UNIVERSIDADE FEDERAL DA PARAÍBA

Centro de Ciências Exatas e da Natureza

Departamento de Matemática

Curso de Graduação em Matemática

LEMA DE GAUSS

GUSTAVO VINICIUS CALISTO DE OLIVEIRA

João Pessoa

Outubro de 2024

Gustavo Vinicius Calisto de Oliveira

Lema de Gauss

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Licenciatura em Matemática da Universidade Federal da Paraíba como requisito parcial para a obtenção do título de Licenciado em Matemática.

Orientador: Prof. Dr. Ricardo Burity Croccia Macedo

João Pessoa
Outubro de 2024

Catalogação na publicação
Seção de Catalogação e Classificação

O48l Oliveira, Gustavo Vinicius Calisto de.
Lema de Gauss / Gustavo Vinicius Calisto de Oliveira. - João Pessoa, 2024.
64 p. : il.

Orientação: Ricardo Burity Croccia Macedo.
TCC (Curso de Licenciatura em Matemática) - UFPB/CCEN.

1. Anel de polinômios. 2. Domínios. 3. Lema de Gauss. I. Macedo, Ricardo Burity Croccia. II. Título.

UFPB/CCEN CDU 51(043.2)

Elaborado por Josélia Maria Oliveira da Silva - CRB-15/113

Gustavo Vinicius Calisto de Oliveira

Lema de Gauss

Trabalho de Conclusão de Curso apresentado à coordenação do Curso de Licenciatura em Matemática da Universidade Federal da Paraíba como requisito parcial para a obtenção do título de licenciado em Matemática. Orientador: Ricardo Burity Croccia Macedo. Aprovado em: 28/10/2024

BANCA EXAMINADORA

Documento assinado digitalmente
gov.br
RICARDO BURITY CROCCIA MACEDO
Data: 19/11/2024 09:48:31-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Ricardo Burity Croccia Macedo

Orientador - UFPB - Campus I

Documento assinado digitalmente
gov.br
WALLACE MANGUEIRA DE SOUSA
Data: 19/11/2024 10:15:06-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Wallace Mangueira de Sousa

Avaliador - UFPB - Campus I

Me. João Pedro Viana Correia Borges

Avaliador - UFPB - Campus I

Ao meu pai, por me apresentar o caminho.

Agradecimentos

Primeiramente, gostaria de agradecer a Deus por me permitir chegar até aqui. Mesmo nas tempestades da vida, foste meu farol de confiança e fé, sustentando-me e dando-me forças para não deixar de sonhar.

Agradeço também aos meus pais, Gilson e Andrea, por tudo. Pelo esforço em me proporcionar uma boa educação formal, em um ambiente onde os estudos sempre foram priorizados, e por me educarem com os valores que carrego comigo. Agradeço ainda ao meu falecido padrasto, Wellington, por ter sido uma pessoa incrível que tive a honra de conhecer. À minha madrasta, Josefa, sou grato por ser como uma mãe para mim, sempre me orientando e instruindo nos melhores caminhos.

Igualmente importantes são meus avós, que plantaram em mim a semente dos sonhos, cujos frutos colho hoje. Em especial, minha avó materna, Rozinete, conhecida como Dona Rosa, minha figura materna que sempre cuidou de mim com todo amor e carinho, e que sempre esteve e estará ao meu lado. Obrigado por tudo.

Aos meus irmãos, que são minha fonte de inspiração e de quem aprendi tanto, obrigado pela amizade e confiança. Aos meus familiares, que sempre me apoiaram e nunca mediram esforços para estar presentes em minha vida, o meu sincero obrigado.

Com todo meu amor e carinho, agradeço à minha namorada por estar ao meu lado em tantos momentos. Ela não mede esforços para me apoiar, nutre meus sonhos e metas, confia em mim com todo o seu amor e enfrentou as minhas batalhas comigo. Obrigado por tudo.

Quero agradecer também ao professor Burity, meu incrível orientador, que, além de ser um grande mestre, tornou-se um grande amigo. Foi ele quem me deu a oportunidade de participar de um projeto científico, o PIBIC. Sua relação com a Matemática, seu amor pela álgebra e seu zelo pelos alunos e pelas pessoas ao seu redor são admiráveis. Estendo meu agradecimento a todos os professores que contribuíram para minha formação.

Não poderia deixar de citar meus amigos, que me acompanharam nessa longa caminhada, tornando-a mais leve e feliz. Aos novos amigos que a matemática trouxe à minha jornada, cursar matemática ao lado de cada um de vocês foi uma honra e um privilégio.

Por fim, um grande obrigado a todos.

”Não é o conhecimento, mas o ato de aprender, não a posse, mas o ato de alcançar, que concede o maior prazer.”(Carl Friedrich Gauss)

Resumo

Esse trabalho se propõe a oferecer uma introdução ao estudo do lema de Gauss. Motivamos a sua exposição baseada em dois objetivos centrais. Primeiramente, construir de forma natural e motivada os conceitos abstratos da teoria de anéis, para que o leitor iniciante possa abstrair as ideias principais e a filosofia central da teoria. Em segundo lugar, damos um enfoque especial em contextualizar e detalhar alguns conceitos menos abordados, porém vitais, a exemplo de noções como domínios de Fatoração Única, Euclideanos e de Ideais Principais, além de Anéis Noetherianos e o Teorema da Base de Hilbert. Nesse viés, os resultados passeiam em torno da estrutura algébrica de um anel, versando em torno de anéis polinomiais. Ao fim, mostramos como o tema central do trabalho se comporta ambientado em domínios.

Palavras-chave: Anel de polinômios, Domínios, Lema de Gauss.

Abstract

This work aims to provide an introduction to the study of Gauss's lemma. We motivate its presentation based on two central objectives. Firstly, to naturally and meaningfully construct the abstract concepts of ring theory, allowing beginner readers to grasp the main ideas and the central philosophy of the theory. Secondly, we place special emphasis on contextualizing and detailing some less-addressed yet vital concepts, such as unique factorization domains, Euclidean domains, principal ideal domains, as well as Noetherian rings and the Hilbert Basis Theorem. In this regard, the results explore the algebraic structure of a ring, focusing on polynomial rings. Finally, we demonstrate how the central theme of the work behaves within the context of domains.

Keywords: Polynomial ring, Domains, Gauss's lemma.

Sumário

Introdução 11

1 Anéis **12**

1.1 Anéis 12

1.2 Subanéis 13

1.3 Domínio de Integridade 14

1.4 Corpos 15

1.5 Ideais 17

1.6 Anel Quociente 21

1.7 Homomorfismo de Anéis 23

2 Anéis de Polinômios **28**

2.1 Polinômios em uma indeterminada 29

2.2 Anéis de Polinômios em uma indeterminada 35

2.2.1 A imersão de A em $A[x]$ 39

2.3 Anéis de Polinômios em um número finito de indeterminadas 41

2.4 Estruturas Finitamente Geradas: A Ascensão de Hilbert e Noether 44

2.4.1 Anéis Noetherianos 45

2.4.2 O Teorema da Base de Hilbert 47

3 Lema de Gauss **50**

3.1 O Clássico Lema de Gauss 50

3.2 Fundamentos da Fatoração: Caminho ao Lema de Gauss 53

3.2.1 Domínio Euclidiano 54

3.2.2 Domínio de Ideais Principais 55

3.2.3 Domínio de Fatoração Única 56

3.3 Generalização do Lema de Gauss 59
3.3.1 Corpo de Frações 60

Introdução

O Lema de Gauss, um dos pilares da teoria dos números, é um resultado que transcende a simples análise de polinômios, oferecendo uma visão profunda sobre a estrutura dos números inteiros e suas propriedades. Este trabalho tem como objetivo explorar o Lema de Gauss em sua forma clássica e suas generalizações, proporcionando uma compreensão abrangente de sua importância e aplicações na matemática contemporânea.

A motivação para o estudo do Lema de Gauss surge da necessidade de entender a irredutibilidade de polinômios em diferentes domínios. A versão clássica do Lema afirma que se um polinômio é irredutível sobre os inteiros, então ele também é irredutível sobre os racionais. Essa propriedade não apenas estabelece uma conexão entre os números inteiros e racionais, mas também serve como uma ferramenta poderosa para a análise de polinômios em contextos mais amplos, como anéis e corpos.

Neste trabalho, abordaremos inicialmente o Lema de Gauss em seu contexto clássico, apresentando definições e exemplos que ilustram sua aplicação. A partir dessa base, avançaremos para o Lema de Gauss generalizado, que se aplica a domínios de integridade, ampliando o escopo do teorema e suas implicações. Através de uma abordagem sistemática, pretendemos construir uma ponte entre a teoria e a prática, permitindo que o leitor compreenda não apenas o ”como”, mas também o ”porquê”por trás das afirmações matemáticas.

Além disso, este trabalho busca motivar o leitor a apreciar a beleza e a elegância da matemática, mostrando como conceitos abstratos podem ser aplicados a problemas concretos ainda que de cunho matemático. A teoria de anéis, que será explorada ao longo do texto, é um campo rico e fascinante que oferece uma nova perspectiva sobre a estrutura algébrica dos números. Ao introduzir esses conceitos de maneira acessível, esperamos que o leitor desenvolva uma compreensão mais profunda e uma apreciação pela matemática.

Por fim, este trabalho é uma homenagem ao legado de Carl Friedrich Gauss, cujas contribuições à matemática continuam a influenciar gerações de matemáticos. Ao estudar o Lema de Gauss, não apenas exploramos um resultado matemático, mas também nos conectamos a uma tradição intelectual que valoriza a curiosidade, a rigorosidade e a busca pelo conhecimento.

Capítulo 1

Anéis

Neste capítulo será apresentado a estrutura algébrica do anel. Ao decorrer do mesmo, apresentaremos algumas definições, propriedades e observações essenciais para melhor interpretação do texto presente. Além disso, eventualmente, serão apresentadas demonstrações e resultados para maior compreensão.

1.1 Anéis

Em álgebra, um anel é uma estrutura algébrica composta por um conjunto A não vazio munido de operações binárias que possuem certas propriedades. Estas operações devem satisfazer uma série de axiomas que garantem a funcionalidade da estrutura.

Definição 1.1.1. Um **anel** é um conjunto A munido de duas operações binárias, denominadas soma e produto,

$$\begin{aligned} + : A \times A &\to A & \cdot : A \times A &\to A \\ (x, y) &\mapsto x + y & (x, y) &\mapsto x \cdot y \end{aligned}$$

que satisfazem, para todos $x, y, z \in A$, as seguintes propriedades:

I) Associatividade da soma: $(x + y) + z = x + (y + z)$;

II) Existência do elemento neuto para soma: $\exists\ 0_A = 0 \in A$ tal que $0 + x = x + 0 = x$;

III) Existência de simétricos aditivos: Dado $x \in A, \exists\ y \in A$ tal que $x + y = y + x = 0$;

IV) Comutatividade da soma: $x + y = y + x$;

V) Associatividade do produto: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;

VI) Distributividade do produto em relação à soma: $x \cdot (y + z) = x \cdot y + x \cdot z, \quad (y + z) \cdot x = y \cdot x + z \cdot x$.

Para cada x elemento de A, o elemento y da condição III) é único, por isso, utilizaremos a notação $y = -x$.

Ao longo desta monografia os respectivos compostos $x + y$ e $x \cdot y$ são denominados **soma** e **produto**.

Definição 1.1.2. Um anel A é chamado de:

I. **Anel comutativo**, se para quaisquer $a, b \in A$, tem-se $a \cdot b = b \cdot a$. (Comutatividade do produto).

II. **Anel unitário** ou, **Anel com unidade**, se $\exists\ 1_A = 1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a, \forall\ a \in A$. (Existência de elemento identidade para o produto).

Convenção 1.1.1. Assumiremos, a partir de agora que todos os anéis presentes neste trabalho são comutativos com unidade. A operação $x \cdot y$ será denotada por xy, $\forall\ x, y \in A$.

Exemplo 1.1.1. O conjunto dos números inteiros $\mathbb{Z}$, com as operações usuais de soma e multiplicação, é um anel comutativo com unidade, assim como os demais conjuntos numéricos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são exemplos de anéis comutativos com unidade munidos das operações usuais de soma e produto.

Exemplo 1.1.2. Um número **Inteiro de Gauss** é um elemento do formato $a + b \cdot i$ em que $a, b \in \mathbb{Z}$ e $i = \sqrt{-1}$. Denote por $\mathbb{Z}[i]$ o conjunto formado por todos esses elementos. Observe que $\mathbb{Z}[i] \subset \mathbb{C}$. Munindo o conjunto $\mathbb{Z}[i]$ com a soma e o produto dos números complexos, temos que $\mathbb{Z}[i]$ é um anel.

1.2 Subanéis

Um subanel é um tipo especial de subconjunto de um anel.

Definição 1.2.1. Sejam A um anel e S um subconjunto não vazio de A. O subconjunto S é chamado de **subanel** de A, se S possui a estrutura de anel com as operações de A.

Proposição 1.2.1. *Sejam A um anel e S um subconjunto não vazio de A. Então, S é um* ***subanel*** *de A se, somente se, para quaisquer $a, b \in S$:*

I) $1 \in S$

II) $a - b \in S$

III) $a \cdot b \in S$

Demonstração. ($\Rightarrow$) Se S é um subanel de A, então para quaisquer $a, b \in S$, tem-se que $-b \in S$ e $a + (-b) = a - b \in S$, já que " $+$ " é uma operação em S. Do mesmo modo, $a \cdot b \in S$, visto que " $\cdot$ " é uma operação em S. Desde que os anéis tratados neste trabalho são comutativos com unidade, a condição I) segue imediatamente.

($\Leftarrow$) Iremos supor que as condições são válidas e que $S \subset A$. Considere $a, b \in S$ com $a = b$. Pelo item (I), segue que $a - b = a - a = 0 \in S$. Se considerarmos $x \in S$, então $-x = 0 - x \in S$. Deste modo, se $x, y \in S$, segue que $x + y = x - (-y) \in S$, isso quer dizer o conjunto S é fechado para soma. Ademais, pelo item (II), tem-se que $x \cdot y \in S$ para quaisquer $x, y \in S$. Por conseguinte, as demais condições da definição de anel são automaticamente herdadas do anel A, visto que $S \subseteq A$. Concluí-se que S é um subanel de A.

□

Exemplo 1.2.1. O conjunto dos inteiros $\mathbb{Z}$ é um subanel do anel dos números dos racionais $\mathbb{Q}$, pois $\mathbb{Z}$ é fechado sob soma e produto e contém o elemento identidade 1 do produto.

Exemplo 1.2.2. O anel dos inteiros de Gauss, o conjunto $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, é um subanel do anel dos números complexos $\mathbb{C}$.

1.3 Domínio de Integridade

Ao vermos uma equação do tipo $(x + 7)(x - 7) = 0$ trabalhada no conjunto $\mathbb{R}$, anel dos números Reais, concluímos de imediato que $x - 7 = 0$ ou $x + 7 = 0$, ou seja, $x = \pm 7$ (isso quer dizer que $x = 7$ ou $x = -7$). Essa conclusão é quase que instantânea, pois o conjunto dos números reais é um anel que não possui divisor de zero diferente do próprio elemento nulo. Vamos a generalização deste fato a um anel qualquer.

Definição 1.3.1. Sejam A um anel e $a \in A$. Dizemos que a é um **divisor de zero** (de A) se existe $b \neq 0$ em A tal que $a \cdot b = 0$.

Note que o elemento nulo é um divisor de zero de A. No entanto, existem exemplos de anéis que possuem divisores de zero não triviais.

Exemplo 1.3.1. Denote o conjunto das funções $f : \mathbb{R} \to \mathbb{R}$ por A. Note que A é um anel com operações de soma e produto dadas de maneira pontual, isto é, $(f + g)(x) = f(x) + g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$, para todo x número real. Note que o elemento

$$f(x) = \begin{cases} 0, & \text{se } x < 0, \\ x, & \text{se } x \geqslant 0 \end{cases}$$

é um divisor de zero de A, pois considerando

$$g(x) = \begin{cases} x^2, & \text{se } x < 0, \\ 0, & \text{se } x \geqslant 0 \end{cases}$$

temos que $f(x) \cdot g(x) = 0$ para todo $x \in \mathbb{R}$, sendo g diferente da função nula.

Definição 1.3.2. Seja A um anel. O anel A é um **domínio de integridade**, ou simplesmente **domínio**, se o mesmo não possui divisor de zero diferente do elemento nulo, de modo que para quaisquer $a, b \in A$ tais que $ab = 0$, ocorre que $a = 0$ ou $b = 0$.

Exemplo 1.3.2. O anel $\mathbb{Z}$, com as operações usuais de soma e produto, é um domínio de integridade, assim como os anéis numéricos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Exemplo 1.3.3. O anel dos inteiros de Gauss é um domínio de integridade. Como visto no **Exemplo 1.1.2**, esse conjunto é $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ e } i = \sqrt{-1}\}$. Considere dois elementos não nulos f_1 e $f_2 \in \mathbb{Z}[i]$. Como $\mathbb{Z}[i] \subset \mathbb{C}$, pode-se denotar esses elementos usando coordenadas polares da seguinte forma $f_1 = r_1 e^{i\theta_1}$ e $f_2 = r_2 e^{i\theta_2}$, sendo r_1 e r_2 números reais maiores do que zero. Ademais, θ_1 e θ_2 são os argumentos, em radianos, de f_1 e f_2 de forma que $0 \leqslant \theta_1, \theta_2 \leqslant 2\pi$. Dessa forma, tem-se que $f_1 f_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$ Uma vez que r_1 e r_2 são reais maiores do que zero e que $e^{i(\theta_1+\theta_2)} \neq 0$, portanto conclui-se que $f_1 f_2 \neq 0$.

1.4 Corpos

No estudo da matemática, especialmente em álgebra comutativa, nos deparamos com estruturas que buscam capturar e formalizar as propriedades das operações que utilizamos

diariamente, como a adição, subtração, multiplicação e divisão. Entre essas estruturas, o conceito de corpo se destaca como um alicerce central na teoria algébrica, oferecendo um ambiente onde essas operações são possíveis e bem definidas.

