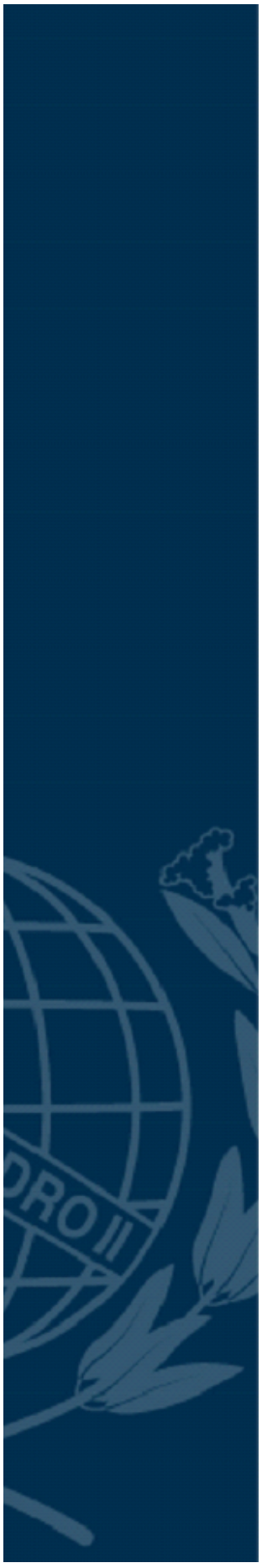


COLÉGIO PEDRO II

Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura
Mestrado Profissional em Matemática em Rede Nacional

Cid de Araújo Moraes

UMA INTRODUÇÃO À COMPUTAÇÃO ALGÉBRICA:

Resolvendo algebricamente um Shidoku

Rio de Janeiro

2019

Cid de Araújo Moraes

UMA INTRODUÇÃO À COMPUTAÇÃO ALGÉBRICA:

Resolvendo algebricamente um Shidoku

Dissertação de Mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional, vinculado à Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura do Colégio Pedro II, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Drª. Patrícia Erthal de Moraes

Rio de Janeiro

2019

COLÉGIO PEDRO II

PRÓ-REITORIA DE PÓS-GRADUAÇÃO, PESQUISA, EXTENSÃO E CULTURA

BIBLIOTECA PROFESSORA SILVIA BECHER

CATALOGAÇÃO NA FONTE

M827 Moraes, Cid de Araújo
Uma introdução à computação algébrica: resolvendo algebricamente um shidoku / Cid de Araújo Moraes. – Rio de Janeiro, 2019.
96 f.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Colégio Pedro II. Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura.
Orientador: Patrícia Erthal de Moraes.

1. Matemática – Estudo e ensino. 2. Álgebra computacional. 3. Bases de Grobner. 4. Algoritmo de Buchberger. 5. Shidoku. I. Moraes, Patrícia Erthal de. II. Título.

CDD 510

Ficha catalográfica elaborada pela Bibliotecária Simone Alves – CRB7 5692.

Cid de Araújo Moraes

UMA INTRODUÇÃO À COMPUTAÇÃO ALGÉBRICA:
Resolvendo algebricamente um Shidoku

Dissertação de Mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional, vinculado à Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura do Colégio Pedro II, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovado em: ___/___/___.

Banca Examinadora:

_____
Drª. Patrícia Erthal de Moraes
Colégio Pedro II

_____
Drª. Liliana Manuela Gaspar Cerveira da Costa
Colégio Pedro II

_____
Dr. Helder Manoel Venceslau
CEFET-RJ

Rio de Janeiro
2019

Dedico este trabalho à minha mãe, Geralda, e ao meu irmão, Osvaldo. Pessoas que não mediram esforços para me ajudar a chegar aqui.

AGRADECIMENTOS

À minha orientadora, Professora Drª. Patrícia Erthal de Moraes, por toda paciência, dedicação e conhecimentos transmitidos.
À todos professores do PROFMAT-CPII, que com muita dedicação, nos guiaram por esses dois anos.
À equipe da Pós Graduação do Colégio Pedro II, por todo suporte durante o mestrado.
À minha namorada, Ana Cristina Beltrán, por todo apoio e motivação.
Ao amigo Professor Diogo Comba Canavezes, pela revisão na parte Histórica.
Ao amigo Professor Me. Jansley Alves Chaves, pela constante motivação, cobrança e as agradáveis corridas.
Aos novos colegas de trabalho do CPII, unidade São Cristovão II, que também muito me apoiaram.
Ao amigo e mentor Professor Gil Max Ferreira, que despertou o meu interesse pela Matemática, e me mostrou o quanto é recompensador ensinar.

"A Matemática não conhece raças ou fronteiras geográficas; para a matemática, o mundo cultural é um país. ".

(David Hilbert)

RESUMO

MORAES, Cid de Araújo. **Uma Introdução à Computação Algébrica:** Resolvendo algebricamente um Shidoku. 2019 96f. Dissertação (Mestrado) – Colégio Pedro II, Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura, Programa de Mestrado Profissional em Matemática em Rede Nacional, Rio de Janeiro, 2019.

Nesse trabalho apresentamos como as Bases de Gröbner juntamente com o sistema de computação algébrica CoCoA podem ser usados para resolver algebricamente um quebra-cabeça *Shidoku* (uma versão reduzida do conhecido *Sudoku*). Apresentamos os pré-requisitos necessários da Álgebra como o Algoritmo da Pseudodivisão até a Teoria das Bases de Gröbner com os S-polinômios e o Algoritmo de Buchberger. Fazemos uma breve introdução ao CoCoA e por fim apresentamos uma implementação da resolução algébrica do Shidoku neste *software*. A dissertação tem o objetivo de ser uma base para um projeto de iniciação científica com estudantes do Ensino Médio e também como fonte de aprofundamento para professores e graduandos de Matemática.

Palavras-chave: Bases de Gröbner; Álgebra Computacional; Shidoku; Pseudodivisão; CoCoA; Algoritmo de Buchberger.

ABSTRACT

MORAES, Cid de Araújo. **Uma Introdução à Computação Algébrica:** Resolvendo algebricamente um Shidoku. 2019 96f. Dissertação (Mestrado) – Colégio Pedro II, Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura, Programa de Mestrado Profissional em Matemática em Rede Nacional, Rio de Janeiro, 2019.

In this work, we present how Gröbner Bases coupled with CoCoA computer algebra system can be used to algebraically solve the *Shidoku* puzzle (a small variant of the well-known *Sudoku*). We show Algebra requirements covering the Pseudo-Divison Algorithm to the Gröbner Bases theory including S-polynomials and Buchberger's Algorithm. We also make a brief introduction to the CoCoA system and propose an algebraic implementation for solving a Shidoku in this software. The dissertation aims to be a scientific project for high school students and also stand as a study source for mathematics teachers and undergraduates.

Keywords: Gröbner Bases; Computational Algebra; Shidoku; Pseudo-Division; CoCoA; Buchberger's Algorithm.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Nesta dissertação apresentamos a teoria das Bases de Gröbner com o objetivo de resolver sistemas de equações polinomiais. Essas Bases generalizam o processo de eliminação Gaussiana para polinômios de várias indeterminadas.

Nos últimos 50 anos, com o desenvolvimento da computação, as Bases de Gröbner tiveram aplicações em diferentes áreas, tais como resolução de Sudokus, Coloração de Grafos, desenvolvimento da Criptografia, Prova Automática de Teoremas, e muitas outras. A escolha pelo estudo deste Tema se deu pelo amplo espectro de aplicações interessantes dessa Teoria possibilitando um aprofundamento de conceitos matemáticos relevantes, além de associar o uso de computadores para resolução de problemas.

Devido à sua especificidade, esse Trabalho é indicado para uma oficina de Iniciação Científica com alunos do Ensino Médio interessados em um aprofundamento de Matemática, bem como para docentes que desejam um maior estudo no campo da Computação Algébrica.

Pensando nessa oficina, optamos por fazer neste Trabalho uma abordagem das Bases de Gröbner visando a resolução de um Shidoku, que é uma versão simplificada do Sudoku. Esses quebra-cabeças se tornaram muito populares nos jornais da Inglaterra em 2004 e desde então aparecem em várias revistas e jornais do mundo. A principal motivação para esse estudo é a oportunidade de apresentar aos alunos o quanto de Matemática Aplicada se "esconde" por trás da modelagem matemática de um simples quebra-cabeça.

A nova BNCC (Base Nacional Comum Curricular) destaca, na competência 5 - Cultura Digital, a importância do uso de linguagens de programação para solucionar Problemas e também, o domínio do uso de Algoritmos. Seguindo essa diretriz, destacamos outra relevância para essa Iniciação Científica que é o papel fundamental do uso da computação na resolução de um Shidoku por uma modelagem matemática, uma vez que, para a determinação de Bases de Gröbner, devido à complexidade dos cálculos, é indicado o uso de sistemas de computação algébrica. Desta forma, os alunos podem, mediante a modelagem de situações problema, ser apresentados ao uso de Algoritmos e linguagens de Programação Básica. Neste trabalho utilizamos o sistema de computação algébrica CoCoA, embora existam outras opções como: SINGULAR, Macaulay 2, SageMath, Derive, entre outros

No capítulo 2, é feita uma breve introdução histórica sobre os dois principais matemáticos que contribuíram para o desenvolvimento da Teoria das Bases de Gröbner: Wolfgang Gröbner e seu aluno, Bruno Buchberger.

Já no capítulo 3, exploraremos os conceitos de Álgebra Abstrata que vamos usar no trabalho. Destacaremos a transição do Anel $\mathbb{K}[x]$ para o Anel $\mathbb{K}[x_1, \ldots, x_n]$, salientando as dificuldades que ocorrem ao tentar estender o Algoritmo da Divisão para várias indeterminadas.

O capítulo 4 trata da importância das Bases de Gröbner para a resolução de sistemas polinomiais em várias indeterminadas. É ressaltado que o processo de escalonamento de sistemas é um caso particular do cálculo de Bases de Gröbner.

No capítulo 5, apresentamos todos os resultados e algoritmos relacionados com o cálculo das Bases de Gröbner. Com isso, fica clara a necessidade do uso de um sistema de computação algébrica.

Já no capítulo 6, introduzimos o *software* CoCoA que é especificamente usado para cálculos em álgebra comutativa. Esse ambiente computacional tem um papel relevante para a determinação das Bases de Gröbner.

O capítulo final, 7, de certa forma, é a culminância dessa Dissertação. Nele, mediante uma modelagem matemática, resolvemos um Shidoku por meio do cálculo das bases de Gröbner, programando no CoCoA.

Finalmente no Capítulo 8 apresentamos as considerações finais e os possíveis desdobramentos desse Trabalho. A leitura desse trabalho pode ser feita de forma independente ao longo dos capítulos, de acordo com o interesse do leitor. Para isso, tivemos o cuidado de detalhar cada etapa da aquisição desse conhecimento de forma que seja possível uma adequação para cada objetivo, seja ele voltado para alunos, no caso da Iniciação Científica, ou para docentes, uma vez que o trabalho fornece uma ideia inicial do tema Álgebra Computacional e abre caminho para uma vasta área de pesquisa.

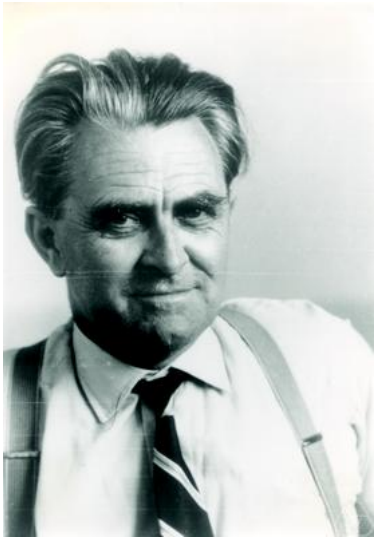
2 HISTÓRIA

Gröbner e Buchberger são os principais responsáveis pelo desenvolvimento da teoria das Bases Gröbner. Baseados nas referências Hong et al. (2006) e Reitberger (2001), apresentaremos neste capítulo, um pouco da história destes importantes matemáticos.

2.1 O início com Wolfgang Gröbner

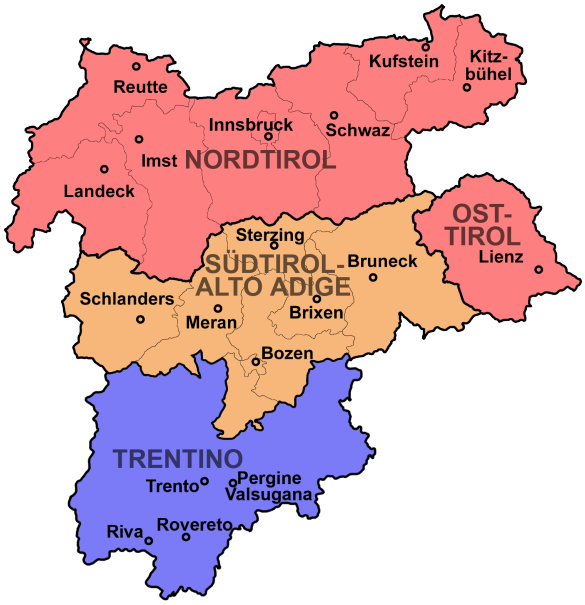
Wolfgang Gröbner, Figura 1, nasceu em 11 de fevereiro de 1899 num território italiano, o Tirol do Sul. A sua cidade natal, Colle Isarco, fica a 10 km da fronteira com a Áustria e na época era predominantemente germanófona. Por tanto, Colle Isarco é também chamado de "Gossenssas" em alemão. No mapa da Figura 2, está próxima de Sterzing. Esse território hoje é Italiano, mas de 1867 à 1918 pertenceu ao Império Austro-Húngaro e também foi dominado pela Alemanha nazista durante a segunda guerra mundial.

Figura 1 – W. Gröbner $*1899$ $-\dagger 1980$



Fonte: COMMONS, 2018. <https://commons.wikimedia.org/w/index.php?title=File:Wolfgang_Grobner.jpg&oldid=311940406>

Figura 2 – Tirol Italiano (roxo e bege) e Tirol Austríaco (vermelho)



Fonte: COMMONS, 2017. <https://commons.wikimedia.org/w/index.php?title=File:Tirol-Suedtirol-Trentino.png&oldid=264555553>

Gröbner cresceu com quatro irmãos e passou por um internato jesuíta, o que influenciou muito a sua visão do mundo. Pode ser considerado por muitos, até mesmo, paradoxal, um cientista ter uma formação também religiosa tão intensa, mas que era algo comum na época. Teve uma breve participação na Primeira Guerra com a frente italiana e logo depois cursou engenharia na Universidade de Tecnologia de Graz na Áustria.

Sua primeira obra foi um livro de cunho religioso *"Der Weg aufwärts." ("O caminho até o céu")*, fruto de uma ruptura pessoal com a igreja Católica após a trágica morte do seu irmão num acidente de moto. Depois de se casar, migrou seus estudos para a matemática pois "passou a rejeitar qualquer autoridade fora da sua própria mente".

Esteve de 1929 a 1932 na universidade de Viena, onde defendeu sua tese de doutorado. Em seguida, por recomendação do seu orientador Philipp Furtwängler, teve aulas com Emmy Noether em Göttingen na Alemanha. Por problemas financeiros voltou para Áustria em 1933 e não conseguindo emprego numa faculdade, acabou por construir centrais elétricas em Gossenssas. Por um acaso, conheceu um professor de Matemática Italiano, de nome Picone, o qual lhe ofereceu emprego na universidade de Roma.

No final da de década de 30, Gröbner teve que escolher entre a cidadania Alemã (Na época Alemanha nazista de Hitler) e a Italiana (Reino da Itália Fascista). Decidindo pela Alemã, teve que sair da Itália. Trabalhou uma temporada para a academia Prussiana de Ciências antes de receber o título de "Extraordinário" na universidade de Viena em 1941. Em seguida, teve que prestar serviço militar de onde se dedicou a constituir um instituto de força aérea para aplicação de métodos matemáticos avançados a problemas aeronáuticos. O instituto estava em Braunschweig e seu diretor se chamava Gustav Doetsch, um matemático de Freiburg.

Em 1938, no trabalho intitulado: *"Ueber eine neue idealtheoretische Grundlegung der algebraischen Geometrie" ["Sobre uma nova fundação ideal teórica de Geometria Algébrica"]*, caracterizou ideais primários por condições diferencias. Basicamente, tratou da relação entre a multiplicidade da raiz de um polinômio e a sua derivada.

Em 1945, Gröbner se refugiou no Tirol (Figura 3), onde vivia sua família. Depois do fim da guerra, não voltou imediatamente para Viena, somente em 1947, foi trabalhar na universidade de Innsbruck.

Figura 3 – Tirol do Sul: Cidade de Gröbner

Fonte: COMMONS, 2018. <https://commons.wikimedia.org/w/index.php?title=File:Gossensass_01.JPG&oldid=323108703>

Seus alunos de doutorado mais famosos são: Heinrich Reitberger, Bruno Buchberger e G. Sonderegger. Especificamente no verão de 1964, Gröbner deu um seminário sobre a teoria da dimensão de ideais de polinômios. Bruno Buchberger indagou Gröbner sobre a possibilidade de desenvolver a sua tese nos problemas abertos apresentados. Recebendo o sim, o resultado do trabalho de Buchberger foi publicado em 1965 na sua tese de doutorado *"Ein Algorithmus zum Auffinden der Basis Elemente des Restklassenrings nach einem nulldimensionalen Polynomideal" [Um algoritmo para determinar os elementos da base de um anel de classes de resíduos de um ideal polinomial de dimensão zero]*. Bruno nomeou essas bases como bases de Gröbner em homenagem ao seu orientador.

Gröbner trabalhou até 1970 em Innsbruck, e morreu em 1980 no Tirol, depois de sofrer um derrame.

2.2 Buchberger: O criador do Algoritmo das Bases de Gröbner

Bruno Buchberger, Figura 4, nasceu no ano de 1942, em Innsbruck, a capital do Tirol Austríaco. Nessa época, a Áustria estava sob domínio da Alemanha nazista. Sabe-se que teve ótimo desempenho acadêmico nos estudos secundários e portanto podia escolher qualquer caminho profissional.

Buchberger escolheu o curso de matemática da Universidade de Innsbruck, onde defendeu em 1965, a sua tese de doutorado intitulada *"Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal" ["Um algoritmo para determinar os elementos da base de um anel de classes de resíduos de um ideal polinomial de dimensão zero"]* sob a orientação de Wolfgang Gröbner. A teoria apresentada nessa tese

Figura 4 – Bruno Buchberger $*1942$

Fonte: COMMONS, 2018. <https://commons.wikimedia.org/w/index.php?title=File:Bruno_Buchberger.jpg&oldid=311937690>

ficou adormecida por aproximadamente 10 anos, quando Bruno, por recomendação de Ruediger Loos, publicou um artigo com a sua teoria no SIGSAM *(Special Interest Group in Symbolic and Algebraic Manipulation)*. A partir daí, a teoria das bases de Gröbner se impulsionou e teve muito sucesso em variados ramos da matemática. Até agora, sobre esta teoria foram publicados 10 livros e mais de 600 artigos. Em particular, nos últimos 10 anos, essa teoria teve mais de 3500 citações. O algoritmo que calcula os elementos dessas bases está presente na maioria dos sistemas de álgebra computacional atuais.

Bruno implementou pela primeira vez o cálculo das Bases de Gröbner na própria Universidade de Innsbruck, onde trabalhava com um time de pesquisadores na vanguarda da pesquisa computacional desta universidade. Depois de ter feito um intercâmbio num instituto de pesquisas nucleares na União Soviética, foi contratado em 1974 pela Universidade de Linz. O seu cargo inicial era o de professor de Teoria dos Algoritmos e Lógica Matemática. Buchberger é professor da Universidade Johannes Kepler de Linz desde então.

Nos seus primeiros anos na Universidade de Linz, Bruno contribuiu de maneira pioneira para a criação de um protótipo de máquina em parelelo. Depois, se voltou a Álgebra Construtiva e coeditou o livro *"Computer Algebra: Symbolic and Algebraic Computation"*.

No início de 1994, Buchberger criou o projeto *Theorema*,[1] cujo objetivo é a integração das demonstrações lógicas com a computação algébrica. Hoje, o projeto foca na extensão dos sistemas de computação algébrica criando funcionalidades que permitam demonstrações matemáticas (raciocínio autônomo).

Em 2002, Bruno se aposentou como professor para se concentrar na pesquisa acadêmica.

[1] <https://risc.jku.at/pj/theorema-project/>

3 PRELIMINARES

No início deste capítulo apresentaremos um rol de noções de Álgebra: Os anéis que são conjuntos com propriedades abstraídas dos inteiros, os ideais que são subconjuntos de um anel com propriedades abstraídas do conjunto dos múltiplos de um inteiro, os corpos que são abstrações do conjunto dos reais. Continuaremos o capítulo introduzindo os polinômios de uma indeterminada juntamente com o seu famoso Algoritmo da Divisão. Posteriormente, estenderemos os resultados anteriores obtidos, para polinômios em várias indeterminadas. Mostraremos a necessidade da incorporação das Ordens Monomiais nesse estudo. Finalizaremos com o mais importante resultado deste capítulo: O Algoritmo da Pseudodivisão, uma forma de dividir um polinômio de várias indeterminadas por uma lista de outros polinômios de várias indeterminadas.

3.1 Anéis e Corpos

A seguir teremos a definição de três estruturas básicas da Álgebra Abstrata: Anéis, Corpos e Ideais. A ideia da definição de anel é estudar conjuntos que possuem duas operações denominadas adição e multiplicação que gozam das propriedades também encontradas no conjunto dos números inteiros[1]. A abstração das particularidades destes conjuntos permite uma análise global que revela importantes resultados acerca dessas estruturas. Não nos alongaremos nesse estudo, que pode ser detalhado no livro de Fraleigh e Katz (2003).

Definição 1 (Anel). *Um anel é um conjunto $A \neq \varnothing$ munido de duas operações usualmente chamadas de adição $\oplus$ e multiplicação $\odot$ que gozam das seguintes propriedades:*

1. *A é fechado em relação à adição: Se $a \in A$ e $b \in A$ então $a \oplus b \in A$.*
2. *A adição é associativa: Se $a, b, c \in A$ então $a \oplus (b \oplus c) = (a \oplus b) \oplus c$.*
3. *Existe um elemento neutro para a adição 0_A tal que $a \oplus 0_A = a = 0_A \oplus a$ para qualquer $a \in A$.*
4. *Para todo $a \in A$ existe um inverso aditivo denotado por $-a$ em A, isto é: a equação $a \oplus x = 0_A$ possui uma solução em A.*
5. *A adição é comutativa: Se $a, b \in A$ então $a \oplus b = b \oplus a$.*
6. *A é fechado em relação à multiplicação: Se $a, b \in A$ então $a \odot b \in A$.*
7. *A multiplicação é associativa: Se $a, b, c \in A$ então $a \odot (b \odot c) = (a \odot b) \odot c$.*

[1] O conjunto $\mathbb{Z}$ goza da comutatividade na multiplicação, porém essa propriedade não faz parte da definição de anel. Veja a definição 4.

8. *As leis distributivas são válidas em A: Se a, b, $c \in A$, então $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ e $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$*

Definição 2 (Anel com unidade). *Um anel $(A, \oplus, \odot)$ possui unidade se existir $1_A \in A$ com a propriedade $a \odot 1_A = a = 1_A \odot a$ para todo $a \in A$. O elemento $1_A \in A$ é chamado de unidade de A.*

Definição 3 (Elemento invertível de um anel com unidade). *Sendo $(A, \oplus, \odot)$ um anel com unidade dizemos que $a \in A$ é um elemento invertível se existir $a^{-1} \in A$ tal que $a \odot a^{-1} = u = a^{-1} \odot a$, ou seja a^{-1} é o inverso multiplicativo de a.*

Definição 4 (Anel comutativo). *Dizemos que $(A, \oplus, \odot)$ é comutativo quando a multiplicação goza da comutatividade, isto é, se $a, b \in A$ então $a \odot b = b \odot a$.*

Exemplo 1. Os conjuntos abaixo, munidos com as operações usuais são anéis:

1. O conjunto dos inteiros $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
2. O conjunto dos racionais $\mathbb{Q} = \left\{\frac{a}{b} \ : \ a, b \in \mathbb{Z} \text{ com } b \neq 0\right\}$.
3. O conjunto dos números reais $\mathbb{R}$.
4. O conjunto dos números complexos $\mathbb{C}$.

Observe que $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ com as operações usuais não é um anel pela falha da propriedade 5 da definição de anéis. Para uma investigação profunda sobre a construção dos conjuntos numéricos recomendamos consultar a obra de Kramer e Pippich (2017).

Definição 5 (Domínio de Integridade). *Um anel comutativo $(A, \oplus, \odot)$ com unidade $1_A \neq 0_A$ é um domínio de integridade se para todo $a, b \in A$ com $a \odot b = 0_A$ implicar que $a = 0_A$ ou $b = 0_A$.*

Exemplo 2. O conjunto das matrizes diagonais quadradas com entradas reais e as operações usuais de adição e multiplicação satisfaz as condições de anel *comutativo com unidade* porém não é um domínio de integridade. Pode verificar-se facilmente que a unidade desse anel é o elemento

$$1_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

É sabido que existem matrizes diagonais não nulas cujo produto é a matriz nula. De fato:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \odot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + 0 \cdot 0 & 1 \cdot 1 + 0 \cdot 0 \\ 0 \cdot 0 + 0 \cdot 0 & 0 \cdot 1 + 0 \cdot 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Exemplo 3. O conjunto $(\mathbb{Z}_4, \oplus, \odot)$ dos inteiros módulo 4 munido das operações usuais satisfaz as condições para ser um anel comutativo com unidade porém não é um domínio de integridade. Na tabela de multiplicação deste anel

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

observa-se que $2 \odot 2 = 4 = 0$ (4 deixa resto 0 quando dividido por 4).

Exemplo 4. O conjunto $(\mathbb{Z}_3, \oplus, \odot)$ dos inteiros módulo 3 é um anel comutativo com unidade e é um domínio de integridade. Observe a tabela de multiplicação do anel $\mathbb{Z}_3$.

$\odot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

É um resultado conhecido da teoria dos números que se tomarmos $a, b \in \mathbb{Z}_n$ com n primo a equação $a \odot b = 0$ implica $a = 0$ ou $b = 0$. Assim, $\mathbb{Z}_p$, p primo, com as operações de $\oplus$ e $\odot$ usuais é um domínio de integridade.

Definição 6 (Corpo). *Um domínio de integridade $(A, \oplus, \odot)$ é um corpo se todo elemento não nulo for invertível.*

Como exemplos de corpos temos: $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ com as operações de adição e de multiplicação usuais. $\mathbb{Z}$ não é corpo pois nem todo elemento possui inverso multiplicativo. Revendo os exemplos 3 e 4 é possível concluir que $\mathbb{Z}_4$ não é corpo, pois não é domínio e que $\mathbb{Z}_3$ é um corpo. Tem-se também que: $\mathbb{Z}_n$ é corpo se, e somente se n é primo.

