s \in I$ satisfaz também (ii). Assim provamos a existência de r.

Para provar a unicidade, suponhamos que existam r_1 e r_2 tais que $f = h_1 + r_1 = h_2 + r_2$ e que satisfaçam as condições da propriedade i). Desta igualdade tiramos que $r_1 + r_2 = h_1 + h_2$ e como $f \in I$ implica que $r_1 - r_2 = h_2 - h_1 \in I$. Se $r_1 \neq r_2$, temos que $TL\,(r_2 - r_1) \in \langle TL\,(I)\rangle = \langle TL(g_1), \ldots, TL(g_s)\rangle$.

Pelo Lema 5 temos que e $TL(r_2 - r_1)$ é divisível por algum $TL(g_i)$. Mas note que isso é impossível, tendo em vista que nenhum termo de r_1 ou de r_2 é divisível por $TL(g_1), \ldots, TL(g_s)$ por definição, sendo assim como o polinômio $r_2 - r_1$ terá os mesmos termos de r_1 e r_2 com coeficientes diferentes, ou alguns termos serão cancelados (não todos tendo em vista que $r_1 \neq r_2$), portanto os termos de $r_2 - r_1$ continuam não sendo divisíveis por nenhum g_i com $i = 1, 2, \ldots, s$. Logo $r_1 - r_2$ deve ser igual a zero e, portanto $r_1 = r_2$, provando deste modo a unicidade de r. □

Agora sim, com o Corolário abaixo, a questão da pertinência de f a um ideal I será solucionada.

Corolário 4. *Se $G = (g_1, \ldots, g_s)$ uma base de Groebner para o ideal I tal que $I \subset K[x_1, \ldots, x_n]$ e seja $f \in K[x_1, \ldots, x_n]$. Então $f \in I$ se, e somente se, o resto da divisão de f por G for zero.*

Demonstração. Se o resto é zero então $f = a_1g_1 + a_2g_2 + \ldots + a_sg_s \in I$. De forma análoga, dado $f \in I$ então $f = f + 0$ satisfaz as duas condições da proposição anterior. Segue, portanto o resto da divisão de f por G será igual a zero. □

Esse corolário ajuda a identificar quando um polinômio $f \in K[x_1, \ldots, x_n]$ pertence a um ideal.

Exemplo 31. *Seja $I \in K[x, y]$ um ideal tal que*

$$I = \langle g_1, g_2, g_3\rangle$$

ao qual, $g_1 = x^5, g_2 = xy + y$ e $g_3 = y$. Como vimos anteriormente no Exemplo 33, $G = \{g_1, g_2, g_3\}$ é uma base de Groebner de I. Verifique que $f = x^2y + xy + 2y$ pertence a I.

Pelo Corolário 4, f pertence a I se, e somente se, $\overline{f}^G = 0$. Sendo assim, através do último algoritmo do capítulo anterior, concluímos que f pode ser representado da seguinte forma,

$$f = (x) \cdot g_2 + (2) \cdot g_3.$$

Portanto $P = (x, 2)$ é conjunto dos quocientes e temos $r = 0$. De fato f pertence a I.

Definição 27. *Sejam $f, g \in K[x, y]$ polinômios não nulos.*

*i) Se $\partial(f) = \alpha_1 + \beta_1$ e $\partial(g) = \alpha_2 + \beta_2$, então tomamos $\gamma = (\gamma_1, \gamma_2)$, onde $\gamma_1 = max(\alpha_1, \alpha_2)$ e $\gamma_2 = max(\beta_1, \beta_2)$. Chamaremos $x^{\gamma_1}y^{\gamma_2}$ o **mínimo múltiplo comum** de $ML(f)$ e $ML(g)$, e escreveremos $x^{\gamma_1}y^{\gamma_2} = MMC(ML(f), ML(g))$.*

