Universidade Federal de Goiás
Instituto de Matemática e Estatística
Programa de Mestrado Profissional em
Matemática em Rede Nacional

A ÁLGEBRA DOS POLINÔMIOS

Reginaldo Jacinto de Sousa

Goiânia

2020

UFG

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO (TECA) PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES

E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo das Teses e Dissertações disponibilizado na BDTD/UFG é de responsabilidade exclusiva do autor. Ao encaminhar o produto final, o autor(a) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do material bibliográfico

[x] Dissertação [ ] Tese

2. Nome completo do autor

Reginaldo Jacinto de Sousa

3. Título do trabalho

A ÁLGEBRA DOS POLINÔMIOS

4. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador)

Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante:
a) consulta ao(à) autor(a) e ao(à) orientador(a);
b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo da tese ou dissertação.
O documento não será disponibilizado durante o período de embargo.
Casos de embargo:
- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

Obs. Este termo deverá ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Ivonildes Ribeiro Martins**, **Professor do Magistério Superior**, em 25/06/2020, às 19:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **REGINALDO JACINTO DE SOUSA**, **Usuário Externo**, em 26/06/2020, às 13:48, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Referência: Processo nº 23070.012159/2020-09 SEI nº 1388751

Criado por sosteneg, versão 3 por ivonildes em 25/06/2020 19:55:34.

Reginaldo Jacinto de Sousa

A ÁLGEBRA DOS POLINÔMIOS

Trabalho de Conclusão de Curso apresentado ao Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos para obtenção do grau de Mestre em Matemática.
Área de Concentração: Matemática do Ensino Básico.
Orientadora: Profª. Drª. Ivonildes Ribeiro Martins Dias.

Goiânia

2020

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Sousa, Reginaldo Jacinto de
A ÁLGEBRA DOS POLINÔMIOS [manuscrito] / Reginaldo Jacinto de Sousa. - 2020.
iv, 84 f.: il.

Orientador: Profa. Dra. Ivonildes Ribeiro Martins Dias.
Trabalho de Conclusão de Curso Stricto Sensu (Stricto Sensu) - Universidade Federal de Goiás, Instituto de Matemática e Estatística (IME), PROFMAT - Programa de Pós-graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RG), Goiânia, 2020.
Bibliografia.
Inclui lista de figuras.

1. Álgebra. 2. Anéis de polinômios. 3. Irredutibilidade polinomial. I. Dias, Ivonildes Ribeiro Martins, orient. II. Título.

CDU 51

UNIVERSIDADE FEDERAL DE GOIÁS

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

ATA DE DEFESA DE DISSERTAÇÃO

Ata nº **04/2020** da sessão de Defesa de Dissertação de **Reginaldo Jacinto de Sousa**, que confere o título de Mestre em Matemática**,** na área de concentração em Álgebra.

Aos vinte e oito dias do mês de maio de dois mil e vinte, a partir das 16 **horas**, por meio de videoconferência devido a covid-19, realizou-se a sessão pública de Defesa de Dissertação intitulada **"A ÁLGEBRA DOS POLINÔMIOS"**. Os trabalhos foram instalados pela Orientadora, Professora Doutora Ivonildes Ribeiro Martins Dias **(IME/UFG)** com a participação dos demais membros da Banca Examinadora: Professor Doutor Mario José de Souza (IME/UFG) e membro titular externo a Professora Doutora Aline Mota de Mesquita Assis (IFG). **Participara por meio de videoconferência:** A Professora Doutora Ivonildes Ribeiro Martins Dias **(IME/UFG)** o Professor Doutor Mario José de Souza (IME/UFG) e a Professora Doutora Aline Mota de Mesquita Assis (IFG). Durante a arguição os membros da banca **não fizeram** sugestão de alteração do título do trabalho. A Banca Examinadora reuniu-se em sessão secreta a fim de concluir o julgamento da Dissertação, tendo sido o candidato **aprovado** pelos seus membros. Proclamados os resultados pela Professora Doutora Ivonildes Ribeiro Martins Dias, Presidente da Banca Examinadora, foram encerrados os trabalhos e, para constar, lavrou-se a presente ata que é assinada pelos Membros da Banca Examinadora, aos vinte e oito dias do mês de maio de dois mil e vinte.

TÍTULO SUGERIDO PELA BANCA

Documento assinado eletronicamente por **Aline Mota de Mesquita Assis**, **Usuário Externo**, em 04/06/2020, às 08:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Ivonildes Ribeiro Martins**, **Professor do Magistério Superior**, em 04/06/2020, às 09:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Mário José De Souza**, **Professor do Magistério Superior**, em 04/06/2020, às 16:31, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1216517** e o código CRC **4B9A05C2**.

Reginaldo Jacinto de Sousa graduou-se em Ciências Contábeis pela Universidade Estadual de Goiás (Campus de Morrinhos) em 2009, especializou-se em Perícia, Auditoria e Direito Tributário pela Faculdade Araguaia em 2014, atualmente é Contador, Distribuidor e Partidor Judiciária da Comarca de Cromínia.

Dedicatória

Primeiramente dedico esse trabalho a Deus, ao meu primo e grande amigo Ismael Adriano dos Santos (in memorian), sua alegria jamais será esquecida. À minha família, principalmente a minha mãe e meu pai.

Agradecimentos

Agradeço primeiramente a Deus por todas suas bênçãos e graças concedidas.

À minha família, agradeço e dedico esse trabalho, assim como todas as minhas conquistas.

Agradeço especialmente à minha mãe por todo apoio, sabedoria e amor que me deu durante toda a vida, especialmente na acadêmica.

Agradeço à minha esposa por todo o seu apoio, amor e carinho.

Agradeço ao meu primo Ismael por todo o seu apoio e ajuda.

Aos meus colegas do PROFMAT que tornaram nossas sextas-ferias de muito estudo em momentos especiais de muita alegria - obrigado por deixar-me caminhar ao lado de vocês nesta jornada.

Aos que integram o PROFMAT e aos professores do Instituto de Matemática e Estatística da Universidade Federal de Goiás.

À Profª. Drª. Ivonildes Ribeiro Martins Dias, por toda orientação neste Trabalho. Agradeço muito por sua paciência e dedicação à conclusão deste trabalho.

Então a todos, muito obrigado pela paciência, pelo incentivo, pelo apoio, pela força e principalmente pelo carinho.

Resumo

Neste trabalho, abordaremos a definição de polinômio utilizando o conceito de sequência, a qual permite remover a ambiguidade do símbolo x, e estudaremos a estrutura algébrica dos anéis de polinômios, o conceito e os critérios de irredutibilidade polinomial e fatoração de um polinômio em produto de polinômios irredutíveis, tendo como objetivo fornecer aos professores de Matemática que atuam no Ensino Médio, um aprofundamento no estudo da álgebra abstrata. Obtendo, algumas sugestões de aplicações em sala de aula, por exemplo, o estudo da racionalidade de um determinado número.

Palavras-chave

Álgebra, Anéis de polinômios, Irredutibilidade polinomial.

Abstract

In this work, we will approach the definition of polynomial using the concept of sequence, which allows you to remove the ambiguity from the symbol x, and we will study the algebraic structure of the polynomial rings, the concept and criteria of polynomial irreducibility and factoring of a polynomial in the product of irreducible polynomials, aiming to provide mathematics teachers who work in high school, a deepening in the study of abstract algebra. Obtaining, some suggestions of applications in the classroom, for example, the study of the rationality of a given number.

Keywords

Algebra, Polynomial rings, Irreducibility polynomial.

Lista de Figuras

Sumário

Introdução

Com os trabalhos de Diofanto surge na grécia antiga um modo de pensar matemática bem próximo do que chamamos de álgebra, uma de suas principais contribuições é ter introduzido uma forma de representar o valor desconhecido de um problema, o qual designou como *arithme*, de onde deu origem ao nome aritmética. A sua principal obra é *Arithmetica*, que era composta originalmente por treze livros, dos quais somente os seis primeiros se preservaram, esta obra contém uma coleção de problemas que faziam parte da tradição matemática da época.

Após a queda da escola de Alexandria em 641, que era por muito tempo o centro matemático do mundo, foram os indianos e os árabes que mantiveram o desenvolvimento da matemática. Durante o califado de *Al-Mamum* é estabelecido em Bagdá uma "Casa de Sabedoria" que é comparado ao antigo Museu de Alexandria, entre os matemáticos da época destaca o matemático *Mohammed ibu-Musa al-Khowarizmi*, sendo sua obra mais importante o livro *Al-jabr wa'l muqabalah* sobre equações. Com esse livro mais tarde a Europa apreendeu o ramo da matemática chamado "Álgebra". A palavra *Al-jabr* significa "restauração" ou "completação" e a palavra *muqabalah* refere-se a "redução" ou "equilíbrio". Mesmo que essa obra não pode ser tida como revolucionária, é muito importante para a matemática, pois foi a primeira a apresentar de forma sistemática a resolução das equações quadráticas.

Houve vários colaboradores durante o passar dos anos para o desenvolvimento da álgebra, seja pela resolução de problemas ou mesmo por desafios intelectuais lançados. Por exemplo, temos a resolução das equações cúbicas.

> No início do século XVI, Scipione Del Ferro obteve uma fórmula usando radicais para a solução de um certo tipo de equação, o que constituiu uma novidade em relação aos trabalhos árabes. Mas esta fórmula foi mantida secreta, como era costume na época. Alguns anos mais tarde, por volta de 1535, outro matemático italiano Niccolo Fontana, conhecido pela alcunha de

> Tartaglia, resolveu diversas equações cúbicas, em particular as do tipo que escrevemos hoje como $x^3 + mx^2 = n$, considerada com coeficientes exclusivamente numéricos. Um terceiro matemático italiano, Girolamo Cardano, que parece ter obtido a fórmula de Tartaglia, com a promessa de manter segredo, publicou esta fórmula por volta de 1545. Ainda que os coeficientes da equação devessem ser números positivos, Cardano chega a admitir soluções negativas para as equações, denominadas "raízes menos puras" ou "números fictícios".([11], p.162-163).

Algum tempo depois o matemático francês François Viète, introduziu uma representação padrão para os coeficientes de uma equação, que consiste na representação das incógnitas pelas vogais e os coeficientes pelas consoantes do alfabeto, ou seja, ele inseriu o uso de letras nas manipulações algébricas, com isso chega a uma concepção próxima da álgebra que conhecemos hoje.

Durante o desenvolvimento da álgebra e da matemática em si, houve várias contribuições de diversos intelectuais, como os trabalhos de Descartes, Leibniz, Newton, etc. Por exemplo, temos o trabalho do matemático René Descartes (1596 - 1650), o qual foi responsável pela aceitação da raiz quadrada de número negativo como resultado de uma equação algébrica, bem como o Teorema Fundamental da Álgebra, que foi enunciado por Jean Le Rond d'Alembert (1717 - 1783), e demonstrado efetivamente por Carl Friedrich Gauss (1777 - 1855) em sua tese de doutorado.

Houve os outros matemáticos como Niels Abel e Évariste Galois, que desenvolveram importantes teorias relacionadas a álgebra, sendo que Évariste Galois mesmo que tenha morrido novo, antes de completar vinte um anos, é considerado um gênio que desenvolveu um trabalho que o qualifica como principal precursor da álgebra abstrata.

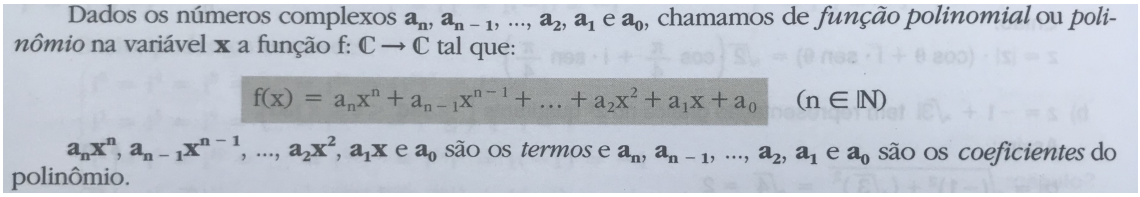
O conceito de polinômio se encontra no âmbito da álgebra, foi Stevin (1548 - 1620) que deu os primeiros passos para a introdução desse conceito, através de seu livro *L' Arithmetique*, que foi publicado em 1585, no qual introduz uma notação exponencial semelhante para denotar as várias potências de uma variável. Ele utilizou os símbolos ⓪, ①, ②, etc., para representar as potências de x, ou seja, para escrever o polinômio $3x^3 + 2x^2 + 5x + 4$, usando sua notação teríamos:

$$3\,③ \;+\; 2\,② \;+\; 5\,① \;+\; 4\,⓪$$

Stevin denomina estas expressões de multinômios e mostra como operar com eles. Além disso, ele observa que as operações com multinômios tem muitas propriedades em comum com as operações entre números aritméticos. O interessante é que vemos

que ele trata seus multinômios como novos objetos matemáticos e estuda as operações entre eles.

O estudo dos polinômios inicia-se no Ensino Médio, apresentaremos na Figura 1 a definição de polinômio que é ensinada no Ensino Médio, a qual foi obtida em [13] p. 358.


Dados os números complexos $\mathbf{a_n}$, $\mathbf{a_{n-1}}$, ..., $\mathbf{a_2}$, $\mathbf{a_1}$ e $\mathbf{a_0}$, chamamos de *função polinomial* ou *polinômio* na variável $\mathbf{x}$ a função $f: \mathbb{C} \to \mathbb{C}$ tal que:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 \quad (n \in \mathbb{N})$$

$\mathbf{a_n x^n}$, $\mathbf{a_{n-1}x^{n-1}}$, ..., $\mathbf{a_2 x^2}$, $\mathbf{a_1 x}$ e $\mathbf{a_0}$ são os *termos* e $\mathbf{a_n}$, $\mathbf{a_{n-1}}$, ..., $\mathbf{a_2}$, $\mathbf{a_1}$ e $\mathbf{a_0}$ são os *coeficientes* do polinômio.

Figura 1: *Definição de polinômio no Ensino Médio*

Fonte: [13] p. 358, 2003.