Proposição 1. *Num anel $(A, \oplus, \odot)$ são válidas as seguintes propriedades:*

1. *O elemento neutro aditivo é único;*
2. *O elemento neutro multiplicativo, quando existe, é único;*
3. *O inverso aditivo de um elemento $a \in A$ é único;*
4. *O inverso multiplicativo de um elemento $a \in A$, quando existe, é único;*

Demonstração.

1. Se existissem dois elementos neutros 0_A e $0'_A$ então

$$0_A = 0'_A \oplus 0_A = 0_A \oplus 0'_A = 0'_A$$

onde na segunda igualdade foi usada a comutatividade da adição;

2. Se u e v são unidades, então pelo fato de u ser unidade tem-se $u \odot v = v$, pelo fato de v ser unidade tem-se $u \odot v = u$, assim, necessariamente, $v = u$;

3. Se a' e a'' são inversos aditivos de $a \in A$ então usando a comutatividade e associatividade da adição obtemos

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

4. Se i e i' são inversos de $a \in A$ e 1_A é a unidade de A então usando a associatividade da multiplicação obtemos

$$i = i \cdot 1_A = i \cdot (a \cdot i') = (i \cdot a) \cdot i' = 1_A \cdot i' = i'$$

□

A partir de agora, simplificaremos as notações e iremos nos referir a um anel $(A, \oplus, \odot)$ simplesmente por A sendo a adição denotada por $+$ e a multiplicação por $\cdot$. Além disso:

- O elemento neutro aditivo, que é único, será representado por 0 e chamado de *zero*;
- Já convencionamos que inverso o aditivo de a, que é único, será representado por $-a$. Além disso, usaremos a notação $a - b$ para representar $a + (-b)$. Esta operação será chamada de *subtração*;
- O elemento neutro multiplicativo, que é único, será representado por 1 e chamado de *unidade* ou *um*;
- O inverso multiplicativo de um elemento a, que é único, será representado por a^{-1};
- A multiplicação de a por b poderá tanto ser representada por ab ou por $a \cdot b$;

Proposição 2. *Se A é um anel então para quaisquer $a, b, c \in A$*

1. *Se $a + b = a + c$ então $b = c$*
2. $-(-a) = a$
3. $0a = a0 = 0$
4. $a(-b) = (-a)b = -(ab)$
5. $(-a)(-b) = ab$

Demonstração.

1. Adicionando $-a$ a ambos membros da igualdade, usando a propriedade associativa, a existência do inverso aditivo e do elemento neutro aditivo, obtemos o resultado;

2. Pelas propriedades 4 e 8 da definição (1) temos $0a = (0+0)a = 0a + 0a$, agora usando a propriedade 5, podemos adicionar $-0a$ à ambos membros dessa igualdade para obter $0a = 0$. De maneira análoga temos $a0 = a(0+0) = a0 + a0 \Rightarrow 0 = a0$ e assim fica provado que $0a = a0 = 0$;

3. Como $a(-b) + ab = a(-b+b) = a0 = 0$ adicionando $-(ab)$ à ambos membros da igualdade obtemos $a(-b) = -(ab)$. Analogamente temos que $(-a)b + ab = (-a+a)b = 0b \Rightarrow (-a)b = -(ab)$.

4. Usando o item anterior temos $(-a)(-b) = -(a(-b))$. Novamente usando o item anterior temos, $-(a(-b)) = -(-(ab))$. Como $-(-(ab))$ é o inverso aditivo de $-(ab)$ temos

$$-(-(ab)) + (-(ab)) = 0$$

Adicionando ab em ambos membros obtemos:

$$-(-(ab)) = ab$$

de forma que fica provadas as igualdades

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$$

□

3.2 Ideais

Seguiremos agora para a terceira ideia deste capítulo: A noção de Ideal.
A ideia básica por trás da definição de um ideal é a de generalizar um tipo específico de subconjunto dos inteiros. Por exemplo, considere o conjunto dos inteiros múltiplos de 5:

$$5\,\mathbb{Z} = \{\ldots, -15, -10, -5, 0, 5, 10, \ldots\} \subset \mathbb{Z}$$

Ao somarmos ou subtrairmos múltiplos de 5 continuaremos com um inteiro múltiplo de 5. Observe que o produto de um múltiplo de 5 por qualquer número inteiro resulta num inteiro também múltiplo de 5. Essas são as propriedades que queremos que um ideal possua.

Definição 7. *Seja $(A, +, \cdot)$ um anel comutativo com unidade. Um ideal I é um subconjunto não vazio de A que goza das propriedades:*

1. *Dados $f, g \in I$ então $f + g \in I$*

2. *Dado $f \in I$ e $h \in A$ então $h \cdot f \in I$*

Exemplo 5.

1. O conjunto unitário $\{0\}$ e o próprio conjunto A são ideais do anel A. Os chamamos de ideais triviais.
2. O conjunto $2\,\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4\ldots\}$ é um ideal de $\mathbb{Z}$
3. O conjunto dos números ímpares $\{\ldots, -3, -1, 1, 3\ldots\}$ *não* é um ideal de $\mathbb{Z}$, pois ao somarmos dois números ímpares *não* obtemos um número ímpar.

Proposição 3. *Seja $(A, +, \cdot)$ um anel comutativo com unidade. Então:*

1. *$0 \in I$ para todo ideal I de A.*
2. *Se I é um ideal de A que contém um elemento invertível então $I = A$.*
3. *Dado um subconjunto não vazio G de A o conjunto*

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

é um ideal de A.

Demonstração.

1. Como um ideal é um subconjunto não vazio de A, podemos tomar um elemento $x \in I$. Como A possui unidade 1, o inverso aditivo de 1 denotado por -1 também pertence à A. Assim pela definição de ideal $(-1)\cdot x = -x \in I$. Como a soma de dois elementos de um ideal tem que permanecer no ideal obtemos $x + (-x) = 0 \in I$.
2. Por definição de ideal temos $I \subseteq A$. Assim, basta provarmos que $A \subseteq I$ para termos $I = A$. De fato, seja $u \in I$ esse elemento invertível cujo inverso denotaremos por v. Dado um $r \in A$ qualquer podemos escrever

$$r = r \cdot 1 = r \cdot (vu) = \underbrace{(rv)}_{\in A} \cdot \underbrace{u}_{\in I} \in I$$

3. Sejam f e g elementos de $\langle G\rangle$. Então

$$f = \sum_{i=1}^{n} h_i f_i \text{ e } g = \sum_{j=1}^{m} q_j g_j$$

com $h_i, q_j \in A$ e $f_i, g_j \in G$. Daí,

$$f + g = \sum_{i=1}^{n} h_i f_i + \sum_{j=1}^{m} q_j g_j$$

Fazendo $h_{n+j} = q_j$ e $f_{n+j} = g_j$ podemos escrever a soma da seguinte forma:

$$f + g = \sum_{k=1}^{n+m} \underbrace{h_k}_{\in A} \underbrace{f_k}_{\in G} \in \langle G\rangle$$

Por fim, dado $h \in A$ temos

$$h \cdot f = h \sum_{i=1}^{n} h_i f_i = \sum_{i=1}^{n} \underbrace{(hh_i)}_{\in A} \underbrace{f_i}_{\in G} \in \langle G \rangle$$

o que termina a demonstração.

□

Chamamos o conjunto $\langle G \rangle$ de **ideal gerado** por G. Quando $\langle G \rangle$ pode ser gerado por um único elemento o chamamos de ideal principal. Por exemplo no anel $(\mathbb{Z}, +, \cdot)$ o ideal gerado pelo conjunto unitário $G = \{5\}$ é um ideal principal. Este ideal é representado por $\langle 5 \rangle = \{\sum_{i=1}^{n} a_i \cdot 5 : n \in \mathbb{N}, a_i \in \mathbb{Z}\}$.

Na próxima seção apresentaremos com detalhes a estrutura do anel de polinômios $\mathbb{K}[x]$. Esse será um conjunto de muita importância neste trabalho. Por exemplo, no conjunto dos polinômios com coeficientes reais, simbolizado por $\mathbb{R}[x]$, considere o ideal $\langle x^2 - 1 \rangle$. Observe que multiplicando $x^2 - 1$ por qualquer polinômio de $\mathbb{R}[x]$ obteremos um polinômio que também estará no ideal. Por exemplo:

- $(x^2 - 1) \cdot x = x^3 - x \in \langle x^2 - 1 \rangle$
- $(x^2 - 1) \cdot 3 = 3x^2 - 3 \in \langle x^2 - 1 \rangle$
- $(x^2 - 1) \cdot (x^2 + 1) = x^4 - 1 \in \langle x^2 - 1 \rangle$

Da mesma forma, se somarmos quaisquer dois elementos do ideal $\langle x^2 - 1 \rangle$ o resultado também pertence no ideal. Por exemplo:

- $(x^2 - 1) + (x^3 - x) = x^3 + x^2 - x - 1 = (x^2 - 1)(x + 1) \in \langle x^2 - 1 \rangle$
- $(x^2 - 1) + (3x^2 - 3) = 4x^2 - 4 = 4(x^2 - 1) \in \langle x^2 - 1 \rangle$
- $(x^2 - 1) + (x^4 - 1) = x^4 + x^2 - 2 = (x^2 - 1)(x^2 + 2) \in \langle x^2 - 1 \rangle$

Como vimos, é fácil obter elementos do ideal $\langle x^2 - 1 \rangle$. A pergunta que naturalmente surge é: Como determinar se um polinômio f pertence a um ideal? Por exemplo $f = x^3$ pertence ao ideal $\langle x^2 - 1 \rangle$? Essa questão será completamente respondida na seção 3.6.

3.3 Polinômios em $\mathbb{K}[x]$

Nesta seção nos concentraremos no conjunto de polinômios em uma indeterminada. Apresentaremos as definições necessárias para ilustrar o Algoritmo da Divisão com mais rigor na próxima seção.

Definição 8. *Um polinômio é uma expressão finita da forma*

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

com $n \in \mathbb{N}$, com os coeficientes a_i num corpo $\mathbb{K}$ e $a_n \neq 0$. O grau do polinômio f é o maior índice para o qual $a_i \neq 0$. Neste caso o grau de f é n. Caso tenhamos $f = 0 = \cdots + 0x^2 + 0x^1 + 0x^0$, definiremos $\deg(f) = -\infty$.

Dado um corpo $\mathbb{K}$, considere o conjunto

$$\mathbb{K}[x] = \{a_n x^n + \cdots + a_1 x + a_0 \ : \ n \in \mathbb{N} \text{ e } a_i \in \mathbb{K}\}$$

dos polinômios em x com coeficientes em $\mathbb{K}$. Sejam

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

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

elementos de $\mathbb{K}[x]$. Definimos a *multiplicação* de f por g como abaixo:

$$f \cdot g = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n+m} x^{n+m}$$

onde

$$\begin{aligned} c_0 &= a_0 b_0 \\ c_1 &= a_0 b_1 + a_1 b_0 \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \\ &\cdots \\ c_k &= \sum_{i+j=k} a_i b_j \end{aligned}$$

Caso seja $m \neq n$, podemos completar alguns termos com coeficientes 0 para que tenhamos $m = n$, assim, definimos a *adição* de f e g como:

$$f + g = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + a_0 + b_0$$

O conjunto $\mathbb{K}[x]$ será de grande importância no nosso estudo. Se $\mathbb{K}$ for um domínio de integridade, então $\mathbb{K}[x]$ também será um domínio de integridade. Demonstraremos esse fato no apêndice seção A.1.

Para exemplificar os próximos conceitos considere o polinômio

$$f = 3x^5 + 7x^2 - 3x + 1 \in \mathbb{Q}[x]$$

Observe que o polinômio f está ordenado segundos as potências decrescentes. Temos que f é a soma de 4 termos, a saber: $3x^5$, $7x^2$, $-3x$ e 1. O termo de maior grau, $3x^5$, chama-se termo líder, sendo x^5 o monômio líder e 3 o coeficiente líder. Usando a simbologia, em inglês, usada na obra de Cox, Little e O'Shea (2015), escrevemos

$$\mathrm{LT}(f) = 3x^5,\ \mathrm{LM}(f) = x^5,\ \mathrm{LC}(f) = 3$$

respectivamente para representar: Termo Líder de f, Monômio Líder de f e Coeficiente Líder de f. Resumindo temos a definição 9

Definição 9. *Dado um polinômio não nulo*

$$f = \sum_{i=0}^{n} a_i x^i = a_n x^n + \cdots + a_1 x + a_0$$

onde os $a_i \in \mathbb{K}$ *e* $a_n \neq 0$ *dizemos que:*

- x^n *é o monômio líder de* f*, simbolicamente denotamos por* $\mathrm{LM}(f) = x^n$.
- a_n *é o coeficiente líder de* f*, simbolicamente denotamos por* $\mathrm{LC}(f) = a_n$.
- $a_n x^n$ *é o termo líder de* f*, simbolicamente denotamos por* $\mathrm{LT}(f) = a_n x^n$.
- *O grau de* f *é* n*, simbolicamente denotamos por* $\deg(f) = n$.

Exemplo 6. Vejamos alguns exemplos:

1. um polinômio de grau 2:
$$f = 3x^2 - 5x + 6$$
com $\mathrm{LM}(f) = x^2$, $\mathrm{LC}(f) = 3$ e $\mathrm{LT}(f) = 3x^2$.

2. um polinômio de grau 8:
$$g = 4x^3 + 6x^8 - 7$$
com $\mathrm{LM}(g) = x^8$, $\mathrm{LC}(g) = 6$ e $\mathrm{LT}(g) = 6x^8$.

3. um polinômio de grau 0:
$$h = 9$$
observe que $h = \cdots + 0x^2 + 0x^1 + 9x^0$. Assim temos $\mathrm{LM}(h) = x^0$, $\mathrm{LC}(h) = 9$ e $\mathrm{LT}(h) = 9x^0$.

4. No polinômio nulo, $f = 0 = \cdots + 0x^2 + 0x^1 + 0x^0$, não se definem LM, LT e LC, mas definiremos $\deg(f) = -\infty$.

Exemplo 7. É muito importante notar que na soma de polinômios em $\mathbb{K}[x]$ pode ocorrer um cancelamento dos termos líderes.

$$(\underbrace{x^2 + 5x}_{\text{grau 2}}) + (\underbrace{-x^2 - 3x}_{\text{grau 2}}) = \underbrace{2x}_{\text{grau 1}}$$

Como veremos na próxima proposição, esse fenômeno não ocorre na multiplicação em $\mathbb{K}[x]$.

Proposição 4. *Sejam $f, g \in \mathbb{K}[x]$. Então:*

1. $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
2. $\deg(f \cdot g) = \deg(f) + \deg(g)$

Demonstração.

1. Suponhamos que $\deg(f) = m > n = \deg(g)$. Daí temos $f = c_m x^m + \cdots + c_1 x^1 + c_0$ com $c_m \neq 0$ e $g = d_n x^n + \cdots + d_1 x^1 + d_0$ com $d_n \neq 0$, então

   $$f + g = (c_m + 0)x^m + \cdots + (c_n + d_n)x^n + \cdots + (c_1 + d_1)x^1 + c_0 + d_0$$

   dessa forma $\deg(f+g) = m = \max\{\deg(f), \deg(g)\}$ pois $c_m \neq 0$. O caso em que $\deg(f) = m < n = \deg(g)$ é completamente análogo.

   Supondo que $\deg(f) = m = \deg(g)$ temos que $f = c_m x^m + \cdots + c_1 x^1 + c_0$ com $c_m \neq 0$ e $g = d_m x^m + \cdots + d_1 x^1 + d_0$ com $d_m \neq 0$ então

   $$f + g = (c_m + d_m)x^m + \cdots (c_1 + d_1)x^1 + c_0 + d_0$$

   Observe que $c_m + d_m$ pode se anular nesse caso. Em qualquer dos casos temos $\deg(f+g) = \max\{\deg(f), \deg(g)\}$.

2. Considere $f = \sum_{i=0}^{m} c_i x^i$, $c_m \neq 0$ e $g = \sum_{i=0}^{n} d_i x^i$, $d_n \neq 0$. Multiplicando esses dois polinômios obtemos

   $$f \cdot g = c_m d_n x^{m+n} + \cdots + c_0 d_0$$

   Como c_m e d_n são ambos não nulos e $\mathbb{K}$ é um corpo, temos que $c_m d_n \neq 0$ portanto $\deg(f \cdot g) = m + n = \deg(f) + \deg(g)$

□

3.4 O Algoritmo da Divisão

Nesta seção revisitaremos o Algoritmo da Divisão visto no ensino médio. Usaremos as notações apresentadas na seção anterior e teremos a apresentação de um algoritmo em *pseudocódigo*[2].

Para fixar as ideias e relembrar as etapas da divisão vamos dividir $f = 3x^5 + 16x^3 + x^2 - 10x + 9$ por $g = x^2 + 6$. Primeiro ordenaremos o dividendo e o divisor pela ordem decrescente do grau e os disporemos no seguinte formato de chave:

$$3x^5 + 16x^3 + x^2 - 10x + 9 \;\big|\; \underline{x^2 + 6}$$

Agora devemos dividir $\mathrm{LT}(f) = 3x^5$ por $\mathrm{LT}(g) = x^2$ obtendo $\frac{\mathrm{LT}\, f}{\mathrm{LT}\, g} = 3x^3$ que é o primeiro termo do quociente. Para encontrar o primeiro resto parcial efetuamos

$$f - \left(\frac{\mathrm{LT}\, f}{\mathrm{LT}\, g}\right) g = 3x^5 + 16x^3 + x^2 - 10x + 9 - 3x^3(x^2 + 6) = -2x^3 + x^2 - 10x$$

Observe que nesta subtração cancelamos os termos líderes e assim o resultado tem grau menor do que 5.

$$\begin{array}{rl|l} 3x^5 + 16x^3 + x^2 - 10x + 9 & & x^2 + 6 \\ \cline{3-3} \underline{-\,3x^5 - 18x^3} & & 3x^3 \\ -\,2x^3 + x^2 - 10x & & \end{array}$$

Agora repetimos a ideia inicial, tomando o resto parcial $r_1 = -2x^3 + x^2 - 10x$ como dividendo e o divisor continua sendo $x^2 + 6$. Dividindo $\mathrm{LT}(r_1) = -2x^3$ por $\mathrm{LT}(g) = x^2$ obtendo $\frac{\mathrm{LT}\, f}{\mathrm{LT}\, g} = -2x$ que é o segundo termo do quociente. Para encontrar o segundo resto parcial efetuamos

$$r_1 - \left(\frac{\mathrm{LT}\, r_1}{\mathrm{LT}\, g}\right) g = -2x^3 + x^2 - 10x - (-2x)(x^2 + 6) = x^2 + 2x + 9$$

Novamente nesta subtração cancelamos os termos líderes e assim o resultado tem grau menor do que 3.

$$\begin{array}{rl|l} 3x^5 + 16x^3 + x^2 - 10x + 9 & & x^2 + 6 \\ \cline{3-3} \underline{-\,3x^5 - 18x^3} & & 3x^3 - 2x \\ -\,2x^3 + x^2 - 10x & & \\ \underline{\quad 2x^3 \qquad + 12x} & & \\ x^2 \;\; + 2x + 9 & & \end{array}$$

Efetuaremos o mesmo processo anterior, considerando $r_2 = x^2 + 2x + 9$ como dividendo e $x^2 + 6$ como divisor. Dividindo $\mathrm{LT}(r_2) = x^2$ por $\mathrm{LT}(g) = x^2$ obtendo $\frac{\mathrm{LT}\, f}{\mathrm{LT}\, g} = 1$ que é o terceiro

[2] Escrever algoritmos em Pseudocódigo é comum na Matemática. Assumindo que o leitor tenha um mínimo de experiência com uma linguagem de programação qualquer, não haverá dificuldades para o entendimento dos algoritmos deste trabalho.

termo do quociente. Para encontrar o terceiro resto parcial efetuamos

$$r_2 - \left(\frac{\mathrm{LT}\, r_2}{\mathrm{LT}\, g}\right) g = x^2 + 2x + 9 - (1)(x^2 + 6) = 2x + 3$$

$$\begin{array}{r|l}
3x^5 + 16x^3 + x^2 - 10x + 9 & x^2 + 6 \\
\cline{2-2}
-\,3x^5 - 18x^3 & 3x^3 - 2x + 1 \\
\cline{1-1}
\quad -\,2x^3 + x^2 - 10x & \\
\quad\ \ 2x^3 \qquad + 12x & \\
\cline{1-1}
\qquad\quad x^2 \ + 2x + 9 & \\
\quad -\,x^2 \qquad - 6 & \\
\cline{1-1}
\qquad\quad 2x + 3 &
\end{array}$$

O algoritmo acaba agora pois não podemos dividir $\mathrm{LT}(r_3) = 2x$ por $\mathrm{LT}(g) = x^2$. Esta divisão não é possível pois o grau de $r_3 = 2x + 3$ é menor do que o de $x^2 + 6$. Assim a divisão está terminada e temos:

$$\underbrace{3x^5 + 16x^3 + x^2 - 10x + 9}_{\text{Dividendo}} = \underbrace{(3x^3 - 2x + 1)}_{\text{Quociente}}\underbrace{(x^2 + 6)}_{\text{Divisor}} + \underbrace{2x + 3}_{\text{Resto}}$$

Exemplo 8. No exemplo a seguir dividiremos $f = x^3 - 4x^2 + x + 6$ por $g = x - 2$.

$$\begin{array}{r|l}
x^3 - 4x^2 \ + x + 6 & x - 2 \\
\cline{2-2}
-\,x^3 + 2x^2 & x^2 - 2x - 3 \\
\cline{1-1}
\quad -\,2x^2 \ + x & \\
\quad\ \ 2x^2 - 4x & \\
\cline{1-1}
\qquad\quad -\,3x + 6 & \\
\qquad\quad\ \ 3x - 6 & \\
\cline{1-1}
\qquad\qquad\quad 0 &
\end{array}$$

Quando o resto da divisão de f por g é zero, diremos que g *divide* f, ou que f é *múltiplo* de g.

$$\underbrace{x^3 - 4x^2 + x + 6}_{\text{Dividendo}} = \underbrace{(x^2 - 2x - 3)}_{\text{Quociente}}\underbrace{(x - 2)}_{\text{Divisor}} + \underbrace{0}_{\text{Resto}}$$

Teorema 1 (Teorema da Divisão). *Seja $g \in \mathbb{K}[x]$ não nulo. Então todo $f \in \mathbb{K}[x]$ pode ser escrito como*

$$f = qg + r$$

onde q e r são polinômios em $\mathbb{K}[x]$ com $r = 0$ ou $\deg(r) < \deg(g)$. Os polinômios q e r são unicamente determinados e existe um algoritmo para determiná-los.

Demonstração. Primeiro provaremos a existência e em seguida a unicidade. Se $f = 0$ tomamos $q = r = 0$. Se $\deg(f) < \deg(g)$ basta tomar $r = f$ e $q = 0$. No caso em que $\deg(f) \geq \deg(g)$

usaremos indução no grau de f. Vamos assumir que o teorema é válido para dividir um polinômio com grau menor do que $\deg(f)$ e iremos mostrar que também vale se o grau for $\deg(f)$. Observe que o polinômio $h = f - \left(\frac{\mathrm{LT}\, f}{\mathrm{LT}\, g}\right) g$ tem grau menor do que $\deg(f)$ pois na subtração $f - \frac{\mathrm{LT}\, f}{\mathrm{LT}\, g} g$ cancelam-se os termos líderes do minuendo e subtraendo. Assim, a hipótese indutiva garante que existam $q', r' \in \mathbb{K}[x]$ tais que

$$h = f - \frac{\mathrm{LT}\, f}{\mathrm{LT}\, g} g = q'g + r'$$

com $r' = 0$ ou $0 \leq \deg r' < \deg g$ Desta forma,

$$f = \left(q' + \frac{\mathrm{LT}\, f}{\mathrm{LT}\, g}\right) g + r'$$

e $q = q' + \frac{\mathrm{LT}\, f}{\mathrm{LT}\, g}$ e $r = r'$ o que conclui a demonstração da existência. Para mostrar a unicidade suponha que $f = q'g + r'$ com $r' = 0$ ou $\deg(r') < \deg(g)$. Isto implicaria que

$$qg + r = f = q'g + r'$$

$$g(q - q') = r' - r$$

Se $q - q' \neq 0$ teríamos que o lado esquerdo da igualdade teria grau maior ou igual do que $\deg(g)$ enquanto que o lado esquerdo teria grau estritamente menor do que $\deg(g)$ Isto é um absurdo, logo temos que ter $q - q' = 0$ donde tiramos pela igualdade que $r' - r = 0$ e assim obtemos que $q = q'$ e $r = r'$. □

Abaixo temos o algoritmo, escrito em pseudocódigo, que efetua a divisão do polinômio f pelo polinômio g não nulo:

Input: f, g com $g \neq 0$
Output: q, r
1 $q := 0$;
2 $r := f$;
3 **while** $r \neq 0$ **and** $\mathrm{LT}(g)$ *divide* $\mathrm{LT}(r)$ **do**
4 $\quad q := q + \frac{\mathrm{LT}\, r}{\mathrm{LT}\, g}$;
5 $\quad r := r - \frac{\mathrm{LT}\, r}{\mathrm{LT}\, g} g$;
6 **return** q, r

Algoritmo 1: O Algoritmo da Divisão em $\mathbb{K}[x]$

O bloco WHILE..DO faz com que as operações inseridas após o comando DO sejam repetidas até que a expressão entre o WHILE e o DO seja falsa. Isto é, até que $r = 0$ ou que $\mathrm{LT}(g)$ não divida $\mathrm{LT}(r)$. A cada iteração do WHILE os comandos das linhas 4 e 5 redefinem as variáveis q e r.

Para provar que este algoritmo funciona temos que mostrar que em todas as etapas sempre é verdade que $f = qg + r$, que o algoritmo em algum momento termina e que os valores de q e r

obtidos no final satisfazem as propriedades de quociente e resto desejadas. Como inicialmente $r = f$ e $q = 0$, note que é válida a relação $f = qg + r$. Mesmo depois das redefinições de q e r esta relação continua válida como se pode verificar por essa igualdade:

$$f = qg + r = \left(q + \frac{\mathrm{LT}\, r}{\mathrm{LT}\, g}\right) g + \left(r - \frac{\mathrm{LT}\, r}{\mathrm{LT}\, g} g\right)$$

Para provar que o algoritmo termina, isto é, que em algum momento $r = 0$ ou que $\mathrm{LT}(g)$ não divide $\mathrm{LT}(r)$, temos que observar que ao calcular o novo resto com a expressão

$$r - \left(\frac{\mathrm{LT}\, r}{\mathrm{LT}\, g}\right) g$$

ou o grau diminui ou a expressão se anula. De fato, se $r = a_m x^m + \cdots + a_0$ e $g = b_n x^n + \cdots + b_0$ com $m \geq n$ então

$$r - \left(\frac{\mathrm{LT}\, r}{\mathrm{LT}\, g}\right) g = (a_m x^m + \cdots + a_0) - \left(\frac{a_m x^m}{b_n x^n}\right) (b_n x^n + \cdots + b_0)$$
$$r - \left(\frac{\mathrm{LT}\, r}{\mathrm{LT}\, g}\right) g = a_m x^m + \cdots + a_0 - a_m x^m - \left(\frac{a_m x^m}{b_n x^n}\right) (b_{n-1} x^{n-1} + \cdots + b_0)$$

onde nesta expressão ocorre um cancelamento de termos líderes e a respectiva diminuição do grau ou possivelmente toda expressão se anula. Como o grau não pode diminuir infinitamente o algoritmo tem que terminar em um número finitos de iterações.