Um corpo pode ser entendido como um sistema numérico que generaliza e estende as propriedades dos números familiares, como os racionais $\mathbb{Q}$, reais $\mathbb{R}$ e complexos $\mathbb{C}$. O que torna os corpos especiais é o fato de que neles é sempre possível, além de somar e multiplicar, dividir (exceto pelo zero) — uma característica ausente em outras estruturas algébricas, como os anéis e os grupos. Isso proporciona uma estrutura robusta e rica para resolver equações e desenvolver teorias, e encontra aplicação em diversas áreas da matemática.

Historicamente, o estudo dos corpos não apenas trouxe uma compreensão mais profunda dos números e de suas propriedades, mas também se mostrou essencial para o desenvolvimento de novas áreas, como a teoria dos números e a álgebra linear. Na teoria dos números, por exemplo, corpos finitos têm um papel central na criptografia moderna e em sistemas de comunicação. Já na álgebra linear, o conceito de corpo é indispensável para definir espaços vetoriais e explorar soluções de sistemas de equações lineares, que estão na base de inúmeras aplicações práticas.

Assim, compreender a teoria dos corpos é muito mais do que explorar uma construção abstrata; é penetrar em um campo que conecta e fundamenta múltiplos aspectos da matemática. A partir desse entendimento, somos capazes de enxergar o potencial transformador e universal desta estrutura algébrica, aplicando seus princípios desde problemas elementares até os mais complexos desafios científicos e tecnológicos.

Definição 1.4.1. Seja A um anel. Um elemento $a \in A$ é dito **invertível** se existe $b \in A$ tal que $a \cdot b = b \cdot a = 1$. O elemento b é chamado de **inverso multiplicativo** de a.

Notação 1.4.1. Dado a em A, o elemento b da definição anterior é único e por isso usaremos a partir de agora a notação a^{-1} para indicar o inverso multiplicativo de a. Deste modo, iremos aderir a notação $\mathcal{U}(A)$ para indicar o conjunto dos elementos invertíveis de A. Por exemplo, é possível expressar $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$.

Definição 1.4.2. Um **corpo** é um anel tal que todo elemento não nulo possui inverso multiplicativo.

Propriedades 1.4.1. Em contraste com anéis, nos corpos não há divisores de zero (exceto o próprio zero), ou seja, todo corpo é ainda um domínio.

Demonstração. Iremos provar a segunda propriedade. Considere um corpo $\mathbb{K}$ e suponha que $a \cdot b = 0$ para algum $a, b \in \mathbb{K}$. Agora, suponha que $a \neq 0$ e $b \neq 0$. Como $\mathbb{K}$ é um corpo, sabemos que todos os elementos não nulos de $\mathbb{K}$ possuem inverso multiplicativo. Como $a \neq 0$, existe $a^{-1} \in \mathbb{K}$ tal que $a \cdot a^{-1} = 1$. Multiplicando ambos lados da igualdade $a \cdot b = 0$ por a^{-1}, obtemos: $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$. Pela propriedade associativa da multiplicação, temos: $(a^{-1} \cdot a) \cdot b = 0$. Deste modo, como $a^{-1} \cdot a = 1$, a expressão se simplifica para: $1 \cdot b = 0$, ou seja, $b = 0$, o que contradiz a suposição inicial que $b \neq 0$. Portanto, a única possibilidade para que $a \cdot b = 0$ seja verdadeira em um corpo é que ao menos um dos elementos a ou b seja igual a zero.

Por fim, concluímos que então, que em um corpo $\mathbb{K}$, o único divisor de zero é o próprio zero. Isso mostra que todo corpo é também um domínio de integridade, pois não possui divisores de zero. □

Observação 1.4.1. Como visto acima, vimos que todo corpo é um domínio. Porém, nem todo domínio é um corpo. Um exemplo clássico de um domínio de integridade que não é um corpo é o anel dos inteiros $\mathbb{Z}$. Pois, os únicos elementos de $\mathbb{Z}$ que possuem inversos multiplicativos dentro dos inteiros são 1 e -1. Por exemplo, o número 2 não possui um inverso multiplicativo em $\mathbb{Z}$(ou seja, não existe um $x \in \mathbb{Z}$ tal que $2 \cdot x = 1$).

Exemplo 1.4.1. Os anéis $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são exemplos de corpos.

Mais adiante, exploraremos exemplos mais interessantes de corpos, assim como de domínios.

1.5 Ideais

Em álgebra comutativa, o conceito de ideal é uma das ferramentas mais poderosas para entender a estrutura interna dos anéis e, com isso, desenvolver uma ampla gama de aplicações em matemática pura e aplicada. Em uma abordagem intuitiva, podemos imaginar um ideal como um “bloco de construção” do anel, organizando elementos que compartilham características específicas e, assim, abrindo caminho para simplificar estruturas complexas em padrões compreensíveis.

A teoria dos ideais permite criar anéis mais simples chamados anéis quocientes, onde a complexidade de um anel original pode ser ”reduzida”ao considerar apenas equivalências entre

elementos. Essa simplificação abre portas para análise de estruturas mais avançadas, como corpos e domínios de integridade, especialmente quando se trabalha com ideais máximos e primos. Por exemplo, na aritmética dos números inteiros, podemos observar os múltiplos de um número fixo como um ideal — uma ideia que se expande para conceitos mais complexos quando aplicados a polinômios e outros tipos de anéis.

Além de organizar a estrutura interna dos anéis, o conceito de ideal é essencial para entender a relação entre anéis distintos por meio de homomorfismos de anéis. Homomorfismos são funções entre anéis que preservam as operações de adição e multiplicação, e permitem comparar anéis, identificar padrões comuns e compreender como estruturas algébricas complexas se inter-relacionam. Uma das ligações mais importantes entre ideais e homomorfismos de anéis é dada pelo Teorema do Isomorfismo.

Outro aspecto fascinante dos ideais é sua capacidade de "absorver" multiplicações com elementos do anel. Isso permite o desenvolvimento de técnicas como a decomposição primária e a teoria de fatoração, que são fundamentais na solução de equações algébricas e no estudo de propriedades geométricas em variedades algébricas. Em um contexto prático, isso é utilizado desde a criptografia moderna até o entendimento de simetrias em física e biologia, onde padrões e estruturas devem ser analisados em camadas.

A partir do estudo dos ideais, o matemático pode explorar o conceito de divisibilidade em contextos abstratos, entender a essência da construção de corpos, e até mesmo lançar as bases para a teoria de Galois, que lida com a simetria de raízes de polinômios. Esse conceito, então, não apenas organiza os elementos de um anel, mas também permite novas abordagens para analisar a matemática como um todo — uma perspectiva rica e motivadora para qualquer estudo na área

Definição 1.5.1. Sejam A um anel e I um subconjunto não vazio de A. Diz-se que I é um **ideal** de A se:

I) $a + b \in I$ para quaisquer $a, b \in I$;

II) $ax \in I$ para todo $a \in A$ e para todo $x \in I$.

Definição 1.5.2. Seja A um anel. Um ideal I de A é chamado de **ideal trivial** se I é igual a A ou se I é o ideal nulo.

Lema 1.5.1. *Seja I um ideal de um anel A. Se I contém algum elemento invertível de A, então $I = A$.*

Demonstração. Seja $f \in I$ um elemento invertível de A. Então existe $f^{-1} \in A$ tal que $f \cdot f^{-1} = 1$. Como I é um ideal, segue que $f \cdot f^{-1} \in I$, isto é, $1 \in I$. Deste modo, como consequência, para qualquer elemento $g \in A$, tem-se $g = 1 \cdot g \in I$. Portanto, $I = A$. □

Definição 1.5.3. Seja I um ideal de um anel A. O ideal I é dito **ideal próprio** de A, se $I \neq A$.

Proposição 1.5.1. *Seja K um corpo. O ideal nulo $\{0\}$ é o único ideal próprio de K.*

Demonstração. Para provarmos a proposição acima, usaremos a prova por contra-positiva. Seja $I \neq \{0\}$ um ideal de K. Considere $p \in I - \{0\}$. Como K é um corpo, todos os seus elementos não nulos são invertíveis. Portanto, p é invertível, pelo **Lema 1.5.1**, tem-se que $I = K$, ou seja, I não é um ideal próprio de A. □

Sejam A um anel e $f \in A$. O conjunto de todos os múltiplos do elemento f por elementos de A, explicitamente

$$(f) = \{r \cdot f \in A \mid r \in A\},$$

é um ideal. O ideal (f) é denominado **ideal principal gerado** por f.

Exemplo 1.5.1. O ideal principal gerado por 7 em $\mathbb{Z}$ é dado por: $(7) = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$. Este ideal contém todos os múltiplos de 7

Exemplo 1.5.2. O ideal principal gerado por $1+i$ em $\mathbb{Z}[i]$ é dado por: $(1+i) = \{(1+i) \cdot z \mid z \in \mathbb{Z}[i]\}$. Este ideal contém todos os múltiplos de $1 + i$ nos inteiros gaussianos.

Definição 1.5.4. Seja P um ideal de um anel A. O ideal P é dito um ideal **primo** de A, se satisfaz as seguintes condições:

I. $P \neq A$; (isto é, o ideal P é próprio em A).

II. (Propriedade de Primalidade): Se um produto de elementos pertence a P, então pelo menos um dos elementos pertence a P.

Formalmente, um ideal próprio P de um anel A é dito primo se:

$$a, b \in A \text{ e } a \cdot b \in P \Longrightarrow a \in P \text{ ou } b \in P.$$

Exemplo 1.5.3. Considerando $\mathbb{Z}$ o anel dos inteiros, o ideal $I = (5)$ é um ideal primo em $\mathbb{Z}$, pois $(5) = \{5r \in \mathbb{Z} \mid r \in \mathbb{Z}\}$ e se $a, b \in \mathbb{Z}$ são tais que $a \cdot b \in (5)$, então 5 divide $a \cdot b$, e como 5 é número primo, temos que $5 \mid a$ ou $5 \mid b$, ou seja, $a \in (5)$ ou $b \in (5)$.

Mais geralmente, temos o seguinte resultado que caracteriza ideais primos em $\mathbb{Z}$.

Proposição 1.5.2. *Seja $p \in \mathbb{Z}$. O ideal $p\mathbb{Z} := (p)$ é um ideal primo do anel $\mathbb{Z}$ se, e somente se, p for um número primo.*

Demonstração. ($\Rightarrow$) Para demonstrarmos a ida desta implicação, procederemos por redução ao absurdo. Suponha que $p\mathbb{Z}$ é um ideal primo de $\mathbb{Z}$ e que p é composto, ou seja, existem $a, b \in \mathbb{Z}$ tal que $p = ab$ e $1 < a$,$b < p$. Desta forma, tem-se que $ab \in p\mathbb{Z}$, porém $a \notin p\mathbb{Z}$ e $b \notin p\mathbb{Z}$, isto é, $p\mathbb{Z}$ não é um ideal primo, que é uma contradição por absurdo. Assim, está provado que p é um número primo.

($\Leftarrow$) Para demonstrarmos a volta desta implicação, vamos supor p é um número primo, então $p\mathbb{Z} = \{p \cdot k \mid k \in \mathbb{Z}\}$ é o conjunto de todos os múltiplos de p em $\mathbb{Z}$. Queremos mostrar que se $a \cdot b \in p\mathbb{Z}$, então $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$. Assim, isso significa que $a \cdot b = p \cdot k$ para algum $k \in \mathbb{Z}$. Como p é primo e divide o produto $a \cdot b$, pela propriedade de primalidade, tem-se que p divide ao menos um dos elementos, ou seja, $p \mid a$ ou $p \mid b$. Portanto, $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$. Assim, está provado que $p\mathbb{Z}$ é um ideal primo.

□

Definição 1.5.5. Um ideal próprio M de um anel A é chamado ideal **maximal** de A se para qualquer ideal I de A com $M \subseteq I \subseteq A$, temos que $I = M$ ou $I = A$.

Exemplo 1.5.4. O ideal nulo $\{0\}$ é maximal em qualquer corpo. Como foi abordado na **Proposição 1.5.1**, um corpo só possui ideais triviais.

A próxima proposição fornece uma condição muito especial aos ideais em $\mathbb{Z}$. Mais adiante exploraremos esta propriedade ao estudarmos domínios em que todos os ideais são principais.

Proposição 1.5.3. *Qualquer ideal I de $\mathbb{Z}$ é da forma $I = n\mathbb{Z}$ para algum $n \in \mathbb{N} \cup \{0\}$.*

Demonstração. Para demonstrarmos a afirmação, suponha que I é um ideal de $\mathbb{Z}$. Se $I = \{0\}$, considerando $n = 0$, temos que $I = 0\mathbb{Z}$. Agora, considere $I \neq \{0\}$. Desta maneira, existe $a \in I$ com $a \neq 0$. Como I é um ideal, segue que $-a \in I$. Assim, o conjunto I possui algum inteiro positivo.

Pelo princípio da boa ordenação, o conjunto de todos os inteiros positivos de I possui um menor elemento, seja $n \in I$ esse elemento.

Observe que $n\mathbb{Z} \subseteq I$, pois $mn \in I$ para todo $m \in \mathbb{Z}$, já que I é um ideal. Por outra perspectiva, considere um elemento $u \in I$ e divida-o pelo elemento n. Dessa forma, pelo algoritmo da divisão de números inteiros, existem, $q, r \in \mathbb{Z}$ tais que $u = nq+r$, com $0 \leqslant r < n$. Como u e nq estão em I, tem-se $u - nq = r \in I$. Sendo n o menor inteiro positivo em I e $0 \leqslant r < n$, temos que $r = 0$. Logo, $u = nq + 0 = nq \in n\mathbb{Z}$. Assim, $I \subseteq n\mathbb{Z}$. Portanto, está demonstrada a dupla inclusão, logo temos que $I = n\mathbb{Z}$.

□

Exemplo 1.5.5. Se $p \in \mathbb{Z}$ é um número primo, então o ideal (p) é um ideal maximal em $\mathbb{Z}$. De fato, se I é um ideal em $\mathbb{Z}$, então pela proposição anterior, temos que $I = (d)$ para algum d. Desta forma, se I contém (p), então, p é múltiplo de d, isto é, d é um divisor de p. Assim, pela primalidade de p, temos que $d = p$ ou $d = 1$, logo, $I = (p)$ ou $I = \mathbb{Z}$. Portanto, (p) é maximal.

1.6 Anel Quociente

Dado um conjunto munido de uma relação de equivalência, é possível associar o conjunto quociente em que os elementos, as classes de equivalência, particionam o conjunto original, o que permite uma melhor análise do mesmo a luz da relação em questão. Nesta seção, estudamos anéis munidos de uma relação de equivalência chamada relação de congruência. Os anéis quocientes permitem simplificar a estrutura de um anel ”eliminando”um ideal específico, ao mesmo tempo que mantém as operações originais e relações algébricas. Eles são essenciais em muitas áreas da álgebra abstrata e na geometria algébrica.

Definição 1.6.1. Sejam A um anel e I um ideal de A. Dados $a, b \in A$, dizemos que a, b são **congruentes módulo** I, se $a - b \in I$.

Notação 1.6.1. Ao decorrer do trabalho será utilizada a notação $a \equiv b \ (mod\ I)$ para indicar que a é congruente à b módulo I.

Observação 1.6.1. Uma relação em um conjunto A é dita uma **relação de equivalência** quando é reflexiva, simétrica e transitiva.

Proposição 1.6.1. *A relação* $\equiv \ (mod\ I)$ *é uma relação de equivalência.*

Demonstração. De fato, a relação $a \equiv b \ (mod\ I)$ satisfaz as três propriedades.

Reflexividade: Se $a \in A$, então $a - a = 0 \in I$. Logo, $a \equiv a \ (mod\ I)$.

Simetria: Sejam $a, b \in A$. Se $a \equiv b \ (mod\ I)$, então $a - b \in I$. Dessa forma, como I é um ideal, segue que $-(a-b) \in I$, ou seja, $-a + b = b - a \in I$. Portanto, $b \equiv a \ (mod\ I)$.

Transitividade: Sejam $a, b, c \in A$. Se $a \equiv b \ (mod\ I)$ e $b \equiv c \ (mod\ I)$, então $a - b \in I$ e $b - c \in I$. Como I é um ideal, então $(a-b) + (b-c) = a - c \in I$. Portanto, $a \equiv c \ (mod\ I)$.

Assim, a relação $\equiv \ (mod\ I)$ é de equivalência. □

Definição 1.6.2. Sejam I um ideal de um anel A e $a \in A$. O conjunto de todos os elementos de A que são congruentes à a módulo I é chamado **classe de equivalência** de a módulo I.

Notação 1.6.2. A classe de equivalência de a módulo I será denotada por $\overline{a}$.

Observação 1.6.2. Observe que, para todo $a \in A$, tem-se que $\overline{a} \neq \varnothing$, pois $a \equiv a \ (mod\ I)$, isto é, $a \in \overline{a}$.

Proposição 1.6.2. *Se I é um ideal do anel A e $x \in A$, então $\overline{x} = x + I := \{x + i \in A \mid i \in I\}$.*

Demonstração. Se $a \in \overline{x}$, então $a \equiv x \ (mod\ I)$, isto é, $a - x \in I$. Desta forma, $a = x + b$ para algum $b \in I$, ou seja, $a \in x + I$. Logo, temos que $\overline{x} \subseteq x + I$. Ademais, se $a \in x + I$, então existe algum $b \in I$ tal que $a = x + b$, em outra perspectiva, $a - x = b$. Desse modo, $b \in I$, ou seja, $a - x \in I$, o que implica em $a \equiv x \ (mod\ I)$. Assim, concluímos que $a \in \overline{x}$. Portanto, $\overline{x} \subseteq x + I$. Por fim, tem-se $\overline{x} = x + I$. □

Observação 1.6.3. Sejam $x, y \in A$. Então, $x + I = y + I$ se, e somente se, $x \equiv y \ (mod\ I)$, isto é, $x - y \in I$.

Notação 1.6.3. O conjunto de todas as classes de equivalência no anel A pelo ideal I é chamado de **conjunto quociente** e será indicado por A/I.

Proposição 1.6.3. *Seja I um ideal de um anel A. O conjunto A/I munido das seguintes operações, para $a, b \in A$, tem-se:*

$$(a + I) + (b + I) = a + b + I \ \ e \ \ (a + I) \cdot (b + I) = a \cdot b + I$$

*é um anel, chamado **anel quociente** de A pelo ideal I.*

Mostraremos apenas que as operações estão bem definidas. Sejam $a_1, a_2, b_1, b_2 \in A$ tais que $(a_1 + I) = (a_2 + I)$ e $(b_1 + I) = (b_2 + I)$.