Observamos primeiramente, que a definição da Figura 1 usa o conceito de função para definir polinômio, mas existe uma diferença entre esses conceitos, pois, polinômio é uma expressão algébrica e a função é uma relação $f : X \to Y$ que, a cada elemento $x \in X$, associa um e somente um elemento $y \in Y$. Essa definição que usa o símbolo x traz uma certa dificuldade para os alunos do Ensino Médio pelo sua ambiguidade, pois, as vezes x representa um número específico, como por exemplo na equação $6x - 3 = 27$. Outras vezes x pode assumir qualquer valor do domínio de uma função, e em outros casos é apenas um símbolo que é manipulado algebricamente, por exemplo $(x + 2)(x + 5) = x^2 + 7x + 10$.

Um dos objetivos desse trabalho é apresentar uma definição rigorosa de polinômio que remove a ambiguidade do símbolo x, a qual utiliza um conceito simples que é o da sequência, assim possibilitando o seu estudo no Ensino Médio. Portanto, permitindo compreender melhor os polinômios e suas propriedades. Outro objetivo é proporcionar ao professor do Ensino Médio um aprofundamento no estudo da álgebra abstrata, possibilitando obter ferramentas para o planejamento de suas atividades buscando diminuir o distanciamento do Ensino Médio do Ensino Superior. Pois, é verifica uma falta de conexão de conceitos algébricos entre esses níveis do Ensino.

> Deveria ter-se uma conexão entre conteúdo específico e conteúdos pedagógicos. Assim os conteúdos algébricos, que de uma forma ou de outra o professor se depara no seu trabalho na Educação Básica, são vistos de forma isolada e aparecem em muitas das disciplinas no curso de Matemática. É

> justamente nestes tópicos algébricos que se verifica um distanciamento maior entre a formação específica e a formação pedagógica. ([1], p. 5).

De acordo com os Parâmetros Curriculares Nacionais (PCNs), o ensino da matemática no Ensino Médio pode ser sistematizado nos três seguintes eixos ou temas estruturadores, desenvolvidos de forma concomitante nas três séries do ensino médio:

1. Álgebra: números e funções;
2. Geometria e medidas;
3. Análise de dados.

Como o ensino de polinômios está no eixo da álgebra, faremos uma breve análise do que diz os Parâmetros Curriculares Nacionais do Ensino Médio da Matemática sobre o eixo da álgebra.

> O primeiro tema ou eixo estruturador, Álgebra, na vivência cotidiana se apresenta com enorme importância enquanto linguagem, como na variedade de gráficos presentes diariamente nos noticiários e jornais, e também enquanto instrumento de cálculos de natureza financeira e prática, em geral. [...] o estudo das funções permite ao aluno adquirir a linguagem algébrica como a linguagem das ciências, necessária para expressar a relação entre grandezas e modelar situações-problema, construindo modelos descritivos de fenômenos e permitindo várias conexões dentro e fora da própria matemática. Assim, a ênfase do estudo das diferentes funções deve estar no conceito de função e em suas propriedades em relação às operações, na interpretação de seus gráficos e nas aplicações dessas funções. [...] com relação à álgebra, há ainda o estudo de equações polinomiais e de sistemas lineares. Esses dois conteúdos devem receber um tratamento que enfatize sua importância cultural, isto é, estender os conhecimentos que os alunos possuem sobre a resolução de equações de primeiro e segundo graus e sobre a resolução de sistemas de duas equações e duas incógnitas para sistemas lineares 3 por 3, aplicando esse estudo à resolução de problemas simples de outras áreas do conhecimento. Uma abordagem mais qualitativa e profunda deve ser feita dentro da parte flexível do currículo, como opção específica de cada escola ([4], p. 120-122).

Observa-se que, conforme os parâmetros curriculares nacionais o tema álgebra tem uma enorme importância para a vivência cotidiana, e apesar dessa importância os autores dos PCNs, considera que não é importante que estude de forma qualitativa e profunda sobre os polinômios, equações polinomiais e função polinomial, pois esse

conteúdo está dentro da parte flexível do currículo. Mas são conteúdos importantes para a aprendizagem e desenvolvimento de outros contéudos do Ensino Superior.

Os resultados obtidos nesse trabalho resultaram em sugestões de aplicações em sala de aula do Ensino Médio muito interessantes, as quais possam despertar o interesse dos alunos pela álgebra, não foram aplicadas efetivamente, por falta de oportunidade, por não atuar como professor.

Mais especificamente, este trabalho está organizado como se segue:

No Capítulo 1 caracterizamos as estruturas algébricas denominadas de anel e de corpo, e ainda traremos algumas propriedades dessas estruturas.

No Capítulo 2 exploramos o conceito de polinômio utilizando uma abordagem diferente da definição da Figura 1 e estudaremos a estrutura algébrica dos anéis de polinômios. Trataremos do conceito de grau de um polinômio, do algoritmo da divisão de polinômios e da divisibilidade de polinômios. Dentro da divisibilidade de polinômios estudaremos os conceitos de máximo divisor comum e mínimo múltiplo comum de dois polinômios.

No Capítulo 3 estudaremos o conceito de irredutibilidade de um polinômio em um anel de polinômios com coeficientes em um corpo. Definiremos o conceito da raiz de um polinômio e estudaremos a relação entre os conceitos de raiz e irredutibilidade de um polinômio. Mostraremos que existe uma fatoração única dos polinômios em polinômios irredutíveis. Além disso, estudaremos os diferentes critérios que podem ser utilizados para determinar se um dado polinômio com coeficientes em $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ é ou não irredutível em relação aos anéis de polinômios $\mathbb{Q}[X], \mathbb{R}[X]$ e $\mathbb{R}[X]$.

No Capítulo 4 abordaremos algumas sugestões de aplicações dos resultados obtidos neste trabalho na sala de aula do Ensino Médio.

Nas Considerações finais faremos um reflexão sobre o que foi abordado e desenvolvido neste trabalho.

Capítulo 1

Anéis e Corpos

Neste capítulo, estudaremos duas estruturas algébricas fundamentais, anéis e corpos, que serão de suma importância para o desenvolvimento deste trabalho.

Contudo, restringimos o nosso estudo, somente aos conceitos e propriedades dessas estruturas que serão necessárias para o desenvolvimento deste trabalho.

1.1 Definições e propriedades de Anéis

Mencionaremos aqui, as principais definições e propriedades de Anéis, necessárias ao desenvolvimento deste trabalho. Nesta seção teremos como referências as obras [10], [9], [2] e [6].

Definição 1.1.1. *Um Anel* $(A, +, \cdot)$ *é um conjunto não vazio* A*, contendo duas operações binárias (geralmente denotadas por adição* $(+)$ *e multiplicação* $(\cdot)$ *) que satisfazem as seguintes propriedades:*

A_1 **(Fechamento da adição)** *Se* $a \in A$ *e* $b \in A$*, então* $a + b \in A$*.*

A_2 **(Associatividade da adição)** *Para todos* $a, b, c \in A$*, temos* $(a+b)+c = a+(b+c)$*.*

A_3 **(Comutatividade da adição)** *Para todos* $a, b \in A$*, temos* $a + b = b + a$*.*

A_4 **(Existência do elemento neutro da adição)** *Existe um elemento* $0_A \in A$*, tal que* $a + 0_A = a = 0_A + a$*, para todo* $a \in A$*.*

A_5 **(Existência do elemento simétrico da adição)** *Para todo $a \in A$, a equação $a + x = 0_A$ tem uma solução em A (denotada por $-a$).*

M_1 **(Fechamento da multiplicação)** *Se $a \in A$ e $b \in A$, então $a \cdot b \in A$.*

M_2 **(Associatividade da multiplicação)** *Para todos $a, b, c \in A$, temos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*

AM **(Distributividade)** *Para todos $a, b, c \in A$, temos $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.*

Exemplo 1.1.2. *O conjunto dos números inteiros $\mathbb{Z}$ com as operações de adição e multiplicação usual é um exemplo de anel, mas o conjunto dos números naturais $\mathbb{N}$ com as operações de adição e multiplicação usual não é um anel, pois não tem a propriedade A_5.*

Um anel tem as propriedades mínimas para que uma estrutura algébrica se assemelhe ao conjunto dos inteiros $\mathbb{Z}$, mas $\mathbb{Z}$ tem algumas propriedades especiais, assim temos estruturas algébricas que possuem propriedades especiais.

Definição 1.1.3. *Anel comutativo é o anel $(A, +, \cdot)$ que possui a seguinte propriedade:*

M_3 **(Comutatividade da multiplicação)** *Para todos $a, b \in A$, temos $a \cdot b = b \cdot a$.*

Definição 1.1.4. *Anel com identidade é o anel $(A, +, \cdot)$ que contém um elemento 1_A que possui a seguinte propriedade:*

M_4 **(Existência do elemento neutro da multiplicação)** *Existe um elemento $1_A \in A$, tal que $a \cdot 1_A = a = 1_A \cdot a$, para todo $a \in A$.*

Exemplo 1.1.5. *Os anéis $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$, onde $+$ e $\cdot$ representam as operações usuais da adição e multiplicação de $\mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$, são comutativos com identidade, tendo 1 como elemento neutro da multiplicação.*

Definição 1.1.6. *Um elemento a em um anel $(A, +, \cdot)$ com identidade, é chamado de unidade se existe $u \in (A, +, \cdot)$ tal que $a \cdot u = 1_A = u \cdot a$.*

Exemplo 1.1.7. *(Anel das classes residuais módulo m) Seja $m > 1$ um número inteiro, a relação de congruência módulo m, é definida da seguinte maneira: dados $a, b \in \mathbb{Z}$*

$$a \equiv b \ mod\ m \text{ se, e somente se, } a - b \text{ é múltiplo de } m.$$

Sejam a e m inteiros com $m > 1$, é definida a classe de congruência de a módulo m, que será denotada por $[a]$, como o conjunto de todos os números inteiros que são congruentes a módulo m, tal que:

$$[a] = \{b \mid b \in \mathbb{Z} \text{ e } b \equiv a \bmod m\}.$$

O conjunto de todas as classes residuais módulo m será denotado por $\mathbb{Z}_m$. Portanto,

$$\mathbb{Z}_m = \{[0], [1], \cdots, [m-1]\}.$$

No conjunto de $\mathbb{Z}_m$ são definidas as seguintes operações:

$$\text{adição } [a] \oplus [b] = [a + b]$$
$$\text{Multiplicação } [a] \odot [b] = [a \cdot b]$$

Sendo que $+$ e $\cdot$ denota respectivamente a adição e multiplicação usuais de $\mathbb{Z}$.

A Tabela 1.1, mostra como fica as operações de adição e multiplicação nas classes residuais de $\mathbb{Z}_4$.

Tabela 1.1: Tabela da adição e multiplicação em $\mathbb{Z}_4$

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\odot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

$\mathbb{Z}_m$ com as operações de adição $\oplus$ e multiplicação $\odot$ satisfazem as propriedades da definição de anel, além disso podemos observar que:

$$[a] \odot [b] = [a \cdot b] \overset{(1)}{=} [b \cdot a] = [b] \odot [a]$$
$$[a] \odot [1] = [a \cdot 1] \overset{(2)}{=} [a] \overset{(3)}{=} [1 \cdot a] = [1] \odot [a]$$

Em (1) aplicamos comutatividade do anel $(\mathbb{Z}, +, \cdot)$ e em (2) e (3) a propriedade do elemento neutro da multiplicação do anel $(\mathbb{Z}, +, \cdot)$, assim a multiplicação $\odot$ é comutativa e tem o elemento neutro $[1]$. Portanto o anel $(\mathbb{Z}_m, \oplus, \odot)$ é comutativo com identidade.

Exemplo 1.1.8. *Seja $M_{2\times2}(\mathbb{R})$ o conjunto de todas as matrizes 2×2 sobre os números reais, ou seja, as matrizes da forma:*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \textit{com } a, b, c \textit{ e } d \textit{ números reais.}$$

Duas matrizes são iguais, desde que as entradas nas posições correspondentes sejam iguais, ou seja,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} r & s \\ t & u \end{bmatrix} \textit{ se, e somente se, } a = r,\ b = s,\ c = t \textit{ e } d = u.$$

No conjunto $M_{2\times 2}(\mathbb{R})$ é definida a operação de adição de matrizes da seguinte forma:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a + a' & b + b' \\ c + c' & d + d' \end{bmatrix}$$

Por exemplo:

$$\begin{bmatrix} 5 & -3 \\ 4 & 1 \end{bmatrix} + \begin{bmatrix} -2 & 6 \\ -9 & 0 \end{bmatrix} = \begin{bmatrix} 5 + (-2) & (-3) + 6 \\ 4 + (-9) & 1 + 0 \end{bmatrix} = \begin{bmatrix} 3 & 3 \\ -5 & 1 \end{bmatrix}$$

No conjunto $M_{2\times 2}(\mathbb{R})$ é definida a operação de multiplicação de matrizes da seguinte forma:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a \cdot a' + b \cdot c' & a \cdot b' + b \cdot d' \\ c \cdot a' + d \cdot c' & c \cdot b' + d \cdot d' \end{bmatrix}$$

Por exemplo:

$$\begin{bmatrix} 5 & -7 \\ 4 & 2 \end{bmatrix} \cdot \begin{bmatrix} -8 & 5 \\ -9 & 0 \end{bmatrix} = \begin{bmatrix} 5 \cdot (-8) + (-7) \cdot (-9) & 5 \cdot 5 + (-7) \cdot 0 \\ 4 \cdot (-8) + 2 \cdot (-9) & 4 \cdot 5 + 2 \cdot 0 \end{bmatrix} = \begin{bmatrix} 23 & 25 \\ -50 & 20 \end{bmatrix}$$

$M_{2\times 2}(\mathbb{R})$ com as operações de adição e multiplicação de matrizes satisfazem as propriedades da definição de anel, sendo o elemento neutro da adição a matriz nula:

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Além disso, para toda matriz pertencente ao conjunto $M_{2\times2}(\mathbb{R})$ *existe uma matriz simétrica da adição, que é a matriz* $X = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$, *pois é solução da equação:*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + X = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Em relação a multiplicação de matrizes, se invertemos a ordem dos fatores, podemos encontrar uma resposta diferente, por exemplo:

$$\begin{bmatrix} -2 & 6 \\ -9 & 0 \end{bmatrix} \cdot \begin{bmatrix} 5 & -3 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} (-2)\cdot 5 + 6\cdot 4 & (-2)\cdot(-3) + 6\cdot 1 \\ (-9)\cdot 5 + 0\cdot 4 & (-9)\cdot(-3) + 0\cdot 1 \end{bmatrix} = \begin{bmatrix} 14 & 12 \\ -45 & 27 \end{bmatrix}$$

$$\begin{bmatrix} 5 & -3 \\ 4 & 1 \end{bmatrix} \cdot \begin{bmatrix} -2 & 6 \\ -9 & 0 \end{bmatrix} = \begin{bmatrix} 5\cdot(-2) + (-3)\cdot(-9) & 5\cdot 6 + (-3)\cdot 0 \\ 4\cdot(-2) + 1\cdot(-9) & 4\cdot 6 + 1\cdot 0 \end{bmatrix} = \begin{bmatrix} 17 & 30 \\ -17 & 24 \end{bmatrix}$$

Portanto a multiplicação de matrizes não é comutativa, mas matriz identidade $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, *é o elemento neutro da multiplicação, pois para toda matriz de* $M_{2\times2}(\mathbb{R})$ *temos o seguinte:*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a\cdot 1 + b\cdot 0 & a\cdot 0 + b\cdot 1 \\ c\cdot 1 + d\cdot 0 & c\cdot 0 + d\cdot 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1\cdot a + 0\cdot c & 1\cdot b + 0\cdot d \\ 0\cdot a + 1\cdot c & 0\cdot b + 1\cdot d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Portanto $M_{2\times2}(\mathbb{R})$ *com as operações de adição e multiplicação de matrizes é um anel com identidade. De modo geral,* $M_{n\times n}(\mathbb{R})$ *o conjunto de todas as matrizes* $n \times n$ *sobre os números reais, com a operações de adição e multiplicação de matrizes usual é um anel com identidade.*

Observamos que a multiplicação de matrizes diferentes da matriz nula, pode ser igual a matriz nula, por exemplo:

$$\begin{bmatrix} 8 & 12 \\ 4 & 6 \end{bmatrix} \cdot \begin{bmatrix} -6 & -18 \\ 4 & 12 \end{bmatrix} = \begin{bmatrix} 8\cdot(-6)+12\cdot 4 & 8\cdot(-18)+12\cdot 12 \\ 4\cdot(-6)+6\cdot 4 & 4\cdot(-18)+6\cdot 12 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Na Tabela 1.1 temos que $[2] \odot [2] = [0]$, ou seja, em $(\mathbb{Z}_4, \oplus, \odot)$ temos que a multiplicação de elementos diferentes de zero, pode ser igual a zero e bem como no anel $(M_{2\times 2}(\mathbb{R}), +, \cdot)$ a multiplicação de matrizes diferentes da matriz nula, pode ser igual a matriz nula, mas em alguns anéis a multiplicação de elementos diferentes de zero sempre é diferente de zero, por exemplo em $(\mathbb{Z}, +, \cdot)$, assim temos a seguinte definição:

Definição 1.1.9. *Domínio de integridade é um anel comutativo com identidade* $(A, +, \cdot)$ *que satisfaz a seguinte propriedade:*

Para todo $a, b \in A$, *se* $a \neq 0_A$ *e* $b \neq 0_A$ *então* $a \cdot b \neq 0_A$.

Para o anel comutativo com identidade ser um domínio de integridade, é válida a contrapositiva de sua propriedade, ou seja, para todos $a, b \in A$, se $a \cdot b = 0_A$ então $a = 0_A$ ou $b = 0_A$.

Exemplo 1.1.10. *Os anéis* $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ *e* $(\mathbb{R}, +, \cdot)$ *são exemplos de domínio de integridade.*

Definição 1.1.11. *Seja o anel* $(A, +, \cdot)$, *um elemento* $a \in A$, *diferente de* 0_A, *é dito divisor de zero, se existe um elemento* $b \in A$, *também diferente de* 0_A, *tal que* $a \cdot b = 0_A$.

Portanto um domínio de integridade é o anel comutativo com identidade que não possui divisores de zero.

Exemplo 1.1.12. *O anel* $(\mathbb{Z}_2, \oplus, \odot)$ *possuí os seguintes elementos* $[0]$ *e* $[1]$, *sendo* $[0]$ *o elemento neutro da adição, e observamos que* $[1] \odot [1] = [1 \cdot 1] = [1]$, *assim não possui divisores de zero. Portanto, o anel* $(\mathbb{Z}_2, \oplus, \odot)$ *é um domínio de integridade.*

Teorema 1.1.13. *O anel* $(\mathbb{Z}_m, \oplus, \odot)$ *é um domínio de integridade, ou seja, não possui divisores de zero, se, e somente se,* m *é um número primo.*

Demonstração. Suponhamos primeiramente que o anel $(\mathbb{Z}_m, \oplus, \odot)$ é um domínio de integridade, vamos provar por contradição, suponhamos que m não seja um número primo. Então m é composto, ou seja, existem $1 < a, b < m$ tais que $m = a \cdot b$, isso implica que $[0] = [m] = [a \cdot b] = [a] \odot [b]$, com $[a] \neq [0]$ e $[b] \neq [0]$, logo se m não é

primo, então $\mathbb{Z}_m$ possui divisores de zero, ou seja, não é um domínio de integridade. Portanto m é primo.

Reciprocamente, seja m um número primo, vamos provar que se $[a] \odot [b] = [0]$ então $[a]$ ou $[b]$ é igual $[0]$ para todo $[a], [b] \in \mathbb{Z}_m$, ou seja, $\mathbb{Z}_m$ não possui divisores de zero, ou seja, é um domínio de integridade.

De fato, como $[a] \odot [b] = [0]$ então $[a \cdot b] = [0]$, portanto $a \cdot b \equiv 0 \bmod m$, ou seja, $m|a \cdot b$, como m é primo, então pelo Lema de Gauss [7, p. 82] $m|a$ ou $m|b$, portanto $[a] = [0]$ ou $[b] = [0]$. □

Quando fazemos as operações aritméticas em $\mathbb{Z}$ nós usamos muitas propriedades que não consta na definição de anel. Por exemplo a subtração, as leis dos cancelamentos e as várias regras para multiplicação de números negativos. Vamos mostrar que muitas dessas propriedades também valem para qualquer anel.

Teorema 1.1.14. *Para qualquer elemento a pertencente ao anel $(A, +, \cdot)$, a equação $a + x = 0_A$ tem uma única solução.*

Demonstração. Sabemos que a equação $a + x = 0_A$ tem pelo menos uma solução u pela propriedade A_5 (Existência do elemento simétrico da adição) do anel $(A, +, \cdot)$. Se v também é uma solução, então temos que $a + u = 0_A$ e $a + v = 0_A$, assim temos o seguinte:

$$v = 0_A + v = (a + u) + v \overset{(1)}{=} (u + a) + v \overset{(2)}{=} u + (a + v) = u + 0_A = u.$$

Em (1) e (2) aplicamos respectivamente as propriedades da comutatividade e da associatividade da adição. Portanto u é a única solução. □

Pelo Teorema 1.1.14 a equação $a + x = 0_A$ tem uma única solução, a qual denotaremos pelo símbolo $-a$, agora estamos pronto para definir a subtração em um anel, que é definida pela regra:

$$b - a \text{ que significa } b + (-a).$$

Como a adição é comutativa em um anel $(A, +, \cdot)$, então temos o seguinte:

$$-a \text{ é o único elemento do anel } (A, +, \cdot) \text{ tal que:}$$
$$a + (-a) = 0_A = (-a) + a.$$

Teorema 1.1.15. (**Lei do cancelamento da adição**) *Se $a + b = a + c$ em um anel $(A, +, \cdot)$, então $b = c$.*

Demonstração. Fazendo a adição de $-a$ em ambos lados da igualdade $a+b=a+c$ e aplicando a associatividade da adição temos o seguinte:

$$\begin{aligned} -a+(a+b) &= -a+(a+c) \\ (-a+a)+b &= (-a+a)+c \\ 0_A+b &= 0_A+c \\ b &= c \end{aligned}$$

□

Teorema 1.1.16. *Para quaisquer a e b de um anel $(A,+,\cdot)$ temos:*

(1) $a\cdot 0_A = 0_A = 0_A\cdot a$.

(2) $a\cdot(-b) = -a\cdot b$ *ou* $(-a)\cdot b = -a\cdot b$.

(3) $-(-a) = a$.

(4) $-(a+b) = (-a)+(-b)$.

(5) $-(a-b) = -a+b$.

(6) $(-a)\cdot(-b) = a\cdot b$.

Se o anel $(A,+,\cdot)$ possui identidade, então:

(7) $(-1_A)\cdot a = -a$.

Demonstração. **(1)** Como $0_A+0_A=0_A$ aplicando a distributividade em $a\cdot(0_A+0_A)$ temos o seguinte:

$$a\cdot 0_A + a\cdot 0_A = a\cdot(0_A+0_A) = a\cdot 0_A + 0_A$$

Agora aplicando o Teorema 1.1.15 na primeira e na última parte da equação obtemos $a\cdot 0_A = 0_A$. A prova $0_A\cdot a = 0_A$ é análoga.

(2) Pela definição, $-a\cdot b$ é a única solução da equação $a\cdot b+x=0_A$ e, portanto, qualquer outra solução dessa equação deve ser igual a $-a\cdot b$. Mas $x=a\cdot(-b)$ também é uma solução da equação, pois, aplicando a distributividade e a Propriedade **(1)** temos o seguinte:

$$a\cdot b + a\cdot(-b) = a\cdot((b)+(-b)) = a\cdot(0_A) = 0_A$$

Portanto, $a \cdot (-b) = -a \cdot b$. A prova $(-a) \cdot b = -a \cdot b$ é análoga.

(3) Pela definição, $-(-a)$ é a única solução da equação $(-a) + x = 0_A$. Mas a é solução desta equação, pois $(-a) + a = 0_A$. Portanto, $-(-a) = a$ pela unicidade da solução da equação $(-a) + x = 0_A$.

(4) Pela definição, $-(a + b)$ é a única solução da equação $(a + b) + x = 0_A$. Mas $(-a) + (-b)$ também é solução equação, pois adição é comutativa, assim temos o seguinte:

$$(a + b) + ((-a) + (-b)) = a + (-a) + b + (-b) = 0_A + 0_A = 0_A.$$

Portanto, $-(a+b) = (-a)+(-b)$ pela unicidade da solução da equação $(a+b)+x = 0_A$.

(5) Pela definição de subtração e aplicando as Propriedades **(4)** e **(3)** temos o seguinte:

$$-(a - b) = -(a + (-b)) = (-a) + (-(-b)) = -a + b.$$

(6) Pela segunda equação da Propriedade **(2)** e com $-b$ no lugar de b temos o seguinte:

$$(-a) \cdot (-b) = -(a \cdot (-b)).$$

Agora pela primeira equação da Propriedade **(2)** e aplicando a Propriedade **(3)** temos o seguinte:

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-a \cdot b) = a \cdot b.$$

(7) Aplicando a Propriedade **(2)** temos o seguinte:

$$(-1_A) \cdot a = -(1_A \cdot a) = -(a) = -a.$$

□

Definição 1.1.17. *O conjunto dos números inteiros não negativos* $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \ldots\}$ *é denominado o conjunto dos números naturais.*

Definição 1.1.18. *Seja* $(A, +, \cdot)$ *um anel. Dado* $a \in A$ *e* $n \in \mathbb{N}$, $n \neq 0$, *definimos:*

$$\begin{aligned} a^1 &= a; \\ a^{n+1} &= a^n \cdot a,\ n \geq 1. \end{aligned}$$

Quando $(A, +, \cdot)$ *é um anel com identidade também definimos* $a^0 = 1_A$.

Teorema 1.1.19. *Sejam $(A, +, \cdot)$ um anel, $a \in A$ e $m, n \in \mathbb{N}\backslash\{0\}$. Então:*

(1) $a^m \cdot a^n = a^{m+n}$;

(2) $(a^m)^n = a^{m \cdot n}$.

Demonstração. Provaremos utilizando o princípio da indução matemática sobre n.

(1) Para $n = 1$ temos pela Definição 1.1.18, que $a^m \cdot a^1 = a^m \cdot a = a^{m+1}$. Portanto, a propriedade vale para $n = 1$.

Agora, suponha que vale para $n \geq 1$, ou seja, $a^m \cdot a^n = a^{m+n}$, vamos provar que vale para $n + 1$:

$$a^m \cdot a^{n+1} = a^m \cdot (a^n \cdot a^1) = (a^m \cdot a^n) \cdot a = a^{m+n} \cdot a = a^{(m+n)+1} = a^{m+(n+1)}.$$

Portanto, pelo princípio da indução matemática a propriedade é válida para todo $n \in \mathbb{N}\backslash\{0\}$.

(2) Para $n = 1$ temos pela Definição 1.1.18, que $(a^m)^1 = a^m = a^{m \cdot 1}$. Portanto, a propriedade vale para $n = 1$.

Agora, suponha que vale para $n \geq 1$, ou seja, $(a^m)^n = a^{m \cdot n}$, vamos provar que vale para $n + 1$:

$$(a^m)^{n+1} = (a^m)^n \cdot a^m = a^{m \cdot n} \cdot a^m \overset{(1)}{=} a^{(m \cdot n)+m} = a^{m \cdot (n+1)}.$$

Em (1) utilizamos a propriedade **(1)** provada anteriormente. Portanto, pelo princípio da indução matemática a propriedade é válida para todo $n \in \mathbb{N}\backslash\{0\}$.

□

Corolário 1.1.20. *Sejam $(A, +, \cdot)$ um anel com identidade, $a \in A$ e $m, n \in \mathbb{N}$. Então:*

(1) $a^m \cdot a^n = a^{m+n}$;

(2) $(a^m)^n = a^{m \cdot n}$.

Demonstração. Basta nas demonstrações do Teorema 1.1.19, acrescentar o caso base $n = 0$:

(1) $a^m \cdot a^0 = a^m \cdot 1_A = a^m = a^{m+0}$.