Como as iterações do WHILE terminam quando $r = 0$ ou quando $\mathrm{LT}(g)$ não divide $\mathrm{LT}(r)$, de fato teremos um resto nulo ou um resto com grau estritamente inferior ao grau do divisor. Também fica provado que q continua sendo um polinômio em $\mathbb{K}[x]$ por conta das operações realizadas em cada iteração serem somas de q com termos monomiais.

Corolário 1. *Todo ideal I de $\mathbb{K}[x]$ é principal, isto é, $I = \langle f \rangle$ para algum $f \in \mathbb{K}[x]$. O polinômio f é único a menos de uma multiplicação por constante não nula em $\mathbb{K}$.*

Demonstração. Considere um ideal $I \subseteq \mathbb{K}[x]$. Se $I = \{0\}$ então $I = \langle 0 \rangle$ e nada temos a provar. Se não, tome um polinômio não nulo f de grau mínimo contido em I. Provaremos que $\langle f \rangle = I$. É fácil ver que $\langle f \rangle \subseteq I$ pois I é um ideal e $f \in I$. Para provar a outra inclusão, tome $g \in I$ e o divida por f, obtendo $g = qf + r$ com $r = 0$ ou $\deg(r) < \deg(f)$. Como I é um ideal $qf \in I$ logo $r \in I$ pois $r = g - qf$. Agora temos duas possibilidades: $r = 0$ ou $\deg(r) < \deg(f)$. Se r não fosse zero, então $\deg(r) < \deg(f)$ implicaria na existência de um polinômio de grau menor ainda do que f em I. Isto não é possível pois contradiz a nossa escolha de f. Desta forma só pode ser $r = 0$ daí $g = qf \in \langle f \rangle$. Isto prova a inclusão $I \subseteq \langle f \rangle$ e termina a demonstração de que $I = \langle f \rangle$. Para provar unicidade, suponha que $\langle f \rangle = \langle g \rangle$. Então $f \in \langle g \rangle$ significa que $f = hg$ para algum polinômio h. Analisando o grau desses polinômios temos $\deg(f) = \deg(h) + \deg(g)$ e consequentemente $\deg(f) \geq \deg(g)$. Analogamente, trocando f por g e usando o mesmo

raciocínio obtemos $\deg(g) \geq \deg(f)$ e por consequência $\deg(f) = \deg(g)$. Unindo isso à equação inicial obtemos

$$\deg(f) = \deg(h) + \deg(g) \Rightarrow \deg(h) = 0$$

e h tem que ser uma constante não nula em $\mathbb{K}$. □

Essa demonstração não é construtiva pois não nos fornece um algoritmo para determinar esse gerador único. Para resolver esse problema usaremos a ideia de máximo divisor comum apresentada na próxima seção.

3.5 O Máximo Divisor Comum de Polinômios

A seguir definiremos o Máximo Divisor Comum de dois polinômios $f, g \in \mathbb{K}[x]$, abreviado por $\mathrm{MDC}\,(f, g)$. A definição segue a mesma lógica da definição para números inteiros.

Definição 10. *Um máximo divisor comum dos polinômios $f, g \in \mathbb{K}[x]$ é um polinômio h tal que*

1. *h divide f e g*
2. *Se p é um outro polinômio que divide f e g, então p divide h*

Se h gozar dessas propriedades escreveremos $h = \mathrm{MDC}\,(f, g)$

Proposição 5. *Sejam $f, g \in \mathbb{K}[x]$. Então:*

1. *$\mathrm{MDC}\,(f, g)$ existe e é único a menos do produto por uma constante não nula em $\mathbb{K}$.*
2. *$\mathrm{MDC}\,(f, g)$ é um gerador do ideal $\langle f, g\rangle$.*
3. *Existe um algoritmo para a determinação do $\mathrm{MDC}\,(f, g)$*

Demonstração. Primeiro provaremos a existência do MDC. Como vimos anteriormente, todo ideal de $\mathbb{K}[x]$ é principal, logo $\langle f, g\rangle = \langle h\rangle$ para algum polinômio $h \in \mathbb{K}[x]$. Afirmamos que $h = \mathrm{MDC}\,(f, g)$. De fato, h divide f e g pois $f, g \in \langle h\rangle = \langle f, g\rangle$. Agora se $p \in \mathbb{K}[x]$ divide f e g temos $f = Cp$ e $g = Dp$ para determinados $C, D \in \mathbb{K}[x]$. Mas como $h \in \langle f, g\rangle$, então pode ser escrito como combinação $h = Af + Bg$ com $A, B \in \mathbb{K}[x]$. Usando as expressões de f e g nesta última equação obtemos:

$$h = Af + Bg = ACp + BDp = (AC + BD)p$$

o que mostra que p divide h e assim $h = \mathrm{MDC}\,(f, g)$.

Para provar a unicidade suponha que h' é um outro MDC de f e g. Pela segunda parte da definição de MDC temos que h' divide h e h divide h'. Isto é, $h = Ah'$ e $h' = Bh$ donde temos

que $AB = 1$ com o grau de AB zero. Isto é, $h = \lambda h'$ onde $\lambda \neq 0 \in \mathbb{K}$ é uma constante. Assim ficam provadas parte 1 e parte 2 da proposição.

Para mostrarmos o algoritmo utilizado para encontrar o MDC de dois polinômios de uma variável estabeleceremos a seguinte notação: Sejam $f, g \in \mathbb{K}[x]$ com $g \neq 0$. Dividindo f por g obtemos q e r tais que $f = qg + r$. Defina r como o resto da divisão de f por g isto é, $r =$ resto (f, g).

Input: f, g
Output: $h = \mathrm{MDC}(f, g)$
1 $h := f$;
2 $s := g$;
3 **while** $s \neq 0$ **do**
4 $\quad rem :=$ resto(h, s);
5 $\quad h := s$;
6 $\quad s := rem$;
7 **return** h

Algoritmo 2: O Algoritmo Euclidiano (Cálculo do MDC)

O Algoritmo apresentado acima é devido a Euclides[3] e seu funcionamento utiliza sucessivas divisões com resto. A ideia principal é usar o fato de que se $f = qg + r$ então $\mathrm{MDC}(f, g) = \mathrm{MDC}(f - qg, g) = \mathrm{MDC}(r, g)$. Isto significa que a cada divisão que é feita troca-se um polinômio por outro de grau menor (f por r). Como os restos não podem diminuir infinitamente, em algum momento teremos um resto 0. Assim teremos $\mathrm{MDC}(r_i, 0) = r_i = \mathrm{MDC}(f, g)$. Para provar que $\mathrm{MDC}(f, g) = \mathrm{MDC}(f - qg, g) = \mathrm{MDC}(r, g)$ lembre-se que $\mathrm{MDC}(f, g)$ é um gerador do ideal $\langle f, g\rangle$. Então se mostrarmos que $\langle f, g\rangle = \langle f - qg, g\rangle$ mostraremos que $\mathrm{MDC}(f, g) = \mathrm{MDC}(f - qg, g)$. De fato,$\langle f, g\rangle \subset \langle f - qg, g\rangle$. Tome $h \in \langle f, g\rangle$, pela definição de ideal gerado temos $h = Af + Bg$ para determinados $A, B \in \mathbb{K}[x]$. Então

$$h = Af + Bg = Af - Aqg + Bg + Aqg = A(f - qg) + (B + Aq)g$$

isto é, $h \in \langle f - qg, g\rangle$. Para provar a outra inclusão tome $s \in \langle f - qg, g\rangle$, assim

$$s = C(f - qg) + Dg = Cf - Cqg + Dg = Cf + (D - Cq)g \in \langle f, g\rangle$$

□

[3] Euclides de Alexandria (300 AC), inicia o seu livro VII, da coleção *Os Elementos*, mostrando como calcular o MDC de duas medidas (números).

3.6 O problema da pertinência à um Ideal

O estudo desenvolvido até aqui resolve um problema de grande relevância neste trabalho: Dados $f_1, \ldots, f_s$ polinômios em $\mathbb{K}[x]$ há como determinar se um polinômio específico f pertence ao ideal $\langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x]$?

Como podemos descobrir se $f = x^3$ pertence ao ideal $\langle x^4 - 1, x^6 - 1 \rangle \subset \mathbb{R}[x]$? Primeiramente sabemos que todo ideal em $\mathbb{K}[x]$ é principal, e para determinar o gerador calculamos o $\mathrm{MDC}(x^4 - 1, x^6 - 1)$. Para isso, usaremos o algoritmo 2, apresentado na seção anterior. Inicialmente $h = f = x^4 - 1$ e $s = g = x^6 - 1$. Observe que dividindo $x^4 - 1$ por $x^6 - 1$ obtemos quociente nulo e o resto igual ao próprio dividendo. Agora, $h = x^6 - 1$ e $s = x^4 - 1$. Continuando o algoritmo agora temos que dividir $x^6 - 1$ por $x^4 - 1$

$$\begin{array}{rr|l} x^6 & -1 & x^4 - 1 \\ \cline{3-3} -x^6 + x^2 & & x^2 \\ \cline{1-1} x^2 - 1 & & \end{array}$$

Continuando o algoritmo, agora com $h = x^4 - 1$ e $x^2 - 1$

$$\begin{array}{rr|l} x^4 & -1 & x^2 - 1 \\ \cline{3-3} -x^4 + x^2 & & x^2 + 1 \\ \cline{1-1} x^2 - 1 & & \\ -x^2 + 1 & & \\ \cline{1-1} 0 & & \end{array}$$

Nesta etapa, obtemos $h = x^2 - 1$ e $s = 0$. Assim, $\mathrm{MDC}(x^4 - 1, x^6 - 1) = \mathrm{MDC}(x^2 - 1, 0) = x^2 - 1$. Com este cálculo, fica provado que $\langle x^4 - 1, x^6 - 1 \rangle = \langle x^2 - 1 \rangle \subset \mathbb{K}[x]$

A pergunta então fica muito mais simples, e é a mesma que havíamos deixado em aberto, na página 23: Como determinar se $f = x^3$ pertence ao ideal $\langle x^2 - 1 \rangle \subset \mathbb{R}[x]$? Agora podemos usar o algoritmo da divisão para dividir $f = x^3$ por $x^2 - 1$ e obter $x^3 = (x^2 - 1)x + x$. Como o resto obtido é x, e temos a garantia que esse resto é o único possível, então fica demonstrado que $f = x^3$ não pode ser escrito como um múltiplo de $x^2 - 1$, isto é, $f = x^3$ *não* pertence ao ideal $\langle x^2 - 1 \rangle = \langle x^4 - 1, x^6 - 1 \rangle$. É verdade que $f \in \langle h \rangle$, $h \in \mathbb{K}[x]$ se e somente se o resto da divisão de f por h for zero.

3.7 Polinômios em $\mathbb{K}[x_1, \ldots, x_n]$

Nesta seção apresentaremos o conjunto $\mathbb{K}[x_1, \ldots, x_n]$ dos polinômios em várias indeterminadas com coeficientes num corpo $\mathbb{K}$. A partir de agora, esse será o ambiente onde efetuaremos nossos cálculos.

Para começar a entender este conjunto, relembre que, se D for um domínio, então $D[x]$ também será um domínio de integridade (apêndice seção A.1). Desta forma, podemos visualizar o conjunto $(D[x])[y]$ também como um domínio integridade, formado pelos polinômios na indeterminada y e com "coeficientes" no domínio $D[x]$. Na verdade, estes "coeficientes" em $D[x]$ são polinômios. Mostramos no apêndice seção A.2, que $(D[x])[y] = (D[y])[x] = D[x, y]$, ou seja, $D[x, y]$ pode ser interpretado como formado por polinômios nas indeterminadas x e y com coeficientes num domínio de integridade D. Indutivamente podemos seguir com esse raciocínio e concluir que $D[x_1, \ldots, x_n]$ é um domínio de integridade, formado por polinômios de várias indeterminadas e coeficientes num domínio D. Toda essa análise é válida substituindo o domínio D por um corpo $\mathbb{K}$, pois todo corpo é um domínio.

Um monômio em $\mathbb{K}[x_1, \ldots, x_n]$ é uma expressão da forma

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

Adotaremos a seguinte notação para esses monômios:

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} = X^\alpha \text{ com } \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}_+^n$$

O *grau total* desse monômio é definido por $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$

Dessa forma, estabelecemos uma relação biunívoca entre os monômios de $\mathbb{K}[x_1, \ldots, x_n]$ e o conjunto dos vetores com entradas inteiras não negativas $\mathbb{Z}_+^n$.

Assim, podemos escrever um polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ como

$$f = a_{\alpha_1} X^{\alpha_1} + \cdots + a_{\alpha_p} X^{\alpha_p},\ a_{\alpha_i} \in \mathbb{K},\ \alpha_i \in \mathbb{Z}_+^n,\ p \in \mathbb{Z}_+ \text{ e } 1 \leq i \leq p$$

e definir o seu *grau total* como sendo $\max\{|\alpha_i| : 1 \leq i \leq p\}$. Também podemos representar

$$\mathbb{K}[x_1, \ldots, x_n] = \left\{ \sum_{i=1}^{p} a_{\alpha_i} X^{\alpha_i} : a_{\alpha_i} \in \mathbb{K},\ \alpha_i \in \mathbb{Z}_+^n,\ p \in \mathbb{Z}_+ \right\}$$

Exemplo 9. Considere os monômios abaixo:

1. $x^2yz^3 = X^\alpha \in \mathbb{Q}[x, y, z]$. Neste caso $\alpha = (2, 1, 3) \in \mathbb{Z}_+^3$ e o grau total é $|\alpha| = 6$
2. $xy^4z^2w^7 = X^\alpha \in \mathbb{R}[x, y, z, w]$. Neste caso $\alpha = (1, 4, 2, 7) \in \mathbb{Z}_+^4$, e o grau total é $|\alpha| = 14$

Exemplo 10. Considere o polinômio

$$f = 5x^2y^3z - 4x^3z - 2x^6y^3 = a_{\alpha_1} X^{\alpha_1} + a_{\alpha_2} X^{\alpha_2} + a_{\alpha_3} X^{\alpha_3}$$

Neste exemplo temos:
$a_{\alpha_1} = 5$, $a_{\alpha_2} = -4$, $a_{\alpha_3} = -2$, $\alpha_1 = (2,3,1)$, $\alpha_2 = (3,0,1)$, $\alpha_3 = (6,3,0)$,

Na próxima seção estenderemos o Algoritmo da Divisão para polinômios de várias indeterminadas. Para isso, precisaremos das Ordens Monomiais.

3.8 Ordem Monomial em $\mathbb{K}[x_1, \ldots, x_n]$

O ingrediente fundamental do algoritmo da divisão que vimos anteriormente é a diminuição do grau do dividendo a cada etapa. Para que isso ocorra, ordenamos os polinômios por grau decrescente e sistematicamente efetuamos cancelamentos com os termos líderes. Com esses cancelamentos o grau do dividendo diminui até eventualmente chegar a zero ou a um resto com grau menor do que o do divisor. Para que possamos estender o algoritmo da divisão para várias indeterminadas o primeiro passo é criar uma forma de ordenar polinômios em $\mathbb{K}[x_1, \ldots, x_n]$. Apresentaremos formas de colocar esses polinômios em ordem crescente ou decrescente sem ambiguidade.

Definição 11. *Uma relação de ordem sobre um conjunto $A \neq \varnothing$ é uma relação $\succcurlyeq$ que satisfaz:*

1. *$a \succcurlyeq a$ para todo $a \in A$ (Reflexividade);*
2. *Se $a, b \in A$ são tais que $a \succcurlyeq b$ e $b \succcurlyeq a$ então $a = b$. (Antissimetria);*
3. *Dados $a, b, c \in A$ com $a \succcurlyeq b$ e $b \succcurlyeq c$, então $a \succcurlyeq c$ (Transitividade).*

Quando ocorrer $a \succcurlyeq b$ com $a \neq b$ escreveremos $a \succ b$.

Definição 12. *Uma relação de ordem $\succcurlyeq$ sobre um conjunto $A \neq \varnothing$ é total, se para quaisquer $a, b \in A$ tem-se*

$$a \succ b,\ b \succ a \text{ ou } a = b$$

Como já foi visto, o conjunto dos monômios de $\mathbb{K}[x_1, \ldots, x_n]$ pode ser identificado com o conjunto dos vetores com entradas inteiras não negativas $\mathbb{Z}_+^n$. Desse modo, definir uma ordem no conjunto dos monômios equivale a definir uma ordem em $\mathbb{Z}_+^n$. Os resultados que serão apresentados para $\mathbb{Z}_+^n$ podem ser traduzidos, usando esta equivalência, para o conjunto dos monômios $\{X^\alpha : \alpha \in \mathbb{Z}_+^n\} \subset \mathbb{K}[x_1, \ldots, x_n]$ e reciprocamente.

Definição 13. *Uma ordem monomial em $\mathbb{K}[x_1, \ldots, x_n]$ é uma relação entre os monômios X^α, com $\alpha \in \mathbb{Z}_+^n$, ou equivalentemente é uma relação $\succ$ em $\mathbb{Z}_+^n$ que satisfaz às seguintes condições:*

1. *$\succ$ é uma relação de ordem total sobre $\mathbb{Z}_+^n$, isto é, para quaisquer $\alpha, \beta \in \mathbb{Z}_+^n$, apenas uma das condições é satisfeita: $\alpha \succ \beta$, $\alpha = \beta$ ou $\beta \succ \alpha$.*

2. *Se* $\alpha \succ \beta$ *e* $\gamma \in \mathbb{Z}_+^n$ *então* $\alpha + \gamma \succ \beta + \gamma$.

3. (**Princípio da Boa Ordenação**) *O conjunto* $\mathbb{Z}_+^n$ *é bem ordenado, isto é, para todo subconjunto não vazio* S *de* $\mathbb{Z}_+^n$ *existe* $\alpha \in S$ *tal que, para todo* $\beta \in S - \{\alpha\}$, $\beta \succ \alpha$. *Neste caso, dizemos que* S *tem um menor elemento* α *com respeito à relação* $\succ$.

Exemplo 11. O grau em $\mathbb{R}[x]$ é uma ordem monomial. De fato, as três condições acima são satisfeitas:

1. O grau é uma relação de ordem total sobre $\mathbb{Z}_+$.

2. Se $i, j, k \in \mathbb{Z}_+$,com $i > j$, então $i + k > j + k$.

3. Finalmente, basta observar que $\mathbb{Z}_+$ é um conjunto bem ordenado em relação à ordem usual.

Para demonstrar que uma relação $\succ$ em $\mathbb{K}[x_1, \ldots, x_n]$ é uma ordem monomial, podemos encontrar dificuldades em justificar o item (3) da Definição (13). O próximo lema facilitará este trabalho. Além disso também desempenhará papel fundamental na demonstração de que determinados algoritmos terminam.

Lema 1. *O conjunto* $\mathbb{Z}_+^n$ *é dito bem ordenado com respeito à relação* $\succ$ *se, e somente se, toda sequência estritamente decrescente em* $\mathbb{Z}_+^n$

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

é finita.

Demonstração. Equivalentemente, vamos provar que $\mathbb{Z}_+^n$ não é bem ordenado se, e só se, existe uma sequência infinita estritamente decrescente em $\mathbb{Z}_+^n$. De fato, se $\mathbb{Z}_+^n$ não é bem ordenado, então algum subconjunto não vazio $S \subset \mathbb{Z}_+^n$ não possui um menor elemento. Assim, tomando $\alpha_1 \in S$, podemos encontrar $\alpha_2 \in S$, com $\alpha_1 \succ \alpha_2$. Analogamente, α_2 não é o menor elemento de S, logo existe $\alpha_3 \in S$, com $\alpha_2 \succ \alpha_3$. Desta forma, formamos uma sequência infinita $\{\alpha_i\}_{i=1}^{\infty}$ estritamente decrescente. Reciprocamente, dada uma sequência infinita $\alpha_1 \succ \alpha_2 \succ \alpha_3 \succ \cdots$, temos que $\{\alpha_1, \alpha_2, \alpha_3, \ldots\}$ é um subconjunto não vazio de $\mathbb{Z}_+^n$ que não possui menor elemento e, por isso, $\mathbb{Z}_+^n$ não é bem ordenado. □

Definição 14 (Ordem Lexicográfica "LEX")**.** *Sejam* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *e* $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}_+^n$. *Dizemos que* $X^\alpha >_{\text{LEX}} X^\beta$ *se* $\alpha \neq \beta$ *e no vetor diferença* $\alpha - \beta \in \mathbb{Z}^n$, *a primeira entrada não nula, da esquerda para direita, é positiva. Também podemos representar essa relação usando a notação vetorial* $\alpha >_{\text{LEX}} \beta$.

Exemplo 12. Em $\mathbb{Q}[x, y, z, w]$ temos:

1. $x^3y^2z^6w >_{\text{LEX}} xy^5z^8w^3$ já que o vetor $(3,2,6,1)-(1,5,8,3)=(2,-3,-2,-2)$ tem a primeira entrada não-nula, da esquerda para a direita, positiva. Isto é, $(3,2,6,1) >_{\text{LEX}} (1,5,8,3)$.

2. $w^2 >_{\text{LEX}} w^1$, já que o vetor $(0,0,0,2)-(0,0,0,1)=(0,0,0,1)$ tem a primeira entrada não-nula, da esquerda para a direita, positiva. Isto é, $(0,0,0,2) >_{\text{LEX}} (0,0,0,1)$.

3. $x >_{\text{LEX}} y >_{\text{LEX}} z >_{\text{LEX}} w$, já que $(1,0,0,0) >_{\text{LEX}} (0,1,0,0) >_{\text{LEX}} (0,0,1,0) >_{\text{LEX}} (0,0,0,1)$.

Com o auxílio do Lema 1, provaremos na próxima proposição que a relação definida acima é uma ordem monomial.

Proposição 6. *A ordem lexicográfica em $\mathbb{Z}_+^n$ é uma ordem monomial.*

Demonstração. Vamos provar que as condições da definição de ordem monomial são satisfeitas. De fato:

1. Para verificar que $>_{\text{LEX}}$ é relação de ordem total, basta usar o fato de que $\mathbb{Z}$ é um anel totalmente ordenado.

2. Se $\alpha >_{\text{LEX}} \beta$, então temos que a primeira entrada não nula (da esquerda para direita) em $\alpha-\beta$, digamos $\alpha_k-\beta_k$, é positiva. Como $X^\alpha X^\gamma = X^{\alpha+\gamma}$ e $X^\beta X^\gamma = X^{\beta+\gamma}$ então, por hipótese, a primeira entrada não nula (da esquerda para direita) de $(\alpha+\gamma)-(\beta+\gamma)=\alpha-\beta$ é $\alpha_k-\beta_k>0$. Logo, $(\alpha+\gamma) >_{\text{LEX}} (\beta+\gamma)$, provando assim que vale o segundo item da definição de ordem monomial.

3. Suponha que, com respeito à ordem $>_{\text{LEX}}$, $\mathbb{Z}_+^n$ não seja um conjunto bem ordenado. Então, pelo Lema 1, existe uma sequência infinita e estritamente decrescente

$$\alpha^1 >_{\text{LEX}} \alpha^2 >_{\text{LEX}} \alpha^3 >_{\text{LEX}} \cdots \tag{3.1}$$

de elementos de $\mathbb{Z}_+^n$. Considere a sequência $\{\alpha_1^i\}_{i=1}^\infty$, onde α_1^i é a primeira entrada do vetor α^i da sequência (3.1). Pela definição da ordem lexicográfica, $\{\alpha_1^i\}_{i=1}^\infty$ é uma sequência de inteiros não negativos e não crescente, com relação a ordem usual $>$. Como $\mathbb{Z}_+$ é bem ordenado em relação à ordem usual, a sequência $\{\alpha_1^i\}_{i=1}^\infty$ estaciona, isto é, existe um inteiro k tal que $\alpha_1^i=\alpha_1^k$, para todo $i\geq k$. A sequência de inteiros não negativos $\{\alpha_2^i\}_{i=k}^\infty$, formada pela segunda entrada de cada elemento da sequência $\alpha^k, \alpha^{k+1}, \ldots$, também é não crescente em relação à ordem usual $>$. De forma análoga, a sequência $\{\alpha_2^i\}_{i=k}^\infty$ estaciona. Continuando com este procedimento, vamos concluir que, para algum l, $\alpha^l, \alpha^{l+1}, \ldots$ são todos iguais, já que a sequência (3.1) é formada por vetores com n entradas. Isto contradiz o fato da sequência (3.1) ser estritamente decrescente. Assim, provamos que vale o terceiro item da definição de ordem monomial e, portanto, provamos a proposição.

□

De forma análoga, podemos provar que as relações definidas adiante também são ordens monomiais.

Definição 15 (Ordem Lexicográfica Graduada "GRLEX"). *Sejam α e $\beta \in \mathbb{Z}_+^n$. Dizemos que $x^\alpha >_{\text{GRLEX}} X^\beta$ se*

1. $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, *onde $>$ é a ordem usual em $\mathbb{N}$, ou*
2. $|\alpha| = |\beta|$ *e* $\alpha >_{\text{LEX}} \beta$.

Observe que a ordem lexicográfica graduada ordena primeiro pelo grau total e depois desempata com a ordem lexicográfica.

Exemplo 13. Em $\mathbb{Q}[x, y, z]$,temos:

1. $xy^4z^5 >_{\text{GRLEX}} x^5yz$ já que $|(1, 4, 5)| = 10 > |(5, 1, 1)| = 7$.
2. $x^3y^2z >_{\text{GRLEX}} x^3yz^2$ já que $|(3, 2, 1)| = 6 = |(3, 1, 2)|$ e $(3, 2, 1) >_{\text{LEX}} (3, 1, 2)$.

Definição 16 (Ordem Lexicográfica Reversa Graduada "GREVLEX"). *Sejam α e $\beta \in \mathbb{Z}_+^n$. Dizemos que $X^\alpha >_{\text{GREVLEX}} X^\beta$ se*

1. $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, *onde $>$ é a ordem usual em $\mathbb{N}$, ou*
2. $|\alpha| = |\beta|$, $\alpha \neq \beta$ *e a primeira entrada não nula, da direita para a esquerda, de $\alpha - \beta \in \mathbb{Z}^{\text{n}}$ é negativa.*

Exemplo 14. Em $\mathbb{R}[x, y, z]$,temos:

1. $x^2y^4z^5 >_{\text{GREVLEX}} x^5yz$ já que $|(2, 4, 5)| = 11 > |(5, 1, 1)| = 7$.
2. $x^3y^2z >_{\text{GREVLEX}} x^3yz^2$ já que $|(3, 2, 1)| = 6 = |(3, 1, 2)|$ e em $\alpha - \beta = (0, 1, -1)$ temos a primeira entrada não nula, da direita para esquerda, negativa.