Para verificarmos que a operação da soma está bem definida, note que que $a_1 - a_2 \in I$ e $b_1 - b_2 \in I$. Como I é um ideal, segue que $(a_1 - a_2) + (b_1 - b_2) \in I$, ou seja,

$(a_1 + b_1) - (a_2 + b_2) \in I$, que equivale a $(a_1 + b_1) + I = (a_2 + b_2) + I$. Logo, a soma está bem definida.

Para verificarmos que a operação produto está bem definida, note que $a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2$, isto é, $a_1b_1 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$. Por hipótese, tem-se $a_1 - a_2 \in I$ e $b_1 - b_2 \in I$. Como sabemos que I é um ideal, portanto ocorre que $a_1(b_1 - b_2) \in I$ e $(a_1 - a_2) \in I$. Concluímos que $a_1(b_1 - b_2) + (a_1 - a_2)b_2 \in I$, ou seja, $a_1b_1 - a_2b_2 \in I$, que é equivalente a $a_1b_1 + I = a_2b_2 + I$. Logo, o produto está bem definido.

De fato, as operações anteriores estão bem definidas, isto é, as operações são independentes do representante de classe.

Exemplo 1.6.1. Dado $n \in \mathbb{N}$, o conjunto das classes de equivalência módulo n, muito utilizado na teoria de números, $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{n-1}\}, n \geqslant 1$, munido da soma e produto de classes de equivalência módulo *n* é um anel.

Exemplo 1.6.2. O ideal gerado por $\overline{3}$ em $\mathbb{Z}_{12}$ é denotado por: $(\overline{3}) = \{\overline{3} \cdot \overline{r} \in \mathbb{Z}_{12} \mid r \in \mathbb{Z}_{12}\}$. Este ideal contém os seus múltiplos $\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ no anel $\mathbb{Z}_{12}$. Logo, $(\overline{3})$ é um ideal principal de $\mathbb{Z}_{12}$.

1.7 Homomorfismo de Anéis

Os homomorfismos de anéis desempenham um papel central na álgebra comutativa, conectando diferentes estruturas e revelando propriedades fundamentais de forma elegante e sistemática. Essas funções não apenas preservam as operações algébricas básicas, como adição e multiplicação, mas também capturam a essência da relação entre os anéis, permitindo que suas características sejam estudadas em conjunto.

Com os homomorfismos, é possível analisar como os ideais, subestruturas e elementos de um anel se comportam em relação a outro, criando uma ponte teórica que facilita a compreensão de problemas complexos. Além disso, eles fornecem ferramentas para construir novos anéis, como quocientes e imagens, que são cruciais para o desenvolvimento de teorias mais avançadas.

Este conceito é aplicado em diversas áreas, como geometria algébrica, onde os homomorfismos conectam coordenadas de variedades e suas equações, e álgebra computacional, onde são usados para simplificar cálculos e criar algoritmos eficientes. Explorar os homomorfismos de anéis não é apenas essencial para a teoria, mas também para compreender

como a álgebra serve como alicerce para inúmeras aplicações modernas, como criptografia e teoria dos números.

Neste trabalho, abordaremos os homomorfismos de anéis como um conceito-chave para compreender a interação entre diferentes estruturas algébricas.

Definição 1.7.1. Sejam A e B anéis. Uma função $\varphi : A \longrightarrow B$ é um **homomorfismo de anéis** se satisfaz as seguintes condições para todos $x, y \in A$:

I. $\varphi(x + y) = \varphi(x) + \varphi(y)$;

II. $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$;

III. $\varphi(1_A) = 1_B$.

Observação 1.7.1. Intuitivamente, um homomorfismo de anéis φ de A em B é uma função que preserva as operações dos anéis.

Observação 1.7.2. Se a função φ for bijetiva, o homomorfismo será denominado **isomorfismo** e os anéis A e B são ditos **isomorfos**. Será usada a notação $A \simeq B$ para indicar que A é isomorfo a B. Além disso, um **automorfismo** de A é um isomorfismo de A em A.

Definição 1.7.2. Seja $\varphi : A \longrightarrow B$ um homomorfismo de anéis. O **núcleo** do homomorfismo φ é o seguinte conjunto:

$$N(\varphi) = \{a \in A : \varphi(a) = 0_B\}.$$

Exemplo 1.7.1. A função de $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$ definida por $\varphi(a + bi) = a - bi$ é um homomorfismo de anéis e seu núcleo é o conjunto $N(\varphi) = \{0\}$. De fato, se $\varphi(a + bi) = 0$, então $a - bi = 0$, consequentemente, $a = b = 0$.

Definição 1.7.3. Seja $\varphi : A \longrightarrow B$ um homomorfismo de anéis. O conjunto **imagem** da função φ é:

$$Im(\varphi) = \{b \in B : b = \varphi(a) \; para \; algum \; a \in A\}.$$

Na proposição a seguir, são apresentadas algumas propriedades sobre homomorfismos de anéis.

Proposição 1.7.1. *Se $\varphi : A \longrightarrow B$ é um homomorfismo de anéis, então:*

I. $\varphi(0_A) = 0_B$;

II. $\varphi(-a) = -\varphi(a)$, para todo $a \in A$;

III. $\varphi(a-b) = \varphi(a) - \varphi(b)$ para quaisquer $a, b \in A$;

IV. $N(\varphi)$ é um ideal de A;

V. φ é injetiva se, e somente se, $N(\varphi) = \{0\}$;

VI. $Im(\varphi)$ é um subanel de B.

Demonstração. (I.) Temos que $\varphi(0_A) = \varphi(0_A + 0_A)$. Como φ é um homomorfismo, então $\varphi(0_A) = \varphi(0_A) + \varphi(0_A)$. Agora, subtraindo $\varphi(0_A)$ em ambos os lados da igualdade, tem-se $0_B = \varphi(0_A)$.

(II.) Seja $a \in A$, tem-se $\varphi(0_A) = \varphi(a + (-a))$. Como φ é um homomorfismo, então $\varphi(0_A) = \varphi(a) + \varphi(-a)$. Pelo item (1.), temos que $0_B = \varphi(a) + \varphi(-a)$, ou seja, $\varphi(-a) = -\varphi(a)$.

(III.) Considerando que $a - b = a + (-b)$, pelo item (2.), temos que $\varphi(a-b) = \varphi(a + (-b)) = \varphi(a) + \varphi(-b) = \varphi(a) - \varphi(b)$, para todos $a, b \in A$.

(IV.) Como $\varphi(0_A) = 0_B$, temos que $N(\varphi) \neq \varnothing$. Agora, iremos provar que para quaisquer $x, y \in N(\varphi)$ e $a \in A$, tem-se $x - y$, $xa \in N(\varphi)$. Como $x, y \in N(\varphi)$, então $\varphi(x) = \varphi(y) = 0_B$. Logo, $\varphi(x-y) = \varphi(x) - \varphi(y) = 0_B - 0_B = 0_B$. Deste modo, $x - y \in N(\varphi)$. Ademais, $\varphi(xa) = \varphi(x) \cdot \varphi(a) = \varphi(a) \cdot 0_B = 0_B$. Consequentemente, $xa \in N(\varphi)$. Portanto, $N(\varphi)$ é um ideal de A.

(V.) ($\Rightarrow$) Para demonstrarmos a ida desta implicação, suponha que φ é injetiva. No item (I.), foi demonstrado $\varphi(0_A) = 0_B$, isto é, $0_A \in N(\varphi)$. Dessa forma, $\{0_A\} \subseteq N(\varphi)$. Por outro lado, se $x \in N(\varphi)$, então $\varphi(x) = 0_B = \varphi(0_A)$. Como φ é injetiva, tem-se que $x = 0_A$. Portanto, $N(\varphi) \subseteq \{0_A\}$. Por conseguinte, $N(\varphi) = \{0_A\}$.

($\Leftarrow$) Para demonstramos a recíproca, suponha que $N(\varphi) = \{0_A\}$. Sejam $x, y \in A$ tais que $\varphi(x) = \varphi(y)$. Como demonstramos no item (3.), temos que $\varphi(x-y) = \varphi(x) - \varphi(y)$. Logo, $\varphi(x-y) = 0_B$, isto é, $x - y \in N(\varphi) = \{0_A\}$. Dessa maneira, $x - y = 0_A$. Assim, φ é injetiva.

(VI.) Como $1_B = \varphi(1_A) \in Im(\varphi)$, então, em particular, $Im(\varphi) \neq \varnothing$. Além disso, se $\varphi(a)$,$\varphi(b) \in Im(\varphi)$, então temos que $\varphi(a) - \varphi(b) = \varphi(a-b)$. Logo, $\varphi(a) - \varphi(b) \in Im(\varphi)$. Tem-se ainda que $\varphi(a) \cdot \varphi(b) = \varphi(a \cdot b)$, isto é, $\varphi(a) \cdot \varphi(b) \in Im(\varphi)$. Portanto, $Im(\varphi)$ é um subanel de B. □

Teorema 1.7.1. *(Teorema do isomorfismo) Se $\varphi : A \longrightarrow B$ é um homomorfismo de anéis, então $A/N(\varphi)$ e $Im(\varphi)$ são isomorfos.*

Demonstração. Considere a função a seguir:

$$\psi : A/N(\varphi) \longrightarrow \mathrm{Im}(\varphi)$$
$$a + N(\varphi) \longmapsto \varphi(a)$$

Temos que esta função está bem definida. De fato, se $a + N(\varphi) = a' + N(\varphi)$, então $a - a' \in N(\varphi)$. Desta forma, $\varphi(a - a') = 0$, ou seja, $\varphi(a) = \varphi(a')$, isto é, $\psi(a + N(\varphi)) = \psi(a' + N(\varphi))$ e portanto, a função está bem definida.

Agora vamos verificar que a função é um homomorfismo. De fato:

$$\begin{aligned}\psi[(a + N(\varphi)) + (b + N(\varphi))] &= \psi((a + b) + N(\varphi)) \\ &= \varphi(a + b) \\ &= \varphi(a) + \varphi(b) \\ &= \psi(a + N(\varphi)) + \psi(b + N(\varphi)).\end{aligned}$$

Além disso, tem-se que:

$$\begin{aligned}\psi[(a + N(\varphi)) \cdot (b + N(\varphi))] &= \psi((a \cdot b) + N(\varphi)) \\ &= \varphi(a \cdot b) \\ &= \varphi(a) \cdot \varphi(b) \\ &= \psi(a + N(\varphi)) \cdot \psi(b + N(\varphi)).\end{aligned}$$

Agora, iremos demonstrar a bijetividade da função.

Injetividade: Suponha que $a + N(\varphi) \in N(\psi)$. Então, $\psi(a + N(\varphi)) = \varphi(a) = 0$. Assim, $a \in N(\varphi)$, o que nos diz que $a + N(\varphi) = 0 + N(\varphi)$. Logo, $N(\psi) = \{0 + N(\phi)\}$. Desta forma, pelo item (5.) da **Proposição 1.7.1**, temos que a função ψ é injetiva.

Sobrejetividade: Ao analisar a função, sabemos que a imagem de ψ está contida na imagem de φ. Desta forma, para provarmos a sobrejetividade, precisamos demonstrar que $Im(\varphi) \subseteq Im(\psi)$. Considere $\varphi(a) \in Im(\varphi)$. Nesta condição, temos que $a \in A$, logo, $a + N(\varphi) \in A/N(\varphi)$ e $\psi(a + N(\varphi)) = \varphi(a)$. Assim, $Im(\varphi) \subseteq Im(\psi)$ e temos que a função ψ é sobrejetiva.

Como essa função é um homomorfismo bijetivo entre os anéis $A/N(\varphi)$ e $Im(\varphi)$, então temos que esses anéis são isomorfos.

□

No próximo capítulo, exploraremos consequências e exemplos do teorema do isomorfimo.

Capítulo 2

Anéis de Polinômios

Os anéis de polinômios são uma estrutura central na álgebra comutativa e na teoria dos anéis, e eles representam uma extensão natural do conceito de polinômios. Esses anéis surgem da necessidade de entender e operar formalmente com polinômios que possuem coeficientes em um determinado anel, geralmente um corpo ou um domínio, e que podem ser somados e multiplicados de maneira sistemática. Mais do que apenas uma coleção de expressões algébricas, os anéis de polinômios são fundamentais para o desenvolvimento de muitas teorias matemáticas, incluindo a fatoração, a teoria dos ideais e a aritmética em anéis.

O estudo de anéis de polinômios nos permite compreender propriedades como divisibilidade, fatoração única e, em certos casos, permite aplicar o algoritmo de divisão, facilitando a resolução de problemas complexos. Quando consideramos polinômios com coeficientes em um corpo, o anel de polinômios resultante possui uma estrutura rica e útil, chamada de domínio euclidiano. Essa propriedade nos garante que qualquer polinômio não nulo pode ser dividido por outro, com quociente e resto bem definidos, algo essencial para o desenvolvimento de algoritmos eficientes de fatoração e para o cálculo de raízes.

Além disso, os anéis de polinômios são peças fundamentais na construção de corpos e extensões de corpos, áreas com aplicações importantes em teoria dos números e criptografia. Por exemplo, ao adentrar o estudo dos corpos finitos, a estrutura dos anéis de polinômios sobre corpos se torna um alicerce para a construção de corpos maiores, permitindo que se definam operações seguras para o processamento e a proteção de informações.

Exploraremos que um anel de polinômios é constituído pelo conjunto de polinômios com coeficientes em um anel A e representa uma extensão natural dos conceitos aritméticos para contextos mais complexos, onde as variáveis assumem papel de indeterminadas. No caso

de polinômios em uma única variável x, o conjunto $A[x]$ é um dos exemplos mais simples e bem compreendidos; contudo, a teoria se expande naturalmente para anéis de polinômios em várias variáveis, como $A[x_1, x_2, \ldots, x_n]$, que se torna indispensável para o estudo de geometria algébrica e sistemas de equações multivariadas.

Esses anéis de polinômios em múltiplas variáveis possuem uma estrutura algébrica rica e são capazes de modelar situações complexas, indo muito além das aplicações com uma única variável. No caso de $A[x_1, x_2, \ldots, x_n]$, a teoria se aprofunda ao permitir que se explorem as relações entre as variáveis e os coeficientes, bem como a possibilidade de construção de ideais, elementos centrais no estudo de subestruturas de anéis. Uma das características fundamentais dos anéis de polinômios é que, sob certas condições sobre A, como ser um anel noetheriano, $A[x_1, x_2, \ldots, x_n]$ também preserva essa propriedade. Anéis noetherianos são aqueles em que todo ideal é finitamente gerado, o que é crucial para a aplicabilidade de diversos teoremas na álgebra comutativa.

Esse resultado é garantido pelo Teorema da Base de Hilbert, que afirma que se A é um anel noetheriano, então o anel de polinômios $A[x_1, x_2, \ldots, x_n]$ também será noetheriano. Esse teorema não apenas confirma a finitude das geradores de ideais, mas também assegura a estabilidade estrutural dos anéis de polinômios sob operações de extensão em termos de variáveis. Essa propriedade é essencial para muitos desenvolvimentos na álgebra e na geometria algébrica, pois permite a manipulação e a resolução de sistemas de equações polinomiais complexos de maneira controlada.

Neste trabalho, exploraremos a construção e as propriedades dos anéis de polinômios em uma e em múltiplas variáveis, analisando sua estrutura noetheriana e aplicando o Teorema da Base de Hilbert. Esse estudo nos permitirá compreender como os anéis de polinômios oferecem um terreno fértil para teorias algébricas avançadas, bem como para aplicações em diversas áreas, incluindo a teoria dos números e a criptografia, onde essas propriedades garantem eficiência e segurança nas operações algébricas.

2.1 Polinômios em uma indeterminada

Definição 2.1.1. Seja A um anel. Uma **sequência** em A é uma função $\alpha : \mathbb{N} \cup \{0\} \longrightarrow A$. A imagem de $i \in \mathbb{N} \cup \{0\}$ pela função α é denotada por a_i. Dessa forma, tem-se:

$$\alpha = (a_0, a_1, a_2, a_3, \ldots, a_i, \ldots)$$

Os elementos $a_i \in A$ são chamados de **coeficientes** da sequência. Ademais, duas sequências α e β em A são iguais se, e somente se, $\alpha(i) = \beta(i)$ para todo $i \geqslant 0$.

Agora, vamos ao conceito de polinômio.

Definição 2.1.2. Uma sequência $\alpha = (a_0, a_1, a_2, a_3, \ldots, a_i, \ldots)$ em um anel A é chamada de **polinômio** com coeficientes em A se existe algum inteiro $n \geqslant 0$ tal que $a_i = 0$ para todo $i > n$, ou seja, $\alpha = (a_0, a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots)$.

Definição 2.1.3. Dizemos que um polinômio α é **identicamente nulo** quando todos os coeficientes são iguais ao elemento nulo do anel A, isto é, se $\alpha = (0, 0, 0, \ldots)$.

Definição 2.1.4. Se $\alpha \neq 0$, então existe algum número natural ou zero n de modo que $a_n \neq 0$ e $a_i = 0$ para todo $i > n$. Desta forma, o coeficiente a_n é chamado de **coeficiente líder**, ou também de **coeficiente dominante**, de α.

Quando o coeficiente líder é igual a 1, o polinômio é chamado de **polinômio mônico**. Ademais, quando os coeficientes do polinômio pertencem ao conjunto dos números inteiros, ele é chamado de **polinômio inteiro**.

Desta forma, dado α um polinômio com coeficientes em uma anel A, podemos denotar $\alpha = (a_0, a_1, a_2, a_3, \ldots, a_n)$.

Definição 2.1.5. Seja α um polinômio da forma $\alpha = (a_0, a_1, a_2, a_3, \ldots, a_n)$ em um anel A, o **grau** do polinômio α é definido como sendo o maior $n \in \mathbb{N} \cup \{0\}$ tal que $a_n \neq 0$ e $a_j = 0$ para todo $j > n$.

Notação 2.1.1. Usaremos a notação $\partial(\alpha)$ para denotar o grau do polinômio α.

O grau do polinômio identicamente nulo não é definido, pois todos os seus coeficientes são iguais a zero.