(2) $(a^m)^0 = 1_A = a^0 = a^{m \cdot 0}$.

□

Teorema 1.1.21. (**Lei do cancelamento da multiplicação**) *Seja o anel* $(A, +, \cdot)$ *um domínio de integridade, e* $a, b, c \in A$ *com* $a \neq 0_A$. *Se* $a \cdot b = a \cdot c$, *então* $b = c$.

Demonstração. Provaremos utilizando as propriedades de anéis e a definição de domínio de integridade, como $a \cdot b = a \cdot c$, pela propriedade A_5 (Existência do elemento simétrico da adiçao) temos $a \cdot b - a \cdot c = a \cdot c - a \cdot c = 0_A$, pela propriedade AM (Distributividade) temos $a \cdot (b - c) = 0_A$, como $a \neq 0_A$ e $(A, +, \cdot)$ é um domínio de integridade, portanto $b - c = 0_A$, novamente pela propriedade A_5, temos $b + 0_A = b - c + c = 0_A + c$, pela propriedade A_4 temos $b = c$. □

Definição 1.1.22. *Um anel* $(A, +, \cdot)$ *que é um domínio de integridade é dito um anel euclideano, se para todo* $a \neq 0_A \in A$, *é definida uma função* $f : A^* \to \mathbb{N}$, *onde* $A^* = A \backslash \{0_A\}$, *tal que:*

i) *Para todos* $a, b \neq 0_A \in A$, *então* $f(a) \leq f(a \cdot b)$;

ii) *Para todos* $a, b \neq 0_A \in A$, *existem* $q, r \in A$ *tais que* $a = q \cdot b + r$, *onde* $r = 0_A$ *ou* $f(r) < f(b)$.

Exemplo 1.1.23. *O anel dos números inteiros* $(\mathbb{Z}, +, \cdot)$ *é um anel euclideano, onde a função* $f : \mathbb{Z} \to \mathbb{Z}$, *tal que* $f(x) = \begin{cases} x, & se\ x \geq 0 \\ -x, & se\ x < 0 \end{cases}$, *a qual faz corresponder um número inteiro com seu valor absoluto é a função requerida pela definição de anel euclideano.*

Definição 1.1.24. *Seja* B *um subconjunto não vazio de um anel* $(A, +, \cdot)$. *Se* B *com as operações de adição* $+$ *e multiplicação* $\cdot$ *do anel* $(A, +, \cdot)$ *for um anel, dizemos que* $(B, +, \cdot)$ *é um subanel do anel* $(A, +, \cdot)$.

Teorema 1.1.25. *Seja* $(A, +, \cdot)$ *um anel e um subconjunto* B *de* $(A, +, \cdot)$ *tal que:*

i) B *é fechado com relação a adição, ou seja, se* $a, b \in B$, *então* $a + b \in B$;

ii) B *é fechado com relação a multiplicação, ou seja, se* $a, b \in B$, *então* $a \cdot b \in B$;

iii) $0_A \in B$;

iv) *Se* $a \in B$, *então a solução da equação* $a + x = 0_A$ *está em* B.

Então B *é um subanel de* $(A, +, \cdot)$.

Demonstração. Sendo B um subconjunto não vazio (por **iii**), então as propriedades A_2 (Associatividade da adição), A_3 (Comutatividade da adição), M_2 (Associatividade da multiplicação) e AM (Distributividade) do anel $(A, +, \cdot)$ valem para os elementos de $(B, +, \cdot)$. Assim, para que $(B, +, \cdot)$ seja um anel basta que possua as outras propriedades da Definição 1.1.1, ou seja, A_1 (Fechamento da adição), M_1 (Fechamento da multiplicação), A_4 (Existência do elemento neutro da adição) e A_5 (Existência do elemento simétrico da adição), as quais são respectivamente as propriedades dos itens **i**, **ii**, **iii** e **iv**. Portanto, $(B, +, \cdot)$ é um subanel de $(A, +, \cdot)$. □

O próximo teorema nós mostra que a subtração fornece um método mais rápido do que o Teorema 1.1.25 para mostrar que um subconjunto de um anel é na verdade um subanel.

Teorema 1.1.26. *Seja $(A, +, \cdot)$ um anel e um subconjunto não vazio B de $(A, +, \cdot)$ tal que:*

(1) *B é fechado com relação a subtração, ou seja, $a, b \in B$, então $a - b \in B$;*

(2) *B é fechado com relação a multiplicação, ou seja, se $a, b \in B$, então $a \cdot b \in B$.*

Então B é um subanel de $(A, +, \cdot)$.

Demonstração. Mostraremos que B satisfaz as condições **(i)-(iv)** do Teorema 1.1.25 e, portanto é um subanel. As condições serão provadas nesta ordem: **(ii), (iii), (iv) e (i)**.

(ii) A hipótese **(2)** é idêntica à condição **(ii)** do Teorema 1.1.25. Assim, B satisfaz a condição **(ii)** do Teorema 1.1.25.

(iii) Uma vez que B é um subconjunto não vazio de $(A, +, \cdot)$, então existe um elemento $c \in B$. Aplicando **(1)** com $a = c$ e $b = c$, temos que $c - c = 0_A$ está em B. Portanto, B satisfaz a condição **(iii)** do Teorema 1.1.25.

(iv) Se a é qualquer elemento de B, então por **(1)**, $0_A - a = -a$ também está em B. Como $-a$ é a solução de $a + x = 0_A$, assim à condição **(iv)** do Teorema 1.1.25 é satisfeita.

(i) Se $a, b \in B$, então $-b$ está em B pela prova de **(iv)**. Por **(1)**, $a - (-b) = a + b$ está em B. Assim, B satisfaz a condição **(i)** do Teorema 1.1.25.

Portanto, B é um subanel de $(A, +, \cdot)$ pelo Teorema 1.1.25.

□

Exemplo 1.1.27. *Seja o anel* $(M_{2\times 2}(\mathbb{R}), +, \cdot)$ *e o subconjunto* S *de todas as matrizes da forma* $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ *com* $a \in \mathbb{R}$*, e usando as operações de adição e multiplicação usuais de matrizes, temos que* S *é fechado com relação a subtração e a multiplicação, pois temos que*

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a - b & 0 \\ 0 & 0 \end{bmatrix} \in S$$

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a \cdot b + 0 \cdot 0 & a \cdot 0 + 0 \cdot 0 \\ 0 \cdot b + 0 \cdot 0 & 0 \cdot 0 + 0 \cdot 0 \end{bmatrix} = \begin{bmatrix} a \cdot b & 0 \\ 0 & 0 \end{bmatrix} \in S$$

Portanto, S *é um subanel de* $(M_{2\times 2}(\mathbb{R}), +, \cdot)$ *pelo Teorema 1.1.26.*

Definição 1.1.28. *Um anel* $(A, +, \cdot)$ *é isomorfo a um anel* $(R, \oplus, \odot)$ *se houver uma função* $f : A \to R$ *tal que:*

i) f *é bijetiva;*

ii) $f(a + b) = f(a) \oplus f(b)$ *e* $f(a \cdot b) = f(a) \odot f(b)$ *para todos* $a, b \in A$*.*

Dois anéis $(A, +, \cdot)$ e $(R, \oplus, \odot)$ isomorfos são do ponto de vista algébrico essencialmente o mesmo anel, exceto que seus elementos e suas operações de adição e de multiplicação são escritos de forma diferentes. Assim, qualquer propriedade do anel $(A, +, \cdot)$ que dependa apenas da sua estrutura de anel permanece válida no anel $(R, \oplus, \odot)$, e vice-versa. Por exemplo, se o anel $(A, +, \cdot)$ é domínio de integridade então o anel $(R, +, \cdot)$ também é um domínio de integridade.

Exemplo 1.1.29. *Seja o anel* $(S, +, \cdot)$ *do Exemplo 1.1.27 e o anel* $(\mathbb{R}, +, \cdot)$*. Então definimos a função* $f : S \to \mathbb{R}$*, tal que* $f\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\right) = a$*, temos que* f *é injetiva, pois, suponhamos que* $f\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\right) = f\left(\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\right)$*, então pela definição de* f

temos que $a = b$, e f é sobrejetiva, porque todo número real a é imagem de f. Portanto f é bijetiva.

Além disso, temos que

$$f\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\right) = f\left(\begin{bmatrix} a+b & 0+0 \\ 0+0 & 0+0 \end{bmatrix}\right)$$

$$= a + b = f\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\right) + f\left(\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\right)$$

e

$$f\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\right) = f\left(\begin{bmatrix} a\cdot b + 0\cdot 0 & a\cdot 0 + 0\cdot 0 \\ 0\cdot b + 0\cdot 0 & 0\cdot 0 + 0\cdot 0 \end{bmatrix}\right)$$

$$= a \cdot b = f\left(\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\right) \cdot f\left(\begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}\right)$$

Portanto, o anel $(S, +, \cdot)$ é isomorfo ao anel $(\mathbb{R}, +, \cdot)$ pela Definição 1.1.28.

Existe muitas funções entre anéis, que não são bijetivas, mas atendem à condição **ii** da Definição 1.1.28. Tais funções recebem um nome especial.

Definição 1.1.30. *Sejam $(A, +, \cdot)$ e $(R, \oplus, \odot)$ anéis. Uma função $f : A \to R$ é considerada um homomorfismo se*

$$f(a + b) = f(a) \oplus f(b) \text{ e } f(a \cdot b) = f(a) \odot f(b) \text{ para todos } a, b \in A.$$

Exemplo 1.1.31. *Seja o anel $(\mathbb{Z}, +, \cdot)$ e o anel $(\mathbb{Z}_6, \oplus, \odot)$. Então definimos a função $f : \mathbb{Z} \to \mathbb{Z}_6$, tal que $f(a) = [a]$. Pela definição das operações de adição e multiplicação em $\mathbb{Z}_6$ temos que*

$$f(a + b) = [a + b] = [a] \oplus [b] = f(a) \oplus f(b)$$

e

$$f(a \cdot b) = [a \cdot b] = [a] \odot [b] = f(a) \odot f(b)$$

Portanto, f é um homomorfismo.

1.2 Definição e propriedades de corpo

Estudaremos uma importante estrutura algébrica para o desenvolvimento desse estudo, que é chamada de corpo. Nesta seção teremos como referências as obras [10] e [2].

Definição 1.2.1. *Corpo é um anel comutativo com identidade* $(A, +, \cdot)$ *que satisfaz a seguinte propriedade:*

M_5 **(Existência do elemento simétrico da multiplicação)** *Para todo* $a \neq 0_A \in A$*, a equação* $a \cdot x = 1_A$*, tem uma solução em* A*. (denotada por* a^{-1} *e é chamado de inverso multiplicativo de* a*)*

Exemplo 1.2.2. *Os anéis* $(\mathbb{Q}, +, \cdot)$ *e* $(\mathbb{R}, +, \cdot)$ *são corpos, pois são anéis comutativos com identidade e todos os números diferentes de zero que pertencem a* $\mathbb{Q}$ *e* $\mathbb{R}$ *possuem inverso multiplicativo.*

Exemplo 1.2.3. *O anel dos números inteiros* $(\mathbb{Z}, +, \cdot)$*, não é um corpo, pois somente os números* 1 *e* -1 *possui inverso multiplicativo.*

Portanto, em um corpo todos os elementos diferente do elemento neutro da adição é uma unidade.

Teorema 1.2.4. *Para qualquer elemento* a *pertencente ao corpo* $(A, +, \cdot)$*, a equação* $a \cdot x = 1_A$ *tem uma única solução.*

Demonstração. Sabemos que a equação $a \cdot x = 1_A$ tem pelo menos uma solução u pela propriedade M_5 (Existência do elemento simétrico da multiplicação) do corpo $(A, +, \cdot)$. Se v também é uma solução, então temos que $a \cdot u = 1_A$ e $a \cdot v = 1_A$, assim temos o seguinte:

$$v = 1_A \cdot v = (a \cdot u) \cdot v \overset{(1)}{=} (u \cdot a) \cdot v \overset{(2)}{=} u \cdot (a \cdot v) = u \cdot 1_A = u.$$

Em (1) e (2) aplicamos respectivamente as propriedades da comutatividade e da associatividade da multiplicação. Portanto u é a única solução. □

Exemplo 1.2.5. *O conjunto dos números complexos* $\mathbb{C}$*, são os números da forma* $a+bi$ *com* $a, b \in \mathbb{R}$ *e* $i^2 = -1$*, sendo que ocorre a igualdade quando:*

$$a + bi = c + di \text{ se, e somente se, } a = c \text{ e } b = d.$$

Podemos mostrar que o conjunto dos números complexos $\mathbb{C}$ com as operações de adição $+$ e multiplicação $\cdot$, definidas da seguinte forma é um anel comutativo com identidade:

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$
$$(a+bi)\cdot(c+di)=(a\cdot c-b\cdot d)+(a\cdot d+b\cdot c)i$$

O corpo $(\mathbb{R},+,\cdot)$ está contido no anel $(\mathbb{C},+,\cdot)$, são os números da forma $a+0i$, ou seja, possui inverso multiplicativo. Para mostrar que $(\mathbb{C},+,\cdot)$ é um corpo, temos que achar uma solução da equação $(a+bi)\cdot x=1$, tal que a solução pertença ao conjunto $\mathbb{C}$, afirmamos que $x=c+di$ é solução, com $c=\dfrac{a}{a^2+b^2}\in\mathbb{R}$ e $d=\dfrac{-b}{a^2+b^2}\in\mathbb{R}$. De fato,

$$(a+bi)\cdot(\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}i)=(a\cdot\frac{a}{a^2+b^2}-b\cdot\frac{-b}{a^2+b^2})+(a.\frac{-b}{a^2+b^2}+b\cdot\frac{a}{a^2+b^2})i$$
$$=1+0i=1$$

Portanto, $(\mathbb{C},+,\cdot)$ é um corpo.

Teorema 1.2.6. *Um corpo $(F,+,\cdot)$ é um domínio de integridade.*

Demonstração. Como um corpo é uma anel comutativo com identidade, por definição, sejam $a,b\in F$, então devemos mostrar que se $a\cdot b=0_F$, então $a=0_F$ ou $b=0_F$.