*ii) O **S-polinômio** de f e g é a combinação:*

$$S(f, g) = \frac{x^{\gamma_1}y^{\gamma_2}}{TL(f)} \cdot f - \frac{x^{\gamma_1}y^{\gamma_2}}{TL(g)} \cdot g. \tag{3.1}$$

A definição acima é importante para a construção de uma base de Groebner justamente por gerar a partir de dois polinômios f, g, um terceiro polinômio s no qual $\partial(s) \leq min(\partial(f), \partial(g))$. Verificamos então, se $f, g \in G$, no qual G fosse nossa possível base de Groebner, s deve estar em G por ser um conjunto gerador, caso contrário, G ainda não é uma base de Groebner.

Exemplo 32. *Sejam $f = x^4 + xy^2 + y$ e $g = y^3 + xy + y$ polinômios onde $f, g \in \mathbb{R}[x, y]$. Pela definição acima temos que $\gamma = (4, 3)$ e com isso o S-polinômio de f e g é dado por:*

$$\begin{aligned} S(f, g) = & \frac{x^4y^3}{x^4} \cdot (x^4 + xy^2 + y) - \frac{x^4y^3}{y^3} \cdot (y^3 + xy + y) \\ = & \ y^3 \cdot (x^4 + xy^2 + y) - x^4 \cdot (y^3 + xy + y) \\ = & \ x^4y^3 + xy^5 + y^4 - x^4y^3 - x^5y - x^4y \\ = & \ -x^5y + xy^5 - x^4y + y^4. \end{aligned}$$

Lema 8. *Sejam $\sum_{i=1}^{s} c_i f_i$, onde $c_i \in K$ e $f_i \in K[x_1, \ldots, x_n]$ e que multigrau $(f_i) = \alpha \in \mathbb{Z}^n_{\geq 0}$ para todo $i = 1, \ldots, s$. Se*

$$multigrau\left(\sum_{i=1}^{s} c_i f_i\right) < \alpha,$$

então $\sum_{i=1}^{s} c_i f_i$ é uma combinação linear com coeficientes em K, dos S-polinômios $S(f_j, f_k)$, para $1 \leq j, k \leq s$. Além disso, cada $S(f_j, f_k)$ tem multigrau menor que α.

Demonstração. Seja $d_i = CL(f_i)$; então $c_i d_i$ é o coeficiente líder de $c_i f_i$. Como $\sum_{i=1}^{s} c_i f_i = \left(\sum_{i=1}^{s} c_i d_i\right) x^\alpha + g$, tal que g é a soma de termos com multigrau menor que α, e essa soma tem

multigrau estritamente menor que α, segue que $\sum_{i=1}^{s} c_i d_i = 0$, ou seja, houve cancelamento dos termos líderes dos f_i com $i = 1, 2, \ldots, s$.

Definimos $p_i = \dfrac{f_i}{d_i}$ e observamos que p_i tem coeficiente líder igual a 1. Considerando a soma "telescópica"

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2).$$

□

Quando $f_1, \ldots, f_s$ satisfazem a hipótese do Lema 8, obtemos uma equação da forma

$$\sum_{i=1}^{s} c_i f_i = \sum_{j,k} c_j S(f_j, f_k),$$

Observação 2. *Note que se $f = xy + y$ um polinômio que pertence a $K[x, y]$ é gerado por $g_1 = x$ e $g_2 = y$, podemos escrevê-lo de formas diferentes em função de g_1 e g_2. Suponha então $h_1 = 0$ e $h_2 = x + 1$, assim $f = h_1 g_1 + h_2 g_2$ e pela ordem lexicográfica graduada reversa temos $multigrau(h_1 g_1) = (1, 0)$ e $multigrau(h_2 g_2) = (1, 1)$. Considere agora $h_1' = -y^2$ e $h_2' = x + xy + 1$, sendo assim $f = h_1' g_1 + h_2' g_2$ e $multigrau(h_1' g_1) = (1, 2)$ e $multigrau(h_2' g_2) = (1, 2)$. Note que $multigrau(h_1 g_1) < multigrau(h_1' g_1)$ Portanto, podemos sempre escrever um polinômio $f \in K[x_1, \ldots, x_n]$ em função de alguns polinômios g_i com $i = 1, 2, \ldots, s$, tal que,*

$$f = \sum_{i=1}^{s} h_i g_i,$$

de maneiras diferentes em que os multigraus de cada parcela da soma acima dependem da escolha do h_i. Logo existe h_i' tal que alguma parcela de $f = \sum_{i=1}^{s} h_i' g_i$, tenha o menor máximo multigrau possível.