Definição 2.1.6. Um polinômio α da forma $\alpha = (a_0, a_1, a_2, a_3, \ldots, a_n)$ em um anel A é chamado de **polinômio constante**, se $a_i = 0, \forall\ i > 0$.

O polinômio constante pode referir-se ao polinômio identicamente nulo ou um polinômio de grau zero.

Suponha que $\alpha = (a_0, a_1, a_2, a_3, \ldots, a_n)$ e $\beta = (b_0, b_1, b_2, b_3, \ldots, b_m)$ são dois polinômios com coeficientes em um anel A. A **soma** entre α e β é definida da seguinte forma:

$$\alpha + \beta = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots, a_i + b_i, \ldots,)$$

e o **produto** é definido da seguinte forma:

$$\alpha \cdot \beta = (c_0, c_1, c_2, c_3, \ldots, c_k, \ldots)$$

em que

$$c_k = \sum_{i+j=k} a_i \cdot b_i = \sum_{i=0}^{k} a_i \cdot b_{k-i}$$

Desta forma, as operações estão bem definidas.

A seguir, apresentaremos um lema em que é possível visualizar que a soma e produto de polinômios são operações não triviais e estão bem definidas (no sentido de grau).

Lema 2.1.1. *Sejam A um anel e α e β dois polinômios não identicamente nulos com coeficientes em A.*

I) Se $\alpha + \beta \neq 0$, então $\partial(\alpha + \beta) \leqslant \max\{\partial(\alpha), \partial(\beta)\}$.

II) Se $\alpha \cdot \beta \neq 0$, então $\partial(\alpha \cdot \beta) \leqslant \partial(\alpha) + \partial(\beta)$.

III) Se A é um domínio de integridade, então $\alpha \cdot \beta \neq 0$ e $\partial(\alpha \cdot \beta) = \partial(\alpha) + \partial(\beta)$.

Demonstração. (I) Sejam $\alpha = (a_0, a_1, a_2, \ldots)$ e $\beta = (b_0, b_1, b_2, \ldots)$ dois polinômios de grau n e m, respectivamente. Sem perda de generalidade, suponha que $n \geqslant m$. Se $n > m$, então o coeficiente líder de $\alpha + \beta$ será a_n e, desse modo, $\partial(\alpha + \beta) = n = \max\{\partial(\alpha), \partial(\beta)\}$. Se $n = m$, então o coeficiente líder $\alpha + \beta$ será $a_n + b_n$ e, assim, $\partial(\alpha + \beta) = n$, caso $a_n + b_n \neq 0$, ou $\partial(\alpha + \beta) < n$, caso $a_n + b_n = 0$. Logo, $\partial(\alpha + \beta) \leqslant \max\{\partial(\alpha), \partial(\beta)\$.

(II) Suponha que $\alpha = (a_0, a_1, a_2, \ldots)$ tenha grau n, $\beta = (b_0, b_1, b_2, \ldots)$ tenha grau m e $\alpha \cdot \beta = (c_0, c_1, c_2, \ldots)$ com $\partial(\alpha \cdot \beta) = k$. Assim, tem-se $c_k \neq 0$ e deve-se mostrar que $c_l = 0$ para todo $l > n + m \geqslant k$. Pela definição, tem-se

$$c_l = \sum_{i+j=l} a_i \cdot b_i$$

Suponha que $l > n + m$ e $i \leqslant n$, então $j = l - i \geqslant l - n > m$. Desse modo, $b_j = 0$. Agora, suponha que $i > n$ e ainda, que $l > n + m$, então $a_i = 0$, pois $\partial(\alpha) = n$. Note que, em qualquer dos dois casos, tem-se $a_i \cdot b_j = 0$, ou seja, $c_l = 0$. Portanto, $\partial(\alpha \cdot \beta) \leqslant (\partial(\alpha) + \partial(\beta))$.

(III) Suponha que A é um domínio e sejam $\alpha = (a_0, a_1, a_2, \ldots)$ e $\beta = (b_0, b_1, b_2, \ldots)$ dois polinômios de grau n e m, respectivamente, com coeficientes em A. Além disso, seja $\alpha \cdot \beta = (c_0, c_1, c_2, \ldots)$. Tem-se $a_i = 0$, para todo $i > n$ e $b_j = 0$, para todo $j > m$. Perceba que o coeficiente de índice $n + m$ é dado por:

$$c_{n+m} = a_0 b_{n+m} + \ldots + a_{n-1} b_{m+1} + a_n b_m + a_{n+1} b_{m-1} + \ldots + a_{n+m} b_0$$

Analise os dois casos a seguir. Se $i < n$, então $n - i > 0$ e, por consequência, $j = n + m - i = (n - i) + m > m$. Assim, neste caso, tem-se $b_j = 0$. Agora, se $i > n$, então $a_i = 0$, pois $\partial(\alpha) = n$. Dessa forma, cada termo do desenvolvimento do coeficiente de índice $n + m$, com exceção de $a_n b_m$, é igual a 0. Consequentemente, $c_{n+m} = a_n b_m$. Sendo $a_n \neq 0$ e $b_m \neq 0$ elementos de um domínio, segue que $c_{n+m} = a_n b_m \neq 0$ e $\alpha \cdot \beta \neq 0$. Ademais, note que para cada $k > n + m$ o desenvolvimento de c_k contém termos da forma $a_i b_{k-i}$. Como $k = i + (k - i) > n + m$, então $i > n$ ou $k - i > m$. Desse modo, o produto $a_i b_{k-i} = 0$ para todo $k > n + m$ e, resulta em, $\partial(\alpha \cdot \beta) = k = n + m = \partial(\alpha) + \partial(\beta)$. □

produto de dois polinômios são finitos, isto é, a soma e o produto de dois polinômios são polinômios.

A seguir, iremos apresentar algumas propriedades:

Propriedades 2.1.1. Sejam f, g, h polinômios com coeficientes em um anel A.

I) Associatividade da soma: $(f + g) + h = f + (g + h)$.

II) Elemento identidade da soma: $\exists\, e \in A$ tal que $e + f = f = f + e$, para todo f polinômio. Este elemento identidade da soma é o polinômio identicamente nulo.

III) Elemento oposto: $\exists\, p \in A$ tal que $f + p = e = p + f$.

IV) Comutatividade da soma: $f + g = g + f$.

V) Associatividade do produto: $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

VI) Distributividade: $f \cdot (g + h) = f \cdot g + f \cdot h$ e .

VII) Comutatividade do produto: $f \cdot g = g \cdot f$.

VIII) Elemento identidade do produto: $\exists\, 1$ tal que $1 \cdot f = f = f \cdot 1$, para todo f polinômio.

Observação 2.1.1. Utilizaremos na observação a seguir, o item (II) e (III) da **Propriedade 2.1.1** para manipularmos a notação de polinômios.

Observação 2.1.2. Agora, vamos abordar a notação usual de polinômios. Vale ressaltar que essa mudança de notação é possível devido à existência de um isomorfismo natural entre as duas formas. Deste modo, com a finalidade de alterarmos a notação, o polinômio $(0, 1, 0, 0 \ldots)$ será identificado por x e denominado **indeterminada**. Ademais, o polinômio constante $(a_0, 0, 0, \ldots)$ será representado por a_0. Pela multiplicação de polinômios como foi definida, tem-se:

$$x \cdot a_0 = (0, 1, 0, 0, \ldots) \cdot (a_0, 0, 0, \ldots) = (0, a_0, 0, 0, \ldots)$$

De forma análoga,

$$a_0 \cdot x = (a_0, 0, 0, \ldots) \cdot (0, 1, 0, 0, \ldots) = (0, a_0, 0, 0, \ldots)$$

Assim, o elemento identidade do produto será indicado por $(1, 0, 0, 0, \ldots) = 1$. Nesse viés, tem-se:

$$x \cdot x = x^2 = (0, 1, 0, 0, \ldots) \cdot (0, 1, 0, 0, \ldots) = (0, 0, 1, 0, \ldots)$$

e também

$$x \cdot x^2 = x^3 = (0, 1, 0, 0, \ldots) \cdot (0, 0, 1, 0, \ldots) = (0, 0, 0, 1, \ldots)$$

E assim sucessivamente para os próximos x^i.

Por essas observações, podemos prenunciar que, no polinômio x^n, com $n \geqslant 1$, o coeficiente de índice n é igual a 1 e os demais são todos nulos. Veremos a seguir que isso de fato acontece.

Lema 2.1.2. *Se $n \geqslant 1$, então o polinômio x^n possui coeficiente de índice n igual a 1 e os demais são todos iguais a zero.*

Demonstração. Usaremos indução sobre n para demonstrarmos este lema. Primeiro, iremos considerar $n = 1$, anteriormente foi visto que $x^1 = x = (0, 1, 0, 0, \ldots)$. Como hipótese de indução, considere que para algum $k \in \mathbb{N}$, o polinômio x^k possui o coeficiente de índice k igual a 1 e os demais iguais a zero. Agora, tem-se que provar que o polinômio x^{k+1} possui coeficiente de índice $k+1$ igual a 1 e todos os outros iguais a zero. De fato, $x^{k+1} = x^k \cdot x$. Sejam $x^{k+1} = (c_0, c_1, c_2, \ldots)$, $x^k = (a_0, a_1, a_2, \ldots)$ e $x = (b_0, b_1, b_2, b_3, \ldots)$, sendo x a indeterminada.

Pela multiplicação de polinômios, tem-se

$$c_l = \sum_{i+j=l} a_i \cdot b_j = \sum_{i=0}^{l} a_i \cdot b_{l-i}.$$

Note que o coeficiente de índice $k+1$ é dado por:

$$c_{k+1} = a_0 b_{k+1} + \ldots + a_1 b_k + \ldots + a_k b_1 + \ldots + a_{k+1} b_0$$

Quando $j = 1$, tem-se $b_j = 1$ e para $j \neq 1$, tem-se $b_j = 0$. Ademais, tem-se $a_i = 1$ para $i = k$ e $a_i = 0$ para $i \neq k$. Assim, conclui-se que $c_{k+1} = a_k b_1 = 1$. Se $l > k+1$, então $l = i + (l-i) > k+1$. Desse modo, $i > k$ ou $l - i = j > 1$. Como consequência, o produto $a_i b_{l-i}$ é igual a zero. Analogamente, utilizando do mesmo viés do argumento anterior, nota-se que quando $l < k+1$, tem-se $l = i + (l-i) < k+1$, ou seja, $i < k$ ou $l - i < 1$. Assim, o produto $a_i b_{l-i}$ também é igual a zero quando $l < k+1$. Portanto, tem-se que todos os coeficientes com índice diferente de $k+1$ são iguais a zero, e o índice igual a k é 1. Logo, é demonstrado que a afirmação é válida para todo $n \geqslant 1$. □

Ao enunciarmos este lema, temos como objetivo recuperar a notação usual.

Observação 2.1.3. Se $\alpha = (a_0, a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots)$ é um polinômio, então podemos denotar $\alpha = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.

De fato,

$$\begin{aligned}
\alpha &= (a_0, a_1, a_2, \ldots, a_n, 0, 0, 0, \ldots) \\
&= (a_0, 0, \ldots) + (0, a_1, 0, \ldots) + (0, 0, a_2, \ldots) + (0, 0, 0, \ldots, a_n) \\
&= a_0(1, 0, 0, \ldots) + a_1(0, 1, 0, \ldots) + a_2(0, 0, 1, \ldots) + a_n(0, 0, 0, \ldots, 1) \\
&= a_0 \cdot 1 + a_1 x + a_2 x^2 + \ldots + a_n x^n \\
&= a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n
\end{aligned}$$

O polinômio α na forma $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ é chamado de polinômio de grau n na indeterminada x.

2.2 Anéis de Polinômios em uma indeterminada

Com base na **Obervação 2.1.3**, iremos formalizar a definição de um anel de polinômios em uma indeterminada.

Definição 2.2.1. Seja A um anel. O conjunto dos polinômios com coeficientes no anel A, onde x é uma indeterminada, é denotado por $A[x]$. Formalmente, um elemento de $A[x]$ é uma expressão da forma:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n.$$

Considerando a soma e o produto de polinômios definidos anteriormente, além das **Propriedades 2.1.1,** temos que $A[x]$ é um anel comutativo com unidade.

Exemplo 2.2.1. $\mathbb{Z}[x], \mathbb{R}[x], \mathbb{Q}[x]$ são exemplos de anéis polinomiais em uma indeterminada.

Exemplo 2.2.2. O ideal de $\mathbb{R}[x]$ gerado por $x^2 + 1$ é dado por:

$$(x^2 + 1) = \{f(x) \cdot (x^2 + 1) \in \mathbb{R}[x] \mid f(x) \in \mathbb{R}[x]\}.$$

Este ideal contém todos os múltiplos de $x^2 + 1$. Logo, $(x^2 + 1)$ é um ideal principal, pois pode ser gerado por um único elemento de $\mathbb{R}[x]$.

Exemplo 2.2.3. Seja $\mathbb{K}$ um corpo. O ideal de $\mathbb{K}[x]$ gerado por $x^3 + x + 1$ é dado por:

$$(x^3 + x + 1) = \{f(x) \cdot (x^3 + x + 1) \in \mathbb{K}[x] \mid f(x) \in \mathbb{K}[x]\}.$$

Este ideal contém todos os múltiplos de $x^3 + x + 1$ no anel de polinômios com coeficientes em $\mathbb{K}[x]$. Logo, $x^3 + x + 1$ é um ideal principal, pois pode ser gerado por um único elemento de $\mathbb{K}[x]$.

Vejamos propriedades importantes sobre anéis de polinômios em uma indeterminada.

Proposição 2.2.1. *Se A é um domínio de integridade, então $A[x]$ é um domínio de integridade.*

Demonstração. Para apresentarmos essa demonstração, usaremos como base o item (III) do **Lema 2.1.1**. Se A é um domínio de integridade e $f, g \in A[x]$ são dois polinômios não identicamente nulos, então $f \cdot g \neq 0$. Assim, $A[x]$ é um domínio de integridade. □

Proposição 2.2.2. *(Algoritmo da Divisão) Seja $\mathbb{K}$ um corpo. Se $f(x), g(x) \in \mathbb{K}[x]$, sendo $g(x) \neq 0$, então, existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que:*

$$f(x) = q(x)g(x) + r(x)$$

sendo $r(x) = 0$ ou grau de $r(x)$ menor que o grau de $g(x)$.

Demonstração. Para demonstrar a proposição em questão, temos como objetivo mostrar que existem únicos polinômios $q(x), r(x) \in \mathbb{K}[x]$ tais que $f(x) = q(x)g(x) + r(x)$, onde $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x))$. Nossa hipótese é que $f(x), g(x) \in \mathbb{K}[x]$ e $g(x) \neq 0$. Vamos utilizar um processo semelhante ao algoritmo de divisão em $\mathbb{Z}$.

Sejam $f(x)$ e $g(x)$ polinômios da forma:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$
$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m,$$

onde a_n e b_m são os coeficientes dos termos de maior grau de $f(x)$ e $g(x)$, respectivamente.

A primeira etapa consiste em cancelar o termo de maior grau de $f(x)$ subtraindo um múltiplo adequado de $g(x)$. Para isso, o primeiro termo do quociente $q(x)$, chamado $q_1(x)$, será o quociente entre os termos de maior grau de $f(x)$ e $g(x)$:

$$q_1(x) = \frac{a_n}{b_m}x^{n-m}$$

Esse termo é escolhido de tal forma que, ao multiplicá-lo por $g(x)$, o termo de maior grau de $f(x)$ seja cancelado.

Multiplicando $q_1(x)$ por $g(x)$ e subtraímos o resultado de $f(x)$ para obter um novo polinômio, $f_1(x)$. A multiplicação de $q_1(x)$ por $g(x)$ resulta em:

$$q_1(x)g(x) = (\frac{a_n}{b_m}x^{n-m}) \cdot (b_0 + b_1x + b_2x^2 + \ldots + b_mx^m)$$
$$q_1(x)g(x) = a_nx^n + \frac{a_n}{b_m}b_{m-1}x^{n-1} + \ldots + \frac{a_n}{b_m}b_0x^{n-m}$$

Agora subtraindo essa expressão de $f(x)$, temos: $f_1(x) = f(x) - q_1(x)g(x)$, ou seja,

$$f_1(x) = (a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) - (a_nx^n + \frac{a_n}{b_m}b_{m-1}x^{n-1} + \ldots + \frac{a_n}{b_m}b_0x^{n-m})$$

Desta forma, cancelando o termo de maior grau de $f(x)$ (o termo $a_n x^n$), deixando um novo polinômio $f_1(x)$ de grau menor que $f(x)$.

Se o polinômio $f_1(x)$ ainda tiver grau maior ou igual a m (o grau de $g(x)$), repetimos o processo. Agora, o termo de maior grau de $f_1(x)$ é dividido pelo termo de maior grau de $g(x)$ para encontrar o próximo termo de $q(x)$:

$$q_2(x) = \frac{\text{termo de maior grau de } f_1(x)}{\text{termo de maior grau de } g(x)}$$

Multiplicando $q_2(x)$ por $g(x)$ e subtraindo o resultado de $f_1(x)$ para obter $f_2(x)$, um novo polinômio com grau ainda menor que $f_1(x)$.

Essa fatoração continua até que o grau do polinômio resultante, chamado $r(x)$, seja menor que o grau de $g(x)$. Nesse ponto, não é mais possível realizar novas divisões, e $r(x)$ é o resto da divisão.

Ao final do processo, temos:

$$f(x) = q(x)g(x) + r(x)$$

onde $q(x)$ é o quociente formado pelos termos $q_1(x), q_2(x), \ldots, q_s(x)$ e $r(x)$ é o polinômio que sobra com grau menor que m, ou seja, $\partial(r(x)) < \partial(g(x))$. Desta forma, está provada a existência da fatoração.

Agora vamos mostrar que os polinômios $q(x)$ e $r(x)$ são únicos. Suponha que existem dois pares de polinômios $(q_1(x), r_1(x))$ e $(q_2(x), r_2(x))$ que satisfaçam: $f(x) = q_1(x)g(x) + r_1(x)$ e $f(x) = q_2(x)g(x) + r_2(x)$. Desta forma, $(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)$.