Suponhamos que $a\cdot b=0_F$, se $b=0_F$ então não temos nada a provar, se $b\neq 0_F$, como $(F,+,\cdot)$ é um corpo, então b possui inverso multiplicativo, ou seja, $b\cdot b^{-1}=1_F$, assim temos:

$$a=a\cdot 1_F=a\cdot(b\cdot b^{-1})=(a\cdot b)\cdot b^{-1}=0_F\cdot b^{-1}=0_F.$$

Em todo o caso, $a=0_F$ ou $b=0_F$. Portanto $(F,+,\cdot)$ é um domínio de integridade. □

No entanto, a recíproca nem sempre é verdadeira, por exemplo o anel dos números inteiros $(\mathbb{Z},+,\cdot)$ é um domínio de integridade mais não é um corpo, mas quando o domínio de integridade é finito a recíproca vale. É exatamente isso que diz o Teorema 1.2.7.

Teorema 1.2.7. *Todo domínio de integridade finito $(D,+,\cdot)$ é um corpo.*

Demonstração. Como $(D, +, \cdot)$ é um anel comutativo com identidade, precisamos somente mostrar que para cada $a \neq 0_D$ com $a \in D$, a equação $a \cdot x = 1_D$ tem solução em D, sejam $a_1, a_2, a_3, \cdots, a_n$ os elementos distintos de D e suponha $a_i \neq 0_D$, para mostrar que $a_i \cdot x = 1_D$ tem solução em D, considere a multiplicação de a_i por todos elementos de D, ou seja, $a_i \cdot a_1, a_i \cdot a_2, a_i \cdot a_3, \cdots, a_i \cdot a_n$, se $a_r \neq a_s$ então $a_i \cdot a_r \neq a_i \cdot a_s$, pois se $a_i \cdot a_r = a_i \cdot a_s$ implicaria pelo Teorema 1.1.21 que $a_r = a_s$. Portanto, pelo fechamento da multiplicação, $a_i \cdot a_1, a_i \cdot a_2, a_i \cdot a_3, \cdots, a_i \cdot a_n$ são n elementos distintos de D, mas D também tem exatamente n elementos, assim $a_i \cdot a_1, a_i \cdot a_2, a_i \cdot a_3, \cdots, a_i \cdot a_n$ representa em alguma ordem todos elementos de D, em particular, existe um j, tal que $a_i \cdot a_j = 1_D$ Portanto, a equação $a \cdot x = 1_A$ tem solução para todo $a \neq 0_D \in D$, então $(D, +, \cdot)$ é um corpo. □

Teorema 1.2.8. *O anel $(\mathbb{Z}_p, \oplus, \odot)$ é um corpo, se, e somente se, p é um número primo.*

Demonstração. Suponhamos primeiramente que $(\mathbb{Z}_p, \oplus, \odot)$ é um corpo, então pelo Teorema 1.2.6, é um domínio de integridade, e pelo Teorema 1.1.13, p é um número primo.

Reciprocamente, se p é um número primo, então pelo Teorema 1.1.13, $(\mathbb{Z}_p, \oplus, \odot)$ é um domínio de integridade, mas como $\mathbb{Z}_p$ é um conjunto com p elementos, ou seja, $(\mathbb{Z}_p, \oplus, \odot)$ é um domínio de integridade finito, portanto pelo Teorema 1.2.7 é um corpo. □

Capítulo 2

Anéis de Polinômios

Neste capítulo, estudaremos os anéis de polinômios. Abordaremos algumas de suas propriedades fundamentais, como o grau, a divisão e as propriedades da divisibilidade de polinômios.

2.1 Polinômios

Nesta seção teremos como referências as obras [10], [6], [2], [7] e [9].

Para definição de polinômio usaremos o conceito de sequência sobre o anel $(A, +, \cdot)$, que é uma função $f : \mathbb{N} \to A$, ou seja, que associa um elemento $n \in \mathbb{N}$ com um elemento de $a \in A$. Sendo que $f(n)$ será denotado por a_n.

Definição 2.1.1. *Um polinômio com coeficientes no anel $(A, +, \cdot)$ é uma sequência infinita:*

$$(a_0, a_1, a_2, a_3, \ldots)$$

com $a_i \in A$, tal que a quantidade de elementos diferentes do elemento neutro da adição 0_A é finita, ou seja, para algum índice k, $a_i = 0_A$ para todos $i > k$. Os elementos $a_i \in A$ são chamados de coeficientes do polinômio.

Exemplo 2.1.2. *A sequência $(1, 5, \sqrt{2}, \pi, 0, 0, 0, \ldots)$ é um polinômio com coeficientes no corpo dos números reais, mas a sequência $(1, 5, \sqrt{2}, \pi, 1, 1, 1, \ldots)$ não é um polinômio com coeficientes no corpo dos números reais, pois, não existe um índice k, tal que $a_i = 0$, para todos $i > k$.*

Definição 2.1.3. *Os polinômios* $(a_0, a_1, a_2, a_3, \ldots)$ *e* $(b_0, b_1, b_2, b_3, \ldots)$ *com coeficientes no anel* $(A, +, \cdot)$ *são iguais se as sequências são iguais, ou seja,* $a_i = b_i$ *para todo* $i \geq 0$.

Agora definiremos operações no anel de polinômios com coeficientes em A.

Definição 2.1.4. *Adição de polinômios será denotado por* $\bigoplus$ *e definida pela regra:*

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

Observe que a adição é definida somando coeficiente a coeficiente.

Definição 2.1.5. *A Multiplicação de polinômios será denotado por* $\bigodot$ *e definida pela regra:*

$(a_0, a_1, a_2, a_3, \ldots) \bigodot (b_0, b_1, b_2, b_3, \ldots) = (c_0, c_1, c_2, c_3, \ldots)$ *onde*

$c_0 = a_0 \cdot b_0$

$c_1 = a_0 \cdot b_1 + a_1 \cdot b_0$

$c_2 = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0$

$c_3 = a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_0$

$\vdots$

$c_n = a_0 \cdot b_n + a_1 \cdot b_{n-1} + a_2 \cdot b_{n-2} + a_3 \cdot b_{n-3} + ... + a_{n-1} \cdot b_1 + a_n \cdot b_0$

$c_n = \sum_{i=0}^{n} a_i \cdot b_{n-i}$ *ou* $\sum_{i+j=n} a_i \cdot b_j$ *com* $i,\ j \geq 0$

Seja P o conjunto dos polinômios com coeficientes no anel $(A, +, \cdot)$ comutativo com identidade 1_A , com as operações de adição $\bigoplus$ e multiplicação $\bigodot$ anteriormente definidas. No Teorema 2.1.6 provaremos que $(P, \bigoplus, \bigodot)$ é um anel comutativo com identidade.

Teorema 2.1.6. *Seja o anel* $(A, +, \cdot)$ *comutativo com identidade* 1_A*, então* $(P, \bigoplus, \bigodot)$ *é um anel comutativo com identidade.*

Demonstração. Vamos mostrar que $(P, \bigoplus, \bigodot)$ satisfaz todas as propriedades da definição de anel, para tanto sejam os polinômios $f = (a_0, a_1, a_2, a_3, \ldots)$, $g = (b_0, b_1, b_2, b_3, \ldots)$ e $h = (c_0, c_1, c_2, c_3, \ldots)$ pertencentes a P:
A_1 (Fechamento da adição), ou seja, $f \bigoplus g \in P$, pela definição da operação de adição

de polinômios, temos que $f \bigoplus g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)$, devemos somente mostrar que existe um índice k, tal que $a_i + b_i = 0_A$ para todos $i > k$, pois $a_i + b_i \in (A, +, \cdot)$, sabemos pela definição de polinômio que existe um índice j, tal que $a_i = 0_A$, para todos $i > j$ e um índice l, tal que $b_i = 0_A$, para todos $i > l$, se tomamos $k = \max\{j, l\}$, teremos $a_i + b_i = 0_A + 0_A = 0_A$, para todos $i > k$.
A_2 (Associatividade da adição), ou seja, $(f \bigoplus g) \bigoplus h = f \bigoplus (g \bigoplus h)$ temos:

$$\begin{aligned}
(f \bigoplus g) \bigoplus h &= ((a_0, a_1, a_2, a_3, \ldots) \bigoplus (b_0, b_1, b_2, b_3, \ldots)) \bigoplus (c_0, c_1, c_2, c_3, \ldots) \\
&= (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots) \bigoplus (c_0, c_1, c_2, c_3, \ldots) \\
&= ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, (a_2 + b_2) + c_2, (a_3 + b_3) + c_3, \ldots) \quad (1) \\
&= (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), a_2 + (b_2 + c_2), a_3 + (b_3 + c_3), v) \\
&= (a_0, a_1, a_2, a_3, \ldots) \bigoplus ((b_0, b_1, b_2, b_3, \ldots) \bigoplus (c_0, c_1, c_2, c_3, \ldots)) \\
&= f \bigoplus (g \bigoplus h).
\end{aligned}$$

Em (1) aplicamos a associatividade da adição do anel $(A, +, \cdot)$.
A_3 (Comutatividade da adição), ou seja, $f \bigoplus g = g \bigoplus f$ temos :

$$\begin{aligned}
f \bigoplus g &= (a_0, a_1, a_2, a_3, \ldots) \bigoplus (b_0, b_1, b_2, b_3, ..) \\
&= (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots) \quad (2) \\
&= (b_0 + a_0, b_1 + a_1, b_2 + a_2, b_3 + a_3, \ldots) \\
&= (b_0, b_1, b_2, b_3, ..) \bigoplus (a_0, a_1, b_2, b_3, \ldots) \\
&= g \bigoplus f.
\end{aligned}$$

Em (2) aplicamos a comutatividade da adição do anel $(A, +, \cdot)$.
A_4 (Existência do elemento neutro da adição), ou seja, existe um $e \in P$ tal que

$f \bigoplus e = f = e \bigoplus f$, para todo $f \in P$ tomando $e = (0_A, 0_A, 0_A, 0_A, \ldots)$ temos:

$$\begin{aligned} f \bigoplus e &= (a_0, a_1, a_2, a_3, \ldots) \bigoplus (0_A, 0_A, 0_A, 0_A, \ldots) \\ &= (a_0 + 0_A, a_1 + 0_A, a_2 + 0_A, a_3 + 0_A, \ldots) \qquad (3) \\ &= (a_0, a_1, a_2, a_3, \ldots) \\ &= f. \end{aligned}$$

Em (3) aplicamos a propriedade do elemento neutro da adição do anel $(A, +, \cdot)$. Além disso, por A_3 temos que $f \bigoplus e = e \bigoplus f = f$. Assim o polinômio $e = (0_A, 0_A, 0_A, 0_A, \ldots)$ é o elemento neutro da adição, também chamado de polinômio nulo.
A_5 (Existência do elemento simétrico da adição), ou seja, para todo $f \in P$, a equação $f \bigoplus x = e$ tem solução em P, tomando $x = (-a_0, -a_1, -a_2, -a_3, \ldots)$, onde $-a_i$ é o elemento simétrico da adição de a_i para todo $i \geq 0$, já que a_i pertence ao anel $(A, +, \cdot)$, assim temos:

$$\begin{aligned} f \bigoplus x &= (a_0, a_1, a_2, a_3, \ldots) \bigoplus (-a_0, -a_1, -a_2, -a_3, \ldots) \\ &= (a_0 + (-a_0), a_1 + (-a_1), a_2 + (-a_2), a_3 + (a_3), \ldots) \qquad (4) \\ &= (0_A, 0_A, 0_A, 0_A, \ldots) \\ &= e. \end{aligned}$$

Em (4) aplicamos a propriedade do elemento simétrico da adição do anel $(A, +, \cdot)$.
M_1 (Fechamento da Multiplicação), ou seja, $f \bigodot g \in P$. Pela definição da operação de multiplicação de polinômios, temos que $f \bigodot g = (d_0, d_1, d_2, d_3, \ldots)$ onde $d_n = \sum_{i=0}^{n} a_i \cdot b_{n-i}$, devemos somente mostrar que existe um índice k, tal que $d_n = 0_A$ para todos $n > k$, pois $d_n = \sum_{i=0}^{n} a_i \cdot b_{n-i} \in (A, +, \cdot)$. Sabemos pela definição de polinômios que existe um índice j, tal que $a_i = 0_A$, para todo $i > j$ e um índice l, tal que $b_i = 0_A$, para todo $i > l$, se tomamos $k = j+l$, teremos $d_n = a_0 \cdot b_n + a_1 \cdot b_{n-1} + a_2 \cdot b_{n-2} + a_3 \cdot b_{n-3} + \ldots + a_{(j+1)} \cdot b_{n-(j+1)} + \ldots + a_{n-1} \cdot b_1 + a_n \cdot b_0$, como os coeficientes a_i com índice maior ou igual a $j+1$ são iguais a 0_A e como $n > k = j+l$, assim $n-(j+1) \geq j+l+1-(j+1) = l$

portanto os coeficientes b_i com índice maior do $i > n-(j+1)$ são iguais a 0_A, portanto $d_n = a_0 \cdot 0_A + a_1 \cdot 0_A + a_2 \cdot 0_A + a_3 \cdot 0_A + ... + 0_A \cdot b_{n-(j+1)} + \ldots + 0_A \cdot b_1 + 0_A \cdot b_0 = 0_A$ para todo $n > k$.