Lema 9. *Seja f um polinômio que pertence ao ideal $I = \langle g_1, \ldots, g_s \rangle$. Se para todos os pares $i \neq j$, o resto da divisão de $S(g_i, g_j)$ por G (listado em alguma ordem) é zero, então existem h_i' tais que $multigrau(f) = max\{multigrau(h_i' g_i)\}$.*

Demonstração. Como comentamos na observação anterior, tome h_i' de forma que os termos de $f = \sum_{i=1}^{s} h_i' g_i$ tenham o menor máximo multigrau possível e defina $multigrau(h_i' g_i) = m(i)$ e $\gamma = max\{m(i)\}$ para todo $1 \leq i \leq s$, e portanto

$$multigrau(f) \leq \gamma.$$

Provaremos, por contradição, que $multigrau(f) = \gamma$. Para isto, supomos que $multigrau(f) < \gamma$ e escrevemos f de modo a isolar os termos de multigrau γ.

$$\begin{aligned} f = & \sum_{m(i)=\gamma} h'_i g_i + \sum_{m(i)<\gamma} h'_i g_i = \sum_{m(i)=\gamma} \left(TL(h'_i) + h'_i - TL(h'_i)\right) g_i + \sum_{m(i)<\gamma} h'_i g_i \\ = & \sum_{m(i)=\gamma} TL(h'_i) g_i + \sum_{m(i)=\gamma} (h'_i - TL(h'_i)) g_i + \sum_{m(i)<\gamma} h'_i g_i. \end{aligned} \tag{3.2}$$

Na última linha da soma anterior, todos os monômios que aparecem no segundo e no terceiro somatório possuem multigrau menor que γ, pois $multigrau(h'_i - TL(h'_i))g_i < \gamma$, para todo i no segundo somatório e o terceiro foi definido com essa propriedade. Deste modo, a hipótese de que $multigrau(f) < \gamma$, implica que o primeiro somatório deve ter multigrau menor do que γ, ou seja,

$$multigrau\left(\sum_{m(i)=\gamma} TL(h'_i) g_i\right) < \gamma.$$

Escrevendo $TL(h'_i) = c_i x_i^{\alpha_i}$, temos que

$$\sum_{m(i)=\gamma} TL(h'_i) g_i = \sum_{m(i)=\gamma} c_i x^{\alpha_i} g_i$$

satisfaz as hipóteses do Lema 8 com $f_i = x^{\alpha_i} g_i$, e portanto este cancelamento pode ser escrito como uma combinação linear de S-polinômios $S\left(x^{\alpha_j} g_j, x^{\alpha_k} g_k\right)$. Temos também que

$$\begin{aligned} S(x^{\alpha_j} g_j, x^{\alpha_k} g_k) = & \frac{x^\gamma}{x^{\alpha_j} TL(g_j)} x^{\alpha_j} g_j - \frac{x^\gamma}{x^{\alpha_k} TL(g_k)} x^{\alpha_k} g_k = \frac{x^\gamma}{TL(g_j)} g_j - \frac{x^\gamma}{TL(g_k)} g_k \\ = & \frac{x^{\gamma - \delta_{jk} + \delta_{jk}}}{TL(g_j)} g_j - \frac{x^{\gamma - \delta_{jk} + \delta_{jk}}}{TL(g_k)} g_k = x^{\gamma - \delta_{jk}} \left(\frac{x^{\delta_{jk}}}{TL(g_j)} g_j - \frac{x^{\delta_{jk}}}{TL(g_k)} g_k\right) \\ = & x^{\gamma - \delta_{jk}} S(g_j, g_k), \end{aligned}$$