Para encerrar a seção, veremos como uma ordem monomial pode ser aplicada em polinômios. Para isso, dados um polinômio $f = \sum_\alpha a_\alpha X^\alpha$ e uma ordem monomial $\succ$ em $\mathbb{K}[x_1, \ldots, x_n]$, podemos ordenar os monômios de f usando a ordem $\succ$. Por exemplo, se $f = x^3y - 3x^4y^2z - xy^2z \in \mathbb{Q}[x, y, z]$, então podemos reordenar, usando a ordem lexicográfica, os termos de f de forma decrescente como

$$f = -3x^4y^2z + x^3y - xy^2z$$

Neste sentido, segue a próxima definição cuja terminologia é a mesma usada anteriormente.

Definição 17. *Sejam $f = \sum_\alpha a_\alpha X^\alpha$ um polinômio não nulo em $\mathbb{K}[x_1, \ldots, x_n]$, $\mathbb{K}$ corpo e $\succ$ uma ordem monomial.*

1. *$a_\alpha X^\alpha$ é um termo de f.*
2. *X^α é um monômio de f.*
3. *O multigrau de f é o vetor n-dimensional*

$$\operatorname{multideg}(f) = \max\{\alpha \in \mathbb{Z}_+^n : a_\alpha \neq 0\},$$

   onde o máximo é tomado com respeito a ordem monomial $\succ$.

4. *O coeficiente líder de f é*

$$\operatorname{LC}(f) = a_{\operatorname{multideg}(f)} \in \mathbb{K}$$

5. *O monômio líder de f é*

$$\operatorname{LM}(f) = X^{\operatorname{multideg}(f)}$$

6. *O termo líder de f é*

$$\operatorname{LT}(f) = \operatorname{LC}(f) \cdot \operatorname{LM}(f)$$

Exemplo 15. Sejam $f = -3x^4y^2z + x^3y - xy^2z \in \mathbb{R}[x, y, z]$ e $\succ$ a ordem lex. Então,

$$\operatorname{multideg}(f) = (4, 2, 1)$$

$$\operatorname{LC}(f) = -3$$

$$\operatorname{LM}(f) = x^4y^2z$$

$$\operatorname{LT}(f) = -3x^4y^2z$$

As propriedades de multigrau, listadas na próxima proposição, são generalizações das propriedades de grau para polinômios em uma variável vistas anteriormente.

Proposição 7. *Sejam f,g polinômios não nulos em $\mathbb{K}[x_1, \ldots, x_n]$ e $\succ$ uma ordem monomial. Então,*

1. $\operatorname{LT}(fg) = \operatorname{LT}(f)\operatorname{LT}(g)$
2. $\operatorname{multideg}(fg) = \operatorname{multideg}(f) + \operatorname{multideg}(g)$
3. *Se $f + g \neq 0$, temos que* $\max\{\operatorname{multideg}(f), \operatorname{multideg}(g)\} \succ \operatorname{multideg}(f + g)$ *ou* $\max\{\operatorname{multideg}(f), \operatorname{multideg}(g)\} = \operatorname{multideg}(f+g)$. *Valendo sempre a igualdade quando* $\operatorname{multideg}(f) \neq \operatorname{multideg}(g)$.

Demonstração. Sejam

$$f = \sum_{\alpha} a_\alpha X^\alpha, \text{ com } \mathrm{LT}(f) = a_{\alpha(0)} X^{\alpha(0)},\ a_{\alpha(0)} \neq 0 \text{ e}$$

$$g = \sum_{\beta} b_\beta X^\beta, \text{ com } \mathrm{LT}(g) = b_{\beta(0)} X^{\beta(0)},\ b_{\beta(0)} \neq 0$$

1. Temos
$$fg = \sum_{\alpha,\beta} a_\alpha b_\beta X^\alpha X^\beta$$
Pela definição 17, temos garantia de que $X^{\alpha(0)} \succcurlyeq X^\alpha$ para todo α, e $X^{\beta(0)} \succcurlyeq X^\beta$ para todo β. Daí, $X^{\alpha(0)}X^{\beta(0)} \succcurlyeq X^{\alpha(0)}X^\beta \succcurlyeq X^\alpha X^\beta$ para todo $\alpha,\ \beta$. Como $a_{\alpha(0)}b_{\beta(0)} \neq 0$, temos assim que $\mathrm{LT}(fg) = a_{\alpha(0)}b_{\beta(0)}X^{\alpha(0)}X^{\beta(0)} = a_{\alpha(0)}X^{\alpha(0)}b_{\beta(0)}X^{\beta(0)} = \mathrm{LT}(f)\,\mathrm{LT}(g)$

2. Usando o item anterior, temos que o termo líder do produto fg é o produto dos termos líderes de f e g, assim, o multigrau de fg será o multigrau de $a_{\alpha(0)}X^{\alpha(0)}b_{\beta(0)}X^{\beta(0)} = a_{\alpha(0)}b_{\beta(0)}X^{\alpha(0)+\beta(0)}$ que é igual a $\alpha(0) + \beta(0)$, portanto $\mathrm{multideg}\,(fg) = \mathrm{multideg}(f) + \mathrm{multideg}(g)$

3. Segue imediatamente da definição de soma de polinômios e da definição de ordem monomial que $\max\{\mathrm{multideg}(f), \mathrm{multideg}(g)\} \succcurlyeq \mathrm{multideg}(f+g)$. Agora, se $\mathrm{multideg}(f) \neq \mathrm{multideg}(g)$, isto é, se $\alpha(0) \neq \beta(0)$, podemos supor, sem perda de generalidade, que $\alpha(0) \succ \beta(0)$. Como $\beta(0) \succcurlyeq \beta$, para todo β, então $\alpha(0) \succ \beta(0) \succcurlyeq \beta$, para todo β. Além disso, também temos que $\alpha(0) \succcurlyeq \alpha$, para todo α. Então, pela definição de soma de polinômios, temos que:
$$\mathrm{multideg}(f+g) = \alpha(0) = \mathrm{multideg}(f) = \max\{\mathrm{multideg}(f), \mathrm{multideg}(g)\}.$$

□

3.9 O Algoritmo da Divisão em $\mathbb{K}[x_1, \ldots, x_n]$

Nesta seção apresentaremos a divisão de f por $g \neq 0$ em $\mathbb{K}[x_1, \ldots, x_n]$. Verificaremos que a divisão termina quando o resto for zero ou não apresentar nenhum termo divisível pelo termo líder de g. Aqui usaremos outra formatação para a divisão. A nossa intenção é a familiarização com as notações adotadas no Algoritmo da Pseudodivisão, que será apresentado na próxima seção.

Exemplo 16. Consideremos $f = x^3 + x^2y + xy^3 + y^3$ e $g = x + y^2$ polinômios em $\mathbb{R}[x, y]$. Usando a ordem lexicográfica graduada, vamos dividir f por g. Para começar, ordenaremos os polinômios com a ordem GRLEX:

$$f = xy^3 + x^3 + x^2y + y^3, \text{ e } g = y^2 + x$$

e os organizaremos numa tabela como se segue:

g	f
y^2+x	$xy^3+x^3+x^2y+y^3$
$q=$	

Observe que $\mathrm{LT}(g)=y^2$ divide $\mathrm{LT}(f)=xy^3$, então o primeiro quociente encontrado é $\frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}=xy$. Subtraindo $xy\cdot g=xy^3+x^2y$ de f obtemos x^3+y^3. Observe abaixo, o quadro atualizado:

g	f
y^2+x	$xy^3+x^3+x^2y+y^3$
xy	$\underline{-xy^3-x^2y}$
	x^3+y^3
$q=xy$	

Note agora que $\mathrm{LT}(g)=y^2$ não divide $\mathrm{LT}(x^3+y^3)=x^3$, porém dividiria y^3 que é um termo menor deste dividendo (segundo a ordem GRLEX). Como a ideia básica da divisão é que nenhum termo do resto seja divisível pelo termo líder de g, vamos adicionar o termo x^3 ao resto e continuar dividindo a expressão remanescente y^3. Essa é a grande diferença entre a divisão em $\mathbb{K}[x]$ e a divisão em $\mathbb{K}[x_1,\ldots,x_n]$: No caso de uma indeterminada, se $\mathrm{LT}(g)$ não divide $\mathrm{LT}(f)$ então $\mathrm{LT}(g)$ não divide nenhum outro termo de f. Para continuar o processo de divisão, adicionaremos ao nosso quadro um coluna extra que acumulará os restos.

g	f	r
y^2+x	$xy^3+x^3+x^2y+y^3$	
xy	$\underline{-xy^3-x^2y}$	
	$\cancel{x^3}+y^3$	x^3
$q=xy+y$		

Continuamos a divisão, agora com o termo x^3 já na coluna dos restos. Observe que $\mathrm{LT}(g)=y^2$ divide $\mathrm{LT}(y^3)=y^3$ e o quociente é y. Agora, subtraindo $y\cdot g=y^3+xy$ do dividendo y^3 obtemos $-xy$.

g	f	r
y^2+x	$xy^3+x^3+x^2y+y^3$	
xy	$\underline{-xy^3-x^2y}$	
	$\cancel{x^3}+y^3$	x^3
y	$\underline{-y^3-xy}$	
	$-xy$	
$q=xy+y$		x^3

Como $-xy$ não é divisível por $\mathrm{LT}(g)=y^2$ a divisão acaba e o termo $-xy$ é adicionado aos restos. Assim obtemos $f=qg+r$ onde $q=xy+y$ e $r=x^3-xy$. Observe que a característica do resto é que nenhum dos seus termos é divisível por $\mathrm{LT}(g)=y^2$.

g	f	r
y^2+x	$xy^3+x^3+x^2y+y^3$	
xy	$\underline{-xy^3-x^2y}$	
	$\cancel{x^3}+y^3$	x^3
y	$\underline{-y^3-xy}$	
	$\cancel{-xy}$	$-xy$
$q=xy+y$		x^3-xy

Exemplo 17. Vamos dividir $f=x^2y^2+x+y$ por $g=xy+y^2$ usando a ordem lexicográfica:

g	f	r
$xy+y^2$	x^2y^2+x+y	
xy	$\underline{-x^2y^2-xy^3}$	
	$-xy^3+x+y$	
$-y^2$	$\underline{xy^3+y^4}$	
	$\cancel{x+y^4+y}$	$x+y^4+y$
$q=xy+y^2$		$x+y^4+y$

Assim obtemos $f=qg+r$ onde $q=xy+y^2$ e $r=x+y^4+y$. Observe que que nenhum dos termos do resto é divisível por $\mathrm{LT}(g)=xy$.

A seguir demonstraremos o Teorema da Divisão para polinômios de várias indeterminadas.

Teorema 2 (O Teorema da Divisão em $\mathbb{K}[x_1,\ldots,x_n]$)**.** *Considere uma ordem monomial $\succ$ fixada. Dados os polinômios $f,g\in\mathbb{K}[x_1,\ldots,x_n]$ com g não nulo, existem $q,r\in\mathbb{K}[x_1,\ldots,x_n]$ unicamente determinados pelas condições*

$$f=qg+r,\ \textit{com } r=0 \textit{ ou os termos de } r \textit{ não são divisíveis por } \mathrm{LT}(g)$$

Demonstração. Se $f = 0$, então $q = r = 0$. Seja $f = f_0 \neq 0$. Se nenhum termo de f_0 for divisível por $\mathrm{LT}(g)$ então $q = 0$ e $r = f = f_0$ satisfazem o teorema. Caso contrário, defina $f_1 = f_0 - \frac{\mathrm{LT}(f_0)}{\mathrm{LT}(g)}g$. Se nenhum termo de f_1 for divisível por $\mathrm{LT}(g)$ então $q = \frac{\mathrm{LT}(f_0)}{\mathrm{LT}(g)}$ e $r = f_1$ satisfazem o teorema. Caso contrário, defina $f_2 = f_1 - \frac{\mathrm{LT}(f_1)}{\mathrm{LT}(g)}g$. Continuando dessa forma criamos uma sequência $f_{i+1} = f_i - \frac{\mathrm{LT}(f_i)}{\mathrm{LT}(g)}g$ onde sempre há uma redução no multigrau ou eventualmente, um anulamento desta diferença. De fato, usando 7.1,

$$\mathrm{LT}\left(\frac{\mathrm{LT}(f_i)}{\mathrm{LT}(g)}g\right) = \frac{\mathrm{LT}(f_i)}{\mathrm{LT}(g)}\,\mathrm{LT}(g) = \mathrm{LT}(f_i)$$

vemos que f_i e $\frac{\mathrm{LT}(f_i)}{\mathrm{LT}(g)}g$ possuem os mesmos termos líderes, portanto a sua diferença tem multigrau menor ou eventualmente pode ser nula. Dessa forma, fica formada uma sequência decrescente de multigraus, e como vimos no Lema 1, essa sequência tem que terminar em algum momento. Digamos que a sequência acaba na etapa $k \in \mathbb{N}$. Então, $f_k = f_{k-1} - \frac{\mathrm{LT}(f_{k-1})}{\mathrm{LT}(g)}g$ com nenhum termo de f_k divisível por $\mathrm{LT}(g)$ ou $f_k = 0$. Definindo

$$q = \sum_{i=0}^{k-1} \frac{\mathrm{LT}(f_i)}{\mathrm{LT}(g)} \in \mathbb{K}[x_1, \ldots, x_n] \text{ e } r = f_k$$

temos o teorema satisfeito.

Para provar a unicidade, suponha $q_1, q_2, r_1, r_2 \in \mathbb{K}[x_1, \ldots, x_n]$ tais que $q_1 g + r_1 = f = q_2 g + r_2$ com os restos nulos ou com nenhum termo de r_1 ou r_2 divisível por $\mathrm{LT}(g)$. Então,

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

Com isso, supor $r_1 \neq r_2$ nos levaria a conclusão de que $\mathrm{LT}(g)$ divide $\mathrm{LT}(r_2 - r_1)$ o que é um absurdo. Concluímos que $r_1 = r_2$. A nossa igualdade então fica

$$0 = (q_1 - q_2)g$$

Como por hipótese $g \neq 0$ e sabemos que $\mathbb{K}[x_1, \ldots, x_n]$ é um domínio de integridade então $q_1 = q_2$ e assim fica provada a unicidade.

□

Da mesma forma que em $\mathbb{K}[x]$, quando dividirmos f por $g \neq 0$ em $\mathbb{K}[x_1, \ldots, x_n]$ obtendo $f = qg + r$, chamaremos o único polinômio q de quociente e o único polinômio r de resto.

Abaixo reproduzimos o algoritmo que utilizamos para efetuar a divisão de f por g não

nulo em $\mathbb{K}[x_1, \ldots, x_n]$.

Input: $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ com $g \neq 0$
Output: q, r satisfazendo $f = qg + r$ com $r = 0$ ou nenhum termo de r divisível por $\mathrm{LT}(g)$

$q := 0$;
$r := 0$;
$h := f$;
while $h \neq 0$ **do**
    if $\mathrm{LT}(g)$ *divide* $\mathrm{LT}(h)$ **then**
        $q := q + \frac{\mathrm{LT}(h)}{\mathrm{LT}(g)}$;
        $h := h - \frac{\mathrm{LT}(h)}{\mathrm{LT}(g)} g$;
    else
        $r := r + \mathrm{LT}(h)$;
        $h := h - \mathrm{LT}(h)$;
return q, r

Algoritmo 3: O algoritmo da divisão em $\mathbb{K}[x_1, \ldots, x_n]$

3.10 O Algoritmo da Pseudodivisão em $\mathbb{K}[x_1, \ldots, x_n]$

Usando o algoritmo da divisão em $\mathbb{K}[x]$ conseguimos provar que todo ideal em $\mathbb{K}[x]$ pode ser gerado por um único elemento, isto juntamente com a unicidade do resto da divisão nos permitiu resolver o problema de decidir se um polinômio f pertence à um ideal $I \subseteq \mathbb{K}[x]$. Agora continuaremos a tratar a questão no caso de várias indeterminadas: Dados $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ como decidir se $f \in \langle f_1, \ldots, f_s \rangle$? Para isto iremos estender o algoritmo da divisão para dividir f por uma lista de polinômios $f_1, ..., f_s$.

Dividir f por uma lista de polinômios $f_1, ..., f_s$ significa escrever f da forma

$$f = q_1 f_1 + ... + q_s f_s + r \tag{3.2}$$

onde os "quocientes" $q_1, \ldots, q_s$ e o resto r são elementos de $\mathbb{K}[x_1, \ldots, x_n]$. Nos próximos exemplos, veremos que a ideia básica do algoritmo da Pseudodivisão é a mesma do algoritmo da divisão: Tentaremos cancelar o termo líder de f com respeito a uma ordem monomial fixada usando o termo líder de algum f_i. O resto, como vimos no algoritmo da divisão, terá uma caracterização especial. Vejamos alguns exemplos:

Exemplo 18. Dados $f = x^2y^2 + x + y$, $f_1 = xy + y^2$ e $f_2 = x + y$, vamos escrever f na forma $f = a_1 f_1 + a_2 f_2 + r$, usando a ordem lexicográfica. Para isto, estabelecemos a seguinte

organização para o cálculo de a_1 e a_2:

f_1	f_2	f
$xy+y^2$	$x+y$	x^2y^2+x+y
$a_1=$	$a_2=$	

Observe que tanto $\mathrm{LT}(f_1) = xy$ como $\mathrm{LT}(f_2) = x$ dividem $\mathrm{LT}(f) = x^2y^2$. Como f_1 foi listado primeiro, dividiremos x^2y^2 por xy, obtendo xy como quociente. Subtraindo $xyf_1 = x^2y^2 + xy^3$ de f, obtemos $-xy^3 + x + y$.

Vamos organizar esses resultados no esquema abaixo:

f_1	f_2	f
$xy+y^2$	$x+y$	x^2y^2+x+y
xy		$\underline{-x^2y^2-xy^3}$
		$-xy^3+x+y$
$a_1=xy$	$a_2=$	

Agora repetimos o mesmo processo para $-xy^3+x+y$. Neste caso, $\mathrm{LT}(-xy^3+x+y) = -xy^3$ também é divisível por $\mathrm{LT}(f_1)$ e por $\mathrm{LT}(f_2)$. Assim, escolhemos dividir $-xy^3 + x + y$ por f_1 obtendo $-y^2$ como quociente. Então, subtraímos $-y^2f_1 = -xy^3 - y^4$ de $-xy^3 + x + y$, obtendo $x + y^4 + y$. Agora, repetimos o processo para $x + y^4 + y$, sendo que $\mathrm{LT}(x + y^4 + y) = x$ é divisível apenas por $\mathrm{LT}(f_2)$. Veja como ficou a tabela:

f_1	f_2	f
$xy+y^2$	$x+y$	x^2y^2+x+y
xy		$\underline{-x^2y^2-xy^3}$
		$-xy^3+x+y$
$-y^2$		$\underline{xy^3+y^4}$
		$x+y^4+y$
	1	$\underline{-x-y}$
		y^4
$a_1=xy-y^2$	$a_2=1$	

Observe que o resto é $r = y^4$, pois este não é divisível nem por $\mathrm{LT}(f_1)$ e nem por $\mathrm{LT}(f_2)$. Assim podemos escrever f da seguinte forma:

$$f = (xy - y^2)f_1 + f_2 + y^4$$

Exemplo 19. Agora vamos dividir $f = x^2y + xy^2 + y^2$ por $f_1 = xy - 1$ e por $f_2 = y^2 - 1$, usando a ordem lexicográfica.

Procedendo exatamente como no exemplo acima, obtemos:

f_1	f_2	f
$xy-1$	y^2-1	$x^2y+xy^2+y^2$
x		$\underline{-x^2y+x}$
		xy^2+x+y^2
y		$\underline{-xy^2+y}$
		$x+y^2+y$
$a_1=x+y$	$a_2=$	

Observe que, $\mathrm{LT}(x+y^2+y)=x$ não é divisível por $\mathrm{LT}(f_1)$ nem por $\mathrm{LT}(f_2)$. Porém o termo y^2 de $x+y^2+y$ é divisível por $\mathrm{LT}(f_2)=y^2$. Da mesma forma como no exemplo 16, iremos considerar como resto, o polinômio cujos termos não são divisíveis por nenhum dos termos líderes dos f_i's. Então para obter um resto com tal característica, daremos continuidade ao algoritmo da seguinte forma:

Criamos, à direita da tabela acima, uma coluna r onde colocamos o termo $\mathrm{LT}(x+y^2+y)=x$ que não é divisível por $\mathrm{LT}(f_1)$ nem por $\mathrm{LT}(f_2)$, conforme a tabela:

$f_1=xy-1$	$f_2=y^2-1$	$f=x^2y+xy^2+y^2$	r
x		$\underline{-x^2y+x}$	
		xy^2+x+y^2	
y		$\underline{-xy^2+y}$	
		$\cancel{x}+y^2+y$	
		y^2+y	x
$a_1=x+y$	$a_2=$		

Como $\mathrm{LT}(f_2)$ divide $\mathrm{LT}(y^2+y)$, procedemos como o usual. Caso não fosse possível efetuar a divisão por $\mathrm{LT}(f_1)$ nem por $\mathrm{LT}(f_2)$, moveríamos o então termo líder de y^2+y para a coluna dos restos até obtermos um termo líder que permita a divisão ou até este polinômio tornar-se zero. Assim temos a seguinte tabela:

$f_1 = xy - 1$	$f_2 = y^2 - 1$	$f = x^2y + xy^2 + y^2$	r
x		$\underline{-x^2y + x}$	
		$xy^2 + x + y^2$	
y		$\underline{-xy^2 + y}$	
		$\cancel{x} + y^2 + y$	
		$y^2 + y$	x
	1	$\underline{-y^2 + 1}$	
		$\cancel{y} + 1$	
		$\cancel{1}$	y
		0	1
$a_1 = x + y$	$a_2 = 1$		$x + y + 1$

Assim, o resto é $x + y + 1$, e obtemos:

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

Exemplo 20. Dividir $g = x^4y + x^3y^3 + xy^4$ por $g_1 = xy + y^3$ e $g_2 = x^4 + y$ usando a ordem lexicográfica e depois usando a ordem lexicográfica graduada.

Usando a ordem lex:

$g_1 = xy + y^3$	$g_2 = x^4 + y$	$g = x^4y + x^3y^3 + xy^4$	r
x^3		$\underline{-x^4y - x^3y^3}$	
		xy^4	
y^3		$\underline{-xy^4 - y^6}$	
		$-y^6$	
$a_1 = x^3 + y^3$	$a_2 = 0$		$-y^6$

Usando a ordem grlex:

$g_1 = y^3 + xy$	$g_2 = x^4 + y$	$g = x^3y^3 + x^4y + xy^4$	r
x^3		$\underline{-x^3y^3 - x^4y}$	
		xy^4	
xy		$\underline{-xy^4 - x^2y^2}$	
		$-x^2y^2$	
$a_1 = x^3 + xy$	$a_2 = 0$		$-x^2y^2$

Observe que ao trocar a ordem monomial tanto os quocientes como o resto mudaram. O próximo teorema formaliza as ideias expostas até agora.

Teorema 3 (Algoritmo da Pseudodivisão em $\mathbb{K}[x_1, \ldots, x_n]$)**.** *Fixada uma ordem monomial sobre $\mathbb{Z}_+^n$, considere a lista $(f_1, ..., f_s)$ de polinômios em $\mathbb{K}[x_1, \ldots, x_n]$. Então todo elemento*

$f \in \mathbb{K}[x_1, \ldots, x_n]$ pode ser escrito como

$$f = q_1 f_1 + ... + q_s f_s + r,$$

onde $q_1, ..., q_s, r \in \mathbb{K}[x_1, \ldots, x_n]$, e $r = 0$ ou os termos de r não são divisíveis por nenhum dos termos líderes dos f_i's. Chamaremos r de um resto de f na divisão por $f_1, ..., f_s$ nesta ordem.

Demonstração. O algoritmo mostrado abaixo prova a existência dos quocientes e do resto. Além disso, mostraremos que o algoritmo sempre funciona independente dos polinômios inseridos.

Input: $f_1, \ldots, f_s, f$
Output: $q_1, \ldots, q_s, r$
1 $q_1 := 0; \ldots; q_s := 0; r := 0;$
2 $p := f;$
3 **while** $p \neq 0$ **do**
4 $i := 1;$
5 ocorreudivisão := FALSE;
6 **while** $i \leq s$ **and** *ocorreudivisão := FALSE* **do**
7 **if** $\mathrm{LT}(f_i)$ *divide* $\mathrm{LT}(p)$ **then**
8 $q_i := q_i + \mathrm{LT}(p)/\mathrm{LT}(f_i);$
9 $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i;$
10 ocorreudivisão := TRUE;
11 **else**
12 $i := i + 1;$
13 **if** *ocorreudivisão := FALSE* **then**
14 $r := r + \mathrm{LT}(p);$
15 $p := p - \mathrm{LT}(p);$
16 **return** $q_1, \ldots, q_s, r$

Algoritmo 4: O algoritmo da Pseudodivisão em $\mathbb{K}[x_1, \ldots, x_n]$

Como podemos observar nas linhas 2, 3, 7, 9 e 15, a variável p representa o dividendo nos seus diferentes estágios da divisão, enquanto que r é o resto que (possivelmente) vai se acumulando cada vez que nenhum dos $\mathrm{LT}(f_i)$ divide $\mathrm{LT}(p)$ (linhas 1,13 e 14). A variável boleana "ocorreudivisão" é iniciada como *FALSE* e muda para *TRUE* quando ocorreu uma divisão, isto é, algum dos $\mathrm{LT}(f_i)$ divide $\mathrm{LT}(p)$. Dentro do loop principal, iniciado na linha 6, somente duas coisas podem acontecer: Ocorrer uma divisão, no caso em que algum dos $\mathrm{LT}(f_i)$ divide $\mathrm{LT}(p)$, ou, não ocorrer uma divisão, no caso em que nenhum dos $\mathrm{LT}(f_i)$ dividir $\mathrm{LT}(p)$. Neste caso, o resto r é acrescido de $\mathrm{LT}(p)$ enquanto o dividendo p é subtraído de $\mathrm{LT}(p)$.

Para mostrar que o algoritmo funciona mostraremos que em todos estágios de sua execução vale

$$f = q_1 f_1 + ... + q_s f_s + p + r \tag{3.3}$$

Para os valores iniciais $q_1 = 0, \ldots, q_s = 0, r = 0$ e $p = f$ a relação (3.3) é óbvia. Agora suponha que estamos num determinado estágio do algoritmo com a a relação (3.3) válida. Se o próximo passo for o de divisão, é porque algum dos $\mathrm{LT}(f_i)$ divide $\mathrm{LT}(p)$. Então

$$q_i f_i + p = (q_i + \mathrm{LT}(p)/\mathrm{LT}(f_i))f_i + (p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i)$$

e assim $q_i f_i + p$ não muda e assim a relação (3.3) continua válida. Se for o caso em que nenhum dos $\mathrm{LT}(f_i)$ dividir $\mathrm{LT}(p)$ o resto r e p mudam porém a soma $r + p$ não muda pois adicionamos $\mathrm{LT}(p)$ à r e subtraímos $\mathrm{LT}(p)$ de p. Dessa maneira a relação (3.3) continua válida. O algoritmo pára quando $p = 0$ e nessa situação a relação (3.3) se torna

$$f = q_1 f_1 + ... + q_s f_s + r$$

Além disso, por construção, é claro que no final do processo de divisão teremos $r = 0$ ou que nenhum dos termos de r é divisível por algum $\mathrm{LT}(f_i)$

Para mostrar que o algoritmo, em algum momento, tem que terminar, basta mostrar que p sempre diminui o seu multigrau ou que p se torna nulo. De fato, se no processo de divisão, for possível dividir, p se tornará $p' = p - \mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$. Mas como sabemos, o grau do produto de polinômios é a soma dos graus dos polinômios então

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

Como p e $\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$ tem os termos líderes iguais então a sua diferença p' tem que ter multigrau menor quando $p' \neq 0$.