M_2 (Associatividade da multiplicação), ou seja, $(f \bigodot g) \bigodot h = f \bigodot (g \bigodot h)$, pela definição de multiplicação temos os seguintes polinômios:

$$f \bigodot g = d = (d_0, d_1, d_2, d_3, \ldots) \text{ onde } d_n = \sum_{i+j=n} a_i \cdot b_j$$

$$g \bigodot h = z = (z_0, z_1, z_2, z_3, \ldots) \text{ onde } z_n = \sum_{i+j=n} b_i \cdot c_j$$

$$(f \bigodot g) \bigodot h = d \bigodot h = p = (p_0, p_1, p_2, p_3, \ldots) \text{ onde } p_n = \sum_{i+j=n} d_i \cdot c_j$$

$$f \bigodot (g \bigodot h) = f \bigodot z = q = (q_0, q_1, q_2, q_3, \ldots) \text{ onde } q_n = \sum_{i+j=n} a_i \cdot z_j.$$

Assim devemos demostrar que os polinômios p e q são iguais, pela igualdade de polinômios temos que mostrar que $p_n = q_n$ para todo $n \geq 0$.

$$p_n = \sum_{i+j=n} d_i \cdot c_j = \sum_{i+j=n} (\sum_{\alpha+\beta=i} a_\alpha \cdot b_\beta) \cdot c_j = \sum_{\alpha+\beta+j=n} (a_\alpha \cdot b_\beta) \cdot c_j \overset{(5)}{=}$$

$$\sum_{\alpha+\beta+j=n} a_\alpha \cdot (b_\beta \cdot c_j) = \sum_{\alpha+\gamma=n} a_\alpha \cdot (\sum_{\beta+j=\gamma} b_\beta \cdot c_j) = \sum_{\alpha+\gamma=n} a_\alpha \cdot z_\gamma = q_n$$

Em (5) aplicamos a associatividade da multiplicação do anel $(A, +, \cdot)$, portanto os polinômios p e q são iguais.

AM (Distributividade), ou seja, $f \bigodot (g \bigoplus h) = (f \bigodot g) \bigoplus (f \bigodot h)$ e $(f \bigoplus g) \bigodot h = (f \bigodot h) \bigoplus (g \bigodot h)$, vamos mostrar $f \bigodot (g \bigoplus h) = (f \bigodot g) \bigoplus (f \bigodot h)$, pela definição de multiplicação e adição temos os seguintes polinômios:

$$f \bigodot (g \bigoplus h) = r = (r_0, r_1, r_2, r_3, \ldots) \text{ onde } r_n = \sum_{i+j=n} a_i \cdot (b_j + c_j)$$

$$f \bigodot g = d = (d_0, d_1, d_2, d_3, \ldots) \text{ onde } d_n = \sum_{i+j=n} a_i \cdot b_j$$

$$f \bigodot h = t = (t_0, t_1, t_2, t_3, \ldots) \text{ onde } t_n = \sum_{i+j=n} a_i \cdot c_j$$

$$(f \bigodot g) \bigoplus (f \bigodot h) = d \bigoplus t = s = (s_0, s_1, s_2, s_3, \ldots) \text{ onde } s_n = d_n + t_n.$$

Assim devemos demostrar que os polinômios r e s são iguais. Pela igualdade de polinômios temos que mostrar que $r_n = s_n$ para todo $n \geq 0$.

$$r_n = \sum_{i+j=n} a_i \cdot (b_j + c_j) \overset{(6)}{=} \sum_{i+j=n} (a_i \cdot b_j) + (a_i \cdot c_j) =$$

$$\sum_{i+j=n} (a_i \cdot b_j) + \sum_{i+j=n} (a_i \cdot c_j) = d_n + t_n = s_n$$

Em (6) aplicamos a distributividade do anel $(A, +, \cdot)$, portanto os polinômios r e s são iguais. A segunda parte, ou seja, $(f \bigoplus g) \bigodot h = (f \bigodot h) \bigoplus (g \bigodot h)$, pode ser provada de modo análogo.

Assim o conjunto dos polinômios P, com as operações de adição $\bigoplus$ e multiplicação $\bigodot$ satisfazem todas as propriedades da definição de um anel, portanto $(P, \bigoplus, \bigodot)$ é um anel. Resta mostrar que é um anel comutativo com identidade.

M_3 (Comutatividade da multiplicação), ou seja, $f \bigodot g = g \bigodot f$, pela definição de multiplicação temos os seguintes polinômios:

$$f \bigodot g = d = (d_0, d_1, d_2, d_3, \ldots) \text{ onde } d_n = \sum_{i+j=n} a_i \cdot b_j$$

$$g \bigodot f = w = (w_0, w_1, w_2, w_3, \ldots) \text{ onde } w_n = \sum_{i+j=n} b_i \cdot a_j$$

Assim devemos demostrar que os polinômios d e w são iguais, pela igualdade de polinômios temos que mostrar que $d_n = w_n$ para todo $n \geq 0$.

$$d_n = \sum_{i+j=n} a_i \cdot b_j \overset{(7)}{=} \sum_{i+j=n} b_j \cdot a_i = w_n$$

Em (7) aplicamos a comutatividade do anel $(A, +, \cdot)$, portanto os polinômios d e w são iguais.

M_4 (Existência do elemento neutro da multiplicação), ou seja, existe um polinômio k tal que $f \bigodot k = f = k \bigodot f$, para todo $f \in P$, se tomamos $k = (1_A, 0_A, 0_A, 0_A, \ldots)$, pela definição de multiplicação temos os seguintes polinômios:

$$f \bigodot k = l = (l_0, l_1, l_2, l_3, \ldots) \text{ onde } l_n = \sum_{i=0}^{n} a_i \cdot k_{n-i}$$

Assim devemos demostrar que os polinômios f e l são iguais, pela igualdade de polinômios temos que mostrar que $a_n = l_n$ para todo $n \geq 0$.

Como $k_i = 0_A$ para todo $i \geq 1$ e $k_0 = 1_A$, temos o seguinte:

$$l_n = \sum_{i=0}^{n} a_i \cdot k_{n-i} = a_0 \cdot 0_A + a_1 \cdot 0_A + a_2 \cdot 0_A + \ldots + a_n \cdot 1_A = a_n$$

Portanto os polinômios f e l são iguais, e o polinômio $k = (1_A, 0_A, 0_A, 0_A, \ldots)$ é o elemento neutro da multiplicação.

□

Teorema 2.1.7. *Seja $(A, +, \cdot)$ um domínio de integridade, então $(P, \bigoplus, \bigodot)$ é um domínio de integridade.*

Demonstração. Pelo Teorema 2.1.6, devemos mostra que a multiplicação de dois polinômios não nulo pertencentes a P é diferente do polinômio nulo $e = (0_A, 0_A, 0_A, 0_A, \ldots)$,

ou seja, devemos mostrar que no polinômio do resultado da multiplicação existe pelo menos um coeficiente diferente do 0_A.

Sejam quaisquer dois polinômios $f = (a_0, a_1, a_2, a_3, \ldots)$ e $g = (b_0, b_1, b_2, b_3, \ldots)$ diferentes do polinômio nulo e, sendo $f \bigodot g = c = (c_0, c_1, c_2, c_3, \ldots)$ onde $c_n = \sum_{i=0}^{n} a_i \cdot b_{n-i}$, pela definição de polinômios existe um índice k, tal que $a_i = 0_A$, para todo $i > k$ e um índice l, tal que $b_i = 0_A$, para todos $i > l$, como f e g são diferentes do polinômio nulo e, então os coeficientes dos índices k e l são diferentes de 0_A, assim temos

$$c_{k+l} = a_0 \cdot b_{k+l} + a_1 \cdot b_{(k+l)-1} + a_2 \cdot b_{(k+l)-2} + a_3 \cdot b_{(k+l)-3} + \ldots + a_k \cdot b_l + \ldots + a_{k+l} \cdot b_0,$$

como $a_i = 0_A$ para todo $i > k$ e $b_i = 0_A$ para todo $i > l$, assim temos

$$c_{k+l} = a_0 \cdot 0_A + a_1 \cdot 0_A + a_2 \cdot 0_A + a_3 \cdot 0_A + \ldots + a_k \cdot b_l + \ldots + 0_A \cdot b_0 = a_k \cdot b_l.$$

Como $(A, +, \cdot)$ é um domínio de integridade, então $c_{k+l} = a_k \cdot b_l \neq 0_A$, portanto no polinômio c existe pelo menos um coeficiente diferente do 0_A, com isso o polinômio c é diferente do polinômio nulo e, como os polinômios f e g foram tomados arbitrariamente, a propriedade vale para todos polinômios não nulos pertencentes a P, assim $(P, \bigoplus, \bigodot)$ é um domínio de integridade.

□

Pelos Teoremas 2.1.6 e 2.1.7 observamos que muitas das propriedades pertencentes ao anel dos coeficientes dos polinômios são transferidas para os polinômios, mas se o anel é um corpo a propriedade da existência do elemento simétrico da multiplicação ou inverso multiplicativo não é transferida para os polinômios, por exemplo, o polinômio $r = (0, 2, 0, 0, 0, \ldots)$ com o coeficiente no anel $(\mathbb{R}, +, \cdot)$ que é um corpo, não possui inverso multiplicativo, ou seja, não existe um polinômio s com coeficiente de números reais, tal que, $r \bigodot s = k = (1, 0, 0, 0, 0, \ldots)$, pois não existe nenhum número real que multiplicado por 0 é igual 1.

Apresentaremos agora, uma associação entre a definição de polinômios que demos e a notação usual de polinômios, para isso, agora em diante o anel $(A, +, \cdot)$ será comutativo com identidade 1_A.

Na notação usual, os polinômios constantes comportam como os elementos do anel. Vamos mostrar que os polinômios da forma $(a, 0_A, 0_A, 0_A, \ldots)$ com $a \in (A, +, \cdot)$, também possui essencialmente esse comportamento.

Teorema 2.1.8. *Seja* $(P, \bigoplus, \bigodot)$ *o anel de polinômios com coeficientes no anel* $(A, +, \cdot)$. *Seja* P^* *o conjunto de todos polinômios em* $(P, \bigoplus, \bigodot)$ *da forma* $(a, 0_A, 0_A, 0_A, \ldots)$ *com* $a \in (A, +, \cdot)$, *então* $(P^*, \bigoplus, \bigodot)$ *é um subanel de* $(P, \bigoplus, \bigodot)$ *e é isomorfo a* $(A, +, \cdot)$.

Demonstração. Primeiramente vamos provar que $(P^*, \bigoplus, \bigodot)$ é um subanel de $(P, \bigoplus, \bigodot)$, temos que P^* é fechado em relação a adição, pois, sendo$(a, 0_A, 0_A, 0_A, \ldots)$ e $(b, 0_A, 0_A, 0_A, \ldots)$ pertencentes a P^* então

$$(a, 0_A, 0_A, 0_A, \ldots) + (b, 0_A, 0_A, 0_A, \ldots) = (a + b, 0_A, 0_A, 0_A, \ldots) \in P^*.$$

Além disso, P^* também é fechado em relação a multiplicação, pois,

$$(a, 0_A, 0_A, 0_A, \ldots) \cdot (b, 0_A, 0_A, 0_A, \ldots) = (a \cdot b, 0_A, 0_A, 0_A, \ldots) \in P^*.$$

Também o polinômio nulo $e = (0_A, 0_A, 0_A, 0_A, \ldots) \in P^*$, e para qualquer polinômio $(a, 0_A, 0_A, 0_A, \ldots) \in P^*$ temos que o polinômio $(-a, 0_A, 0_A, 0_A, \ldots) \in P^*$ é solução da equação $(a, 0_A, 0_A, 0_A, \ldots) + x = (0_A, 0_A, 0_A, 0_A, \ldots)$. Portanto pelo Teorema 1.1.25, $(P^*, \bigoplus, \bigodot)$ é um subanel de $(P, \bigoplus, \bigodot)$.

Agora considere a função $f : A \to P^*$ dada por:

$$f(a) = (a, 0_A, 0_A, 0_A, \ldots)$$

A função f é injetiva, pois, se $f(a) \neq f(b)$ então $(a, 0_A, 0_A, 0_A, \ldots) \neq (b, 0_A, 0_A, 0_A, \ldots)$ pela igualdade de polinômios temos que $a \neq b$. Além disso, f é sobrejetiva, pois, para todo polinômio da forma $(a, 0_A, 0_A, 0_A, \ldots)$ existe um $a \in A$ tal que $f(a) = (a, 0_A, 0_A, 0_A, \ldots)$. Portanto a função f é bijetiva.

Agora, em decorrência da adição e multiplicação de polinômios temos que

$$f(a+b) = (a+b, 0_A, 0_A, 0_A, \ldots) = (a, 0_A, 0_A, 0_A, \ldots) \bigoplus (b, 0_A, 0_A, 0_A, \ldots) = f(a) \bigoplus f(b)$$

$$f(a \cdot b) = (a \cdot b, 0_A, 0_A, 0_A, \ldots) = (a, 0_A, 0_A, 0_A, \ldots) \bigodot (b, 0_A, 0_A, 0_A, \ldots) = f(a) \bigodot f(b)$$

Portanto f é um isomorfismo e $(P^*, \bigoplus, \bigodot)$ é isomorfo a $(A, +, \cdot)$. □

Pelo isomorfismo do Teorema 2.1.8 passaremos a denotar o polinômio constante $(a, 0_A, 0_A, 0_A, \ldots)$ por a.

Para continuar passaremos a utilizar a seguinte notação para o polinômio:

$$x = (0_A, 1_A, 0_A, 0_A, \ldots)$$

Lema 2.1.9. *Seja* $(P, \bigoplus, \bigodot)$ *o anel de polinômios com coeficientes no anel* $(A, +, \cdot)$ *e o polinômio* $x = (0_A, 1_A, 0_A, 0_A, \ldots)$, *então, para* $n \geq 1$,

$$x^n = (0_A, 0_A, \ldots, 0_A, 1_A, 0_A, \ldots), \textit{ onde } 1_A \textit{ está na posição } n.$$

Demonstração. O polinômio x pode ser descrito assim:

$$x = (e_0, e_1, e_2, e_3, \ldots), \text{onde } e_i = 0_A \text{ para todo } i \neq 1, \text{ e } e_1 = 1_A.$$

Provaremos o lema por indução sobre n. Para $n = 1$ a propriedade é válida por definição, pois, $x^1 = x$ e como o elemento neutro da multiplicação 1_A está na posição 1 no polinômio x. Suponha que a propriedade é válida para algum $n > 1$, ou seja, suponha que:

$$x^n = (d_0, d_1, d_2, d_3, \ldots), \text{onde } d_i = 0_A \text{ para todo } i \neq n, \text{ e } d_n = 1_A.$$

Então temos o seguinte:

$$x^{n+1} = x^n \cdot x = (d_0, d_1, d_2, d_3, \ldots) \bigodot (e_0, e_1, e_2, e_3, \ldots) = (r_0, r_1, r_2, r_3, \ldots)$$

Onde para cada $j \geq 0$, $r_j = \sum_{i=0}^{j} d_i \cdot e_{j-i}$.