em que $x^{\delta_{jk}} = MMC(ML(g_j), ML(g_k))$. Portanto existem constantes $c_{jk} \in K$ tais que,

$$\sum_{m(i)=\gamma} TL(h'_i) g_i = \sum_{j,k} c_{jk} x^{\gamma - \delta_{jk}} S(g_j, g_k), \tag{3.3}$$

O próximo passo é usar nossa hipótese que o resto de $S(g_j, g_k)$ na divisão por $g_1, \ldots, g_s$ é zero. Utilizando o algoritmo da divisão, isto significa que cada polinômio $S(g_j, g_k)$ pode ser escrito na forma

$$S(g_j, g_k) = \sum_{i=1}^{s} a_{ijk} g_j, \quad \text{com} \quad a_{ijk} \in K[x_1 \ldots, x_n].$$

Fixe i, j, k de forma que $a_{ijk}g_j$ seja o termo líder de $S(g_j, g_k)$. Assim, pela definição de termo líder, o $multigrau(a_{ijk}g_j)$ é o maior dentre os outros termos e $multigrau(S(g_j, g_k)) = multigrau(a_{ijk}g_j)$. E para qualquer outro termo $multigrau(S(g_j, g_k))$ é maior, logo

$$multigrau(a_{ijk}g_i) \leq multigrau(S(g_j, g_k)), \text{ para todos } \quad i, j, k.$$

Intuitivamente isto mostra que, quando o resto é zero, podemos encontrar uma expressão para $S(g_j, g_k)$ em termos de G, em que nem todos os termos líderes se cancelam. Para explorar isso, multipliquemos $S(g_j, g_k)$ por $x^{\gamma-\delta_{jk}}$ obtendo,

$$x^{\gamma-\delta_{jk}}S(g_j, g_k) = \sum_{i=1}^{s} b_{ijk}g_i, \quad \text{onde} \quad b_{ijk} = x^{\gamma-\delta_{jk}}a_{ijk},$$

e pelo Lema 8 temos

$$multigrau(b_{ijk}g_i) \leq multigrau(x^{\gamma-\delta_{jk}}S(g_j, g_k)) < \gamma. \tag{3.4}$$

Substituindo esta expressão em (3.3), obtemos

$$\sum_{m(i)=\gamma} TL(h_i)g_i = \sum_{j,k} c_{jk}x^{\gamma-\delta_{jk}}S(g_j, g_k) = \sum_{j,k} c_{jk}\left(\sum_i b_{ijk}g_i\right) = \sum_i \tilde{h}_i g_i$$

tal que $\tilde{h}_i = TL(h'i)$, de acordo com (3.4) obtemos $multigrau(h'_i g_i) < \gamma$, para todo i.

Finalmente substituímos $\sum_{m_i=\gamma} TL(h'_i)g_i = \sum_i \tilde{h}_i g_i$ em (3.2) para obter uma expressão para f como combinação dos polinômios g_i para todo i, em que todos tem multigrau menor que γ, contradizendo a minimalidade de γ. Deste modo, encerramos a demonstração. □

Usando S-polinômios e os Lemas 8 e 9, provaremos o Critério de Buchberger para determinar quando um conjunto gerador de um ideal é uma base de Groebner.

Teorema 7. *(Critério de Buchberger) Seja $I \neq 0$ um ideal polinomial. Então a base $G = (g_1, \ldots, g_s)$ de I é uma base de Groebner de I se, e somente se, o resto da divisão de $S(g_i, g_j)$ por G (listados em alguma ordem) é zero, para todos os pares (i, j) com $i \neq j$.*

Demonstração. Se G é uma base de Groebner de I temos que $I = \langle G \rangle$, então como $S(g_i, g_j)$ é gerado por elementos de G temos $S(g_i, g_j) \in I$, assim pelo Corolário 4, o resto da divisão de $S(g_i, g_j)$ por G é igual a zero.