Por outro lado, se no processo de divisão não for possível dividir, então $p' = p - \mathrm{LT}(p)$. Assim temos que ter $\mathrm{multideg}(p') < \mathrm{multideg}(p)$ quando $p' \neq 0$. Em qualquer um dos dois casos o multigrau sempre diminui. Se o algoritmo nunca terminasse, teríamos uma sequência infinita decrescente de multigraus, um absurdo pelo princípio da boa ordenação para ordens monomiais. Então p se torna nulo num número finito de passos do algoritmo. □

Apesar de termos um algoritmo de pseudodivisão para polinômios em $\mathbb{K}[x_1, \ldots, x_n]$, este ainda não satisfaz a importante propriedade do algoritmo da divisão. Já vimos que ao trocar a ordem monomial o resto pode mudar, como no exemplo (20). Mesmo usando a mesma ordem monomial, podem-se obter restos distintos. Vamos ilustrar este fato no próximo exemplo.

Exemplo 21. Sejam $f = y^2x - x$, $g = y^2 - x$ e $h = xy - y$. Usando a ordem lexicográfica graduada, se enumerarmos $f_1 = g$ e $f_2 = h$, então, aplicando o algoritmo da pseudodivisão, teremos $f = xf_1 + 0 \cdot f_2 + (x^2 - x)$, mas se enumerarmos $f_1 = h$ e $f_2 = g$ teremos $f = yf_1 + 1 \cdot f_2$.

Esse exemplo mostra que, se ao aplicarmos o algoritmo da divisão obtemos $r = 0$, então $f = \sum_{i=1}^{s} a_i f_i$, isto é, $f \in \langle f_1, \ldots, f_s \rangle$. Porém se $f = \sum_{i=1}^{s} q_i f_i + r$ com $r \neq 0$, então não

podemos afirmar que $f \notin \langle f_1, \ldots, f_s \rangle$, uma vez que o algoritmo não garante a unicidade do resto. Desse modo, o algoritmo da Pseudodivisão apresentado no teorema acima não é uma generalização perfeita do algoritmo da divisão para polinômios em uma indeterminada. No entanto, na Proposição 9, veremos que existe um tipo particular de ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ em que verificaremos facilmente quando um dado polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ pertence ou não a I.

4 SISTEMAS POLINOMIAIS

Muitas das aplicações práticas das Bases de Gröbner recaem na resolução de sistemas polinomiais, como é o caso da resolução de sudokus, coloração de grafos, quebra de sistemas criptográficos, dentre muitos outros. Neste capítulo, apresentaremos qual é a vantagem de usar essas bases para resolver esses complicados sistemas.

4.1 Sistemas Polinomiais em Várias Indeterminadas

Uma das mais importantes aplicações para as Bases de Gröbner, é a resolução de Sistemas Polinomiais em Várias Variáveis. Para entender este uso das Bases de Gröbner, é importante observar que um ideal polinomial tem uma relação muito importante com um sistema de equações polinomiais. Sejam $f_1, \ldots, f_s$ e $g_1, \ldots, g_t$ bases de um mesmo ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Consideremos os sistemas de equações associados a cada conjunto gerador:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \ldots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases} \qquad \begin{cases} g_1(x_1, \ldots, x_n) = 0 \\ g_2(x_1, \ldots, x_n) = 0 \\ \ldots \\ g_t(x_1, \ldots, x_n) = 0 \end{cases}$$

Como por hipótese $\langle f_1, \ldots, f_s \rangle = I = \langle g_1, \ldots, g_t \rangle$, podemos escrever cada g_j como combinação dos f_i's, isto é,

$$g_j = \sum_i c_{j,i} f_i, \text{ para } 1 \leq j \leq t$$

Analogamente, cada f_i pode ser escrito como combinação dos g_j's.

$$f_i = \sum_j d_{i,j} g_j, \text{ para } 1 \leq i \leq s$$

Dessa forma, se temos $(a_1, \ldots, a_n) \in \mathbb{C}^n$ tal que $f_i(a_1, \ldots, a_n) = 0$ para $1 \leq i \leq s$ então

$$g_j(a_1, \ldots, a_n) = \sum_i c_{j,i} f_i(a_1, \ldots, a_n) = 0, \text{ para } 1 \leq j \leq t$$

Concluímos que se $(a_1, \ldots, a_n)$ é solução do sistema de equações formado pelos polinômios g_j's, então $(a_1, \ldots, a_n)$ é solução do sistema formado pelos polinômios f_i's.

Analogamente, prova-se que toda solução do sistema formado pelos f_i's é solução do sistema formado pelos g_j's.

Em resumo, mostramos que se temos duas bases diferentes para o mesmo ideal I, então as soluções dos sistemas associados a cada conjunto gerador são as mesmas.

Para ser mais específico, consideremos o seguinte sistema em $\mathbb{C}[x, y, z]$:

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

Calculando uma base de Gröbner[1], usando a ordem lexicográfica, para o ideal $I = \langle x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z\rangle$ obtemos que I pode ser gerado por $G = \{2x - 1, 3y + z - 1, 40z^2 - 8z - 23\}$. Isto significa que o sistema (B), formado pelos polinômios dessa nova base G, é equivalente ao sistema inicial (A).

$$\begin{cases} 2x - 1 = 0 \\ 3y + z - 1 = 0 \\ 40z^2 - 8z - 23 = 0 \end{cases} \tag{B}$$

Observemos que o processo de resolução desse sistema equivalente seria muito mais simples do que o anterior. Poderíamos determinar os valores de z usando a última equação. Depois, substituindo os valores de z na segunda equação, determinaríamos os valores de y e, por fim, usando a primeira equação, determinaríamos o valor de x.

A grande questão é que, ao calcularmos uma base de Gröbner usando a ordem lexicográfica com $x > y > z$ para o ideal $I = \langle x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z\rangle$, encontramos uma base $G = \{2x - 1, 3y + z - 1, 40z^2 - 8z - 23\}$ mais simples. Mais especificamente, houve um processo de eliminação de variáveis. Repare que na segunda equação não há variável x, enquanto que na terceira não há variável x nem y. Este fenômeno foi provocado pela escolha da ordem lexicográfica com $x > y > z$. Não é uma coincidência que esse processo se assemelhe ao processo de Eliminação Gaussiana (ou escalonamento) de sistemas lineares. Na verdade, podemos dizer que o processo de eliminação Gaussiana é um caso particular do processo de obtenção de uma Base de Gröbner.

Para exemplificar, consideremos o sistema linear abaixo:

$$\begin{cases} x + y + z = 6 \\ 2x - 3y + 2z = 2 \\ 5x + 2y - z = 6 \end{cases} \tag{C}$$

Ao calcularmos uma Base de Gröbner, usando a ordem lexicográfica com $x > y > z$, para o ideal $I = \langle x+y+z-6, 2x-3y+2z-2, 5x+2y-z-6\rangle$ obtemos $G = \{x+y+z-6, y-2, z-3\}$ que nada mais é do que o sistema (C) escalonado

[1] Veremos no capítulo Capítulo 5 como calcular uma Base de Gröbner para um ideal.

$$\begin{cases} x + y + z - 6 = 0 \\ y - 2 = 0 \\ z - 3 = 0 \end{cases}$$

O próximo capítulo apresentará os resultados e algoritmos necessários para o cálculo de uma Base de Gröbner.

5 BASES DE GRÖBNER

Neste capítulo apresentaremos a teoria básica das Bases de Gröbner. Algumas demonstrações foram reservadas para uma leitura posterior no apêndice, seção A.3, da dissertação.

5.1 Ideais Monomiais

Ideais monomiais são a ponte para obter os resultados para Ideais Polinomiais. Nesta seção apresentaremos o importante Lema de Dickson, que desempenhará papel fundamental na teoria das Bases de Gröbner.

A proposição a seguir nos ajudará a mostrar que dois ideais são iguais.

Proposição 8. *Seja $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ um ideal e $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, então $f_1, \ldots, f_s \in I$ se, e somente se $\langle f_1, \ldots, f_s \rangle \subseteq I$.*

Para a demonstração, veja o apêndice seção A.3, na página 91.

Definição 18. *Um ideal I de $\mathbb{K}[x_1, \ldots, x_n]$ é dito ideal monomial, se I pode ser gerado por monômios. Neste caso, escrevemos $I = \langle X^\alpha : \alpha \in A \rangle$ para algum subconjunto $A \subset \mathbb{Z}_+^n$ (A pode ser um conjunto infinito).*

Exemplo 22.

1. $I = \mathbb{Q}[x]$ é monomial, pois em $\mathbb{Q}[x]$, $I = \mathbb{Q}[x] = \langle 1, x, x^2, x^3, \ldots \rangle = \langle 1 \rangle = \langle x^0 \rangle$.
2. $I = \langle x^3 y, xy^2 \rangle$ é ideal monomial.
3. $I = \langle x^3 + xy^4, y^2 \rangle \subseteq \mathbb{Q}[x, y]$ é monomial. Usaremos a proposição (8) para provar que $I = \langle x^3, y^2 \rangle$. De fato,$I \subseteq \langle x^3, y^2 \rangle$ pois $x^3 + xy^4 = 1 \cdot (x^3) + xy^2(y^2)$ e $y^2 = 1 \cdot (y^2) \in I$. $\langle x^3, y^2 \rangle \subseteq I$ pois $x^3 = 1 \cdot (x^3 + xy^4) - xy^2 \cdot (y^2) \in I$. Dessa forma temos $I = \langle x^3, y^2 \rangle$.
4. $I = \langle x^3, x^2 + x + 1, x - 1 \rangle \subseteq \mathbb{R}[x]$ é um ideal monomial. Mostraremos que $I = \mathbb{R}[x] = \langle 1 \rangle$. De fato, observe que $x^3 - 1 = (x^2 + x + 1)(x - 1) \in I$ e portanto $x^3 - (x^3 - 1) = 1 \in I$. Logo $I = \mathbb{R}[x] = \langle 1 \rangle$.
5. $I = \langle x^2 + 1 \rangle \subset \mathbb{R}[x]$ não é monomial. Caso contrário, como todo ideal de $\mathbb{R}[x]$ é principal, deveríamos ter $I = \langle x^n \rangle$, para algum $n \in \mathbb{N}^*$ (já que $I \neq \mathbb{R}[x]$), isto é, $x^2 + 1 = h(x)x^n$, para algum $h(x) \in \mathbb{R}[x]$. Mas isso seria um absurdo, uma vez que $x^2 + 1$ é irredutível em $\mathbb{R}[x]$.

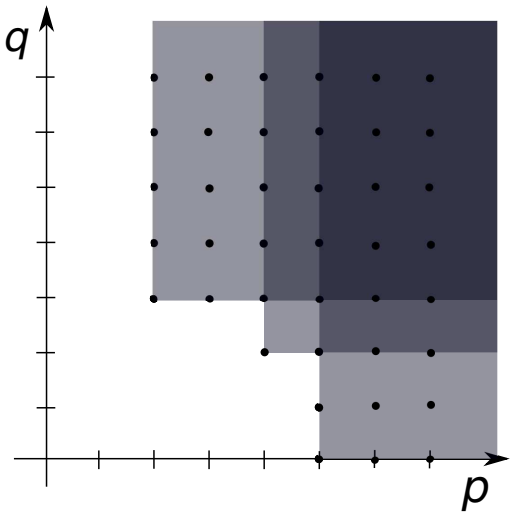
Nos próximos resultados veremos importantes propriedades dos ideais monomiais.

Proposição 9. *Seja $I = \langle X^\alpha : \alpha \in A \rangle$ um ideal monomial. Então um monômio X^β pertence ao ideal I se e somente se X^β é divisível por X^α para algum $\alpha \in A$.*

Para a demonstração, veja o apêndice seção A.3, na página 91.

Exemplo 23. Consideremos o ideal monomial $I = \langle x^2y^3, x^5, x^4y^2 \rangle \subset \mathbb{K}[x, y]$. Baseados na proposição anterior, podemos visualizar os monômios em I como o conjunto de todos os pontos de coordenadas inteiras da região escura do primeiro quadrante como na Figura 5 a seguir:

Figura 5 – Monômios de um Ideal Monomial



Fonte: O autor

Na Figura 5, cada ponto (p, q) de coordenadas inteiras corresponde a um monômio $x^p y^q$. Por exemplo, qualquer monômio múltiplo de x^2y^3 pertence a I: x^4y^4, x^5y^4, $x^6y^4, \ldots$ são monômios de I.

Como vimos acima, determinar se um monômio pertence à um ideal monomial é simples. A próxima proposição fornece uma condição necessária e suficiente para que um polinômio pertença a um ideal monomial.

Proposição 10. *Sejam I um ideal monomial de $\mathbb{K}[x_1, \ldots, x_n]$ e $f \in \mathbb{K}[x_1, \ldots, x_n]$. Então são equivalentes:*

1. *$f \in I$*
2. *todo termo de f está em I*
3. *f é uma $\mathbb{K}$-combinação linear de monômios em I*

Para a demonstração, veja o apêndice seção A.3, na página 91.

Corolário 2. *Dois ideais monomiais são iguais se e somente se eles contém os mesmos monômios.*

Demonstração. Se $I = J$, então I e J possuem os mesmos monômios. Agora, suponhamos que I e J possuam os mesmos monômios. Então, se $f \in I$, sabemos pela Proposição 10 que f é uma $\mathbb{K}$-combinação linear de monômios em I, logo é uma $\mathbb{K}$-combinação linear de monômios em J e portanto $f \in J$. De forma análoga, também podemos concluir que se $f \in J$, então $f \in I$, provando assim que $I = J$. □

Exemplo 24. O polinômio $x^4y^2 + 7x^3y^3 + xy^5 \in \langle x^3y, y^2 \rangle$, uma vez que os monômios x^4y^2, x^3y^3 e xy^5 são divisíveis pelo monômio $y^2 \in I$.

5.2 Teoria de Gröbner

Nesta seção, vamos solucionar o problema da unicidade do resto não garantida no Algoritmo da Pseudodivisão. Para isso, vamos provar que todo ideal em $\mathbb{K}[x_1, \ldots, x_n]$ possui um conjunto gerador finito, de forma que o resto da divisão de qualquer polinômio $f \in \mathbb{K}[x_1, \ldots, x_n]$ por tais geradores seja único. Essas bases, que garantem a unicidade do resto, foram nomeadas Bases de Gröbner por Buchberger em homenagem ao seu orientador Wolfgang Gröbner.

Observe que fixada uma ordem monomial, cada polinômio em $\mathbb{K}[x_1, \ldots, x_n]$ possui um único termo líder, então podemos definir o ideal dos termos líderes como abaixo.

Definição 19. *Sejam $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal não nulo e uma ordem monomial estabelecida em $\mathbb{K}[x_1, \ldots, x_n]$.*

1. *O conjunto dos termos líderes de I é o conjunto,*

$$\mathrm{LT}(I) = \{cX^\alpha : \textit{ existe } f \in I \textit{ com } \mathrm{LT}(f) = cX^\alpha,\ c \in \mathbb{K},\ \alpha \in \mathbb{Z}_+^n\}$$

2. *Denotaremos por $\langle \mathrm{LT}(I) \rangle$ o ideal gerado pelos elementos de $\mathrm{LT}(I)$.*

Observação 1. Se $I \subset \mathbb{K}[x_1, \ldots, x_n]$ é um ideal diferente de $\{0\}$, então $\langle \mathrm{LT}(I) \rangle$ é um ideal monomial. De fato, basta notar que $\mathrm{LM}(g)$ e $\mathrm{LT}(g)$ obtêm-se um do outro pelo produto de uma constante não nula. Dessa forma o ideal monomial $\langle \mathrm{LM}(g) : g \in I - \{0\} \rangle$ é igual ao ideal $\langle \mathrm{LT}(g) : g \in I - \{0\} \rangle = \langle \mathrm{LT}(I) \rangle$

Observe que, se $I = \langle f_1, \ldots, f_t \rangle$ então $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t) \rangle \subset \langle \mathrm{LT}(I) \rangle$. Por outro lado, a inclusão contrária nem sempre é garantida, como mostra o exemplo abaixo.

Exemplo 25. Seja $I = \langle f_1, f_2 \rangle$, onde $f_1 = x^3 - 2xy$ e $f_2 = x^2y - 2y^2 + x$. Usando a ordem lexicográfica graduada em $\mathbb{K}[x, y]$ temos que

$$x(x^2y - 2y^2 + x) - y(x^3 - 2xy) = x^2 \in I,$$

e portanto $\mathrm{LT}(x^2) = x^2 \in \langle \mathrm{LT}(I) \rangle$. Mas, x^2 não é divisível por $x^3 = \mathrm{LT}(f_1)$ nem por $x^2y = \mathrm{LT}(f_2)$. Logo pela proposição 10.2, temos que $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$ e, conseqüentemente, $\langle \mathrm{LT}(I) \rangle \not\subset \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$. Adiante, definiremos que se $I = \langle f_1, \ldots, f_r \rangle$, com $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r) \rangle = \langle \mathrm{LT}(I) \rangle$ então $f_1, \ldots, f_r$ é uma Base de Gröbner para I.

Definição 20. *Fixada uma ordem monomial, um subconjunto $G = \{g_1, \ldots, g_t\}$ de um ideal I é dito Base de Gröbner se*

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$$

Equivalentemente, segue da Proposição 10 item 2, que $G = \{g_1, \ldots, g_t\}$ é base de Gröbner se, e somente se, o termo líder de qualquer elemento de I é divisível por $\mathrm{LT}(g_i)$, para algum $1 \leq i \leq t$.

Exemplo 26.

1. Se $I = \langle X^{\alpha_1}, \ldots, X^{\alpha_k} \rangle$, então $G = \{X^{\alpha_1}, \ldots, X^{\alpha_k}\}$ é uma Base de Gröbner para I.
2. Se $I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$, então $G = \{x^3 - 2xy, x^2y - 2y^2 + x\}$ não é Base de Gröbner para I, com relação a ordem lexicográfica graduada, pois pelo Exemplo 25, temos que $x^2 \in I$, porém x^2 não é divisível por $\mathrm{LT}(x^3 - 2xy)$ nem por $\mathrm{LT}(x^2y - 2y^2 + x)$.

A pergunta que naturalmente surge é se todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ possui uma Base de Gröbner. Veremos a seguir que sim.

Lema 2 (Lema de Dickson)**.** *Se I um ideal monomial de $\mathbb{K}[x_1, \ldots, x_n]$, então existe um conjunto finito de monômios que geram I.*

Para a demonstração, veja o apêndice seção A.3, na página 92.

O Lema de Dickson permite provarmos que todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$ possui uma base de Gröbner e que todo ideal de $\mathbb{K}[x_1, \ldots, x_n]$, não somente os ideais monomiais, possui um conjunto finito de geradores.

Proposição 11. *Todo ideal não nulo de $\mathbb{K}[x_1, \ldots, x_n]$ possui uma Base de Gröbner.*

Demonstração. Seja $I \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal não nulo. Como $\langle \mathrm{LT}(I) \rangle$ é ideal monomial, segue do Lema de Dickson que existem monômios $m_1, \ldots, m_t \in \langle \mathrm{LT}(I) \rangle$ tais que $\langle \mathrm{LT}(I) \rangle = \langle m_1, \ldots, m_t \rangle$. Escolhendo elementos $g_i \in I$ tais que $\mathrm{LT}(g_i) = m_i$, para todo $i = 1, \ldots, t$, formamos o conjunto $G = \{g_1, \ldots, g_t\}$. Assim, se tomarmos $f \in I$ qualquer, então $\mathrm{LT}(f) \in \langle \mathrm{LT}(I) \rangle$ e $\mathrm{LT}(f)$ é divisível por algum $m_i = \mathrm{LT}(g_i)$ e portanto G é uma Base de Gröbner para I conforme visto na definição 20. □

Teorema 4 (Teorema da Base de Hilbert)**.** . *Todo ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ possui um conjunto gerador finito. Isto é, $I = \langle g_1, \ldots, g_t \rangle$ para $g_1, \ldots, g_t \in I$*

Demonstração. Se $I = \{0\}$ tomamos como conjunto gerador $\{0\}$ que é finito. Se $I \neq \{0\}$, então, pela Proposição 11, existe $\{g_1, \ldots, g_t\}$ com $g_i \in I$ tal que $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Afirmamos que $I = \langle g_1, \ldots, g_t \rangle$. De fato:

É claro que $\langle g_1, \ldots, g_t \rangle \subset I$ pois cada g_i está em I. Para provarmos a outra inclusão considere um polinômio $f \in I$. Dividindo f pela t-upla $(g_1, \ldots, g_t)$ segue, do algoritmo da Pseudodivisão 3, que f pode ser escrito como

$$f = a_1 g_1 + \ldots + a_t g_t + r$$

onde $a_i, r \in \mathbb{K}[x_1, \ldots, x_n]$, para $1 \leq i \leq t$, e r é uma $\mathbb{K}$-combinação linear de monômios em $\mathbb{K}[x_1, \ldots, x_n]$, nenhum deles sendo divisível por $\mathrm{LT}(g_i)$ para $1 \leq i \leq t$. Afirmamos que $r = 0$. De fato, note que $r = f - a_1 g_1 - \ldots a_t g_t \in I$ e se $r \neq 0$, então $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Mas, pela Proposição 9, segue que $\mathrm{LT}(r)$ deve ser divisível por algum $\mathrm{LT}(g_i)$, o que contradiz a definição de resto. Logo $r = 0$ e $f = a_1 g_1 + \ldots + a_t g_t \in \langle g_1, \ldots, g_t \rangle$. □

Observe que o Teorema da Base de Hilbert responde uma questão crucial: todo ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ possui um conjunto gerador finito. E mais do que isso, na demonstração do referido teorema, vimos que se $G = \{g_1, \ldots, g_t\}$ é uma Base de Gröbner para I, então $I = \langle g_1, \ldots, g_t \rangle$ e, por definição de Base de Gröbner, $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Como vimos no Exemplo 25 nem todos os geradores de um ideal possuem esta propriedade.

A proposição que se segue mostra que as Bases de Gröbner resolvem o problema do resto único na pseudodivisão.

Proposição 12. *Sejam $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner para um ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ e $f \in \mathbb{K}[x_1, \ldots, x_n]$. Então existe um único $r \in \mathbb{K}[x_1, \ldots, x_n]$ com as seguintes propriedades:*

(i) *Nenhum termo de r é divisível por algum dos $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$.*

(ii) *Existe $g \in I$ tal que $f = g + r$.*

Em particular, r é o resto na divisão de f por g, não importando a ordem em que os elementos de G são listados, quando usamos o algoritmo da divisão.

Demonstração. Segue do Algoritmo da Divisão que $f = a_1 g_1 + \cdots + a_s g_s + r$, $a_i, r \in \mathbb{K}[x_1, \ldots, x_n]$, onde r satisfaz a condição (i). A condição (ii) pode ser atendida se tomarmos $g = a_1 g_1 + \cdots + a_s g_s$. Isso mostra a existência de r.

Para provar a unicidade, suponhamos que $f = g_1 + r_1 = g_2 + r_2$ satisfaça as condições (i) e (ii). Então $r_2 - r_1 = g_1 - g_2 \in I$. Se $r_2 - r_1 \neq 0$, temos que $\mathrm{LT}(r_2 - r_1) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Pela Proposição 9 segue que $\mathrm{LT}(r_2 - r_1)$ é divisível por algum dos

$\mathrm{LT}(g_i)$, o que contradiz (i). Desse modo, $r_2 = r_1$ e a unicidade está provada. A parte final da proposição segue da unicidade de r.

□

Finalmente, com essa propriedade, somos capazes de saber quando um polinômio pertence a um dado ideal polinomial, como mostra o próximo corolário.

Corolário 3. *Sejam $G = \{g_1, \ldots, g_s\}$ uma base de Gröbner para um ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ e $f \in \mathbb{K}[x_1, \ldots, x_n]$. Então $f \in I$ se e somente se o resto da pseudodivisão de f por G é zero.*

Demonstração. Se o resto é zero, então é claro que $f \in I$. Reciprocamente, dado $f \in I$, temos $f = f + 0$ satisfazendo as duas condições da Proposição 12. Assim, 0 é o resto de f na divisão por G. □

5.3 Critério e Algoritmo de Buchberger

O objetivo desta seção é identificar e construir Bases de Gröbner. Para identificar e construir tais bases utilizaremos, respectivamente, o Critério e o Algoritmo de Buchberger.

Por definição, dado um ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, um conjunto $G = \{g_1, \ldots, g_s\} \subset I$ é uma Base de Gröbner para I quando $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle = \langle \mathrm{LT}(I)\rangle$. Como sempre vale a inclusão $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle \subset \langle \mathrm{LT}(I)\rangle$, então para verificar se $G = \{g_1, \ldots, g_s\}$ é Base de Gröbner para I, basta verificar se vale a inclusão $\langle \mathrm{LT}(I)\rangle \subset \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$. Como vimos no Exemplo 25, esta última inclusão pode não ocorrer e, portanto, G não será Base de Gröbner. Uma forma disso ocorrer é o caso em que numa determinada combinação

$$aX^{\alpha}g_i - bX^{\beta}g_j,$$

$\mathrm{LT}(aX^{\alpha}g_i)$ e $\mathrm{LT}(bX^{\beta}g_j)$ se cancelam implicando em $\mathrm{LT}(aX^{\alpha}g_i - bX^{\beta}g_j) \notin \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$ mas, com $\mathrm{LT}(aX^{\alpha}g_i - bX^{\beta}g_j) \in \langle \mathrm{LT}(I)\rangle$, uma vez que $aX^{\alpha}g_i - bX^{\beta}g_j \in I$. Esses tipos de cancelamentos são de vital importância para verificar se um determinado conjunto é uma base de Gröbner para um ideal. Assim, introduziremos na próxima definição, um tipo especial de combinação chamada de S-processo ou S-polinômio.