Como $e_i = 0_A$ para $i \neq 1$ e $d_i = 0_A$ para $i \neq n$, então temos que para o coeficiente r de índice $n+1$:

$$r_{n+1} = \underbrace{d_0 \cdot e_{n+1} + \ldots + d_{n-1} \cdot e_2}_{0_A} + d_n \cdot e_1 + \underbrace{d_{n+1} \cdot e_0}_{0_A} = d_n \cdot e_1 = 1_A \cdot 1_A = 1_A$$

Para os coeficientes r de índice $j \neq n+1$ temos:

$$r_j = \underbrace{d_0 \cdot e_j + \ldots + d_{j-2} \cdot e_2}_{0_A} + d_{j-1} \cdot e_1 + \underbrace{d_j \cdot e_0}_{0_A} = d_{j-1} \cdot e_1 = d_{j-1} \cdot 1_A = d_{j-1}$$

Mas como $j \neq n+1$ então $j - 1 \neq n$, portanto $d_{j-1} = 0_A$, assim $r_j = d_{j-1} = 0_A$ para todo $j \neq n+1$, daí temos $x^{n+1} = (r_0, r_1, r_2, r_3, \ldots) = (0_A, 0_A, \ldots, 0_A, 1_A, 0_A, \ldots)$ onde 1_A está na posição $n+1$. Assim a propriedade é válida para $n+1$.

Portanto, pelo princípio da indução matemática, a propriedade é válida para todo $n \geq 1$.

□

Agora estamos pronto para demonstrar o teorema que permite expressar os polinômios em termos das potências de x, ou seja, utilizar a notação usual de polinômios.

Teorema 2.1.10. *Seja $(P, \bigoplus, \bigodot)$ o anel de polinômios com coeficientes no anel $(A, +, \cdot)$. Então $(P, \bigoplus, \bigodot)$ contém um subanel isomorfo $(P^*, \bigoplus, \bigodot)$ de $(A, +, \cdot)$ e um elemento x de tal forma que:*

i) *Cada elemento* $p \in (P, \bigoplus, \bigodot)$ *pode ser escrito na forma* $p = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$;

ii) *A representação de* $p \in (P, \bigoplus, \bigodot)$ *é única no sentido que:*

Se $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ *com* $n \leq m$, *então* $a_i = b_i$ *para* $i \leq n$ *e* $b_i = 0_A$ *para* $i > n$.

Demonstração. Para demonstrar **i)**, considere $p = (a_0, a_1, a_2, a_3, \ldots)$. Sabemos que pela definição de polinômios, existe um índice n_0, tal que $a_i = 0_A$, para todos $i > n_0$. Assim, $p = (a_0, a_1, a_2, \ldots, a_n, 0_A, 0_A, \ldots)$, logo, pela definição de adição de polinômios, $p = (a_0, 0_A, 0_A, \ldots) \bigoplus (0_A, a_1, 0_A, \ldots) \bigoplus (0_A, 0_A, a_2, 0_A, \ldots) \bigoplus \ldots \bigoplus (0_A, \ldots, 0_A, a_n, 0_A, \ldots)$. Agora, pela definição de multiplicação de polinômios, temos que

$$p = (a_0, 0_A, 0_A, \ldots) \bigoplus ((a_1, 0_A, 0_A, 0_A, \ldots) \bigodot (0_A, 1_A, 0_A, \ldots)) \bigoplus$$
$$((a_2, 0_A, 0_A, 0_A, \ldots) \bigodot (0_A, 0_A, 1_A, 0_A, \ldots)) \bigoplus \ldots$$
$$\bigoplus ((a_n, 0_A, 0_A, 0_A, \ldots) \bigodot (0_A, \ldots, 0_A, 1_A, 0_A, \ldots)).$$

Pelo isomorfismo do Teorema 2.1.8 e o Lema 2.1.9 temos:

$$p = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n.$$

Para demonstrar **ii)**, como $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ representa o polinômio $(a_0, a_1, a_2, \ldots, a_n, 0_A, 0_A, \ldots)$ e como $b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ representa o polinômio $(b_0, b_1, b_2, \ldots, b_m, 0_A, 0_A, \ldots)$ usando o Item **i)**, pela igualdade de polinômios, então $a_i = b_i$ para $i \leq n$ e $0_A = b_i$ para $n < i \leq m$. □

Observação 2.1.11. *O Teorema 2.1.10 é verdadeiro para o anel de polinômios com coeficientes em um anel que não seja comutativo com identidade, cuja a demonstração pode ser encontrada em [10] p. 550-551.*

A partir de agora utilizaremos a notação usual de polinômios, ou seja, $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = \sum_{i=0}^{n} a_ix^i$, onde $n \geq 0$ e $a_i \in A$. O coeficiente a_0 é chamado termo constante ou independente de x, e cada termo a_ix^i, com $0 \leq i \leq n$ será chamado de termo ou monômio de $p(x)$ com $a_i \neq 0$. Além disso, $(P, \bigoplus, \bigodot)$ o anel de polinômios com coeficientes no anel $(A, +\cdot)$ será denotado por $A[X]$.

O elemento x às vezes é chamado por indeterminada, mas esse termo é enganador, como podemos observar não tem nada de indeterminado ou ambíguo sobre x, é um elemento específico de $A[X]$ que não está no anel $(A, +\cdot)$.

Para as operações de adição e multiplicação de polinômios, na notação usual, devemos calcular os coeficientes conforme as regras das definições de adição e multiplicação de polinômios, e multiplicar pela potência de x que tem como expoente o índice do coeficiente, ou seja, x^i. Assim, sejam os polinômios $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ e $q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$, a adição de polinômios na notação usual será representada por:

$$p(x) + q(x) = (p+q)(x) = \sum_{i=0}^{n} c_i x^i \text{ com } c_i = a_i + b_i,$$

e a multiplicação de polinômios na notação usual será representada por:

$$p(x) \cdot q(x) = (p \cdot q)(x) = \sum_{i=0}^{n+m} c_i x^i \text{ com } c_i = \sum_{\alpha+\beta=i} a_\alpha b_\beta \begin{cases} a_\alpha = 0_A, & \text{se } \alpha > n \\ b_\beta = 0_A, & \text{se } \beta > m \end{cases}.$$

Observação 2.1.12.

1. *O polinômio $p(x) = 0_A + 0_Ax + 0_Ax^2 + \ldots + 0_Ax^n$ com $a_i = 0_A$ para todo $i \geq 0$, será chamado de polinômio identicamente nulo.*
2. *O polinômio $p(x) = a_0$ será chamado de polinômio constante.*
3. *Os polinômios serão escritos, convenientemente, na ordem crescente ou decrescente das potências de x.*
4. *Quando $a_i = 0_A$ não escreveremos o termo ou monômio a_ix^i, fazendo o uso somente quando necessário.*
5. *Os polinômios $p(x) = a_0+a_1x+a_2x^2+\ldots+a_nx^n$ e $q(x) = b_0+b_1x+b_2x^2+\ldots+b_mx^m$ são iguais, ou seja, $p(x) = q(x)$, se, e somente se, $n = m$ e $a_i = b_i$ para todo $i \leq n$.*
6. *Para facilitar a notação passaremos a indicar o anel $(A, +, \cdot)$ por somente A.*

2.1.1 Grau de um polinômio

Definição 2.1.13. *Seja $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ um polinômio não nulo pertencente a $A[X]$ com $a_n \neq 0_A$, então a_n é denominado coeficiente líder de $p(x)$ e o grau de $p(x)$ é o número natural n, que será denotado por $Gr(p(x))$.*

Em outras palavras, podemos dizer que o grau do polinômio $p(x)$ é o maior expoente natural de x que tem o coeficiente diferente de 0_A entre os termos que o formam $p(x)$.

Exemplo 2.1.14. a) *Se $p(x) = a_0$ e $a_0 \neq 0_A$, então o $Gr(p(x)) = 0$.*

b) *Se* $q(x) = a_0 + a_1x$ *e* $a_1 \neq 0_A$, *então o* $Gr(q(x)) = 1$.

c) *Se* $g(x) = a_0 + a_1x + a_2x^2$ *e* $a_2 \neq 0_A$, *então o* $Gr(g(x)) = 2$.

d) *Se* $f(x) = a_0 + a_5x^5$ *e* $a_5 \neq 0_A$, *então o* $Gr(f(x)) = 5$.

Os polinômios constantes não nulos tem grau 0, não é definido o grau do polinômio constante $p(x) = 0_A$, porque nenhuma potência de x tem coeficiente diferente de 0_A.

Os polinômios de grau n com coeficiente líder $a_n = 1_A$ são chamados de *polinômios mônicos*.

Teorema 2.1.15. *Sejam os polinômios não nulos* $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ *e* $q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ *pertencente a* $A[X]$, *tais que a adição* $(p+q)(x)$ *é diferente do polinômio nulo. Então*

$$Gr((p+q)(x)) \leq max\{Gr(p(x)), Gr(q(x))\}$$

Demonstração. Suponhamos que $a_n \neq 0_A$ e $b_m \neq 0_A$, assim temos $Gr(p(x)) = n$ e $Gr(q(x)) = m$, com isso temos que considerar quatro caso:

i) $n = m$ e $a_n + b_n \neq 0_A$.

Então $(p+q)(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n$ onde $a_n + b_n \neq 0_A$ é o coeficiente líder da adição $(p+q)(x)$ e o grau da adição é $Gr((p+q)(x)) = n = m$.

ii) $n = m$ e $a_n + b_n = 0_A$.

Então $(p+q)(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_k + b_k)x^k + (a_n + b_n)x^n = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_k + b_k)x^k$.

Se $a_k + b_k \neq 0_A$, então será o coeficiente líder da adição $(p+q)(x)$ e o grau da adição será $Gr((p+q)(x)) = k < n = m$.

Se $a_k + b_k = 0_A$, então repetindo o argumento novamente, quantas vezes forem necessárias, concluímos que existe um índice i tal que $a_i + b_i \neq 0_A$, pois a adição $(p+q)(x)$ é diferente do polinômio nulo por hipótese, então $a_i + b_i$ será o coeficiente líder da adição $(p+q)(x)$ e o grau da adição será $Gr((p+q)(x)) = i < k < n = m$.

iii) $n \neq m$ e $n < m$.

Então $(p+q)(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (0_A + b_m)x^m$, pois $a_i = 0_A$ para todos $i > n$.

Então $0_A + b_m = b_m \neq 0_A$ é o coeficiente líder da adição $(p+q)(x)$ e o grau da adição é $Gr((p+q)(x)) = m$.

iv) $n \neq m$ e $m < n$.

Então $(p+q)(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + 0_A)x^n$, pois $b_i = 0_A$ para todos $i > m$.

Então $a_n + 0_A = a_n \neq 0_A$ é o coeficiente líder da adição $(p+q)(x)$ e o grau da adição é $Gr((p+q)(x)) = n$.

Portanto, em qualquer caso temos que $Gr((p+q)(x)) \leq max\{Gr(p(x)), Gr(q(x))\}$.

□

Teorema 2.1.16. *Sejam os polinômios não nulos* $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ *e* $q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ *pertencentes a* $A[X]$*, tais que a multiplicação* $(p \cdot q)(x)$ *é diferente do polinômio nulo. Então*

$$Gr((p \cdot q)(x)) \leq Gr(p(x)) + Gr(q(x))$$

No entanto, se A *for um domínio de integridade então somente ocorre a igualdade.*

Demonstração. Suponhamos que $a_n \neq 0_A$ e $b_m \neq 0_A$, assim temos $Gr(p(x)) = n$ e $Gr(q(x)) = m$. Vimos na demonstração do Teorema 2.1.6 na propriedade do fechamento da multiplicação M_1, que para todos os coeficientes de índice $i > n + m$ o coeficiente é igual a 0_A, ou seja, $c_i = 0_A$, assim o maior índice possível para o coeficiente c_i ser diferente de 0_A é o do índice $n + m$, portanto a maior possibilidade para o maior expoente de x que tem o coeficiente diferente de 0_A é $n + m$, assim o $Gr((p \cdot q)(x)) \leq n + m = Gr(p(x)) + Gr(q(x))$.

Agora suponhamos que A é um domínio de integridade, assim temos para o coeficiente c_{n+m} o seguinte:

$$c_{n+m} = \sum_{\alpha+\beta=n+m} a_\alpha b_\beta \begin{cases} a_\alpha = 0_A, & \text{se } \alpha > n \\ b_\beta = 0_A, & \text{se } \beta > m \end{cases}$$

Portanto $c_{n+m} = a_0 \cdot 0_A + a_1 \cdot 0_A + \ldots + a_n \cdot b_m + 0_A \cdot b_{m-1} + \ldots + 0_A \cdot b_0 = a_n \cdot b_m$, e como A é um domínio de integridade e $a_n \neq 0_A$ e $b_m \neq 0_A$, então $a_n \cdot b_m \neq 0_A$, assim o coeficiente líder da multiplicação $(p \cdot q)(x)$ é o $a_n \cdot b_m$ e o grau da multiplicação é $Gr((p \cdot q)(x)) = n + m = Gr(p(x)) + Gr(q(x))$.

□

Corolário 2.1.17. *Sejam* A *um domínio de integridade e* $p(x) \in A[X]$*. Então* $p(x)$ *é uma unidade em* $A[X]$ *se, e somente se,* $p(x)$ *é um polinômio constante e* a_0 *é uma unidade em* A*. Em particular, se* A *é um corpo, as unidades em* $A[X]$ *são os polinômios constantes não nulos.*

Demonstração. Suponhamos primeiramente, que $p(x)$ é uma unidade em $A[X]$. Então $p(x) \cdot g(x) = 1_A$ para algum $g(x) \in A[X]$, pelo Teorema 2.1.16 temos:

$$Gr(p(x)) + Gr(g(x)) = Gr(p(x) \cdot g(x)) = Gr(1_A) = 0$$

como o grau de polinômio é um número inteiro não negativo, temos que $Gr(p(x)) = 0$ e $Gr(g(x)) = 0$, Portanto, $p(x)$ e $g(x)$ são polinômios constantes, sendo $p(x) = a_0$ e $g(x) = b_0$, temos que $p(x) \cdot g(x) = a_0 \cdot b_0 = 1_A$, portanto a_0 é uma unidade em A.