Agora, observe que o grau de $r_1(x)$ e $r_2(x)$ é menor que m, o grau de $g(x)$. Por outro lado, o grau de $(q_1(x) - q_2(x))g(x)$ deve ser maior ou igual ao grau de m, exceto se $q_1(x) = q_2(x)$.

Portanto, para que essa igualdade seja verdadeira, devemos ter $q_1(x) = q_2(x)$ e, consequentemente, $r_1(x) = r_2(x)$. Desta forma, está provada a unicidade de $q(x)$ e $r(x)$.

□

Proposição 2.2.3. *Se $\mathbb{K}$ é um corpo, então todo ideal de $\mathbb{K}[x]$ é principal.*

Demonstração. Sejam $\mathbb{K}$ um corpo e $\mathbb{K}[x]$ o anel de polinômios com coeficientes em $\mathbb{K}$.

Sabemos que os elementos de $\mathbb{K}[x]$ são da forma:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

onde $a_0, a_1, a_2, \ldots, a_n \in \mathbb{K}$ e $a_n \neq 0$.

Seja $I \subseteq \mathbb{K}[x]$ um ideal não trivial, isto é, $I \neq \{0\}$. O objetivo é mostrar que existe um polinômio $g(x) \in \mathbb{K}[x]$ tal que $I = (g(x))$, ou seja, I é gerado por $g(x)$. Como $I \neq \{0\}$, existe pelo menos um polinômio não nulo em I. Seja $g(x) \in I$ um polinômio de menor grau, ou seja, se $f(x) \in I$ e $f(x) \neq 0$, então o $\partial(g(x)) \leqslant \partial(f(x))$.

Queremos provar que todo $f(x) \in I$ é um múltiplo de $g(x)$, ou seja, $f(x) = q(x)g(x)$ para algum $q(x) \in \mathbb{K}[x]$. Seja $f(x) \in I$. Como $\mathbb{K}$ é um corpo, pela proposição anterior, podemos dividir $f(x)$ por $g(x)$ no sentido usual da divisão de polinômios. Logo, existem polinômios $q(x)$ e $r(x) \in \mathbb{K}[x]$ tais que:

$$f(x) = q(x)g(x) + r(x)$$

onde o grau de $r(x)$ é menor que o grau de $g(x)$.

Desta forma, como $f(x) \in I$ e $g(x) \in I$, e como I é fechado sob soma e produto por elementos de $\mathbb{K}[x]$, segue que $r(x) = f(x) - q(x)g(x) \in I$. Se $r(x) \neq 0$, então o grau de $r(x)$ seria menor que o grau de $g(x)$. Porém, isso contradiz a escolha de $g(x)$ como o polinômio de menor grau em I. Portanto, deve ser o caso que $r(x) = 0$, e assim $f(x) = q(x)g(x)$, ou seja, $f(x)$ é um múltiplo de $g(x)$.

Por fim, como todo polinômio $f(x) \in I$ é um múltiplo de $g(x)$, temos que $I = (g(x))$, o que prova que I é um ideal principal. □

Se A é um domínio de integridade, o conjunto dos elementos invertíveis de $A[x]$ coincide com os de A, ou seja, $\mathcal{U}(A) = \mathcal{U}(A[x])$. Desta forma, nem todos os elementos não nulos de $A[x]$ possuem inverso multiplicativo, assim, $A[x]$ não é corpo.

Iremos demonstrar este resultado na proposição a seguir.

Proposição 2.2.4. *Se A é um domínio de integridade, então $\mathcal{U}(A) = \mathcal{U}(A[x])$.*

Demonstração. Suponha que $f(x) \in A[x]$ é invertível. Dessa forma, existe $g \in A[x]$ tal que $f(x) \cdot g(x) = 1$. Como $\partial(f(x)) + \partial(g(x)) = \partial(f(x) \cdot g(x)) = 0$, então $\partial(f(x)) = \partial(g(x)) = 0$. Logo, os polinômios f e g são constantes. Pela imersão apresentada anteriormente, temos que

esses polinômios constantes são os elementos invertíveis do domínio A. Portanto, o conjunto dos elementos invertíveis de $A[x]$ é igual ao dos de A. □

2.2.1 A imersão de A em $A[x]$

Ao falarmos de imersão de A em $A[x]$, citamos indiretamente que essa imersão se dá pelo homomorfismo injetor que mapeia cada elemento de A para o polinômio constante correspondente em $A[x]$, permitindo que A seja visto como um subanel de $A[x]$.

Definição 2.2.2. Sejam A um anel e $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in A[x]$. A função $\varphi : A \longrightarrow A$, definida por $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n$ é chamada de **função polinomial** associada a $f(x)$.

Teorema 2.2.1. *Sejam A um anel e a seguinte função $\varphi : A \longrightarrow A[x]$ que associa a cada $\alpha \in A$ o polinômio $f_\alpha(x) = \alpha$. A função como foi definida é um homomorfismo injetivo entre os anéis A e $A[x]$.*

Demonstração. De fato, $\varphi(\alpha+\beta) = f_{\alpha+\beta}(x) = \alpha+\beta$. Todavia, $(f_\alpha+f_\beta)(x) = f_\alpha(x)+f_\beta(x) = \alpha + \beta$. Desse modo, $\varphi(\alpha + \beta) = f_\alpha(x) + f_\beta(x) = \varphi(\alpha) + \varphi(\beta)$. Analogamente, tem-se $\varphi(\alpha \cdot \beta) = \varphi(\alpha) \cdot \varphi(\beta)$. Logo, a função φ é um homomorfismo.

Para a injetividade, considere $\alpha, \beta \in A$ com $\alpha \neq \beta$. Note que, $f_\alpha(1_A) = \alpha$ e $f_\beta(1_A) = \beta$. Portanto, $\varphi(\alpha) \neq \varphi(\beta)$. Assim, está provado que $\varphi : A \longrightarrow A[x]$ é um homomorfismo injetivo. □

Como $A/N(\varphi) = A$, então pelo **Teorema do Isomorfismo 1.7.1**, tem-se $A \simeq Im(\varphi)$, ou seja, estes anéis são isomorfos. Nesse viés, pode-se considerar $A \subset A[x]$ e A como um subanel de $A[x]$.

Finalizamos esta seção com um exemplo bem interessante envolvendo o conjunto dos números complexos e a teoria de anéis quocientes.

Proposição 2.2.5. *Seja $\mathbb{C}$ o anel dos números complexos, então $\mathbb{C}$ é isomorfo ao anel quociente $\frac{\mathbb{R}[x]}{(x^2+1)}$.*

Demonstração. Considere o anel de polinômios $\mathbb{R}[x]$ com coeficientes reais. O ideal (x^2+1) é o conjunto de todos os múltiplos do polinômio $x^2 + 1$ em $\mathbb{R}[x]$. Quando tomamos o quociente $\frac{\mathbb{R}[x]}{(x^2+1)}$, estamos essencialmente identificando polinômios que diferem por um múltiplo de x^2+1 como equivalentes.

No anel quociente $\frac{\mathbb{R}[x]}{(x^2+1)}$, cada elemento pode ser representado por um polinômio de grau no máximo 1, pois qualquer termo de grau 2 ou maior pode ser reduzido usando a relação $x^2 \equiv -1 (\text{mod } x^2+1)$. Assim, um elemento genérico em $\frac{\mathbb{R}[x]}{(x^2+1)}$ pode ser escrito como $a+bx$ onde $a, b \in \mathbb{R}$.

Agora, vamos definir o isomorfismo entre $\mathbb{C}$ e $\frac{\mathbb{R}[x]}{(x^2+1)}$. Considere o mapeamento $\varphi : \mathbb{C} \longrightarrow \frac{\mathbb{R}[x]}{(x^2+1)}$ definido por:

$$\varphi(a+bi) = a+bx,$$

onde $a, b \in \mathbb{R}$ e i é o número imaginário de $\mathbb{C}$, isto é, $i^2 = -1$.

Precisamos verificar se φ preserva a soma e o produto, ou seja, se φ é um homomorfismo de anéis.

I) Preservação da soma:

$$\varphi((a+bi)+(c+di)) = \varphi((a+c)+i(b+d)) = (a+c)+x(b+d)$$
$$\text{e } \varphi(a+bi)+\varphi(c+di) = (a+bx)+(c+dx) = (a+c)+x(b+d)$$

Logo, $\varphi((a+bi)+(c+di)) = \varphi(a+bi)+\varphi(c+di)$.

II) Preservação do produto:

$$\varphi((a+bi)(c+di)) = \varphi((ac-bd)+i(ad+bc)) = (ac-bd)+x(ad+bc)$$
$$\text{e } \varphi(a+bi)\varphi(c+di) = (a+bx)(c+dx) = (a+c)+(b+d)x$$

Logo, $\varphi((a+bi)(c+di)) = \varphi(a+bi)\varphi(c+di)$.

Assim, φ é um homomorfismo de anéis. Para mostrar que φ é um isomorfismo, precisamos verificar que φ é injetiva e sobrejetiva.

I) Injetiva: Suponha que $\varphi(a+bi) = 0$. Isso significa que $a+bx \equiv 0$ em $\frac{\mathbb{R}[x]}{(x^2+1)}$, o que implica $a = 0$ ou $b = 0$, já que o polinômio x^2+1 tem grau 2. Portanto, $a+bi = 0$, e φ é injetiva.

II) Sobrejetiva: Dado qualquer elemento $a+bx$ em $\frac{\mathbb{R}[x]}{(x^2+1)}$, basta considerar $a+bi \in \mathbb{C}$ tal que $\varphi(a+bi) = a+bx$. Portanto, φ é sobrejetiva.

Por fim, concluímos que φ é um homomorfismo bijetivo de anéis, isto é, ele é um isomorfismo. Assim, o anel dos números complexos $\mathbb{C}$ é isomorfo ao anel quociente $\frac{\mathbb{R}[x]}{(x^2+1)}$, ou seja:

$$\mathbb{C} \cong \frac{\mathbb{R}[x]}{(x^2+1)}$$

□

2.3 Anéis de Polinômios em um número finito de indeterminadas

A noção de anéis de polinômios em um número finito de indeterminadas é uma generalização de anéis de polinômios em uma indeterminada e desempenham um papel central em álgebra abstrata e geometria algébrica.

De acordo com a **Definição 2.2.1**, um polinômio em uma indeterminada sobre um anel A é uma expressão do tipo:

$$f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

Aqui, x é a indeterminada e os coeficientes $a_0, a_1, \ldots, a_n$ são elementos do anel A.

Se tivermos mais de uma indeterminada, digamos x_1, x_2, um **polinômio em duas indeterminadas** com coeficientes inteiros é algo como:

$$f(x_1, x_2) = 3x_1^2x_2 + 2x_1 + 5x_2^3 + 7.$$

Podemos analisar f como um polinômio na indeterminada x_2 e coeficientes no anel de polinômios $\mathbb{Z}[x_1]$

$$f(x_1, x_2) = 5x_2^3 + (3x_1^2)x_2 + 2x_1 + +7.$$

Ou seja, pensamos f como um elemento do anel de polinômios $(\mathbb{Z}[x_1])[x_2]$. Deste modo, podemos definir o conjunto dos polinômios nas indeterminadas x_1, x_2 com coeficientes em $\mathbb{Z}$ por $\mathbb{Z}[x_1, x_2] = (\mathbb{Z}[x_1])[x_2]$. Sendo assim, este conjunto possui estrutura de anel. Note que construção análoga poderia ser feita destacando a indeterminada x_2.

Ao adicionarmos mais indeterminadas a expressão polinomial, chegaremos a generalização do mesmo. Desta forma, teremos um anel de polinômios da forma $A[x_1, x_2, \ldots, x_n]$, na qual é o conjunto de todos esses polinômios em n variáveis, com coeficientes vindos de um anel A.

Definição 2.3.1. Seja A um anel. O conjunto dos polinômios em n indeterminadas sobre A, denotado por $A[x_1, x_2, \ldots, x_n]$, é o conjunto de expressões da forma:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1, i_2 \ldots, i_n} a_{i_1, i_2 \ldots, i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

onde $a_{i_1, i_2 \ldots, i_n} \in A$ e $i_1, i_2, \ldots, i_n \in \mathbb{N} \cup \{0\}$.

Proposição 2.3.1. *Seja A um anel e $k \in \mathbb{N}$. Se A é um domínio de integridade, então $A[x_1, \ldots, x_k]$ é um domínio de integridade.*

Demonstração. Para demonstrar a proposição, utilizaremos da indução em k que $A[x_1, \ldots, x_k]$ é um domínio de integridade se A é um domínio de integridade.

Suponha que $k = 1$, logo $A[x]$ é o anel de polinômios em uma indeterminada com coeficientes em A. Neste caso, o resultado segue da **Proposição 2.2.1**.

Considere que $A[x_1, \ldots, x_k]$ é um domínio de integridade para algum $k \geqslant 1$. Vamos mostrar que $A[x_1, \ldots, x_{k+1}]$ também é um domínio de integridade.

Considere dois polinômios não nulos $f(x_1, \ldots, x_{k+1})$ e $g(x_1, \ldots, x_{k+1})$ em $A[x_1, \ldots, x_{k+1}]$. Podemos escrever esses polinômios como:

$$f(x_1, \ldots, x_{k+1}) = \sum_{i=0}^{m} f_i(x_1, \ldots, x_k) x_{k+1}^i$$
$$g(x_1, \ldots, x_{k+1}) = \sum_{i=0}^{n} g_j(x_1, \ldots, x_k) x_{k+1}^j,$$

onde

$f_i(x_1, \ldots, x_k), g_j(x_1, \ldots, x_k) \in A[x_1, \ldots, x_k]$. O produto $f(x_1, \ldots, x_{k+1}) g(x_1, \ldots, x_{k+1})$ é dado por:

$$f(x_1, \ldots, x_{k+1}) g(x_1, \ldots, x_{k+1}) = \sum_{l=0}^{m+n} \Big(\sum_{i+j=l} f_i(x_1, \ldots, x_k) g_j(x_1, \ldots, x_k) \Big) x_{k+1}^l$$

Suponha que $f(x_1, \ldots, x_{k+1}) g(x_1, \ldots, x_{k+1}) = 0$. Então, todos os coeficientes devem

ser zero:

$$\sum_{i+j=l} f_i(x_1, \ldots, x_k) g_j(x_1, \ldots, x_k) = 0, \text{ para todo } l.$$

Em particular, considere o coeficiente do termo de maior grau em x_{k+1}. Esse coeficiente é dado por $f_m(x_1, \ldots, x_k) g_n(x_1, \ldots, x_k)$. Como $A[x_1, \ldots, x_k]$ é um domínio de integridade (pela hipótese de indução), temos que $f_m(x_1, \ldots, x_k) = 0$ ou $g_n(x_1, \ldots, x_k) = 0$.

Se $f_m(x_1, \ldots, x_k) = 0$, então $f(x_1, \ldots, x_{k+1})$ tem grau menor que m, contradizendo a suposição de que $f(x_1, \ldots, x_{k+1})$ era um polinômio não nulo.

Se $g_n(x_1, \ldots, x_k) = 0$, então $g(x_1, \ldots, x_{k+1})$ tem grau menor que n, contradizendo a suposição de que $g(x_1, \ldots, x_{k+1})$ era um polinômio não nulo.

Portanto, $f(x_1, \ldots, x_{k+1}) g(x_1, \ldots, x_{k+1})$ só pode ser zero se pelo menos um dos polinômios $f(x_1, \ldots, x_{k+1})$ ou $g(x_1, \ldots, x_{k+1})$ for zero. Isso mostra que $A[x_1, \ldots, x_{k+1}]$ também é um domínio de integridade.

□

Embora possamos ainda trabalhar com o conceito de ideais principais em um anel de polinômios com mais indeterminadas, diferentemente do caso de uma indeterminada, como na **Proposição 2.2.3**, existem ideais que não são necessariamente desta forma neste ambiente com mais indeterminadas.

Exemplo 2.3.1. O ideal $I = (x_1^2 - x_2)$ no anel $\mathbb{R}[x_1, x_2]$ contém todos os polinômios da forma $(x_1^2 - x_2) \cdot g(x_1, x_2)$, onde $g(x_1, x_2)$ é um polinômio de $\mathbb{R}[x_1, x_2]$. Já o conjunto J dado por todos os polinômios da forma $x_1 \cdot f(x_1, x_2) + x_2 \cdot g(x_1, x_2)$, onde $f(x_1, x_2), g(x_1, x_2)$ são elementos de $\mathbb{R}[x_1, x_2]$, é um ideal de $\mathbb{R}[x_1, x_2]$ que não é principal.

Agora, vamos provar que o conjunto J, definido como:

$$J = \{x_1 \cdot f(x_1, x_2) + x_2 \cdot g(x_1, x_2) \in \mathbb{R}[x, y,] \mid f(x_1, x_2), g(x_1, x_2) \in \mathbb{R}[x_1, x_2]\}$$

é um ideal de $\mathbb{R}[x_1, x_2]$ que não é principal.

Iremos provar que J é um ideal de $\mathbb{R}[x_1, x_2]$, precisamos verificar que:

I. J é fechado para a soma;

II. J é fechado para o produto.

(I.) J é fechado para a soma: Sejam $p(x_1, x_2) = x_1 \cdot f_1(x_1, x_2) + x_2 \cdot g_1(x_1, x_2)$ e $q(x_1, x_2) = x_1 \cdot f_2(x_1, x_2) + x_2 \cdot g_2(x_1, x_2)$ dois elementos de J. A soma de $p(x_1, x_2)$ e $q(x_1, x_2)$ é: $p(x_1, x_2) + q(x_1, x_2) = (x_1 \cdot f_1(x_1, x_2) + x_2 \cdot g_1(x_1, x_2)) + (x_1 \cdot f_2(x_1, x_2) + x_2 \cdot g_2(x_1, x_2))$. Isso pode ser reescrito como: $p(x_1, x_2) + q(x_1, x_2) = x_1 \cdot (f_1(x_1, x_2) + f_2(x_1, x_2)) + x_2 \cdot (g_1(x_1, x_2) + g_2(x_1, x_2))$. Como $f_1(x_1, x_2) + f_2(x_1, x_2)$ e $g_1(x_1, x_2) + g_2(x_1, x_2)$ são polinômios em $\mathbb{R}[x_1, x_2]$, temos que $p(x_1, x_2) + q(x_1, x_2) \in J$. Logo, J é fechado para a soma.