Definição 21. *Sejam $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ polinômios não nulos.*

Considere $\mathrm{multideg}(f) = \alpha$, $\mathrm{multideg}(g) = \beta$ *e* $\gamma = (\gamma_1, \ldots, \gamma_n)$, *com* $\gamma_i = max\{\alpha_i, \beta_i\}$ *para cada* $i \in \{1, \ldots, n\}$. *Chamaremos* X^{γ} *o mínimo múltiplo comum de* $\mathrm{LM}(f)$ *e* $\mathrm{LM}(g)$ *e escreveremos* $X^{\gamma} = \mathrm{MMC}(\mathrm{LM}(f), \mathrm{LM}(g))$

O S*-processo de f e g é a combinação:*

$$\mathrm{S}(f, g) = \frac{X^{\gamma}}{\mathrm{LT}(f)}f - \frac{X^{\gamma}}{\mathrm{LT}(g)}g$$

Exemplo 27. Sejam $f = x^3 - 2xy$ e $g = x^2y - 2y^2 + x$. Usando a ordem lexicográfica graduada, temos $X^\gamma = \mathrm{MMC}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{MMC}(x^3, x^2y) = x^3y$ ou seja $\gamma = (3, 1)$. Assim, o S-processo de f e g é:

$$\begin{aligned}
\mathrm{S}(f,g) &= \frac{X^\gamma}{\mathrm{LT}(f)}f - \frac{X^\gamma}{\mathrm{LT}(g)}g \\
&= x^3y\left(\frac{f}{x^3} - \frac{g}{x^2y}\right) \\
&= x^3y\left(\frac{yf - xg}{x^3y}\right) \\
&= x^3y - 2xy^2 - x^3y + 2xy^2 - x^2 \\
&= -x^2
\end{aligned}$$

Observemos que o objetivo do S-processo é cancelar termos líderes entre polinômios. O próximo lema garante que toda combinação que cancela termos líderes de polinômios de mesmo multigrau é resultado de um de S-processo.

Lema 3. *Considere $\succ$ uma ordem monomial e $\sum_{i=1}^{s} c_i f_i$, com $c_i \in \mathbb{K}$ e $\mathrm{multideg}(f_i) = \delta \in \mathbb{Z}_+^n$, para todo $i \in \{1, \ldots, s\}$. Se $\delta \succ \mathrm{multideg}(\sum_{i=1}^{s} c_i f_i)$, então $\sum_{i=1}^{s} c_i f_i$ é uma $\mathbb{K}$-combinação linear de S-processos $S(f_j, f_k)$ para $1 \leq j, k \leq s$. Além disso, $\delta \succ \mathrm{multideg}\,(\mathrm{S}(f_j, f_k))$, para $1 \leq j, k \leq s$.*

Para a demonstração, veja o apêndice seção A.3, na página 92.

Antes de passarmos aos resultados mais importantes da seção, vejamos uma nova notação a ser utilizada:

Denotareremos $\overline{f}^F$ o resto da pseudodivisão de f pela s-upla ordenada $F = (f_1, \ldots, f_s)$. Se F é uma base de Gröbner para $\langle f_1, \ldots, f_s \rangle$ então, pela Proposição 12, podemos considerar F como um conjunto sem uma ordem particular.

Exemplo 28. Sejam $f = x^4y + x^3y^3 + xy^4$, $F = (xy + y^3, x^4 + y)$ e a ordem monomial lexicográfica fixada, então $\overline{f}^F = -y^6$.

Teorema 5 (Critério de Buchberger)**.** *Seja $I = \langle g_1, \ldots, g_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal. Então $G = \{g_1, \ldots, g_s\}$ é uma Base de Gröbner para I se, e somente se, para todos os pares $i \neq j$, o resto na pseudodivisão de $S(g_i, g_j)$ por G (com qualquer ordenação) é zero.*

Para a demonstração, veja o apêndice seção A.3, na página 93.

O próximo exemplo ilustra a utilização do Critério de Buchberger.

Exemplo 29. Considere o ideal $I = \langle y - x^2, z - x^3 \rangle \subset \mathbb{K}[x, y, z]$. Afirmamos que $G = \{y - x^2, z - x^3\}$ é uma base de Gröbner com relação a ordem lexicográfica com $y > z > x$. De

fato, considere o S-processo

$$S(y-x^2, z-x^3) = \frac{yz}{y}(y-x^2) - \frac{yz}{z}(z-x^3) = -zx^2 + yx^3.$$

Dividindo $S(y-x^2, z-x^3)$ por $(y-x^2, z-x^3)$ encontramos:

$$-zx^2 + yx^3 = x^3(y-x^2) + (-x^2)(z-x^3),$$

isto é, $\overline{S(y-x^2, z-x^3)}^{G} = 0$. Então, pelo Critério de Buchberger, G é uma base de Gröbner para I.

Antes de passarmos a construção de uma Base de Gröbner para um ideal I, vamos estabelecer a seguinte notação:

Se $G = \{f_1, \ldots, f_s\} \subset \mathbb{K}[x_1, \ldots x_n]$, denotaremos por $\langle G \rangle$ e por $\langle \mathrm{LT}(G) \rangle$ os seguintes ideais:

$$\langle G \rangle = \langle f_1, \ldots, f_s \rangle$$
$$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle .$$

Teorema 6 (Algoritmo de Buchberger)**.** *Seja $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{K}[x_1, \ldots x_n]$ um ideal não nulo. Então uma base de Gröbner para I pode ser construída em número finito de passos pelo seguinte algoritmo:*

Input: $F = (f_1, \ldots, f_s)$
Output: *Uma base de Gröbner $G = (g_1, \ldots, g_s)$ para I, com $F \subseteq G$*
$G := F$;
repeat
  $G' := G$;
  for *Cada par $\{p, q\}$, $p \neq q$ em G'* **do**
    $r := \overline{S(p,q)}^{G'}$;
    if $r \neq 0$ **then**
      $G := G \cup \{r\}$;
until $G = G'$;
return G

Algoritmo 5: O algoritmo de Buchberger

Demonstração. Começaremos mostrando que $G \subset I$ em todas as etapas do algoritmo. Isto é verdade inicialmente, pois $G = F \subset I$. No fim de cada passo, aumentamos o conjunto G adicionando o resto $r = \overline{S(p,q)}^{G'}$ com $p, q \in G$. Assim, se $G \subset I$, então $p, q \in I$ e, portanto $\mathrm{S}(p, q) \in I$. Como dividimos $\mathrm{S}(p, q)$ por $G' \subset I$, então $G \cup \{r\} \subset I$.

Observamos que, no final da execução do algoritmo, G gera I, pois $F \subset G$. Além disso, o algoritmo termina quando $G = G'$, isto é, $\overline{S(p,q)}^{G'} = 0$, para todo $p, q \in G$. Com isto, o Critério de Buchberger garante que G é uma base de Gröbner para I.

Finalmente, devemos provar que o algoritmo termina. Para isso, precisamos observar o conjunto G após cada iteração. Note que o conjunto G consiste de G' (o antigo G) unido com os restos não nulos dos S-processos dos elementos de G'. Como $G' \subset G$, temos que:

$$\langle \mathrm{LT}(G') \rangle \subset \langle \mathrm{LT}(G) \rangle .$$

Agora, considere a afirmação: se $G \neq G'$, então $\langle \mathrm{LT}(G') \rangle$ é estritamente menor que $\langle \mathrm{LT}(G) \rangle$. De fato, suponha que um resto não nulo r de um S-processo foi adicionado a G' formando G. Como r é um resto na divisão por G', $\mathrm{LT}(r)$ não é divisível pelos termos líderes dos elementos de G', e assim, $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$. Mas, $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$, o que prova a afirmação.

Assim, se o algoritmo não termina, os ideais $\langle \mathrm{LT}(G') \rangle$ das sucessivas iterações do algoritmo formam uma cadeia ascendente de ideais monomiais distintos em $\mathbb{K}[x_1, \ldots, x_n]$. Como, pelo Lema de Dickson, todo ideal monomial é finitamente gerado, então a cadeia construída estaciona, ou seja, $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$ após certo número finito de iterações. Logo, pela afirmação do parágrafo anterior, isso implica em $G' = G$, ou seja, o algoritmo termina. □

Exemplo 30. Calcular uma base de Gröbner para o ideal $I = \langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle \subset \mathbb{Q}[x, y]$ usando a ordem lexicográfica.

Utilizando o algoritmo de Buchberger, temos:

$F = (f_1, f_2) = (2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$

$G = (f_1, f_2)$

G'	S	G	$G = G'$
(f_1, f_2)	$S = \overline{S(f_1, f_2)}^{G'} = y^2 - 1$	$(f_1, f_2, f_3) =$ $(2x^2 + 3y^2 - 11, x^2 - y^2 - 3, y^2 - 1)$	Falso
(f_1, f_2, f_3)	$S = \begin{cases} \overline{S(f_1, f_2)}^{G'} = 0 \\ \overline{S(f_1, f_3)}^{G'} = 0 \\ \overline{S(f_2, f_3)}^{G'} = 0 \end{cases}$	$(f_1, f_2, f_3) =$ $(2x^2 + 3y^2 - 11, x^2 - y^2 - 3, y^2 - 1)$	Verdadeiro

Nessa disposição, cada coluna possui os valores assumidos pelas variáveis do algoritmo em cada iteração. Em especial, a última coluna corresponde a condição de parada do algoritmo. Quando $G = G'$ é verdadeiro, concluímos que o algoritmo termina e que temos como saída uma base de Gröbner $G = \{2x^2 + 3y^2 - 11, x^2 - y^2 - 3, y^2 - 1\}$ para o ideal I.

Ao construírmos bases de Gröbner, freqüentemente encontramos conjunto de geradores muito grandes. Podemos eliminar alguns elementos desnecessários desse conjunto de acordo com a próxima proposição.

Proposição 13. *Sejam G uma base de Gröbner para um ideal $I \subset \mathbb{K}[x_1, \ldots x_n]$ e $p \in G$ um polinômio tal que $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$. Então $G - \{p\}$ também é uma base de Gröbner para I.*

Demonstração. Sabemos que $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$. Se $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\})\rangle$, então $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(G - \{p\})\rangle$ e, portanto, $\langle \mathrm{LT}(G - \{p\})\rangle$ é base de Gröbner para I. □

Com esta proposição, podemos definir uma base de Gröbner mais simples como se segue:

Definição 22. *Uma base de Gröbner G para um ideal polinomial I é dita mínima quando:*

1. $\mathrm{LC}(p) = 1, \forall p \in G$
2. $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\})\rangle, \forall p \in G$

Podemos construir uma base de Gröbner mínima para um ideal não nulo, aplicando o algoritmo de Buchberger e a Proposição 13. Vejamos um exemplo.

Exemplo 31. Vamos calcular uma base de Gröbner mínima para o ideal do exemplo 30: Com $I = \langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3\rangle$, obtemos uma base de Gröbner para a ordem lexicográfica $G = \{2x^2 + 3y^2 - 11, x^2 - y^2 - 3, y^2 - 1\}$.

Agora, fazendo $p_1 = 2x^2 + 3y^2 - 11$, temos $\mathrm{LT}(p_1) = 2x^2$ e observe que $\mathrm{LT}(p_1) = 2x^2 \in \langle x^2, y^2\rangle = \langle \mathrm{LT}(G - \{p_1\})\rangle$. Dessa forma podemos remover p_1 de G. Continuando, fazendo $p_2 = x^2 - y^2 - 3$, temos $\mathrm{LT}(p_2) = x^2$ e observe que $\mathrm{LT}(p_2) = x^2 \notin \langle y^2\rangle$. Finalmente, fazendo $p_3 = y^2 - 1$, temos $\mathrm{LT}(p_3) = y^2$ e observe que $\mathrm{LT}(p_3) = y^2 \notin \langle x^2\rangle$. Assim o conjunto $G = \{x^2 - y^2 - 3, y^2 - 1\}$ de acordo com a Definição 22, é base de Gröbner mínima para I.

Podemos ter eventualmente várias bases de Gröbner mínimas distintas. Isto é facilmente verificado, como mostra o próximo exemplo.

Exemplo 32. No Exemplo 31, podíamos ter removido p_2 ao invés de p_1 e assim obter uma outra base de Gröbner mínima: $\{x^2 + 3/2y^2 - 11/2, y^2 - 1\}$. Assim, podemos concluir que não existe uma única base de Gröbner mínima.

Seria muito útil se existisse algum tipo de base de Gröbner unicamente determinada. Por exemplo, dados dois ideais polinomiais I e J, como saber se eles são iguais? Se houvesse algum conjunto de geradores para tais ideais unicamente determinados, seria simples resolver essa questão. A próxima definição vem responder à questão da unicidade para bases de Gröbner.

Definição 23. *Uma base de Gröbner G para um ideal polinomial I é dita reduzida quando:*

1. $\mathrm{LC}(p) = 1$, *para todo* $p \in G$;

2. *Nenhum monômio de p pertence $\langle \mathrm{LT}(G - \{p\})\rangle$, para todo $p \in G$.*

O próximo teorema estabelecerá a unicidade das bases de Gröbner reduzidas. Primeiramente, vejamos um lema.

Lema 4. *Sejam G e G' bases de Gröbner mínimas para o ideal polinomial $I \subset \mathbb{K}[x_1, \ldots, x_n]$. Então G e G' têm a mesma cardinalidade e $\mathrm{LT}(G) = \mathrm{LT}(G')$.*

Demonstração. Sendo $G = \{f_1, \ldots, f_s\}$ e $G' = \{g_1, \ldots, g_l\}$ bases de Gröbner mínimas, então temos que $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(G')\rangle$. Assim, se $\mathrm{LT}(f_i) \in \langle \mathrm{LT}(G')\rangle$, temos:

$$\mathrm{LT}(f_i) = X^\alpha \,\mathrm{LT}(g_j), \tag{5.1}$$

para algum $g_j \in G'$. Com o mesmo raciocínio obtemos:

$$\mathrm{LT}(g_j) = X^\beta \,\mathrm{LT}(f_r), \tag{5.2}$$

para algum $f_r \in G$. Relacionando as duas equações acima encontramos:

$$\mathrm{LT}(f_i) = X^\alpha X^\beta \,\mathrm{LT}(f_r)$$

Como G é mínima, $X^\alpha X^\beta = 1$ e $f_i = f_r$, ou ainda, $X^\alpha = X^\beta = 1$ e $f_i = f_r$. De (5.1) temos $\mathrm{LT}(f_i) = \mathrm{LT}(g_j)$, provando assim que $\mathrm{LT}(G) \subset \mathrm{LT}(G')$. De modo análogo, temos que $\mathrm{LT}(G') \subset \mathrm{LT}(G)$, o conclui a demonstração. □

Teorema 7. *Seja $I \neq \{0\}$ um ideal polinomial. Então, dada uma ordem monomial, I possui uma única base de Gröbner reduzida.*

Para a demonstração, veja o apêndice seção A.3, na página 95.

A demonstração do Teorema 7, mostra como calcular a base de Gröbner reduzida a partir de uma base mínima. Dada uma base mínima $G = \{g_1, g_2, \ldots, g_t\}$ a ideia é dividir g_1 por $G - \{g_1\}$ obtendo o resto $g_1' = \overline{g_1}^{(G-\{g_1\})}$. Depois, substituímos g_1 por g_1' na base, que agora denotaremos por G'. Seguindo, repetiríamos o processo, agora com g_2. Calculamos $g_2' = \overline{g_2}^{(G'-\{g_2\})}$ e trocamos g_2 por g_2' obtendo uma nova base G''. Ao terminar esse processo com cada um dos g_i's, teremos uma base de Gröbner reduzida.

Exemplo 33. Considere $I = \langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3\rangle \subset \mathbb{Q}[x, y]$. Utilizando a ordem lexicográfica, segue do exemplo 31 que $G = \{x^2 - y^2 - 3, y^2 - 1\}$ é uma base de Gröbner mínima para I. Fazendo $g_1 = x^2 - y^2 - 3$, temos que ${g_1}' = \overline{g_1}^{G'-\{g_1\}} = x^2 - 4$ e, assim obtemos $G' = \{x^2 - 4, y^2 - 1\}$. Finalmente, fazendo $g_2 = y^2 - 1$, temos que ${g_2}' = \overline{g_2}^{G'-\{g_2\}} = y^2 - 1$, e, pela demonstração do Teorema 7, temos que $G'' = \{x^2 - 4, y^2 - 1\}$ é uma base de Gröbner reduzida para I já que agora todos os termos foram reduzidos.

Finalmente, temos todas as ferramentas para tratar o nosso problema aplicado. No próximo capítulo apresentaremos um “curso básico” do software CoCoA, para que possamos aplicar nossos conhecimentos algébricos para resolver sistemas polinomiais muito complexos.

6 O SOFTWARE COCOA

Como vimos no capítulo anterior, o processo de obtenção de uma base de Gröbner toma muito tempo mesmo nos exemplos mais fáceis. Por esse motivo, nesta seção apresentaremos uma introdução ao sistema de computação algébrica CoCoA, que facilitará todos os cálculos relativos à essas bases. A referência utilizada é o próprio manual que se encontra no site oficial.[1].

CoCoA é um acrônimo para "Computations in Commutative Algebra". Este *software* é gratuito para fins educacionais e pesquisa. Basicamente efetua cálculos com polinômios de várias variáveis. Usaremos o CoCoA para efetuar cálculos com bases de Gröbner . A versão que usaremos será a 4.7.5 (Windows) que possui uma interface gráfica.

6.1 Instalação no Windows

Observe na (Figura 6), a página principal do site do CoCoA *(<http://cocoa.dima.unige.it/)>* com a sua divisão em 9 blocos principais. Para descarregar o arquivo, basta clicar no segundo bloco da primeira coluna, no link *"CoCoA-4.7.5 old system (2009)"*. Na página aberta, procure pela versão MSWindows *"CoCoA-4.7.5 (7.5M)"*. Clicando neste link, o navegador fará o download do arquivo compactado em formato compactado de extensão .zip. Depois, basta extrair os arquivos para uma pasta do seu computador. Para iniciar o programa, basta executar o arquivo *cocoaqt.exe* que está localizado pasta raiz do programa.

Figura 6 – Página principal do CoCoA

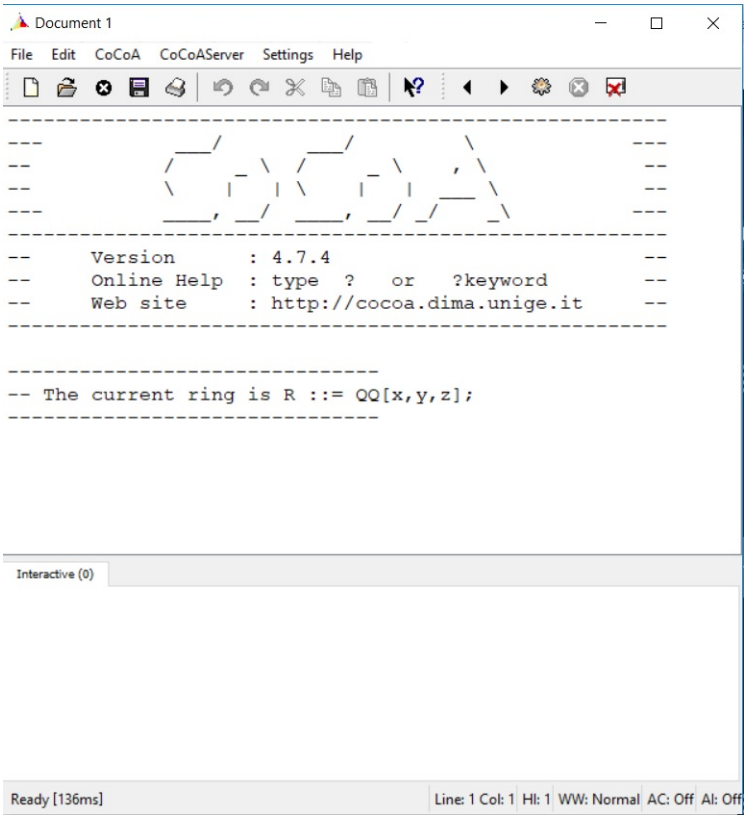
Fonte: Print Screen da página principal do CoCoA. Disponível em: http://cocoa.dima.unige.it/. Acesso em: 5 fev. 2019

[1] Neste trabalho, utilizamos a versão 4.7.5 cujo manual se encontra em <http://cocoa.dima.unige.it/download/doc/GUI_help/toc.html>

6.2 Interface e Alguns Comandos

A interface gráfica do CoCoA é dividida em duas partes: Na superior, temos os resultados que obtemos a partir dos comandos inseridos na inferior, como na Figura 7.

Figura 7 – Tela principal do CoCoA



Fonte: Print Screen da interface do CoCoA 4.7.5

Execute o CoCoA e digite na parte inferior:

```
1+1;
```

com o cursor nesta linha pressione CRTL+ENTER. Você terá na tela superior como resultado deste comando:

```
1+1;
------------------
2
```

Todos os comandos do CoCoA devem ser terminados por um ponto e vírgula. Por exemplo, escreva a sequência de comandos a seguir:

```
A:=2*5;
B:=3;
A+B;
A/B;
A^B;
Fact(B);
Mod(A,B);
```

Nesta sequência, observe que usamos o comando de atribuição :=, desta forma, atribuímos a variável A, o valor 2*5=10, e a variável B, o valor 3. Para executar todas essas linhas de comandos, selecione todas as linhas e pressione CRTL+ENTER. O resultado obtido na parte superior será:

```
A:=2*5;
B:=3;
A+B;
A/B;
A^B;
Fact(B);
Mod(A,B);
13
------------------------------
10/3
------------------------------
1000
------------------------------
6
------------------------------
1
------------------------------
```

Além do uso do comando :=, também usamos os comandos *,+,/,∧, Fact e Mod. Estes comandos respectivamente efetuam: multiplicação, adição, divisão, exponenciação, cálculo do fatorial de um número e o cálculo do resto da divisão de dois números. É importante observar que as variáveis que guardam resultados efetuados pelo CoCoA sempre tem que ser maiúsculas, assim também as funções (Fact, Mod etc). Para ilustrar isso, execute os comandos abaixo:

```
A:=8;
```

```
fact(A);
Fact(A);
b:=4;
B:=4;
Fact(B);
```

O Resultado obtido é:

```
A:=8;
fact(A);
Fact(A);
b:=4;
B:=4;
Fact(B);
ERROR: Undefined indeterminate f
CONTEXT: f * a * c * t * (A)
-------------------------------
40320
-------------------------------
ERROR: parse error in line 4 of device
-------------------------------
4
-------------------------------
24
-------------------------------
```

Observe que o CoCoA não aceitou o comando fact(A); pois a função está iniciada por letra minúscula. Da mesma forma ao tentar armazenar o valor 4 na variável b (minúscula) é apresentado um erro.

6.3 Polinômios no CoCoA

Os comandos LC, LT, LM e Deg retornam respectivamente o coeficiente líder, o monômio líder, o termo líder e o grau de um polinômio. É importante observar que no CoCoA, as definições de termo líder e monômio líder diferem das usadas neste trabalho. Note abaixo que ao usar o comando LT(F) onde $F = 3x^5 + 7x^2 - 3x + 1$, é retornado apenas x^5, enquanto que ao usar o comando LM(F), é retornado $3x^5$.

```
Use R ::= QQ[x];-- Usa o anel Q[x]
F := 3x^5+7x^2-3x+1;--Polinômio atribuído à variável F
```

```
LC(F);
3
------------------------------
LT(F);
x^5
------------------------------
LM(F);
3x^5
------------------------------
Deg(F);
5
------------------------------
```

Na primeira linha desse exemplo, tudo o que vem depois dos dois traços seguidos: – é ignorado pelo CoCoA. Este comando permite que façamos comentários nas linhas de programação.

Para dividir dois polinômios no CoCoA usamos o comando DivAlg. Por exemplo:

```
Use R ::= QQ[x];-- Usa o anel Q[x]
F := 3x^5+16x^3+x^2-10x+9;--Dividendo
G := [x^2+6];-- Lista com os polinomios Divisores
DivAlg(F,G);-- Comando para dividir F por G
------------------------------
Record[Quotients := [3x^3 - 2x + 1], Remainder := 2x + 3]
```

O Comando DivAlg retorna um RECORD com dois campos: Quotients - uma lista com os quocientes e Remainder - O resto da divisão ou pseudodivisão como no exemplo abaixo:

```
Use R ::= QQ[x,y], Lex; -- Especifica o uso da ordem lexicográfica
F:=x^2y^2+x+y;
G:=x+y;
H:=xy+y^2;

DivAlg(F,[G,H]);
Record[Quotients := [xy^2 - y^3 + 1, 0], Remainder := y^4]
------------------------------
```

No exemplo acima, depois do comando Use, onde informamos o anel em que queremos efetuar os cálculos, também especificamos qual ordem monomial queremos usar. Algumas opções possíveis são: Lex (lexicográfica), DegLex (lexicográfica graduada), DegRevLex (Lexicográfica Graduada Reversa) que é a ordem usada por padrão.

Para calcular o MDC de dois polinômios F e G usamos o comando GCD(F, G); No exemplo abaixo estamos calculando o $\mathrm{MDC}(f, g)$ com $f = x^2-4 = (x+2)(x-2)$ e $g = (x-2)^3$

```
Use R ::= QQ[x];
F := x^2-4;
G := (x-2)^3;
GCD(F, G);
------------------------------
x-2
```

Para verificar se um polinômio pertence à um ideal usamos o comando IsIn. O comando Ideal(F,G), cria o ideal gerado pelos polinômios F e G.

```
Use R ::= QQ[x];
F := x^3;
I := Ideal(x^6-1,x^4-1);
F IsIn  I; --Verifica se F pertence à I
(retorna um valor boleano True False)
------------------------------
False
```

O exemplo abaixo, mostra que o Algoritmo da PseudoDivisão não goza da unicidade do resto.

```
Use R ::= QQ[x,y],  DegLex; --muda para ordem Lexicográfica Graduada
F:=y^2x-x;
D:=[y^2-x,xy-y];
E:=[xy-y,y^2-x];
DivAlg(F,D);
------------------------------
Record[ Quotients := [x,0], Remainder:= x^2 - x]
DivAlg(F,E);
------------------------------
Record[ Quotients := [y,1], Remainder := 0]
```

Com o CoCoA podemos calcular bases de Gröbner interativamente como se segue:

```
Use R ::= QQ[x,y],  Lex;
I:=Ideal([2x^2+3y^2-11,x^2-y^2-3]);
$gb.Start_GBasis(I);  -- inicia o cálculo da Base de Grobner
I.GBasis;  -- inicialmente a Base está vazia
```

```
------------------------------
Null
$gb.Steps(I,1); -- uma etapa do cálculo da Base de Grobner
I.GBasis;
------------------------------
[x^2 - y^2 - 3]
$gb.Complete(I); -- cálculo completo
I.GBasis;
------------------------------
[  2x^2 + 3y^2 - 11,-5/2y^2 + 5/2]
```

Para calcular uma base de Gröbner reduzida para um ideal I, usamos o comando ReducedGBasis(I).

```
Use R ::= QQ[x,y],  Lex;
I:=Ideal([2x^2+3y^2-11,x^2-y^2-3]);
ReducedGBasis(I);
------------------------------
[y^2 - 1, x^2 - 4]
```

7 APLICAÇÃO DAS BASES DE GRÖBNER NA RESOLUÇÃO DE UM SHIDOKU

Neste capítulo mostraremos que a resolução algébrica de um Shidoku está associada à resolução de um sistema polinomial de várias indeterminadas com mais de 40 equações. Desse modo, utilizaremos as Bases de Gröbner para transformar esse sistema em outro equivalente, cuja resolução será muito mais simples. Nesse caso, o uso das Bases de Gröbner vai atuar de forma semelhante à eliminação gaussiana dos sistemas lineares. O software CoCoA, estudado no capítulo 6, será o meio pelo qual conseguiremos efetuar os cálculos extremamente complicados que surgem nessa aplicação.