Reciprocamente, seja $f \in I$, $f \neq 0$. Queremos mostrar que se todos os S-polinômios têm resto zero na divisão por G, então $TL(f) \in \langle TL(g_1), \ldots, TL(g_s) \rangle$, ou seja, G é uma base de Groebner de I.

Note que dado $f \in I = \langle g_1, \ldots, g_s \rangle$, como o resto da divisão de $S(g_i, g_j)$ por G (listados em alguma ordem) é zero, para todos os pares (i, j) com $i \neq j$ por hipótese, decorre do Lema 9 que existem polinômios $h'_i \in K[x_1, \ldots, x_n]$ tais que,

$$multigrau(f) = max\{multigrau(h'_i g_i)\}.$$

Da igualdade acima tiramos que $TL(f)$ é divisível por $TL(g_i)$ para algum i, e isto nos garante que $TL(f) \in \langle TL(g_1), \ldots, TL(g_s)\rangle$, e nossa prova está completa. □

Exemplo 33. *No Exemplo 30 afirmamos que o conjunto gerador $\{g_1, g_2, g_3\}$ em que, $g_1 = x^5, g_2 = xy + y$ e $g_3 = y$, de I é uma **Base de Groebner**. Agora que provamos o **critério de Buchberger**, temos ferramentas suficientes para provar tal afirmação.*

Para isso, seja $G = \{g_1, g_2, g_3\}$, precisamos que $\overline{S(g_i, g_j)}^G = 0$ para todos os pares $i, j = 1, 2, 3$ com $i \neq j$. De fato,

$$S(g_1, g_2) = \frac{x^5 y}{x^5} \cdot (x^5) - \frac{x^5 y}{xy} \cdot (xy + y) = xy,$$

e como $xy = g_2 - g_3$ temos $\overline{xy}^G = 0$. Dando continuidade temos que,

$$S(g_1, g_3) = \frac{x^5 y}{x^5} \cdot (x^5) - \frac{x^5 y}{y} \cdot (y) = 0,$$

o qual possui obviamente resto zero na divisão por G. E por último,

$$S(g_2, g_3) = \frac{xy}{xy} \cdot (xy + y) - \frac{xy}{y} \cdot (y) = y$$

que acaba sendo o próprio g_3 que pertence a G, portanto $\overline{g_3}^G = 0$.

Sendo assim $G = \{g_1, g_2, g_3\}$ é de fato uma base de Groebner de I.

Definido o conceito de S-polinômio e o comentário acima, direcionamos o estudo para a criação de uma base de Groebner. Com isso, seguimos com o *Algoritmo de Buchberger*.

Teorema 8 (Algoritmo de Buchberger)**.** *Sejam I um ideal de $K[x, y]$ e $G = \{g_1, g_2, \ldots, g_r\}$ um conjunto gerador de I. Para formar uma base de Groebner a partir de G usaremos o algoritmo a seguir.*

1. *Defina $G_0 = G$ e $r_0 = |G_0| = |G| = r$;*
2. *Defina $|G_k| = r_k$;*
3. *Para cada $g_j \neq g_i \in G_k$ calcule $\alpha_{ij} := \overline{S(g_i, g_j)}^{G_k}$*

   Se $\alpha_{ij} \neq 0$, defina $\alpha_{ij} = g_{r_k+1}$, $G_{k+1} = G_k \cup \{g_{r_{k+1}}\}$, $k = k + 1$ e reinicie o passo 3.