(II.) J é fechado para o produto: Se $p(x_1, x_2) = x_1 \cdot f_1(x_1, x_2) + x_2 \cdot g_1(x_1, x_2) \in J$ e $h(x_1, x_2) \in \mathbb{R}[x_1, x_2]$, então: $h(x_1, x_2) \cdot p(x_1, x_2) = h(x_1, x_2) \cdot x_1 \cdot f_1(x_1, x_2) + x_2 \cdot g_1(x_1, x_2)$. Aplicando a distributividade: $h(x_1, x_2) \cdot p(x_1, x_2) = x_1 \cdot (h(x_1, x_2) \cdot f(x_1, x_2)) + x_2 \cdot (h(x_1, x_2) \cdot g(x_1, x_2))$. Como $h(x_1, x_2) \cdot f(x_1, x_2)$ e $h(x_1, x_2) \cdot g(x_1, x_2)$ são polinômios em $\mathbb{R}[x_1, x_2]$, temos que $h(x_1, x_2) \cdot p(x_1, x_2) \in J$. Logo, J é fechado para o produto por polinômios de $\mathbb{R}[x_1, x_2]$.

Agora, vamos provar que J não é um ideal principal. Suponha, por absurdo, que J seja um ideal principal, ou seja, existe um polinômio $p(x_1, x_2) \in \mathbb{R}[x_1, x_2]$ tal que $J = (p(x_1, x_2))$, isto é, todos os elementos de J podem ser escritos como múltiplos de $p(x_1, x_2)$.

Note que, x_1 e x_2 são ambos elementos de J, pois podemos escrever como: $x_1 = x_1 \cdot 1 + x_2 \cdot 0$ e $x_2 = x_2 \cdot 0 + x_2 \cdot 1$. Portanto, $x_1, x_2 \in J$. Assim, tanto x_1 quanto x_2 seriam múltiplos de $p(x_1, x_2)$. No entanto, isso implicaria que $p(x_1, x_2)$ divide tanto x_1 quanto x_2, o que é um absurdo, pois x_1 e x_2 são indeterminadas independentes, e não existe um polinômio não constante que divida simultaneamente x_1 e x_2. Assim, chegamos a uma contradição. Portanto, J não pode ser um ideal principal.

Esta é uma diferença significativa quando passamos a um anel polinomial com mais indeterminadas sobre um corpo que será discutido melhor na próxima seção.

2.4 Estruturas Finitamente Geradas: A Ascensão de Hilbert e Noether

Nessa seção iremos falar um pouco da contribuição de Emmy Noether e David Hilbert na teoria dos anéis.

Noether fez contribuições profundas e revolucionárias na teoria dos anéis que desempenham um papel central na álgebra abstrata. Uma das principais contribuições foi a definição e o estudo do que veio a ser os **Anéis Noetherianos**.

Hilbert, outro célebre matemático, desenvolveu **O Teorema da Base de Hilbert**, o qual tem uma importância fundamental na teoria dos anéis. Esse teorema é importante porque formaliza a noção de finitude em álgebra, garantindo que as soluções de sistemas de equações polinomiais podem ser descritas por um número finito de geradores. Essa contribuição de Hilbert abriu caminho para à álgebra moderna e a formalização da geometria algébrica.

2.4.1 Anéis Noetherianos

Os anéis noetherianos representam uma das classes mais importantes de anéis na álgebra comutativa, com aplicações que vão desde a teoria dos números até a geometria algébrica. Caracterizam-se por uma estrutura que garante que todo ideal seja finitamente gerado, o que confere organização e previsibilidade ao estudo de suas propriedades. Esse conceito, formalizado a partir do trabalho pioneiro de Emmy Noether, não apenas simplifica a análise de subestruturas algébricas, mas também permite a construção de teorias elegantes que sustentam o avanço da álgebra abstrata moderna. Sua relevância está em oferecer um alicerce teórico sólido para a resolução de problemas que envolvem sistemas de equações e ideais, assegurando que o número de elementos necessários para descrever essas estruturas seja sempre finito.

Vamos iniciar apresentando uma generalização dos ideais principais.

Proposição 2.4.1. *Sejam A um anel e $f_1, f_2, \ldots, f_n \in A$, o conjunto definido como*

$$(f_1, f_2, \ldots, f_n) = \{a_1 \cdot f_1 + \cdots + a_n \cdot f_n \in A \mid a_i \in A, \forall i = 1, \ldots n\}$$

é um ideal chamado de **ideal finitamente gerado** *por $f_1, \ldots, f_n$.*

Demonstração. Iremos verificar que $I := (f_1, f_2, \ldots, f_n)$ é fechado sob soma.

Sejam $x = a_1f_1 + a_2f_2 + \cdots + a_nf_n$ e $y = b_1f_1 + b_2f_2 + \cdots + b_nf_n$, onde $a_i, b_i \in A$. A soma de x e y é:

$$x + y = (a_1f_1 + a_2f_2 + \cdots + a_nf_n) + (b_1f_1 + b_2f_2 + \cdots + b_nf_n)$$

reorganizando os termos, tem-se:

$$x + y = (a_1 + b_1)f_1 + (a_2 + b_2)f_2 + \ldots + (a_n + b_n)f_n$$

como $a_i + b_i \in A \ \forall i$. Daí, segue que $x + y \in I$. Portanto, I é fechado sob soma.

Agora, iremos verificar que I é fechado sob produto. Seja $r \in A$ e $x \in I$, onde $x = a_1f_1 + a_2f_2 + \cdots + a_nf_n \in I$. Então, para $r \in A$ temos:

$$r \cdot x = r \cdot (a_1f_1 + a_2f_2 + \cdots + a_nf_n)$$

reorganizando os termos, tem-se:

$$r \cdot x = (ra_1)f_1 + (ra_2)f_2 + \cdots + (ra_n)f_n$$

como $ra_i \in A$ para todo i, segue que $r \cdot x \in I$. Portanto, I é fechado sob produto por elementos de A.

Por fim, mostramos que I é fechado sob e produto por elementos de A. Logo, I é um ideal de A.

□

Esse ideal é chamado de ideal finitamente gerado pelos elementos $f_1, f_2, \ldots, f_n$ porque todo elemento de I pode ser escrito como uma combinação linear finita desses elementos com coeficientes em A.

Definição 2.4.1. Seja A um anel qualquer. Dizemos que A é um anel **Noetheriano** se qualquer ideal I em A for finitamente gerado, isto é, existem $a_1, \ldots, a_s \in A$ tais que: $I = (a_1, \ldots, a_s)$.

Proposição 2.4.2. *Seja A um anel. São equivalentes as seguintes condições:*

I. A é Noetheriano;

II. Toda cadeia ascendente de ideais de A

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

é estacionária, isto é, existe $m \geqslant 1$ tal que $I_m = I_{m+1}$, $\forall\ m \in \mathbb{N}$.

III. Qualquer família não-vazia de ideais de A possui elemento maximal (com respeito a inclusão).

Demonstração. $(I. \Rightarrow II.)$ Para demonstramos esta implicação, considere uma cadeia ascendente de ideias em A

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$$

Como os ideais $I_n,\ n \in \mathbb{N}$, estão em cadeia, note que $I = \bigcup_{j=1}^{\infty} I_j$ é um ideal de A. Sendo A um anel Noetheriano, temos que I é finitamente gerado. Assim, existem $f_1, \ldots, f_k \in I$ tais que $I = \bigcup_{j=1}^{\infty} I_j = (f_1, \ldots, f_k)$. Observe que para cada $i = 1, \ldots, k$ existe $n_i \in \mathbb{N}$ tal que $f_i \in I_{n_i}$. Além disso a menos de uma reordenação na lista de geradores de I, podemos assumir que $n_1 \leqslant n_2 \leqslant \cdots \leqslant n_k$. Logo, conclui-se que $(f_1, \ldots, f_k) \subseteq I_{n_k}$. Deste modo,

$$I = (f_1, \ldots, f_k) \subseteq I_{n_k} \subseteq \bigcup_{j=1}^{\infty} I_j = I$$

Portanto, concluí-se que toda cadeia ascendente de ideais de A é estacionária.

$(II. \Rightarrow III.)$ Para demonstramos esta implicação faremos uso da contra positiva. Considere F uma família não-vazia de ideais de A que F não admite elemento maximal com respeito a inclusão. Como F é não vazia, considere $I_1 \in F$. Logo, I_1 não é elemento maximal, por definição segue que $\exists\ I_2 \in F$ tal que $I_1 \subsetneq I_2$. De maneira recursiva, podemos considerar $I_1, I_2, \ldots, I_{n-1} \in F$ tais que $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_{n-1}$, e I_{n-1} não é elemento maximal em F. Logo, temos que existe $I_n \in F$ tal que $I_{n-1} \subsetneq I_n$. Portanto, obtemos uma cadeia ascendente de ideais de A que não é estacionária.

$(III. \Rightarrow I.)$ Para demonstramos esta implicação considere I um ideal de A. Seja G a família dos ideais K de A que são finitamente gerados e tais que $K \subseteq I$. Como $(0_A) \subseteq I$ então $G \neq \varnothing$. Por hipótese, segue que G admite um elemento maximal, digamos J. Como $J \in G$ então J é finitamente gerado e $J \subseteq I$. Supondo por absurdo que $J \neq I$. Então $J \subsetneq I$, o que significa que $\exists\ f \in I$ tal que $f \notin J$. Como J é finitamente gerado, temos $J + (f)$ é finitamente gerado e $J + (f) \subseteq I$, desta forma, temos que $J + (f) \in G$, mas $f \notin J$, logo temos $J \subsetneq J + f$, contradizendo a maximalidade de J na família G. Portanto, $I = J$ é finitamente gerado. Concluímos que A é Noetheriano. □

Os exemplos mais naturais de Anéis Noetherianos são os corpos, por exemplo, $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$, com p primo e os anéis em que todo ideal é principal, como por exemplo, o anel dos números inteiros, como visto em **Proposição 1.5.3** ou mesmo o anel de polinômios em uma indeterminada sobre um corpo $\mathbb{K}$, como visto em **Proposição 2.2.3**.

2.4.2 O Teorema da Base de Hilbert

O Teorema da Base de Hilbert é um marco na história da álgebra, estabelecendo a estabilidade estrutural dos anéis de polinômios em extensões finitas. Ele afirma que, se o anel

de partida é noetheriano, então o anel de polinômios formado a partir dele também herda essa propriedade. Essa ideia revolucionária, introduzida por David Hilbert, trouxe uma compreensão mais profunda sobre a finitude e a organização em álgebra, permitindo o estudo sistemático de sistemas polinomiais complexos e suas soluções. Mais do que um resultado técnico, o Teorema da Base de Hilbert abriu novas fronteiras na geometria algébrica e na álgebra computacional, fornecendo ferramentas que tornaram possível descrever e manipular sistemas algébricos com eficiência e clareza.

Teorema 2.4.1. *Seja A um anel. Se A é Noetheriano então, $A[x_1, \ldots, x_n]$ é Noetheriano.*

Demonstração. Como podemos identificar o anel de polinômios em um número finito de indeterminadas da seguinte maneira: $A[x_1, \ldots, x_n] = (A[x_1, \ldots, x_{n-1}])[x_n]$, é suficiente, por indução, mostrarmos o caso $n = 1$. Ou seja, queremos provar que A Noetheriano $\Rightarrow$ $A[x]$ Noetheriano. Demonstraremos que $A[x]$ não-Noetheriano $\Rightarrow$ A não-Noetheriano.

Considere $I \subseteq A[x]$ ideal que não é finitamente gerado. Escolha $f_1 \in I\backslash\{0\}$ de grau menor possível. Considere $f_2 \in I\backslash(f_1)$ de grau mínimo. Considere $f_3 \in I\backslash(f_1, f_2)$ de grau mínimo, e assim por diante: $f_k \in I\backslash(f_1, \ldots, f_{k-1})$, $k \geqslant 2$ de grau mínimo.

Denote por d_k o grau de f_k, e por a_k o coeficiente líder de f_k, ou seja: $f_k = a_k x^{d_k} +$ (termos de grau menor que d_k). Pela escolha de cada f_k, temos $d_1 \leqslant d_2 \leqslant \ldots \leqslant d_k \leqslant \ldots$.

Afirmamos que a cadeia $(a_1) \subseteq (a_1, a_2) \subseteq \ldots \subseteq (a_1, \ldots, a_k) \subseteq \ldots$ é uma cadeia de ideais de A não estacionária.

Suponha por absurdo que ela estacione, isto é, $\exists\ k$ tal que $(a_1, \ldots, a_k) = (a_1, \ldots, a_k, a_{k+1})$. Daí, $a_{k+1} \in (a_1, \ldots, a_k) \Rightarrow a_{k+1} = \sum_{i=1}^{k} b_i a_i$ com $b_i \in A$.

Defina

$$g = \sum_{i=1}^{k} b_i x^{d_{k+1}-d_i} f_i,$$

e note que $g \in (f_1, \ldots, f_k)$. Deste modo, tem-se:

$$g = b_1 x_1^{d_{k+1}-d_1}(a_1 x^{d_1} + \cdots) + b_2 x^{d_{k+1}-d_2}(a_2 x^{d_2} + \cdots) + \cdots + b_k^{d_{k+1}-d_k}(a_k x^{d_k} + \cdots).$$

Logo,

$$g = a_1 b_1 x^{d_{k+1}} + a_2 b_2 x^{d_{k+1}} + \cdots + a_k b_k x^{d_{k+1}} + (\text{termos de grau menor que } d_{k+1}).$$

Assim,

$$g = (a_1b_1 + \ldots + a_kb_k)x^{d_{k+1}} + (\text{termos de grau menor que } d_{k+1}).$$

Como $a_1b_1 + \cdots + a_kb_k = a_{k+1}$ temos que

$$g = a_{k+1}x^{d_{k+1}} + (\text{termos de grau menor que } d_{k+1}).$$

Considere

$$\begin{aligned} h := f_{k+1} - g = \ & a_{k+1}x^{d_{k+1}} + (\text{termos de grau menor que } d_{k+1}) \\ & -a_{k+1}x^{d_{k+1}} - (\text{ termos de grau menor que } d_{k+1}) \end{aligned}$$

Observe que $\text{grau}(h) < d_{k+1} = \text{grau}(f_{k+1})$. Além disso, como $g \in (f_1, \ldots, f_k) \subseteq I$, $f_{k+1} \in I$ e $f_{k+1} \notin (f_1, \ldots, f_k)$, temos que $h = f_{k+1} - g \in I \backslash (f_1, \ldots, f_k)$, o que contradiz a minimalidade de d_{k+1}.

Assim, conseguimos uma cadeia de ideais em A que não estaciona. Portanto, A é não-Noetheriano.

□

Capítulo 3

Lema de Gauss

Neste capítulo, abordaremos inicialmente a versão clássica do Lema de Gauss sobre o conjunto dos inteiros $\mathbb{Z}$ como uma motivação para o resultado final. Ao final, apresentaremos o principal resultado de nosso trabalho, o Lema de Gauss generalizado para domínios, para tanto, exploraremos definições e propriedades relacionadas.

3.1 O Clássico Lema de Gauss

Na disciplina de introdução à álgebra, em específico na parte de anéis, estudamos sobre o clássico Lema de Gauss. Nesta seção iremos abordar alguns conceitos prévios e iremos apresentar alguns exemplos essências para abordar o que é em si o Lema de Gauss. Iremos ver agora o Lema de Gauss sobre o conjunto dos números inteiros $\mathbb{Z}$.

Definição 3.1.1. Um polinômio $f(x) \in \mathbb{Z}[x]$ é chamado **irredutível** sobre $\mathbb{Z}$ se, $f(x) = g(x) \cdot h(x)$ com $g(x), h(x) \in \mathbb{Z}[x]$, então $g(x)$ ou $h(x)$ deve ser um polinômio constante. Em outras palavras, $f(x)$ é irredutível se não pode ser fatorado em um produto de dois polinômios com coeficientes inteiros não constantes. Do contrário, dizemos que $f(x)$ é **redutível** sobre $\mathbb{Z}$.

Exemplo 3.1.1. O polinômio $f(x) = x^2 + 1$ é irredutível sobre $\mathbb{Z}$ porque não pode ser fatorado em dois polinômios de grau menor com coeficientes inteiros.

Exemplo 3.1.2. O polinômio $g(x) = x^2 - 4$ é redutível sobre $\mathbb{Z}$, pois pode ser fatorado como $(x - 2)(x + 2)$, ambos com coeficientes inteiros.

Definição 3.1.2. Um polinômio $f(x) \in \mathbb{Q}[x]$ é chamado **irredutível** sobre $\mathbb{Q}$ se, $f(x) = g(x) \cdot h(x)$ com $g(x), h(x) \in \mathbb{Q}[x]$, então $g(x)$ ou $h(x)$ deve ser um polinômio constante. Em

outras palavras, $f(x)$ é irredutível se não pode ser fatorado em um produto de dois polinômios com coeficientes racionais não constantes. Do contrário, dizemos que $f(x)$ é **redutível** sobre $\mathbb{Q}$.

Exemplo 3.1.3. O polinômio $f(x) = x^2 - 2$ é irredutível sobre $\mathbb{Q}$ porque não pode ser fatorado em $\mathbb{Q}[x]$. Note que sua fatoração envolveria $\sqrt{2}$, que não é racional.

Lema 3.1.1. *(Lema de Gauss sobre $\mathbb{Z}$) Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$, então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. Temos como hipótese que $f(x) \in \mathbb{Z}[x]$ é irredutível sobre $\mathbb{Z}$, ou seja, não pode ser fatorado como o produto de dois polinômios não constantes em $\mathbb{Z}[x]$. Iremos mostrar que $f(x)$ também é irredutível sobre $\mathbb{Q}$.

Faremos a prova pela contra positiva. Vamos supor que $f(x)$ não seja irredutível sobre $\mathbb{Q}$, ou seja, existe uma fatoração de $f(x)$ como o produto de dois polinômios não constantes com coeficientes racionais e a partir dessa suposição, trabalharemos para mostrar que $f(x)$ não é irredutível em $\mathbb{Z}$.