Iniciaremos este capítulo apresentando o quebra-cabeças Sudoku e sua versão reduzida, o Shidoku. Depois de entendidas as regras desses quebra-cabeças, modelaremos algebricamente o Shidoku como um sistema de equações polinomiais com mais de 40 equações e 16 incógnitas. Como vimos no Capítulo 4, podemos relacionar esse sistema polinomial com um ideal I, e então calculando uma base de Gröbner para I, obteremos um sistema equivalente ao original, mas num formato muito mais simples de se resolver. O uso do CoCoA atua na obtenção dessa base, uma vez que obtê-la com o Algoritmo de Buchberger é um processo muito trabalhoso até mesmo nos exemplos mais simples. Além disso, usaremos técnicas básicas de programação para não precisar inserir manualmente os mais de 40 polinômios que compõem esse referido sistema.

7.1 O que é um Sudoku?

O Sudoku é um popular quebra-cabeças, figurando em muitos jornais, revistas e até em aplicativos de celular. Segundo Hayes (2006), as aparições mais antigas conhecidas remontam ao ano de 1979 numa revista americana entitulada *Dell Pencil Puzzles e Word Games*, onde o jogo era conhecido por *Number Place*. Porém, no final do século XIX, na França, vários jornais e revistas publicavam jogos que eram muito próximos ao Sudoku como conhecemos hoje. (BOYER, 2007). A palavra Sudoku tem sua origem do japonês *Su*, que significa número e *Doku*, que significa sozinho. (HAYES, 2006).

O tradicional quebra-cabeças é composto por uma grade com 9 linhas e 9 colunas, subdividida em 9 blocos de tamanho 3x3. O desafio consiste em preencher as células vazias com os dígitos de 1 a 9 de tal maneira que cada linha, coluna e bloco 3x3 contenha cada dígito exatamente uma vez. Na figura Figura 8 temos um exemplo de um Sudoku com 28 células já preenchidas. Chamaremos de *valores iniciais*, os dígitos dessas células preenchidas.

7.2 O que é um Shidoku?

O Shidoku é uma versão 4x4 do Sudoku que conhecemos. Isto é, temos uma grade com 4 linhas e 4 colunas, subdividida em 4 blocos de tamanho 2x2, como na Figura 9. Chamamos

Figura 8 – Um Sudoku

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

Fonte: O autor

de região, qualquer linha, coluna ou cada um dos quatro blocos 2x2 da grade. As células vazias devem ser preenchidas com os dígitos de 1 a 4 de tal maneira que cada linha, coluna e bloco 2x2 contenha cada dígito uma única vez. A Figura 9 mostra um exemplo de Shidoku.

Figura 9 – Um Shidoku

		1	
4			
	2		3

Fonte: O autor

7.3 Representando um Shidoku usando polinômios

Baseados em Arnold, Lucas e Taalman (2010), apresentaremos uma modelagem do Shidoku por meio de polinômios. Considere o quadro abaixo com as 16 células de um Shidoku. Usaremos a notação $x_{i,j}$, com $1 \leq i, j \leq 4$ para representar o dígito que ocupa a célula que está na linha i e coluna j. Pelas regras do jogo, em qualquer região temos sempre os dígitos 1, 2, 3, 4 presentes uma única vez.

Figura 10 – Modelando um Shidoku

$x_{1,1}$	$x_{1,2}$	$x_{1,3}$	$x_{1,4}$
$x_{2,1}$	$x_{2,2}$	$x_{2,3}$	$x_{2,4}$
$x_{3,1}$	$x_{3,2}$	$x_{3,3}$	$x_{3,4}$
$x_{4,1}$	$x_{4,2}$	$x_{4,3}$	$x_{4,4}$

Fonte: O autor

Inicialmente, podemos notar que cada uma das células $x_{i,j}$ é um dígito escolhido entre 1, 2, 3 ou 4, portanto temos:

$$(x_{i,j} - 1)(x_{i,j} - 2)(x_{i,j} - 3)(x_{i,j} - 4) = 0$$
$$x_{i,j}^4 - 10x_{i,j}^3 + 35x_{i,j}^2 - 50x_{i,j} + 24 = 0$$

para todo $1 \leq i, j \leq 4$, totalizando 16 equações. Por exemplo, a equação $(x_{1,1} - 1)(x_{1,1} - 2)(x_{1,1} - 3)(x_{1,1} - 4) = 0$ modela o fato de que $x_{1,1} \in \{1, 2, 3, 4\}$.

Além disso, em cada região, o produto das 4 incógnitas tem que ser $1 \times 2 \times 3 \times 4 = 24$, portanto se chamarmos as incógnitas de a, b, c, d, temos que ter:

$$abcd - 24 = 0$$

Por exemplo, considerando a primeira linha, teremos a equação $x_{1,1}x_{1,2}x_{1,3}x_{1,4} - 24 = 0$. Se considerarmos a segunda coluna, teremos a equação $x_{1,2}x_{2,2}x_{3,2}x_{4,2} - 24 = 0$. Por fim, considerando o bloco inferior direito, teremos a equação $x_{3,3}x_{3,4}x_{4,3}x_{4,4} - 24 = 0$. Como temos 4 linhas, 4 colunas e 4 blocos, isso acrescenta 12 equações às 16 já existentes.

Por fim, se a, b, c, d são elementos de uma região, então a sua soma tem que resultar em $1 + 2 + 3 + 4 = 10$. Assim temos mais 12 equações da forma

$$a + b + c + d - 10 = 0$$

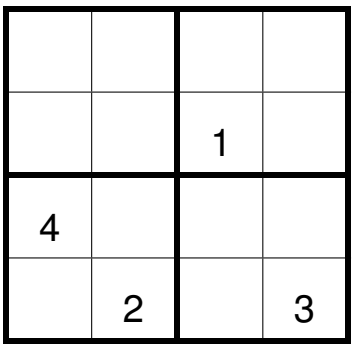
Por exemplo, considerando a terceira linha, teremos a equação $x_{3,1} + x_{3,2} + x_{3,3} + x_{3,4} - 10 = 0$. Se considerarmos a segunda coluna, teremos a equação $x_{1,2} + x_{2,2} + x_{3,2} + x_{4,2} - 10 = 0$. Por fim, considerando o bloco inferior esquerdo, teremos a equação $x_{3,1} + x_{3,2} + x_{4,1} + x_{4,2} - 10 = 0$.

Com essa modelagem, obtemos um total de $16 + 12 + 12 = 40$ equações, que é geral para qualquer Shidoku.

Agora, considerando os valores iniciais apresentados, outras equações serão acrescentadas ao sistema.

Relembrando o Shidoku que propusemos no início Nesse caso teríamos que acrescentar

Figura 11 – O Shidoku proposto



Fonte: O autor

ao sistema as equações:

$$x_{2,3} - 1 = 0,\ x_{3,1} - 4 = 0,\ x_{4,2} - 2 = 0,\ x_{4,4} - 3 = 0$$

Temos agora a modelagem completa do Shidoku proposto. O sistema possui 16 indeterminadas e 44 equações. Na próxima seção, iremos implementar no CoCoA o cálculo da base de Gröbner associada à esse sistema. Além disso, exibiremos o sistema equivalente gerado a partir dessa base.

7.4 Programando para resolver um Shidoku

Para implementar a obtenção da base de Gröbner Reduzida no CoCoA, precisaremos criar um ideal I com os 44 polinômios que formam o sistema associado ao Shidoku proposto e posteriormente calcularemos uma base de Gröbner reduzida para I. Dessa maneira, como vimos no capítulo 4, transformaremos o complexo sistema de 44 equações num sistema muito mais simples de resolver. No que se segue, comentaremos passo a passo toda a programação envolvida: Criaremos um método para automatizar a tediosa inserção manual dos mais de 40 polinômios que modelam o nosso quebra-cabeças e também apresentaremos alguns novos comandos do CoCoA ao longo do processo de implementação.

Inicialmente devemos definir o anel onde efetuaremos os cálculos. Isto é feito usando o comando *Use*.

```
Use R ::= QQ[x[1..4,1..4]];
```

Neste caso estamos criando um anel de 16 indeterminadas $\mathbb{Q}[x_{(1,1)}, x_{(1,2)}, x_{(1,3)}, \ldots, x_{(4,4)}]$ e usando a ordem monomial padrão do CoCoA: A ordem Lexicográfica Graduada Reversa "GREVLEX". Observe que x[1..4,1..4] faz todas as combinações possíveis de $x_{(i,j)}$ com i, j variando de 1 à 4.

Agora, usaremos técnicas básicas de programação para evitar que tenhamos que escrever manualmente as 44 equações na tela de entrada do CoCoA. Usamos o código *C:=NewMat(4,4)* para criar uma matriz 4x4 e atribuí-la a variável C. Essa matriz guardará os 16 polinômios referentes às 16 células do Shidoku. Depois temos um comando de repetição chamado *For*. Por meio dessa estrutura, podemos criar várias equações de forma automática. Observe que o primeiro *For* faz variar o índice i de 1 à 4 enquanto o segundo, que está dentro do primeiro, faz variar o índice j de 1 à 4. Quando $i = 1$ e $j = 1$ construímos o polinômio

$$C[1,1] = (x[1,1] - 1)(x[1,1] - 2)(x[1,1] - 3)(x[1,1] - 4);$$

que ocupa a primeira linha e primeira coluna da matriz C. Na próxima iteração desse duplo *For*, teremos $i = 1$ e $j = 2$, assim cria-se

$$C[1,2] = (x[1,2] - 1)(x[1,2] - 2)(x[1,2] - 3)(x[1,2] - 4);$$

e assim sucessivamente. Ao final das iterações, teremos os 16 polinômios ($C[I,J] := (x[I,J] - 1)(x[I,J]-2)(x[I,J]-3)(x[I,J]-4)$) referentes a cada uma das células do Shidoku preenchidas na matriz 4x4 C. Usamos o comando *Set Indentation* para que a formatação dos resultados fique mais legível.

```
Set Indentation;
C:=NewMat(4,4);
I:=1;
J:=1;
For I:=1 To 4 Do
For J:=1 To 4 Do
C[I,J]:=(x[I,J]-1)(x[I,J]-2)(x[I,J]-3)(x[I,J]-4);
EndFor;
EndFor;
C;
```

Depois de executar esse comando junto com o anterior, o resultado será esse:

```
Use R ::= QQ[x[1..4,1..4]];
Set Indentation;
C:=NewMat(4,4);
I:=1;
```

```
J:=1;
For I:=1 To 4 Do
For J:=1 To 4 Do
C[I,J]:=(x[I,J]-1)(x[I,J]-2)(x[I,J]-3)(x[I,J]-4);
EndFor;
EndFor;
C;
---------------------------------------
Mat([
  [x[1,1]^4 - 10x[1,1]^3 + 35x[1,1]^2 - 50x[1,1] + 24,
   x[1,2]^4 - 10x[1,2]^3 + 35x[1,2]^2 - 50x[1,2] + 24,
   x[1,3]^4 - 10x[1,3]^3 + 35x[1,3]^2 - 50x[1,3] + 24,
   x[1,4]^4 - 10x[1,4]^3 + 35x[1,4]^2 - 50x[1,4] + 24],
  [x[2,1]^4 - 10x[2,1]^3 + 35x[2,1]^2 - 50x[2,1] + 24,
   x[2,2]^4 - 10x[2,2]^3 + 35x[2,2]^2 - 50x[2,2] + 24,
   x[2,3]^4 - 10x[2,3]^3 + 35x[2,3]^2 - 50x[2,3] + 24,
   x[2,4]^4 - 10x[2,4]^3 + 35x[2,4]^2 - 50x[2,4] + 24],
  [x[3,1]^4 - 10x[3,1]^3 + 35x[3,1]^2 - 50x[3,1] + 24,
   x[3,2]^4 - 10x[3,2]^3 + 35x[3,2]^2 - 50x[3,2] + 24,
   x[3,3]^4 - 10x[3,3]^3 + 35x[3,3]^2 - 50x[3,3] + 24,
   x[3,4]^4 - 10x[3,4]^3 + 35x[3,4]^2 - 50x[3,4] + 24],
  [x[4,1]^4 - 10x[4,1]^3 + 35x[4,1]^2 - 50x[4,1] + 24,
   x[4,2]^4 - 10x[4,2]^3 + 35x[4,2]^2 - 50x[4,2] + 24,
   x[4,3]^4 - 10x[4,3]^3 + 35x[4,3]^2 - 50x[4,3] + 24,
   x[4,4]^4 - 10x[4,4]^3 + 35x[4,4]^2 - 50x[4,4] + 24]
])
```

Depois disso, criamos uma outra matriz L, dessa vez 4x2, para guardar os 8 polinômios referentes as linhas: Os 4 polinômios referentes a soma 10 e os 4 polinômios referentes ao produto 24. Para exemplificar, vejamos os exemplos de polinômios para a segunda linha do Shidoku:

$$x[2,1]x[2,2]x[2,3]x[2,4] - 24$$

Este polinômio modela o produto da linha 2 do Shidoku. Iremos alocar os polinômios referentes ao produto na primeira coluna de L.

$$x[2,1] + x[2,2] + x[2,3] + x[2,4] - 10$$

Este polinômio modela a soma da linha 2 do Shidoku. Iremos alocar os polinômios referentes à soma na segunda coluna de L. A programação desta vez é mais simples, pois temos apenas um

For simples que faz variar o índice i de 1 a 4. Abaixo mostramos o código, com o seu respectivo resultado:

```
L:=NewMat(4,2);
I:=1;
J:=1;
For I:=1 To 4 Do
        L[I,1]:=x[I,J]x[I,J+1]x[I,J+2]x[I,J+3]-24;
        L[I,2]:=x[I,J]+x[I,J+1]+x[I,J+2]+x[I,J+3]-10;
EndFor;
L;
------------------------------
Mat([
  [x[1,1]x[1,2]x[1,3]x[1,4] - 24, x[1,1] + x[1,2] + x[1,3] + x[1,4] - 10],
  [x[2,1]x[2,2]x[2,3]x[2,4] - 24, x[2,1] + x[2,2] + x[2,3] + x[2,4] - 10],
  [x[3,1]x[3,2]x[3,3]x[3,4] - 24, x[3,1] + x[3,2] + x[3,3] + x[3,4] - 10],
  [x[4,1]x[4,2]x[4,3]x[4,4] - 24, x[4,1] + x[4,2] + x[4,3] + x[4,4] - 10]
])
```

Nessa parte, criamos uma matrix 2x4 chamada COL que guardará as 8 equações referentes às colunas. Para exemplificar, vejamos os exemplos de polinômios para a terceira coluna:

$$x[1,3]x[2,3]x[3,3]x[4,3] - 24$$

Este polinômio modela o produto da coluna 3 do Shidoku. Iremos alocar os polinômios referentes ao produto na primeira linha da matriz COL.

$$x[1,3] + x[2,3] + x[3,3] + x[4,3] - 10$$

Este polinômio modela a soma da coluna 3 do Shidoku. Iremos alocar os polinômios referentes à soma na segunda linha da matriz COL.

```
COL:=NewMat(2,4);
I:=1;
J:=1;
For J:=1 To 4 Do
        COL[1,J]:=x[I,J]x[I+1,J]x[I+2,J]x[I+3,J]-24;
        COL[2,J]:=x[I,J]+x[I+1,J]+x[I+2,J]+x[I+3,J]-10;
        EndFor;
COL;
------------------------------
Mat([
 [x[1,1]x[2,1]x[3,1]x[4,1] - 24,  x[1,2]x[2,2]x[3,2]x[4,2] - 24,
```

```
  x[1,3]x[2,3]x[3,3]x[4,3] - 24, x[1,4]x[2,4]x[3,4]x[4,4] - 24],
 [x[1,1]+x[2,1]+x[3,1]+x[4,1]-10, x[1,2]+x[2,2]+x[3,2]+x[4,2]-10,
  x[1,3]+x[2,3]+x[3,3]+x[4,3]-10, x[1,4]+x[2,4]+x[3,4]+x[4,4]-10]
])
```

Faremos o mesmo processo para as condições dos blocos 2x2. Criamos uma matriz BOX 4x4 para guardar as 8 equações. Para exemplificar, vejamos os exemplos de polinômios para o bloco superior direito do Shidoku:

$$x[1,3]x[1,4]x[2,3]x[2,4] - 24$$

Este polinômio modela o produto do bloco superior direito do Shidoku. Iremos alocar os polinômios referentes ao produto na primeira linha da matriz BOX.

$$x[1,3] + x[1,4] + x[2,3] + x[2,4] - 10$$

Este polinômio modela a soma do bloco superior direito do Shidoku. Iremos alocar os polinômios referentes à soma na terceira linha da matriz BOX.

```
BOX:=NewMat(4,4);
I:=1;
J:=1;
For I:=1 To 4 Step 2 Do -- Faz com que o índice varie de 2 em 2
        For J:=1 To 4 Step 2 Do
        BOX[I,J]:=x[I,J]x[I,J+1]x[I+1,J]x[I+1,J+1]-24;
        BOX[I,J+1]:=x[I,J]+x[I,J+1]+x[I+1,J]+x[I+1,J+1]-10;
        EndFor;
EndFor;
BOX;
-------------------------------
Mat([
  [x[1,1]x[1,2]x[2,1]x[2,2] - 24, x[1,1] + x[1,2] + x[2,1] + x[2,2] - 10,
   x[1,3]x[1,4]x[2,3]x[2,4] - 24, x[1,3] + x[1,4] + x[2,3] + x[2,4] - 10],
  [Null, Null, Null, Null],
  [x[3,1]x[3,2]x[4,1]x[4,2] - 24, x[3,1] + x[3,2] + x[4,1] + x[4,2] - 10,
   x[3,3]x[3,4]x[4,3]x[4,4] - 24, x[3,3] + x[3,4] + x[4,3] + x[4,4] - 10],
  [Null, Null, Null, Null]
])
```

Repare que a matriz fica com a segunda e quarta linhas vazias. Para nos desfazermos das duas linhas vazias da matriz BOX iremos criar uma outra matriz P 2x4 que será composta pela linha

1 e linha 3 da matriz BOX. Além disso usaremos o comando *Transposed* para obter a transposta da matriz P e da matriz COL. Dessa forma todas as matrizes, C,L, COL e P serão matrizes com 4 linhas. Isso é fundamental para que possamos unir todas essas matrizes em uma só. Usaremos para isso o comando *BlockMatrix*.

```
P:=NewMat(2,4);
P[1]:=BOX[1];
P[2]:=BOX[3];
P:=Transposed(P);
COL:=Transposed(COL);
COL;
H:=BlockMatrix([[L,C,COL,P]]);
```

Agora temos as 40 equações distribuídas em uma única matriz H. Para que consigamos criar o ideal com todos esses polinômios, é necessário que tenhamos uma lista ao invés de uma matriz. Para converter uma matriz numa lista, usaremos o comando *Cast*. O problema é que, quando transformamos uma matriz numa lista, cada linha da matriz se torna um elemento da lista. Por exemplo, a matriz a seguir:

```
Mat([
  [1, 2],
  [3, 4]
])
```

se transforma na lista:

```
[[1,2],[3,4]];
```

Repare que essa lista possui dois elementos, que por sua vez são listas também. Para obter uma lista, onde cada elemento ocupe uma entrada separada, devemos usar o comando *Flatten*:

```
Flatten([[1,2],[3,4]]);
----------------------
[1,2,3,4]
```

Então, para obtermos o resultado que queremos, devemos seguir a sequência a seguir:

```
H:=Cast(H, LIST);
H:=Flatten(H);
Len(H);
```

```
--------------------------
40
```

Observe o uso do comando *Len* que retorna o tamanho da lista H, assim temos certeza que obtivemos os 40 polinômios.

Finalmente, devemos adicionar os polinômios que caracterizam os valores iniciais dados no nosso Shidoku. Escreveremos manualmente os 4 polinômios que descrevem os valores iniciais e usaremos o comando *Append* para anexar cada um desses polinômios à nossa lista H. Para criar o ideal com todos os nossos 44 polinômios utilizamos a sintaxe *Ideal* e por fim calculamos a base de Gröbner reduzida para este ideal com o comando *ReducedGBasis*.

```
A:=x[2,3]-1;
B:=x[3,1]-4;
C:=x[4,2]-2;
D:=x[4,4]-3;
Append(H,A);
Append(H,B);
Append(H,C);
Append(H,D);
Len(H);
I:=Ideal(H);
Time ReducedGBasis(I);
------------------------------
[
  x[4,3] - 4,
  x[2,4] - 2,
  x[2,2] - 4,
  x[4,4] - 3,
  x[4,2] - 2,
  x[2,3] - 1,
  x[3,3] - 2,
  x[1,4] - 4,
  x[4,1] - 1,
  x[1,3] - 3,
  x[3,1] - 4,
  x[1,2] - 1,
  x[2,1] - 3,
  x[1,1] - 2,
  x[3,2] - 3,
```

```
  x[3,4] - 1]
Cpu time = 0.01, User time = 0
```

Com o cálculo da base de Gröbner reduzida para o ideal I, obtemos um novo conjunto gerador com apenas 16 polinômios da forma $x_{ij} - a_{ij}$, com $1 \leq i, j \leq 4$, $a_{ij} \in \{1, 2, 3, 4\}$.

Dessa forma, obtemos o seguinte sistema equivalente ao original:

$$\begin{cases} x_{11} - 2 = 0 \\ x_{12} - 1 = 0 \\ x_{13} - 3 = 0 \\ x_{14} - 4 = 0 \\ x_{21} - 3 = 0 \\ x_{22} - 4 = 0 \\ x_{23} - 1 = 0 \\ x_{24} - 2 = 0 \\ x_{31} - 4 = 0 \\ x_{32} - 3 = 0 \\ x_{33} - 2 = 0 \\ x_{34} - 1 = 0 \\ x_{41} - 1 = 0 \\ x_{42} - 2 = 0 \\ x_{43} - 4 = 0 \\ x_{44} - 3 = 0 \end{cases} \quad \text{(A)}$$

Claramente, a solução de (A) é dada por:

$$\begin{aligned} &x_{11} = 2,\ x_{12} = 1,\ x_{13} = 3,\ x_{14} = 4, \\ &x_{21} = 3,\ x_{22} = 4,\ x_{23} = 1,\ x_{24} = 2, \\ &x_{31} = 4,\ x_{32} = 3,\ x_{33} = 2,\ x_{34} = 1, \\ &x_{41} = 1,\ x_{42} = 2,\ x_{43} = 4,\ x_{44} = 3 \end{aligned}$$

Voltando ao Shidoku proposto inicialmente, como cada x_{ij} obtido representa o dígito que ocupa cada uma de suas células (i, j) com $1 \leq i, j \leq 4$, temos que a Figura 12 é a representação do Shidoku preenchido com sua respectiva solução.

Figura 12 – Shidoku Resolvido

2	1	3	4
3	4	1	2
4	3	2	1
1	2	4	3

Fonte: O autor

8 CONCLUSÃO

Nesse trabalho resolvemos algebricamente um Shidoku por meio do cálculo de uma Base de Gröbner Reduzida. Essa resolução foi possível graças a modelagem do Shidoku por meio de um sistema de equações que foi implementado no software de computação algébrica CoCoA. Além disso, foi apresentada a teoria matemática que sustenta o cálculo de tais Bases.

A fim de tornar a leitura dessa dissertação mais leve, algumas demonstrações foram retiradas do texto principal e alocadas num Apêndice, assim como vários exemplos foram inseridos para que o entendimento das definições e dos resultados ocorresse de forma mais natural. O grande foco que foi dado à transição entre o anel de polinômios $\mathbb{K}[x]$ e o anel $\mathbb{K}[x_1, \ldots, x_n]$ tem a justificativa de que o caso unidimensional serve de base para a extensão para o caso multidimensional. Nesse aspecto, foi muito importante a observação da perda da unicidade do resto na chamada Pseudodivisão, para que então outra Teoria se apresentasse para cobrir essa "falha".

Uma possibilidade de continuação desse Trabalho consiste nas análises que podem ser feitas com a modelagem polinomial do Shidoku, como por exemplo, o estudo da relação da quantidade de valores iniciais do Shidoku com o seu número de soluções. Além disso, uma extensão possível é a implementação da solução de um Sudoku. Possivelmente, nesse caso, uma maior base em programação será necessária.

É importante salientar que a Teoria das Bases de Gröbner tem muitas outras aplicações, que podem servir de inspiração para outras pesquisas, como: braços robóticos no espaço tridimensional; quebra de sistemas criptográficos; prova automática de teoremas da Geometria (raciocínio autônomo); problemas de Programação Inteira; Coloração de Grafos; entre outras.

Em uma Iniciação Científica, espera-se que o aluno se aproprie do conteúdo e da execução da Pseudodivisão usando as principais Ordens Monomiais apresentadas. Além disso, que o discente ganhe autonomia com o uso do CoCoA. Isso permitirá que verifique respostas e crie seus próprios procedimentos. Lembramos que a habilidade de programar é uma nova habilidade indicada na BNCC.

REFERÊNCIAS

ARNOLD, E.; LUCAS, S.; TAALMAN, L. Gröbner basis representations of sudoku. *The College Mathematics Journal*, Washington, v. 41, p. 101–112, 03 2010.

BOYER, C. Sudoku's french ancestors. *The Mathematical Intelligencer*, Heidelberg, v. 29, n. 1, p. 37–44, Dec 2007. Disponível em: <https://doi.org/10.1007/BF02984758>. Acesso em: 05 fev. 2019.

COX, D.; LITTLE, J.; O'SHEA, D. *Ideals, Varieties, and Algorithms*. [S.l.]: Springer Verlag, 2015.

FRALEIGH, J.; KATZ, V. *A first course in abstract algebra*. [S.l.]: Addison-Wesley, 2003. (Addison-Wesley world student series).

HAYES, B. Computing science: Unwed numbers. *American Scientist*, Sigma Xi, The Scientific Research Society, UK, v. 94, n. 1, p. 12–15, 2006. Disponível em: <http://www.jstor.org/stable/27858699>. Acesso em: 05 fev. 2019.

HONG, H. et al. Bruno buchberger — a life devoted to symbolic computation. *J. Symb. Comput.*, Linz, v. 41, p. 255–258, 03 2006.

KRAMER, J.; PIPPICH, A.-M. von. *From Natural Numbers to Quaternions*. [S.l.: s.n.], 2017.

REITBERGER, H. Wolfgang grobner (11.2.1899–20.8.1980) zum 20. todestag. *Internationale Mathematische Nachrichten*, Wien, v. 184, p. 1–27, 08 2001.

APÊNDICES

APÊNDICE A – ALGUMAS DEMONSTRAÇÕES

A.1 $\mathbb{K}[x]$ é um domínio de integridade

Teorema 8. *Dado D um domínio de integridade, o conjunto*

$$D[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \ : \ n \in \mathbb{N} \ e \ a_i \in D\}$$

dos polinômios em x com coeficientes num domínio de integridade D é um domínio de integridade.