   Se $\alpha_{ij} = 0$, encontre outro par $g_j \neq g_i \in G_k$ e repita o processo dado no passo 3;

   Se $\alpha_{ij} = 0$ para todos g_j, $g_i \in G_k$ vá para o passo 4.
4. *G_k é uma base de Groebner para I.*

Demonstração. Se $G = \{g_1, \ldots, g_r\}$ então $\langle G\rangle$ e $\langle TL(G)\rangle$ irão denotar os seguintes ideais,

$$\langle G\rangle = \langle g_1, \ldots, g_r\rangle \text{ e } \langle TL(G)\rangle = \langle TL(g_1), \ldots, TL(g_r)\rangle .$$

Vamos primeiramente mostrar que $G_k \subset I$, em qualquer estágio do algoritmo, tal que G_k aumenta, já que a cada volta no algoritmo em que $\alpha_{ij} \neq 0$ fazemos $k := k + 1$ e adicionamos $g_{r_{k+1}} = \alpha_{ij}$ ao conjunto G_k. Para os valores iniciais a afirmativa é óbvia, e toda vez que ampliamos G_k fazemos isto adicionando o resto de $\overline{S(g_i, g_j)}^{G_k}$ onde $g_i, g_j \in G_k$, e como todo $\alpha_{ij} \in G_k$ são gerados por certos g_i para alguns i temos $G_k \subset I$. Observe também que como $g_i \in G$ para todo i temos que G_k é um conjunto gerador de I.

O algoritmo termina quando $\overline{S(g_i, g_j)}^{G_k} = 0$ para todos $g_i \neq g_j$ que pertencem a G_k. Logo, pelo Teorema 7, G_k é uma Base de Groebner de I.

Temos que provar ainda que o algoritmo termina após um número finito de iterações. Observe então que o conjunto G_k consiste de G_0 (o velho G) juntamente com os restos não nulos dos S-polinômios de elementos de G_k dividido por G_k. Então,

$$\langle TL(G)\rangle \subset \langle TL(G_k)\rangle , \tag{3.5}$$

já que $G_0 \subset G_k$. Ainda, se $G_0 \neq G_k$ afirmamos que $\langle TL(G)\rangle$ é estritamente menor do que $\langle TL(G_k)\rangle$. Para ver isto, suponha que $r \neq 0$ tal que $p = \overline{S(g_i, g_j)}^{G_k}$ para alguns $i \neq j$ tenha sido adicionado a G_k. Já que p é o resto da divisão por G_k, $TL(p)$ não é divisível por nenhum dos termos líderes de elementos de G_k antes de adicionar o p, e desta forma $TL(p) \notin \langle TL(G_k - \{p\})\rangle$. Mas a partir do momento em que $p \in G_k$ é nítido que $TL(p) \in \langle TL(G_k)\rangle$, o que prova a nossa afirmação.

Por (3.5) os ideais $\langle TL(G_k)\rangle$ das sucessivas iterações dentro do algoritmo formam uma cadeia ascendente de ideais em $K[x_1, \ldots, x_n]$, o qual é Noetheriano, decorre da Proposição 3 que ele possui a propriedade cca, o que implica que ao final de uma quantidade finita de iterações a cadeia estabiliza, de forma que $\langle TL(G_k)\rangle = \left\langle TL(g_1), \ldots, TL(g_s), \ldots, TL(g_{r_{k+1}})\right\rangle$. Isto implica que portanto o algoritmo termina após um número finito de iterações. □

Sendo assim, com o Algoritmo de Buchberger conseguimos formar uma Base de Groebner de um ideal I a partir de qualquer conjunto gerador finito de I. Perceba também que ao aplicar o Critério de Buchberger já estamos fazendo alguns passos do algoritmo e assim que encontrarmos o primeiro resto de $\overline{S(g_i, g_j)}^{G}$ diferente de zero já podemos concluir que tal conjunto não é uma Base de Groebner e assim iniciar o algoritmo.

4 Conclusão

Durante todo o estudo e a elaboração do texto, eu como discente, tive ganhos não somente pelo conhecimento adquirido sobre os assuntos abordados, mas também pela proximidade com textos mais elaborados, desafios de interpretações matemáticas e estruturação de textos. Além disso tive contato com uma outra face da matemática pura em que talvez eu não teria tal oportunidade durante a graduação de licenciatura.