Suponha que $f(x)$ não seja irredutível em $\mathbb{Q}[x]$. Então, podemos escrever $f(x)$ como o produto de dois polinômios não constantes em $\mathbb{Q}[x]$:

$$f(x) = g(x)h(x),$$

onde $g(x), h(x) \in \mathbb{Q}[x]$. Sabemos que $g(x), h(x)$ tem coeficientes racionais, ou seja, podemos escrever:

$$g(x) = \frac{g_1(x)}{a},\ h(x) = \frac{h_1(x)}{b},$$

onde $g_1(x), h_1(x) \in \mathbb{Z}[x]$ são polinômios com coeficientes inteiros, e $a, b \in \mathbb{Z} \setminus \{0\}$ são os denominadores comuns dos coeficientes de $g(x), h(x)$, respectivamente.

Substituindo essas expressões em $f(x) = g(x)h(x)$, temos:

$$f(x) = \left(\frac{g_1(x)}{a}\right)\left(\frac{h_1(x)}{b}\right) = \frac{g_1(x)h_1(x)}{ab}$$

Multiplicando ambos o lado da equação por $m =: ab$, obtemos:

$$mf(x) = g_1(x)h_1(x)$$

Aqui, $g_1(x), h_1(x)$ são polinômios com coeficientes inteiros e, portanto, $mf(x)$ é fatorado como o produto de dois polinômios não constantes em $\mathbb{Z}[x]$.

Assim, temos:

$$g_1(x) = a_0 + a_1x + \cdots + a_rx^r, a_i \in \mathbb{Z}.$$
$$h_1(x) = b_0 + b_1x + \cdots + b_sx^s, b_j \in \mathbb{Z}.$$

Agora, supondo que $p \mid m$, sendo p primo. Vamos provar que $p \mid a_i \ \forall \ i \in \{1, \ldots, r\}$ ou $p \mid b_j \ \forall \ j \in \{1, \ldots, s\}$.

De fato, se $\exists \ i \in \{1, \ldots, r\}$ e $\exists \ j \in \{1, \ldots, s\}$ tais que $p \nmid a_i$ e $p \nmid b_j$, considerando que i e j são os menores termos possíveis com esta propriedade.

Desta forma, como $p \mid m$ temos que p divide o coeficiente de x^{i+j} do polinômio $mf(x) = g_1(x) \cdot h_1(x)$, isto é,

$$p \mid (b_0 \cdot a_{i+j} + b_1 \cdot a_{i+j-1} + \cdots + b_j \cdot a_i + \cdots + b_{i+j-1} \cdot a_1 + b_{i+j} \cdot a_0).$$

Pela escolha de i e j, temos que p divide cada parcela, com exceção de $b_j \cdot a_i$, do coeficiente de x^{i+j} de $g_1(x) \cdot h_1(x)$.

Como p divide toda a expressão segue também que $p \mid b_j \cdot a_i$ e como p é um número primo temos que $p \mid a_i$ ou $p \mid b_j$ que é uma contradição. Portanto, se p primo, $p \mid m \Rightarrow p \mid a_i \ \forall \ i \in \{1, \ldots, r\}$ ou $p \mid b_j \ \forall \ j \in \{1, \ldots, s\}$.

Nesse mesmo viés, suponha que $p \mid a_i \ \forall \ i \in \{1, 2, \ldots, r\}$. Assim, $g_1(x) = p \cdot g_2(x)$ onde $g_2(x) \in \mathbb{Z}[x]$. E, se $m = p \cdot m_1$ temos:

$$p \cdot m_1 f(x) = p \cdot g_2(x) \cdot h_1(x)$$
$$m_1 f(x) = g_2(x) \cdot h_1(x).$$

Deste modo, como o número de fatores primos de m é finito baseado no argumento acima (como também pela indução sobre o número de fatores primos de m), temos que:

$$f(x) = G(x) \cdot H(x),$$

na qual, $G(x), H(x) \in \mathbb{Z}[x]$. Além disso, $G(x)$ e $H(x)$ são múltiplos racionais de $g(x)$ e $h(x)$,

respectivamente, contradizendo a irredutibilidade de $f(x)$ sobre $\mathbb{Z}$.

□

3.2 Fundamentos da Fatoração: Caminho ao Lema de Gauss

Nesta seção apresentaremos algumas noções preliminares que são fundamentais para o desenvolvimento do resultado principal deste trabalho o Lema de Gauss generalizado para domínios. Introduziremos uma aritmética sobre domínios.

Definição 3.2.1. Sejam A um domínio e $a, b \in A$. Dizemos que a **divide** b, em símbolos, $a \mid b$, se $\exists\, c \in A$, tal que $b = a \cdot c$. Em linguagem de ideais, se $(b) \subseteq (a)$.

Definição 3.2.2. Sejam A um domínio e $a, b \in A$. Dizemos que a e b são **associados** se, $a \mid b$ e $b \mid a$. Equivalentemente, se $(a) = (b)$.

Agora vamos as noções de irredutibilidade e primalidade em domínios. Posteriormente, discutiremos as diferenças entre as mesmas, assim como a importância de estarmos em domínios (**Proposição 3.2.1**).

Definição 3.2.3. Sejam A um domínio e $a, b \in A$. Um elemento $f \in A\backslash(\mathcal{U}(A) \cup \{0\})$ é dito um elemento **irredutível**, se sempre que $f = g \cdot h$, com $g, h \in A$, então $g \in \mathcal{U}(A)$ ou $h \in \mathcal{U}(A)$. Do contrário, f é dito um elemento **redutível**.

Definição 3.2.4. Sejam A um domínio e $a, b \in A$. Um elemento $f \in A\backslash(\mathcal{U}(A) \cup \{0\})$ é dito um elemento **primo**, se sempre que $f \mid g \cdot h$, com $g, h \in A$, então $f \mid g$ ou $f \mid h$.

Note que em linguagem de ideais, se f é primo então, o ideal principal gerado por f é um ideal primo.

Proposição 3.2.1. *Sejam A um domínio e $p \in A$ com $p \neq 0$ e $p \notin \mathcal{U}(A)$. Se p é primo, então p é irredutível.*

Demonstração. Sejam $a, b \in A$, tais que $p = a \cdot b$. Como $p = a \cdot b$, temos que $p \mid (a \cdot b)$, o que por hipótese implica que $p \mid a$ ou $p \mid b$.

Se $p \mid a$, então existe $c \in A$, tal que $a = c \cdot p$. Deste modo, $p = (c \cdot p) \cdot b$ e como $p \neq 0$ e A é um domínio, então $c \cdot b = 1$. O que implica que $b \in \mathcal{U}(A)$.

Se $p \mid b$, então existe $c \in A$, tal que $b = c \cdot p$. Deste modo, $p = (c \cdot p) \cdot a$ e como $p \neq 0$ e A é um domínio, então $c \cdot a = 1$. O que implica que $a \in \mathcal{U}(A)$. Portanto, p é irredutível. □

Exemplo 3.2.1. Considere o anel $\mathbb{Z}[\sqrt{-5}]$, uma variação do anel dos inteiros de Gauss. Note que neste anel o elemento 3 é irredutível, porém não é primo. De fato, note que claramente 3 divide 6, porém, neste anel também podemos escrever $6 = (1+\sqrt{-5})(1-\sqrt{-5})$ e 3 não divide $(1+\sqrt{-5})$ e também não divide $(1-\sqrt{-5})$. Esta "patologia"ocorreu devido ao fato deste anel admitir fatorações diferentes para o mesmo elemento. Discutiremos isto mais adiante.

3.2.1 Domínio Euclidiano

Um Domínio Euclidiano é um tipo especial de domínio que possui uma função auxiliar denominada de **função Euclideana**. Neste ambiente é possível realizar divisões de maneira semelhante ao que é feito no conjunto dos números inteiros.

Definição 3.2.5. Seja D um domínio. Dizemos que D é um **Domínio Euclideano (DE)** se existe uma função $\varphi : D\backslash\{0\} \to \mathbb{Z}_+ \cup \{0\}$ satisfazendo

I. Dados $a, b \in D$ com $b \neq 0$, existem $q, r \in D$ tais que

$$a = b \cdot q + r, \text{ com } r = 0 \text{ ou } \varphi(r) < \varphi(b);$$

II. $\varphi(a) \leqslant \varphi(ab)$, para todos $a, b \in D\backslash\{0\}$.

A definição acima significa que dados a e b, podemos sempre encontrar um "quociente"q e um "resto"r de forma que o tamanho (medido pela função φ) de r seja estritamente menor que o de b, isto é, a divisão "termina"em um resto suficientemente pequeno.

Agora, iremos apresentar alguns exemplos de domínios Euclideanos. O exemplo mais natural de um domínio Euclideano é o conjunto dos números inteiros $(\mathbb{Z})$.

Exemplo 3.2.2. Considere o domínio dos inteiros $\mathbb{Z}$ e a função euclideana sendo o **valor absoluto** dos inteiros, $\varphi(n) = |n|$, para cada $n \in \mathbb{Z}$. Considerando o algoritmo da divisão dos inteiros, temos que para quaisquer $a, b \in \mathbb{Z}$ com $b \neq 0$, podemos encontrar um quociente q e um resto r tais que $a + b \cdot q + r$ com $0 \leqslant |r| < |b|$. Assim, garantimos que $\mathbb{Z}$ é um domínio Euclideano.

Exemplo 3.2.3. Seja $\mathbb{K}$ um corpo. O anel dos polinômios em um indeterminada sobre o corpo $\mathbb{K}$, denotado por $\mathbb{K}[x]$, é um domínio Euclideano. De fato, neste caso, podemos considerar a função Euclideana como sendo o grau do polinômio dado em $\mathbb{K}[x]$, explicitamente:

$\varphi(f(x)) = \partial(f(x))$, com $f(x) \in \mathbb{K}[x]$. De fato, pela **Proposição 2.2.2**, temos que para quaisquer polinômios $f(x), g(x) \in \mathbb{K}[x]$ com $g(x) \neq 0$, podemos dividir $f(x)$ por $g(x)$ de modo que: $f(x) = g(x) \cdot q(x) + r(x)$ com $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x))$. Deste modo, garantimos que $\mathbb{K}[x]$ é um domínio Euclideano.

Exemplo 3.2.4. O anel dos Inteiros Gaussianos $\mathbb{Z}[i]$ é um domínio Euclideano. Neste anel,os elementos são da forma $a + bi$, onde $a, b \in \mathbb{Z}$ e $i = \sqrt{-1}$. A função Euclideano neste caso é a **norma** de um número complexo $N(a + bi) = a^2 + b^2$. Para $\alpha, \beta \in \mathbb{Z}[i]$ com $\beta \neq 0$, podemos encontrar um quociente q e um resto r tais que $\alpha = \beta \cdot q + r$ com $N(r) < N(\beta)$. Portanto, $\mathbb{Z}[i]$ é um domínio Euclideano.

3.2.2 Domínio de Ideais Principais

Vimos anteriormente na **Definição ??** o conceito de ideal principal, agora iremos ver um tipo especial de domínio onde todo ideal é desta forma, ou seja, domínios em que todos os ideais são gerados por um único elemento.

Definição 3.2.6. Seja D um domínio. Dizemos que D é um **Domínio de Ideais Principais (DIP)** se para cada ideal I de D, existe um elemento $a \in D$ tal que

$$I = (a) = \{r \cdot a \in D \mid r \in D\}.$$

Agora, iremos apresentar exemplos de Domínios de Ideais Principais. Mais uma vez, o exemplo mais clássico de um Domínio de Ideais Principais é o conjunto dos números inteiros $\mathbb{Z}$.

Exemplo 3.2.5. O anel dos inteiros $\mathbb{Z}$ é um Domínio de Ideais Principais. Este fato foi mostrado na **Proposição 1.5.3**.

Exemplo 3.2.6. O anel de polinômios em uma indeterminada sobre um corpo $\mathbb{K}$, denotado por $\mathbb{K}[x]$, é um Domínio de Ideais Principais. Este fato foi mostrado na **Proposição 2.2.3**.

Proposição 3.2.2. *Sejam D um DIP e $p \in D$. Então, p é um elemento primo, se e somente se, p é um elemento irredutível.*

Demonstração. ($\Rightarrow$) Segue diretamente da **Proposição 3.2.1**.

($\Leftarrow$) Suponha que $p \in D$ é um elemento irredutível. Queremos mostrar que p é primo, ou seja, se p divide $a \cdot b$, com $a, b \in D$, então p divide a ou p divide b. Vamos mostrar que o ideal principal gerado por p é um ideal maximal, em particular, (p) é um ideal primo, logo, por definição, p é um elemento primo. Primeiro, como p é irredutível, temos que (p) é um ideal próprio em D. Seja J um ideal próprio de D tal que $(p) \subseteq J$. Como D é um DIP, temos que $J = (q)$ para algum $q \in D$. Portanto, $p = aq$ para algum $a \in D$. Como p é irredutível, temos que $a \in \mathcal{U}(D)$ ou $q \in \mathcal{U}(D)$. Mas $q \notin \mathcal{U}(D)$, pois $J = (q) \subsetneq D$, por isso, $a \in \mathcal{U}(D)$ e assim, $q = a^{-1}p$ e $J = (q) \subseteq (p)$. Portanto, $(p) = J$.

□

Por fim, ainda apresentamos o exemplo do anel dos inteiros de Gauss como Domínio de Ideais Principais. Note que todos os exemplos de Domínios Euclideanos que apresentamos na seção anterior são exemplos de Domínios de Ideais Principais. Isto decorre do fato de todo Domínio Euclideano ser Domínio de Ideais Principais. Veremos isto mais a frente.

Exemplo 3.2.7. O anel dos inteiros gaussianos $\mathbb{Z}[i]$ é um Domínio de Ideais Principais.

3.2.3 Domínio de Fatoração Única

Um Domínio de Fatoração Única é um tipo especial de domínio onde existe a garantia de que qualquer elemento pode ser fatorado em elementos irredutíveis de forma única. Isso generaliza a familiar propriedade dos números inteiros de terem uma fatoração única com respeito aos números primos.

Definição 3.2.7. Um domínio D é dito um **Domínio de Fatoração Única (DFU)** se todo elemento não nulo e não inversível de D pode ser escrito como um produto (finito) de elementos irredutíveis de maneira única, a menos de ordem e elementos associados. Explicitamente:

- (Existência da fatoração) Se $d \in D$, então $d = d_1 d_2 \cdots d_m$ com $d_i \in D,\ i = 1, \ldots, m$, elementos irredutíveis;
- (Unicidade da fatoração) Se $d = q_1 q_2 \cdots q_n$ é outra fatoração em elementos irredutíveis $q_j \in D,\ j = 1, \ldots, n$, então $m = n$, isto é a quantidade de fatores das duas fatorações é igual e existe uma permutação (função bijetora) $\varphi : \{1, \ldots, m\} \to \{1, \ldots, m\}$ tal que d_i é associado a $\varphi(d_i)$, para todo $i = 1, \ldots, m$.

Exemplo 3.2.8. Como sabemos, devido ao Teorema Fundamental da Aritmética, todo número inteiro não nulo pode ser fatorado de maneira única (a menos de ordem e dos elementos associados 1 e -1) em fatores primos, isto é, o domínio $\mathbb{Z}$ é um Domínio de Fatoração Única. Por exemplo:

$$30 = 2 \cdot 3 \cdot 5$$

Essa fatoração é única, exceto pela permutação dos fatores e pelos sinais ± 1, que são as unidades no anel $\mathbb{Z}$.

Uma informação bastante útil é que em Domínios de Fatoração Única as noções de elementos primo e irredutível são equivalentes.

Lema 3.2.1. *Sejam D um DFU e $p \in D$, com $p \neq 0$ e $p \notin \mathcal{U}(D)$. Então,*

$$p \text{ é irredutível } \Leftrightarrow p \text{ é primo } .$$

Demonstração. ($\Rightarrow$) Sejam $a, b \in D$ tais que $p \mid (a \cdot b)$. Daí, $a \cdot b = p \cdot c$, para algum $c \in D$. Se $a = 0$ ou $b = 0$, então $p \mid a$ ou $p \mid b$. Por isso, podemos supor que $a \neq 0$ e $b \neq 0$. Se $a \in \mathcal{U}(D)$, então, $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (c \cdot p)$, logo, $b = (a^{-1} \cdot c) \cdot p$, e portanto, $p \mid b$. Analogamente, se $b \in \mathcal{U}(D)$, então, $p \mid a$. Assim, vamos supor que $a, b \in D \backslash (\mathcal{U}(D) \cup \{0\})$.

Como D é um DFU podemos escrever $a = a_1 \cdots a_r$ e $b = b_1 \cdots b_s$, onde $a_1, \ldots, a_r, b_1, \ldots, b_s$ são elementos irredutíveis em D. Assim, $p \cdot c = a \cdot b = (a_1 \cdots a_r)(b_1 \cdots b_s)$. Daí, pela unicidade da fatoração, como p é irredutível, segue que p é associado à algum a_i ou p é associado à algum b_j, implicando que $p \mid a$ ou $p \mid b$. Portanto, p é primo.

($\Leftarrow$) Segue imediatamente da **Proposição 3.2.1**. □

Teorema 3.2.1. *Seja D um domínio. Se D é um DE, então, D é um DIP.*

Demonstração. Para mostrar esta implicação, vamos supor que D seja um DE e φ sua função Euclideana. Queremos demonstrar que todo ideal I de D é principal. Seja I um ideal de D. Se $I = \{0\}$, ou seja, I é o ideal nulo, então, I é principal gerado pelo elemento zero. Se $I \neq \{0\}$, podemos considerar $a \in I$ tal que $a \neq 0$ e $\varphi(a)$ é mínimo entre os $\varphi(b)$, para todos $b \in I \backslash \{0\}$, ou seja, entre todos os elementos elementos não nulos de I. Este elemento a existe devido ao Princípio da Boa Ordenação (PBO) do conjunto dos números naturais, já que a imagem da φ está contida em $\mathbb{N}$.

Agora iremos provar que $I = (a)$. De fato, seja $b \in I$. Pela hipótese Euclideana, existem $q, r \in D$ tais que $b = aq + r$, onde $r = 0$ ou $\varphi(r) < \varphi(a)$. Como $b \in I$ e $a \in I$, tem-se que $r = b - aq \in I$. Se $r \neq 0$, então, por hipótese segue que $\varphi(r) < \varphi(a)$, e isto contradiz a escolha de a como elemento de I com $\varphi(a)$ mínimo. Portanto, pela minimalidade de $\varphi(a)$ temos $r = 0$, ou seja, $b = aq$. Desta forma, qualquer $b \in I$ pode ser escrito como um múltiplo de a, ou seja, $I \subseteq (a)$. Como obviamente, $(a) \subseteq I$, já que $a \in I$, temos que $I = (a)$ como desejávamos demonstrar.