Demonstração. Considere dados

$$f = \sum_{i=0}^{m} f_ix^i \ , \ g = \sum_{i=0}^{n} g_ix^i \text{ e } h = \sum_{i=0}^{l} h_ix^i$$

polinômios em $D[x]$ com f_m, g_n e h_l todos não nulos. Para facilitar, completaremos alguns termos com coeficientes 0 para que tenhamos $m = n = l$.

1. **Fechamento da adição:** Como D é domínio de integridade,

$$f + g = \sum_{i=0}^{n} f_ix^i + \sum_{i=0}^{n} g_ix^i = \sum_{i=0}^{n} \underbrace{(f_i + g_i)}_{\in D} x^i$$

   é um elemento de $D[x]$.

2. **Associatividade da adição:**

$$\begin{aligned}
f + (g + h) &= \sum_{i=0}^{n} f_ix^i + \left(\sum_{i=0}^{n} g_ix^i + \sum_{i=0}^{n} h_ix^i \right) \\
&= \sum_{i=0}^{n} f_ix^i + \sum_{i=0}^{n} (g_i + h_i)x^i \\
&= \sum_{i=0}^{n} (f_i + (g_i + h_i))x^i \\
&= \sum_{i=0}^{n} ((f_i + g_i) + h_i)x^i \\
&= \sum_{i=0}^{n} (f_i + g_i)x^i + \sum_{i=0}^{n} h_ix^i \\
&= \left(\sum_{i=0}^{n} f_ix^i + \sum_{i=0}^{n} g_ix^i \right) + \sum_{i=0}^{n} h_ix^i \\
&= (f + g) + h
\end{aligned}$$

3. **Comutatividade da adição:**

$$f+g=\sum_{i=0}^{n} f_i x^i+\sum_{i=0}^{n} g_i x^i=\sum_{i=0}^{n}(f_i+g_i)x^i=\sum_{i=0}^{n}(g_i+f_i)x^i=\sum_{i=0}^{n} g_i x^i+\sum_{i=0}^{n} f_i x^i=g+f$$

4. **Elemento neutro da adição:** O polinômio $0=0+0x+0x^1+\cdots$ é o elemento neutro aditivo. De fato, dado qualquer polinômio $p \in D[x]$ temos $p+0=p=0+p$;

5. **Inverso aditivo:** O inverso aditivo do polinômio $f=\sum_{i=0}^{n} f_i x^i$ é o polinômio $\sum_{i=0}^{n}(-f_i)x^i$, de fato

$$\sum_{i=0}^{n} f_i x^i+\sum_{i=0}^{n}(-f_i)x^i=\sum_{i=0}^{n}(f_i-f_i)x^i=\sum_{i=0}^{n}(0)x^i=0$$

6. **Fechamento da multiplicação:** Como D é domínio de integridade,

$$f \cdot g=\sum_{k=0}^{m+n}\underbrace{\left(\sum_{i+j=k} f_i g_j\right)}_{\in \mathbb{K}} x^k$$

é um elemento de $D[x]$;

7. **Associatividade da multiplicação:**

$$\begin{aligned}
(fg)h &= \left[\sum_{q=0}^{m+n}\left(\sum_{i+j=q} f_i g_j\right)x^q\right]h \\
&= \left[\sum_{q=0}^{m+n}\left(\sum_{i+j=q} f_i g_j\right)x^q\right]\sum_{k=0}^{l} h_k x^k \\
&= \sum_{h=0}^{m+n+l}\left[\sum_{q+k=h}\left(\sum_{i+j=q} f_i g_j\right)h_k\right]x^h \\
&= \sum_{h=0}^{m+n+p}\left[\sum_{i+j+k=h} f_i g_j h_k\right]x^h \\
&= \sum_{h=0}^{m+n+p}\left[\sum_{i+r=h} f_i\left(\sum_{j+k=r} g_j h_k\right)\right]x^h \\
&= \sum_{s=0}^{m} f_s x^s\left[\sum_{r=0}^{n+l}\left(\sum_{j+k=r} g_j h_k\right)x^r\right] \\
&= f\left[\sum_{r=0}^{n+l}\left(\sum_{j+k=r} g_j h_k\right)x^r\right] \\
&= f(gh)
\end{aligned}$$

8. **Comutatividade da multiplicação:**

$$fg=\sum_{k=0}^{m+n}\left(\sum_{i+j=k} f_i g_j\right)x^k=\sum_{k=0}^{m+n}\left(\sum_{i+j=k} g_j f_i\right)x^k=gf$$

9. **Leis Distributivas** Como já provamos a comutatividade basta demonstrar que vale $f(g+h) = fg + fh$. De fato,

$$\begin{aligned} f(g+h) &= f\left(\sum_{j=0}^{n}(g_j+h_j)x^j\right) \\ &= \sum_{k=0}^{m+n}\left(\sum_{i+j=k} f_i(g_j+h_j)\right)x^k \\ &= \sum_{k=0}^{m+n}\left(\sum_{i+j=k} (f_ig_j + f_ih_j)\right)x^k \\ &= \sum_{k=0}^{m+n}\left(\sum_{i+j=k} f_ig_j\right)x^k + \sum_{k=0}^{m+n}\left(\sum_{i+j=k} f_ih_j\right)x^k \\ &= fg + fh \end{aligned}$$

Observe que a unidade de $D[x]$ é o polinômio $1 \in D$, de fato, $f \cdot 1 = f$ qualquer que seja f. Assim fica provado que $D[x]$ é um anel comutativo, com unidade. Para provar que $D[x]$ é um domínio de integridade basta considerar o produto de f por g ambos não-nulos. Neste produto o termo de maior grau será $f_m g_n x^{m+n}$. Como por hipótese temos f_m e g_n não nulos e D é um domínio de integridade então $fg \neq 0$. □

A.2 O domínio de integridade $(D[x])[y]$

Lema 0. *Se $D[x]$ é um domínio então $(D[x])[y] = (D[y])[x]$.*

Um elemento de $(D[x])[y]$ é um polinômio da forma abaixo:

$$P = f_n y^n + \cdots + f_1 y + f_0$$

onde $f_i = \sum_{j=0}^{m_i} a_{ij}x^j \in D[x],\ n, m_i \in \mathbb{Z}_+,\ a_{ij} \in \mathbb{K}, \forall i \in \{0, 1, \ldots n\}$

Dessa maneira:

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

então P pode também ser interpretado como um polinômio em $(D[y])[x]$. Fica assim provado que $(D[x])[y] = (D[y])[x]$, e, para aliviar as notações, nos referenciaremos a esse domínio simplesmente por $D[x, y]$.

A.3 Demonstrações do capítulo 5

Proposição 8. *Seja $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ um ideal e $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, então $f_1, \ldots, f_s \in I$ se, e somente se $\langle f_1, \ldots, f_s \rangle \subseteq I$.*

Demonstração. ($\Rightarrow$) Tome $f \in \langle f_1, \ldots, f_s \rangle$ então $f = \sum_{i=1}^{s} h_i f_i = h_1 f_1 + \cdots + h_s f_s$ para determinados $h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$. Como I é um ideal e por hipótese $f_1, \ldots, f_s \in I$ temos $h_i f_i \in I$ para cada i e finalmente $f = h_1 f_1 + \cdots + h_s f_s \in I$ pois é uma soma de elementos de I.

($\Leftarrow$) É claro que $f_1, \ldots, f_s \in \langle f_1, \ldots, f_s \rangle$ e como por hipótese $\langle f_1, \ldots, f_s \rangle \subseteq I$ então $f_1, \ldots, f_s \in I$ □

Proposição 9. *Seja $I = \langle X^\alpha : \alpha \in A \rangle$ um ideal monomial. Então um monômio X^β pertence ao ideal I se e somente se X^β é divisível por X^α para algum $\alpha \in A$.*

Demonstração. Suponhamos que $X^\beta \in I$. Assim, $X^\beta = \sum_{i=1}^{s} h_i X^{\alpha_i}$, onde $h_i \in \mathbb{K}[x_1, \ldots, x_n]$ e $\alpha_i \in A$. Como cada h_i pode ser expandido como uma soma de monômios com coeficientes em $\mathbb{K}$, temos:

$$X^\beta = \sum_{i=1}^{s} h_i X^{\alpha_i} = \sum_{i=1}^{s} \left(\sum_{j=1}^{k_i} a_{ij} X^{\beta_{ij}} \right) X^{\alpha_i} = \sum_{i,j} a_{ij} X^{\beta_{ij}} X^{\alpha_i}$$

onde a expressão à direita é uma soma de monômios, cada um, divisível por algum X^α, com $\alpha \in A$. Logo, o monômio X^β é divisível por algum X^α. Reciprocamente, se X^β for divisível por X^α, para algum $\alpha \in A$, então $X^\beta \in I$, pela definição de ideal. □

Proposição 10. *Sejam I um ideal monomial de $\mathbb{K}[x_1, \ldots, x_n]$ e $f \in \mathbb{K}[x_1, \ldots, x_n]$. Então são equivalentes:*

1. *$f \in I$*
2. *todo termo de f está em I*
3. *f é uma $\mathbb{K}$-combinação linear de monômios em I*

Demonstração. (3)$\Rightarrow$(2)$\Rightarrow$ (1) Seguem da definição de ideal.

(1)$\Rightarrow$(3) Se $f \in I$, temos que $f = \sum_{i=1}^{s} h_i X^{\alpha_i}$, com $h_i \in \mathbb{K}[x_1, \ldots, x_n]$ e $X^{\alpha_i} \in I$. Como fizemos na proposição (9), expandindo cada h_i como uma combinação linear de monômios podemos escrever

$$f = \sum_{i=1}^{s} \sum_{j=1}^{k_i} a_{ij} X^{\beta_{ij}} X^{\alpha_i}, \tag{A.1}$$

onde $a_{ij}X^{\beta_{ij}}$ é um termo do polinômio h_i, com $j = 1, \ldots, k_i$ e $a_{ij} \in \mathbb{K}$. Como I é um ideal, o produto $X^{\beta_{ij}}X^{\alpha_i}$ é um monômio de I. Assim, podemos concluir que f é uma $\mathbb{K}$-combinação linear de monômios em I.

□

Lema 2 (Lema de Dickson)**.** *Se I um ideal monomial de $\mathbb{K}[x_1, \ldots, x_n]$, então existe um conjunto finito de monômios que geram I.*

Demonstração. Vamos provar o teorema usando indução sobre o número de indeterminadas de $\mathbb{K}[x_1, \ldots, x_n]$. O caso de uma indeterminada é verdadeiro, uma vez que em $\mathbb{K}[x_1]$ todo ideal é principal, consequentemente, pode ser gerado por um único polinômio, que neste caso se resume a um monômio.

Vamos considerar o teorema válido para $n-1$ indeterminadas. Agora, se I é um ideal monomial de $\mathbb{K}[x_1, \ldots, x_n]$, escolha um elemento $f_1 = g_1 x_n^{\alpha_{n1}} \in I$, com g_1 um monômio em $\mathbb{K}[x_1, \ldots, x_{n-1}]$ e α_{n1} o menor possível. Se $I = \langle f_1 \rangle$, então o teorema está demonstrado. Caso contrário, escolha um elemento $f_2 = g_2 x_n^{\alpha_{n2}} \in I \setminus \langle f_1 \rangle$, com g_2 um monômio em $\mathbb{K}[x_1, \ldots, x_{n-1}]$ e α_{n2} o menor possível. Observe que, obrigatoriamente, temos que $\alpha_{n2} \geq \alpha_{n1}$ pois, caso contrário, f_1 foi escolhido de forma errada. Se $I = \langle f_1, f_2 \rangle$, então o teorema está demonstrado. Caso contrário, continuamos com o procedimento.

Vamos supor que este procedimento continua indefinidamente, ou seja, é possível obter uma seqüência infinita $f_1, f_2, \ldots$ tal que $f_i = g_i x_n^{\alpha_{ni}} \in I \setminus \langle f_1, \ldots, f_{i-1} \rangle$, com g_i um monômio em $\mathbb{K}[x_1, \ldots, x_{n-1}]$, α_{ni} o menor possível e $\alpha_{ni} \geq \alpha_{n(i-1)}$.

Por hipótese de indução, temos que o ideal $J \in \mathbb{K}[x_1, \ldots, x_{n-1}]$ gerado pelos monômios $g_1, g_2, \ldots$ é finitamente gerado, digamos que $I = \langle g_1, \ldots g_k \rangle$, para algum índice k. Deste modo, segue da Proposição 9, que g_{k+1} é divisível por algum g_i, para $i = 1, \ldots k$, digamos, $g_{k+1} = hg_m$, para algum monômio $h \in \mathbb{K}[x_1, \ldots, x_{n-1}]$. Logo

$$f_{k+1} = g_{k+1}x_n^{\alpha_{n(k+1)}} = hg_m x_n^{\alpha_{n(k+1)}} = hx_n^{\alpha_{n(k+1)}-\alpha_{nm}}(g_m x_n^{\alpha_{nm}}) = hx_n^{\alpha_{n(k+1)}-\alpha_{nm}} f_m$$

e então $f_{k+1} \in \langle f_m \rangle$, contrariando a escolha do f_{k+1}. Assim, I é finitamente gerado. □

Lema 3. *Considere $\succ$ uma ordem monomial e $\sum_{i=1}^{s} c_i f_i$, com $c_i \in \mathbb{K}$ e $\operatorname{multideg}(f_i) = \delta \in \mathbb{Z}_+^n$, para todo $i \in \{1, \ldots, s\}$. Se $\delta \succ \operatorname{multideg}(\sum_{i=1}^{s} c_i f_i)$, então $\sum_{i=1}^{s} c_i f_i$ é uma $\mathbb{K}$-combinação linear de* S*-processos* $\mathrm{S}(f_j, f_k)$ *para $1 \leq j, k \leq s$. Além disso, $\delta \succ \operatorname{multideg}(\mathrm{S}(f_j, f_k))$, para $1 \leq j, k \leq s$.*

Demonstração. Seja $d_i = \mathrm{LC}(f_i)$ de modo que $c_i d_i = \mathrm{LC}(c_i f_i)$. Como $c_i f_i$ tem multigrau δ e $\delta \succ \operatorname{multideg}(\sum_{i=1}^{s} c_i f_i)$, segue que $\sum_{i=1}^{s} c_i d_i = 0$.

Definindo $p_i = f_i/d_i$, temos que p_i é um polinômio com coeficiente líder igual à 1. Agora, considere a seguinte soma:

$$\begin{aligned}\textstyle\sum_{i=1}^{s} c_i f_i &= \textstyle\sum_{i=1}^{s} c_i d_i p_i \\ &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \ldots \\ &+ (c_1 d_1 + \ldots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \ldots + c_s d_s) p_s\end{aligned} \tag{A.2}$$

Sabemos que $\mathrm{LT}(f_i) = d_i X^\delta$, para todo $i = 1, \ldots, s$, o que implica em

$$\mathrm{MMC}(\mathrm{LM}(f_j), \mathrm{LM}(f_k)) = X^\delta$$

. Então:

$$\mathrm{S}(f_j, f_k) = \frac{X^\delta}{\mathrm{LT}(f_j)} f_j - \frac{X^\delta}{\mathrm{LT}(f_k)} f_k = \frac{X^\delta}{d_j X^\delta} f_j - \frac{X^\delta}{d_k X^\delta} f_k = \frac{f_j}{d_j} - \frac{f_k}{d_k} = p_j - p_k \tag{A.3}$$

Usando as igualdades (A.3) e (A.2), e o fato de que $\sum_{i=1}^{s} c_i d_i = 0$, temos que:

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 \,\mathrm{S}(f_1, f_2) + (c_1 d_1 + c_2 d_2)\,\mathrm{S}(f_2, f_3) + \ldots + (c_1 d_1 + \ldots + c_{s-1} d_{s-1})\,\mathrm{S}(f_{s-1}, f_s),$$

que é a soma desejada. Finalmente, observe que $\delta \succ \mathrm{multideg}(p_j - p_k)$, pois p_j e p_k têm multigrau δ e coeficiente líder 1. Pela igualdade (A.3), temos que $\delta \succ \mathrm{multideg}(\mathrm{S}(f_j, f_k))$. □

Teorema 5 (Critério de Buchberger)**.** *Seja $I = \langle g_1, \ldots, g_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$ um ideal. Então $G = \{g_1, \ldots, g_s\}$ é uma Base de Gröbner para I se, e somente se, para todos os pares $i \neq j$, o resto na pseudodivisão de $\mathrm{S}(g_i, g_j)$ por G (com qualquer ordenação) é zero.*

Demonstração. ($\Rightarrow$) Se G é uma base de Gröbner, então como $\mathrm{S}(g_i, g_j) \in I$, segue do Corolário 3 que o resto na divisão por G é zero.

($\Leftarrow$) Seja $f \in I = \langle g_1, \ldots, g_s \rangle$ um polinômio não nulo. Precisamos mostrar que $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Antes, porém, faremos um esboço da prova para facilitar o entendimento.

Sabemos que f pode ser escrito da forma:

$$f = \sum_{i=1}^{s} h_i g_i, \tag{A.4}$$

com $h_i \in \mathbb{K}[x_1, \ldots, x_n]$, e do Lema 7 temos que:

$$\max\{\mathrm{multideg}(h_i g_i)\} \succcurlyeq \mathrm{multideg}(f). \tag{A.5}$$

Observe que o teorema já estaria provado se ocorresse a igualdade em (A.5). De fato, teríamos $\mathrm{LT}(f)$ divisível por $\mathrm{LT}(g_i)$, para algum $i \in \{1, \ldots, s\}$ e, pelo Lema 9, poderíamos concluir que $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$.

Assim, vamos mostrar que existem $\widetilde{h}_1, \ldots, \widetilde{h}_s \in \mathbb{K}[x_1, \ldots, x_n]$, tais que $f = \sum_{i=1}^{s} \widetilde{h}_i g_i$ e $\max\{\mathrm{multideg}(\widetilde{h}_i g_i)\} = \mathrm{multideg}(f)$.

Passemos aos detalhes da prova. Considere f como em (A.4), $m(i) = \mathrm{multideg}(h_i g_i)$ e $\delta = \max\{m(1), \ldots, m(s)\}$. Assim, segue de (A.5) que $\delta \succcurlyeq \mathrm{multideg}(f)$.

Agora considere todos os modos possíveis de se escrever f na forma (A.4). Talvez tenhamos um δ diferente para cada um desses modos. Mas, como vale o Princípio da Boa Ordenação para ordens monomiais, podemos tomar, dentre os possíveis δ, o mínimo, que designaremos por δ_0. Logo, existem $\widetilde{h}_1, \ldots, \widetilde{h}_s \in \mathbb{K}[x_1, \ldots, x_n]$, tais que $f = \sum_{i=1}^{s} \widetilde{h}_i g_i$ com $\delta_0 \succcurlyeq \mathrm{multideg}(f)$.

Vamos mostrar que $\delta_0 = \mathrm{multideg}(f)$, provando assim o teorema. De fato, vamos supor que $\delta_0 \succ \mathrm{multideg}(f)$. Reescrevendo f, isolando os termos de multigrau δ_0, temos:

$$f = \sum_{m(i)=\delta_0} \widetilde{h}_i g_i + \sum_{\delta_0 \succ m(i)} \widetilde{h}_i g_i \tag{A.6}$$

$$= \sum_{m(i)=\delta_0} \mathrm{LT}(\widetilde{h}_i) g_i + \sum_{m(i)=\delta_0} (\widetilde{h}_i - \mathrm{LT}(\widetilde{h}_i)) g_i + \sum_{\delta_0 \succ m(i)} \widetilde{h}_i g_i \tag{A.7}$$

Observe que δ_0 é maior ($\succ$) que o multigrau dos monômios da segunda soma e da terceira soma na segunda linha. Mas como $\delta_0 \succ \mathrm{multideg}(f)$, então δ_0 também é maior ($\succ$) que o multigrau da primeira soma.

Se $\mathrm{LT}(\widetilde{h}_i) = c_i X^{\alpha^i}$, então a primeira soma $\sum_{m(i)=\delta_0} \mathrm{LT}(\widetilde{h}_i) g_i = \sum_{m(i)=\delta_0} c_i X^{\alpha^i} g_i$ atende às condições do Lema 3, considerando $f_i = X^{\alpha^i} g_i$. Então essa soma é uma combinação linear de S-processos $\mathrm{S}(X^{\alpha^j} g_j, X^{\alpha^k} g_k)$. Entretanto:

$$\mathrm{S}(X^{\alpha^j} g_j, X^{\alpha^k} g_k) = \frac{X^{\delta_0}}{X^{\alpha^j} \mathrm{LT}(g_j)} X^{\alpha^j} g_j - \frac{X^{\delta_0}}{X^{\alpha^k} \mathrm{LT}(g_k)} X^{\alpha^k} g_k = X^{\delta_0 - \gamma^{jk}} \mathrm{S}(g_j, g_k),$$

onde $X^{\gamma^{jk}} = \mathrm{MMC}(\mathrm{LM}(g_j), \mathrm{LM}(g_k))$. Portanto, existem constantes $c_{jk} \in \mathbb{K}$ tais que:

$$\sum_{m(i)=\delta_0} \mathrm{LT}(\widetilde{h}_i) g_i = \sum_{jk} c_{jk} X^{\delta_0 - \gamma^{jk}} \mathrm{S}(g_j, g_k) \tag{A.8}$$

Temos ainda a hipótese de $\overline{\mathrm{S}(g_j, g_k)}^{G} = 0$. Assim, usando o algoritmo da divisão, podemos escrever $\mathrm{S}(g_j, g_k)$ na forma:

$$\mathrm{S}(g_j, g_k) = \sum_{i=1}^{s} a_{ijk} g_i, \tag{A.9}$$

onde $a_{ijk} \in \mathbb{K}[x_1, \ldots, x_n]$. O algoritmo da divisão também nos diz que:

$$\text{multideg}(\text{S}(g_j, g_k)) \succcurlyeq \text{multideg}(a_{ijk} g_i), \tag{A.10}$$

para todo i, j, k. Multiplicando a expressão (A.9) por $X^{\delta_0 - \gamma^{jk}}$ obtemos:

$$X^{\delta_0 - \gamma^{jk}} \, \text{S}(g_j, g_k) = \sum_{i=1}^{s} b_{ijk} g_i, \tag{A.11}$$

onde $b_{ijk} = X^{\delta_0 - \gamma^{jk}} a_{ijk}$. Então a condição (A.8) e o Lema 3 implicam em:

$$\delta_0 \succ \text{multideg}(X^{\delta_0 - \gamma^{jk}} \, \text{S}(g_j, g_k)) \succcurlyeq \text{multideg}(b_{ijk} g_i) \tag{A.12}$$

Substituindo (A.11) em (A.8) temos a igualdade:

$$\textstyle\sum_{m(i)=\delta_0} \text{LT}(\widetilde{h}_i) g_i = \sum_{jk} c_{jk} X^{\delta - \gamma^{jk}} \overline{\text{S}(g_j, g_k)}^{G} = \sum_{jk} c_{jk} (\sum_i b_{ijk} g_i) = \sum_i \bar{h}_i g_i,$$

que por (A.12) tem a propriedade válida para todo i:

$$\delta_0 \succ \text{multideg}(\bar{h}_i g_i)$$

Finalmente, substituindo $\sum_{m(i)=\delta_0} \text{LT}(\widetilde{h}_i) g_i = \sum_i \bar{h}_i g_i$ em (A.3), temos que:

$$f \;\; = \textstyle\sum_{m(i)=\delta_0} \bar{h}_i g_i + \sum_{m(i)=\delta_0} (\widetilde{h}_i - \text{LT}(\widetilde{h}_i)) g_i + \sum_{\delta_0 \succ m(i)} \widetilde{h}_i g_i.$$

Observe que, agora passamos a ter não somente δ_0 maior ($\succ$) que todos os multigraus dos termos da segunda e da terceira soma, mas também maior ($\succ$) que todos os multigraus dos termos da primeira soma (repare que em (A.3) tínhamos apenas que δ_0 era maior ($\succ$) que o multigrau da primeira soma como um todo). Mas, isso contradiz a minimalidade de δ_0 e o teorema está provado. □

Teorema 7. *Seja $I \neq \{0\}$ um ideal polinomial. Então, dada uma ordem monomial, I possui uma única base de Gröbner reduzida.*

Demonstração. (**Existência**) Seja G uma base de Gröbner mínima para I. Dizemos que $g \in G$ é reduzido para G quando nenhum monômio de g pertence a $\langle \text{LT}(G - \{g\}) \rangle$. Nosso objetivo é modificar a base G até que todos os seus elementos sejam reduzidos.

Dado $g \in G$, considere $g' = \overline{g}^{(G - \{g\})}$ e o conjunto $G' = (G - \{g\}) \cup \{g'\}$. Afirmamos que G' é uma base de Gröbner mínima para I. De fato, quando dividimos g por $G - \{g\}$, $\text{LT}(g)$ é um termo do resto, pois ele não é divisível por nenhum elemento de $\text{LT}(G - \{g\})$. Assim $\text{LT}(g') = \text{LT}(g)$, e portanto $\text{LT}(G) = \text{LT}(G')$ e $\langle \text{LT}(G') \rangle = \langle \text{LT}(G) \rangle = \langle \text{LT}(I) \rangle$. Como $G' \subset$

I, da igualdade anterior temos que G' é uma base de Gröbner e, por construção, mínima. Além disso, g' é reduzido para G'. Realmente, nenhum monômio de g' está em $\langle \mathrm{LT}(G' - \{g'\})\rangle = \langle \mathrm{LT}(G - \{g\})\rangle$, pois g' é o resto da divisão de g por $G - \{g\}$.

Por fim, repetindo o processo acima para cada elemento de G, encontraremos uma base de Gröbner reduzida. É claro que a base de Gröbner mudará a cada etapa do processo. Entretanto, uma vez que o elemento é reduzido, ele permanecerá assim até o fim do processo, pois em cada passo os termos líderes são conservados, isto é, $\mathrm{LT}(G) = \mathrm{LT}(G')$.

(**Unicidade**) Suponha que G e $\widetilde{G}$ são duas bases de Gröbner reduzidas para I. Então, G e $\widetilde{G}$ são duas bases de Gröbner mínimas e, pelo Lema 4, elas têm os mesmos termos líderes, isto é, $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$. Assim, dado $g \in G$, existe $\widetilde{g} \in \widetilde{G}$ tal que $\mathrm{LT}(g) = \mathrm{LT}(\widetilde{g})$. Se mostrarmos que $g = \widetilde{g}$, seguirá que $G = \widetilde{G}$, e a unicidade estará provada.

Para mostrar que $g = \widetilde{g}$, considere $g - \widetilde{g}$. Sabemos que $g - \widetilde{g} \in I$, e como G é uma base de Gröbner, temos $\overline{g - \widetilde{g}}^{G} = 0$. Mas, $\mathrm{LT}(g) = \mathrm{LT}(\widetilde{g})$, esses termos se cancelam em $g - \widetilde{g}$ e os termos restantes não são divisíveis por nenhum dos elementos de $\mathrm{LT}(G) = \mathrm{LT}(\widetilde{G})$, pois G e $\widetilde{G}$ são bases de Gröbner reduzidas. Então, $\overline{g - \widetilde{g}}^{G} = g - \widetilde{g}$ e $g - \widetilde{g} = 0$. Logo, $g = \widetilde{g}$. □