Nosso objetivo era de fato apresentar a definição de Bases de Groebner, e para isso tivemos um grande caminho em que estudamos toda a fundamentação teórica de anéis e seus ideais. Definido os anéis polinomiais em uma e n indeterminadas estudamos os teoremas de divisões polinomiais, em que foram necessários em várias partes do nosso capítulo principal e o método que decidimos adotar para provar a existência de cada teorema de divisão, citado no texto, foi trabalhar com algoritmos em que construímos as condições necessárias descritas nos teoremas além de nos fornecer sempre os restos e quocientes tão desejados. Esse método me pareceu, além de mais sucinto, mais didático devido aos diagramas que direcionam os algoritmos, além de introduzir ao texto o conceito de algoritmos computacionais no qual usamos fortemente quando trabalhamos o algoritmo que constrói uma Base de Groebner.

Definimos então as Bases de Groebner, que possui uma propriedade a qual permite solucionar o problema da pertinência muito mais fácil. Essa propriedade determina que ao dividir um polinômio f por um conjunto G, que é Base de Groebner, o resto dessa divisão será único, independente da ordem dos divisores. E para garantir que essa Base de Groebner é finita demonstramos o Teorema da Base de Hilbert. Apresentamos também o Critério de Buchberger, cuja finalidade é determinar se um conjunto gerador é ou não uma Base de Groebner, e e dele concluímos o critério de parada para Algoritmo de Buchberger, garantido deste modo que este terá passos finitos.

Um possível seguimento desse estudo é abordar o conceito de Base de Groebner Reduzidas, uma vez que o algoritmo estudado apenas incluí polinômios até que o conjunto gerador original se torne uma Base de Groebner, no entanto a inclusão desses novos elementos pode fazer com que elementos mais antigos no conjunto se tornem redundantes e obviamente saber como removê-los é algo de grande interesse computacional. Outro possível seguimento é o de abordar aplicações desta teoria, como por exemplo resolução de sistemas polinomiais observando propriedades de seu conjunto solução (Conjuntos de zeros de polinômios).

Referências

COUTINHO, S. C. *Polinômios e Computação Algébrica*. Rio de Janeiro/RJ: SBM, 2012. (Coleção Matemática e Aplicações).

FILHO, D. C. d. M. *Um convite à Matemática*. 3. ed. Rio de Janeiro/RJ: SBM, 2016. (Coleção Professor de Matemática).

GONÇALVES, A. *Introdução à Álgebra*. 6. ed. Rio de Janeiro/RJ: IMPA, 2017. (Projeto Euclides).

HEFEZ, A. *Curso de Álgebra, vol. 1*. Rio de Janeiro/RJ: IMPA, 1993. (Coleção Matemática Universitária).

HEFEZ, A.; VILLELA, M. L. T. *Polinômios e equações algébricas*. 1. ed. Rio de Janeiro/RJ: SBM, 2012. (Coleção PROFMAT).

IEZZI, G. *Fundamentos da Matemática Elementar*. São Paulo/SP: Atual, 2005. (Coleção Matemática e Aplicações).

MENDES, B. R. A. F. *Bases de Groebner e Aplicações em Álgebra Comutativa.* Monografia (Licenciatura em Matemática) — Universidade Federal de São Carlos, 2012.

MONTEIRO, L. H. J. *Elementos de Álgebra*. Rio de Janeiro/RJ: S.A, 1974. (Livros Técnicos e Científicos).

RAMOS, A. *Algumas aplicações de bases de Gröber em Álgebra Comutativa.* Dissertação (Mestrado em Matemática) — Universidade de Campinas, 2003.

VIDIGAL, A. M. *Fundamentos de Álgebra*. Belo Horizonte/MG: UFMG, 2005.