□

Teorema 3.2.2. *Seja D um domínio. Se D é um DIP, então D é um DFU.*

Demonstração. Para mostrar esta implicação, vamos supor que D seja um DIP. Queremos demonstrar que cada elemento de D pode ser fatorado em elementos irredutíveis. Seja $a \in D$ um elemento não nulo e não unidade. Se a é irredutível, então, nada temos a fazer. Se a não for irredutível, então, a pode ser escrito como produto de dois elementos $a = a_1 \cdot b_1$, com a_1, b_1 não nulos e não unidades. Se a_1, b_1 são irredutíveis, nada a fazer. Se algum dos fatores a_1 ou b_1 não for irredutível, repetiremos o processo de fatoração. Em linguagem de ideais, ao continuarmos com este processo, estamos montando uma cadeia ascendente de ideais

$$(a) \subsetneq (a_1) \subsetneq (a_2) \cdots .$$

Mas como D é um DIP, temos que D é Noetheriano, logo esta cadeia precisa estacionar, isto é, esse processo de fatoração deve terminar. Portanto, o elemento a deve ser escrito como um produto $a = a_1 \cdots a_m$ sendo $a_1, \ldots, a_m$ elementos irredutíveis de D.

Para demonstramos que a fatoração é única, supomos que existem duas fatorações para o mesmo elemento. Desta forma, a pode ser fatorado como $a = p_1 \cdot p_2 \cdots p_n$ e também como $a = q_1 \cdot q_2 \cdots q_m$, com $n \leqslant m$, sem perda de generalidade, onde p_i e q_j são irredutíveis para todos i, j. Mas, pela **Proposição 3.2.2** temos que os elementos p_i e q_j são primos. Temos que demonstrar que essas fatorações são equivalentes a menos da ordem e dos elementos associados.

De fato, da igualdade $p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m$, vamos reescrever da seguinte maneira: $p_1 \cdot (p_2 \cdots p_n) = q_1 \cdot q_2 \cdots q_m$. Como p_1 é irredutível, logo primo pelo comentando anteriormente, temos que $p_1 \mid q_j$, para algum j. Daí, $q_j = p_1 \cdot u_1$, para algum $u_1 \in \mathcal{U}(D)$, visto que q_j também é irredutível. Reordenando, se necessário, podemos supor que $j = 1$. Assim, $q_1 = p_1 \cdot u_1$.

Substituindo q_1 por $p_1 \cdot u_1$, temos que $p_1 \cdot p_2 \cdots p_n = p_1 \cdot u_1 \cdot (q_2 \cdots q_m)$. Como estamos em

um domínio, podemos usar a lei do cancelamento e obter $\cancel{p_1} \cdot p_2 \cdot p_3 \dots p_n = \cancel{p_1} \cdot u_1 \cdot (q_2 \cdot q_3 \dots q_m)$, isto é, $p_2 \cdot p_3 \cdots p_n = u_1 \cdot (q_2 \cdot q_3 \cdots q_m)$.

Se aplicarmos este mesmo argumento repetidamente, chegaremos a conclusão da seguinte igualdade $1 = u_1 \cdot u_2 \cdots u_n \cdot (q_{n+1} \cdots q_m)$, sendo $u_1, \dots, u_n \in \mathcal{U}(D)$. Portanto, $n = m$ e $q_i = u_i p_i$ para todo $i = 1, \dots, n$, a menos de reordenação.

□

Por fim, demonstramos que se D é um DIP, então, D também é um DFU, pois cada elemento não nulo e não associado pode ser fatorado em elementos irredutíveis e essa fatoração é única, a menos da ordem e elementos associados. Como uma consequência do resultado anterior, podemos exibir os seguintes exemplos de Domínios de Fatoração Única.

Exemplo 3.2.9. O anel de polinômios em uma indeterminada sobre um corpo $\mathbb{K}$, denotado por $\mathbb{K}[x]$, é um Domínio de Fatoração Única. De fato, foi mostrado no **Exemplo 3.2.6** que $\mathbb{K}[x]$ é um Domínio de Ideais Principais. Logo, a conclusão segue do resultado anterior.

Por exemplo, em $\mathbb{R}[x]$, o polinômio se fatora como:

$$x^2 - 1 = (x - 1)(x + 1),$$

exceto pela ordem dos fatores e sinal.

Exemplo 3.2.10. O anel dos inteiros gaussianos $\mathbb{Z}[i]$ é um Domínio de Fatoração Única. De fato, foi mostrado no **Exemplo 3.2.7** que $\mathbb{Z}[i]$ é um Domínio de Ideais Principais. Logo, a conclusão segue do resultado anterior. Neste domínio, todo número não nulo pode ser fatorado de maneira única em elementos irredutíveis, a menos da ordem e das unidades $1, -1, i, -i$.

Por exemplo, em $\mathbb{Z}[i]$, o número 5 se fatora como:

$$5 = (2 + i)(2 - i),$$

exceto pela ordem dos fatores e sinal.

3.3 Generalização do Lema de Gauss

Nesta seção apresentaremos o resultado principal do trabalho: uma versão mais geral do Lema de Gauss para domínios.

Definição 3.3.1. Sejam D um DFU e $p(x) \in D[x]\backslash\{0\}$. Dizemos que $p(x)$ é **primitivo**, se dado $\rho \in D$ um elemento primo, tem-se que ρ não divide todos os coeficientes do polinômio $p(x)$.

Observação 3.3.1. Iremos discutir a funcionalidade desta definição, pois,a mesma é uma definição vital para o decorrer desta seção.

Para esta definição, observe que os coeficientes de $p(x)$ só podem ser divididos simultaneamente por um divisor não primo. Considere o seguinte polinômio $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, onde $a_i \in D$ para todo i e $a_n \neq 0$.

Supor que $p(x)$ é primitivo significa que não existe um $\rho \in D$ elemento primo tal que este divida todos os coeficientes a_i de p.

Do contrário, vamos supor que existe um primo $\rho \in D$ tal que ρ divide todos os coeficientes a_i de $p(x)$. Desta forma, que $a_i = \rho b_i$, onde $b_i \in D$ para todo i e $b_n \neq 0$. Substituindo $a_i = \rho b_i$ na expressão polinomial de $p(x)$, temos que $p(x) = \rho b_0 + \rho b_1 x + \rho b_2 x^2 + \cdots + \rho b_n x^n$. Colocando ρ em evidência, temos $p(x) = \rho(b_0 + b_1x + b_2x^2 + \cdots + b_nx^n)$.

Exemplo 3.3.1. Seja $p(x) = 5x^3 + 7x^2 + x + 2 \in \mathbb{Z}[x]$. Note que os coeficientes de $p(x)$ são $5, 7, 1$ e 2. O MDC (Máximo Divisor Comum) entre estes coeficientes é 1, portanto, não existe primo que divide tais inteiros simultaneamente. Logo, $p(x)$ é um polinômio primitivo.

O próximo resultado nos garantirá informações interessantes sobre o como se comporta esta noção de polinômio primitivo na passagem de $D[x]$ para $K[x]$ sendo K o corpo de frações do domínio D.

3.3.1 Corpo de Frações

O corpo de frações de um domínio D é o menor corpo que contém D como um subanel. Ele é formado a partir dos elementos de D de maneira análoga à construção dos números racionais $\mathbb{Q}$ a partir dos inteiros $\mathbb{Z}$. O conceito é importante porque, em muitos casos, ao trabalhar com domínios, queremos ter a habilidade de dividir elementos (exceto o zero), e o corpo de frações fornece essa possibilidade.

Definição 3.3.2. Seja D um domínio. O **corpo de frações** de D, denotado por $Frac(D)$, é o conjunto quociente da seguinte relação de equivalência no produto cartesiano $D \times (D\backslash\{0\})$:

$$(a, b) \sim (c, d) \text{ se, e somente se, } ad = bc.$$

A cada par ordenado (a, b) associamos a sua classe de equivalência denotada por $\frac{a}{b}$.

Propriedades 3.3.1. O corpo de frações $Frac(D)$ contém elementos da forma $\frac{a}{b}$, com as seguintes operações:

I. Soma: A soma de duas frações $\frac{a}{b}$ e $\frac{c}{d}$, onde $a, b, c, d \in D$ e $b, d \neq 0$, é dada por:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Esta operação está bem definida porque D é um domínio, ou seja, $bd \neq 0$.

II. Produto: O produto de duas frações $\frac{a}{b}$ e $\frac{c}{d}$, onde $a, b, c, d \in D$ e $b, d \neq 0$, é dado por:

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Esta operação está bem definida porque D é um domínio, ou seja, $bd \neq 0$.

III. Elementos Identidades: O elemento identidade da soma é $\frac{0}{1}$, sendo $0 \in D$. O elemento identidade do produto é $\frac{1}{1}$, sendo $1 \in D$.

IV. Inverso Multiplicativo: Cada fração $\frac{a}{b}$, com $a, b \in D$ e $b \neq 0$, possui um inverso multiplicativo dado por $\frac{b}{a}$, com a condição que $a \neq 0$.

Com essas operações, o conjunto $Frac(D)$ satisfaz todas as propriedades de um corpo: fechamento para soma e produto, existência de elementos identidades etc.

Exemplo 3.3.2. Um exemplo clássico é a construção do corpo $\mathbb{Q}$ dos números racionais a partir do domínio $\mathbb{Z}$ dos inteiros. Cada número racional $\frac{a}{b}$ com $a \in \mathbb{Z}$ e $b \neq 0 \in \mathbb{Z}$ é uma fração onde as operações são as usuais de soma e multiplicação de frações.

Lema 3.3.1. *Sejam D um DFU, $K = Frac(D)$ seu corpo de frações e $f, g \in D[x]$.*

I. Se f, g são primitivos, então $f \cdot g$ são primitivos;

II. Se f é primitivo e $f \mid g$ em $K[x]$, então, $f \mid g$ em $D[x]$;

III. Se f é primitivo, então, f é irredutível em $K[x] \Leftrightarrow f$ é irredutível em $D[x]$.

Demonstração. (I.) Para demonstramos que o produto de dois polinômios primitivos é primitivo, vamos considerar que $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, onde $a_i \in D$ para

todo i e $a_n \neq 0$ e $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$, onde $b_j \in D$ para todo j e $b_m \neq 0$, são polinômios primitivos em $D[x]$. Seja $h(x) = f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_kx^k$, onde $c_l = \sum_{i+j=l} a_i \cdot b_j$.

Seja $\rho \in D$ um elemento primo. Devemos mostrar que ρ não divide os coeficientes c_l simultaneamente. De fato, como $f(x)$ e $g(x)$ são primitivos, temos que ρ não divide simultaneamente os coeficientes a_i de $f(x)$ e os coeficientes b_j de $g(x)$. Logo, no anel polinomial $\frac{D}{(\rho)}[x]$ temos que $\overline{f(x)}$ e $\overline{g(x)}$ são não nulos. Como ρ é um elemento primo, temos que (ρ) é um ideal primo, assim, $\frac{D}{(\rho)}$ é um domínio, e pela **Proposição 2.2.1**, temos que $\frac{D}{(\rho)}[x]$ é um domínio. Portanto, $\overline{h(x)} = \overline{f(x)} \cdot \overline{g(x)}$ é não nulo. Logo, em particular, ρ não divide simultaneamente todos os coeficientes c_l de $h(x)$ e assim, $h(x)$ é primitivo.

(II.) Para demonstrarmos que se f é primitivo e $f \mid g$ em $K[x]$ então, $f \mid g$ em $D[x]$, é necessário provar que existe $h \in D[x]$ tal que $g = f \cdot h$. Dado que f divide g em $K[x]$, existe $h \in K[x]$ tal que $g = f \cdot h$. Como K é o corpo de frações de D, podemos escrever h na forma $h = \frac{h_1}{b}$, onde $h_1 \in D[x]$ e $b \in D$. Considere ainda $a \in D$ tal que $h_1 = ah_2$ sendo $h_2 \in D[x]$ seja primitivo. Para concluirmos este item, basta mostrarmos que b divide a em D.

Desta forma, temos $g = f \cdot \frac{ah_2}{b}$ sendo f, h_2 elementos primitivos. Pelo item (I.), temos que fh_2 é primitivo. Da igualdade anterior, temos que $bg = afh_2$. Seja $p \in D$ um elemento irredutível da fatoração de b. Note que b possui fatoração, pois D é um DFU. Note que este elemento p é também primo pela **Proposição 3.2.1**. Daí, p divide todos os coeficientes dos termos de afh_2, mas como fh_2 é primitivo, segue que p divide a. Logo, b divide a e consequentemente f divide g em $D[x]$.

(III.) ($\Rightarrow$) Para demonstrarmos esta implicação, faremos uso da contra recíproca. Suponha que f não é irredutível em $D[x]$. Então existe uma fatoração não trivial $f = g \cdot h \in D[x]$, onde $g, h \in D[x]$ com g, h não unidades. Como $\mathcal{U}(D[x]) = \mathcal{U}(D)$, pela **Proposição 2.2.4**, note que $\partial(g) > 0$ e $\partial(h) > 0$. Do contrário, se um dos polinômios da fatoração tivesse grau zero, então, este elemento seria um elemento de D e consequentemente, f não seria primitivo. Como g e h estão em $D[x]$, ambos também estão em $K[x]$. Isso significa que f pode ser fatorado em $K[x]$ como $f = g \cdot h$.

($\Leftarrow$) Para demonstrarmos esta implicação, vamos trabalhar com a contra recíproca. Suponha que f não é irredutível em $K[x]$. Então existe uma fatoração não trivial $f = g \cdot h$ em $K[x]$, onde $g, h \in K[x]$ com g, h não unidades, ou seja, $\partial(g) > 0$ e $\partial(h) > 0$, já que mais uma vez pela **Proposição 2.2.4** temos que $\mathcal{U}(K[x]) = \mathcal{U}(K) = K\backslash\{0\}$, pois K é um corpo.

Analogamente ao que foi feito no item (II.), podemos supor que $g \in D[x]$ e g é um elemento primitivo. Assim, temos que $g \in D[x]$ é um elemento primitivo que divide f em $K[x]$. Logo, pelo item (II.) temos que $g \mid f$ em $D[x]$, logo, existe $q \in D[x]$ tal que $f = gq$. Portanto, f é redutível em $D[x]$.

□

Agora, iremos apresentar o principal resultado deste trabalho que é o Lema de Gauss em sua versão para domínios.

Teorema 3.3.1. (Lema de Gauss) *Sejam D um domínio e $K = Frac(D)$. Se D é um DFU então, $D[x]$ é um DFU.*

Demonstração. Primeiro vamos mostrar que se $p \in D[x]$ é irredutível, então, p é primo. Isto é suficiente para mostrar que a fatoração (que será mostrada a seguir) é única. Se $\partial(p) = 0$, então, $p \in D$, logo, p é primo, pois D é um DFU por hipótese. Se $\partial(p) > 0$, então afirmamos que p é primitivo, do contrário, existiria $a \in D$ elemento primo tal que $p = ab$, uma fatoração não trivial de p. Logo, pelo item (III.) do Lema anterior temos que p é irredutível em $K[x]$, em particular, p é primo, já que $K[x]$ é um DFU, pois K é um corpo (segue pelo **Exemplo 3.2.9**). Agora, sejam $g, h \in D[x]$ tais que $p \mid gh$ em $D[x]$. Assim, $p \mid gh$ em $K[x]$ e consequentemente, $p \mid g$ ou $p \mid h$ em $K[x]$, já que p é primo em $K[x]$. Logo, pelo item (II.) do Lema anterior, temos que $p \mid g$ ou $p \mid h$ em $D[x]$ e p é primo por definição.

Para a fatoração, seja $f \in D[x]$. Como $K[x]$ é um DFU, temos que $f = ap_1 \cdots p_r$ com $a \in K$ e $p_1, \ldots, p_r \in K[x]$ elementos irredutíveis. Mais uma vez, podemos supor que $p_1, \ldots, p_r \in D[x]$ e que são primitivos. Assim, pelo item (III.) do Lema anterior, temos que $p_1, \ldots, p_r$ são irredutíveis em $D[x]$. Além disso, o elemento $P := p_1 \cdots p_r$ é primitivo pelo item (I.) do Lema anterior. Como P divide f em $K[x]$, mais uma vez pelo item (II.) do Lema anterior temos que P divide f em $D[x]$. Logo, $a \in D$. Considerando a fatoração de a em D, que é DFU, tem-se $a = a_1 \cdots a_s$, sendo $a_1, \ldots, a_s \in D$ irredutíveis. Portanto, $f = a_1 \cdots a_s p_1 \cdots p_r$ é uma fatoração de f em $D[x]$.

□

Uma consequência imediata do resultado anterior nos garante que o anel de polinômios em um número finito de indeterminadas sobre um corpo é um Domínio de Fatoração Única.

Corolário 3.3.1. *Se K é um corpo, então, $K[x_1, \ldots, x_n]$ é um DFU.*

Referências Bibliográficas

BIAZZI, Ricardo Neves. **Polinômios irredutíveis**: critérios e aplicações. 2014. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Instituto de Geociências e Ciências Exatas, Universidade Estadual Paulista, Rio Claro, 2014.

DOMINGUES, Hygino,; IEZZI, Gelson. **Álgebra moderna**. Vol. 4. ed. reform. São Paulo: Atual, 2003.

EVARISTO, Jaime.; PERDIGÃO, Eduardo. **Introdução à álgebra abstrata**. Vol. 3. ed. Maceió: Edufal, 2020.

GONÇALVES, Adilson. **Introdução à álgebra**. Vol. 6. ed. Rio de Janeiro: IMPA, 2017.

KLEINER, Israel. **A History Of Abstract Algebra**. [S.I.]. Birkhäuser, 2007.

LEE, Gregory T. **Abstract Algebra: An Introductory Course**. [S.I.]. Springer, 2018.

TENGAN, Eduardo.; BORGES, Herivelto. **Álgebra Comutativa em 4 movimentos**. Ed. Rio de Janeiro: IMPA, 2014.

SARACINO, Dan. **Abstract Algebra: A first Course**. Vol. 2. ed. Long Grove: Waveland Press, 2008.