Reciprocamente, suponhamos que $p(x) = a_0$ é um polinômio constante e a_0 é uma unidade em A, assim existe $g(x)$ tal que $g(x) = a_0^{-1}$, onde a_0^{-1} é o inverso multiplicativo de a_0. Então $p(x) \cdot g(x) = a_0 \cdot a_0^{-1} = 1_A$. Portanto $p(x)$ é uma unidade em $A[X]$.

Se A é um corpo, então os elementos diferentes do elemento neutro da adição são unidades, então os polinômios constantes não nulos, são unidades em $A[X]$. □

Corolário 2.1.18. *Sejam F um corpo e $p(x), q(x) \in F[X]$ polinômios não nulos, então $Gr(p(x)) \leq Gr(p(x) \cdot q(x))$.*

Demonstração. Como $F[X]$ é um domínio de integridade, então pelo Teorema 2.1.16, temos que $Gr(p(x) \cdot q(x)) = Gr(p(x)) + Gr(q(x))$, e como $Gr(q(x)) \geq 0$. Portanto, temos que $Gr(p(x)) \leq Gr(p(x) \cdot q(x))$.

□

2.1.2 Algoritmo da divisão de polinômios

Agora apresentaremos o algoritmo da divisão de polinômios que possui os coeficientes em um corpo, que consiste em dividir um polinômio por outro, resultando em um polinômio no quociente e outro polinômio no resto, igual a divisão euclideana dos números inteiros.

Teorema 2.1.19. Divisão Euclideana

Seja F um corpo e sejam os polinômios $f(x), g(x) \in F[X]$, com $g(x)$ diferente do polinômio nulo, então existem únicos polinômios $q(x), r(x) \in F[X]$ tais que

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

onde $r(x) = 0_F$ ou $Gr(r(x)) < Gr(g(x))$.

Demonstração. **(Prova da existência)**

Se $f(x) = 0_F$ ou $Gr(f(x)) < Gr(g(x))$, então o teorema é verdadeiro com $q(x) = 0_F$ e $r(x) = f(x)$, porque $f(x) = 0_F \cdot g(x) + f(x)$.

Se $f(x) \neq 0_F$ e $Gr(g(x)) \leq Gr(f(x))$, então a demonstração da existência será por indução completa sobre o grau de $f(x)$. Sejam $Gr(f(x)) = n$, digamos $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ com $a_n \neq 0_F$ e digamos $Gr(g(x)) = m$ e $g(x) = b_m x^m + b_{n-1}x^{m-1} + \ldots + b_1 x + b_0$ com $b_m \neq 0_F$, onde $m \leq n$.

Se $Gr(f(x)) = 0$, então $Gr(g(x)) = 0$. Portanto $f(x) = a_0$ e $g(x) = b_0$ com $a_0, b_0 \neq 0_F$, como F é um corpo, b_0 é uma unidade, ou seja, possui inverso multiplicativo, assim $a_0 = b \cdot (b^{-1}a_0) + 0_F$, então o teorema é verdadeiro para $n = 0$, com $q(x) = b^{-1}a_0$ e $r(x) = 0_F$.

Suponhamos que o teorema é verdadeiro para polinômios com grau menor do que $n = Gr(f(x))$, devemos mostrar que o teorema é verdadeiro para polinômios com grau n. Como F é um corpo e $b_m \neq 0_F$, b_m é uma unidade, assim multiplicamos o polinômio $g(x)$ por $a_n b_m^{-1} x^{n-m}$ para obter

$$\begin{aligned} a_n b_m^{-1} x^{n-m} \cdot g(x) &= a_n b_m^{-1} x^{n-m}(b_m x^m + b_{n-1}x^{m-1} + \ldots + b_1 x + b_0) \\ &= a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \ldots + a_n b_m^{-1} b_1 x^{n-m+1} + a_n b_m^{-1} b_0 x^{n-m} \end{aligned}$$

Como os polinômios $f(x)$ e $a_n b_m^{-1} x^{n-m} \cdot g(x)$ tem o mesmo grau n e o mesmo coeficiente líder a_n, a diferença $f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x)$ é um polinômio de grau menor que n. Por hipótese de indução, existem $q_1(x)$ e $r_1(x)$ em $F[X]$ tais que

$$f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x) = q_1(x) \cdot g(x) + r_1(x)$$

com $r_1(x) = 0_F$ ou $Gr(r_1(x)) < Gr(g(x))$. Portanto,

$$f(x) = q_1(x) \cdot g(x) + r_1(x) + a_n b_m^{-1} x^{n-m} \cdot g(x)$$

$$f(x) = g(x) \cdot [q_1(x) + a_n b_m^{-1} x^{n-m}] + r_1(x)$$

Se tomamos $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r(x) = r_1(x)$, temos que o teorema é verdadeiro para os polinômios com grau n. Portanto pelo princípio da indução completa o teorema é verdadeiro para todo polinômio de qualquer grau.

(Prova da unicidade)

Sejam $q_1(x), q_2(x), r_1(x), r_2(x) \in F[X]$, tais que $f(x) = q_1(x) \cdot g(x) + r_1(x)$ e $f(x) = q_2(x) \cdot g(x) + r_2(x)$, onde $r_1 = 0_F$ ou $Gr(r_1(x)) < Gr(g(x))$, e $r_2 = 0_F$ ou $Gr(r_2(x)) < Gr(g(x))$. Assim

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

$$q_1(x) \cdot g(x) - q_2(x) \cdot g(x) = r_2(x) - r_1(x)$$

$$g(x) \cdot (q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

Se $q_1(x) \neq q_2(x)$, temos $Gr(g(x) \cdot (q_1(x) - q_2(x))) = Gr(r_2(x) - r_1(x))$, mas como F também é um domínio de integridade e pelo Teorema 2.1.16, temos

$$Gr(g(x) \cdot (q_1(x) - q_2(x))) = Gr(g(x)) + Gr(q_1(x) - q_2(x)) \text{ então,}$$

$$Gr(r_2(x) - r_1(x)) = Gr(g(x)) + Gr(q_1(x) - q_2(x)). \text{ Assim}$$

$$Gr(r_2(x) - r_1(x)) \geq Gr(g(x))$$

No entanto, pelo Teorema 2.1.15, temos $Gr(r_2(x) - r_1(x)) \leq max\{Gr(r_1(x)), Gr(r_2(x))\}$, mas como $Gr(r_1(x)) < Gr(g(x))$ e $Gr(r_2(x)) < Gr(g(x))$, temos que,

$$Gr(r_2(x) - r_1(x)) \leq max\{Gr(r_1(x)), Gr(r_2(x))\} < Gr(g(x)$$

Portanto, temos uma contradição. Então $q_1(x) = q_2(x)$ e temos

$$g(x) \cdot (q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

$$g(x) \cdot 0_F = r_2(x) - r_1(x)$$

$$0_F = r_2(x) - r_1(x)$$

$$r_2(x) = r_1(x)$$

Portanto, são únicos os polinômios $q(x)$ e $r(x)$, tais que $f(x) = q(x) \cdot g(x) + r(x)$.

□

O algoritmo da divisão de polinômios consiste em primeiro multiplicar o polinômio divisor por outro polinômio de forma que o polinômio do resultado da multiplicação tenha o mesmo grau e coeficiente líder do polinômio dividendo, isso é possível pois o coeficiente líder do polinômio divisor pertencente a um corpo, ou seja, possui inverso multiplicativo, com isso ao realizar a subtração de ambos, obteremos um polinômio de grau menor. Em seguida, realizamos novamente o procedimento com o polinômio obtido no lugar do polinômio dividendo e repetimos o procedimento com o polinômio obtido novamente, como em cada procedimento o grau do polinômio obtido diminui pelo menos um grau, assim, após sucessivas repetições o grau do polinômio obtido será menor que o grau do polinômio divisor, então esse será o resto da divisão e o quociente da divisão é o polinômio da soma dos polinômios que foram multiplicados com o polinômio divisor em cada procedimento. Vejamos um exemplo.

Exemplo 2.1.20. *Sejam os polinômios* $f(x) = 5x^3+5x^2+x+10$ *e* $g(x) = 2x^2+3x+2$ *em* $\mathbb{Q}[X]$*, para proceder a divisão do polinômio* $f(x)$ *pelo polinômio* $g(x)$ *consiste:*

Primeiro passo: multiplicar o polinômio $g(x) = 2x^2 + 3x + 2$ *por* $\frac{5}{2}x$ *e subtrair de* $f(x)$ *o resultado da multiplicação, assim temos*

$$r_1(x) = f(x) - [\frac{5}{2}x(g(x))]$$
$$r_1(x) = 5x^3 + 5x^2 + x + 10 - [\frac{5}{2}x(2x^2 + 3x + 2)$$
$$r_1(x) = -\frac{5}{2}x^2 - 4x + 10$$

Segundo passo: multiplicar o polinômio $g(x) = 2x^2 + 3x + 2$ *por* $-\frac{5}{4}$ *e subtrair de* $r_1(x)$ *o resultado da multiplicação, assim temos*

$$r_2(x) = r_1(x) - [-\frac{5}{4}(g(x))]$$
$$r_2(x) = -\frac{5}{2}x^2 - 4x + 10 - [-\frac{5}{4}(2x^2 + 3x + 2)]$$
$$r_2(x) = -\frac{1}{4}x + \frac{25}{2}$$

Terceiro passo: Como $Gr(r_2(x)) = 1 < 2 = Gr(g(x))$ *não é possível continuar a divisão, pois, não é possível multiplicar o polinômio* $g(x)$ *por outro polinômio pertencente* $\mathbb{Q}[X]$*, tal que o polinômio do resultado da multiplicação tenha grau igual do polinômio* $r_2(x)$*. Assim o polinômio* $r_2(x)$ *é o resto da divisão, agora devemos determinar o polinômio quociente da divisão, temos o seguinte:*

$$r_2(x) = r_1(x) - [-\frac{5}{4}(g(x))]$$
$$r_2(x) = f(x) - [\frac{5}{2}x(g(x))] - [-\frac{5}{4}(g(x))]$$
$$f(x) = g(x)[\frac{5}{2}x - \frac{5}{4}] + r_2(x)$$

Assim o polinômio $q(x) = \frac{5}{2}x - \frac{5}{4}$ *é o quociente da divisão, ou seja, é soma dos polinômios que foram multiplicados com o polinômio* $g(x)$*.*

Podemos arrumar os procedimentos do Exemplo 2.1.20 através do seguinte dispositivo que no Ensino Médio é chamado de Método da chave:

$$\overbrace{5x^3 + 5x^2 + x + 10}^{f(x)} \quad \Big| \overbrace{2x^2 + 3x + 2}^{g(x)}$$

$$\begin{array}{r|l} -5x^3 - \frac{15}{2}x^2 - 5x & \underbrace{\frac{5}{2}x - \frac{5}{4}}_{q(x)} \\ \hline -\frac{5}{2}x^2 - 4x + 10 & \\ \underline{\frac{5}{2}x^2 + \frac{15}{4}x + \frac{5}{2}} & \\ \underbrace{-\frac{1}{4}x + \frac{25}{2}}_{r(x)} & \end{array}$$

Observação 2.1.21. *O Teorema 2.1.19 também é verdadeiro na seguinte situação: seja $(A, +, \cdot)$ um anel e sejam $f(x), g(x) \in A[X]$, com $g(x) \neq 0$ e o coeficiente líder de $g(x)$ é invertível em $(A, +, \cdot)$. [8] p. 87-88.*

Teorema 2.1.22. *Seja F um corpo. Então $F[X]$ é um anel euclideano.*

Demonstração. Como $F[X]$ é um domínio de integridade, então pela Definição 1.1.22, devemos encontrar uma função que tem as propriedades **i** e **ii** da definição, mas essa função é a função grau do polinômio, pois as propriedades foram provadas respectivamente pelo Corolário 2.1.18 e pelo Teorema 2.1.19. □

De modo geral, as propriedades que serão provadas em relação $F[X]$, sendo F um corpo, valem para todos os anéis euclideanos.

2.1.3 Divisibilidade dos polinômios

Nesta subseção, estudaremos a divisibilidade dos polinômios com os coeficientes em um corpo F e suas propriedades. Além disso, estudaremos os conceitos de máximo divisor comum e mínimo múltiplo comum.

Definição 2.1.23. *Sejam F um corpo e $a(x), b(x) \in F[X]$ com $b(x)$ não nulo. Dizemos que $b(x)$ divide $a(x)$, ou que $b(x)$ é um fator de $a(x)$, e escrevemos $b(x) \mid a(x)$, se $a(x) = h(x) \cdot b(x)$ para algum $h(x) \in F[X]$. Neste caso, diremos que $a(x)$ é múltiplo de $b(x)$.*

Portanto, aplicando o algoritmo da divisão nos polinômios $a(x), b(x) \in F[X]$ com $b(x)$ não nulo, se o polinômio do resto da divisão é o polinômio nulo, então $b(x)$ divide $a(x)$.

Teorema 2.1.24. *Sejam F um corpo e $a(x), b(x) \in F[X]$ com $b(x)$ não nulo. Então valem as seguintes propriedades:*

1. *Se $b(x) \mid a(x)$, então $c \cdot b(x) \mid a(x)$, para todo $c \in F$ não nulo.*

2. *Se $a(x) \mid b(x)$ e $b(x) \mid c(x)$, então $a(x) \mid c(x)$.*

3. *Se $a(x) \mid b(x)$ e $a(x) \mid c(x)$, então $a(x) \mid (b(x) + c(x))$.*

4. *Se $a(x) \mid b(x)$, então $a(x) \mid b(x) \cdot c(x)$, para todo $c(x) \in F[X]$.*

5. *Se $a(x) \mid b(x)$ e $a(x) \mid c(x)$, então $a(x) \mid (b(x) \cdot d(x) + c(x) \cdot e(x))$, para quaisquer $d(x), e(x) \in F[X]$.*

6. *Se $a(x) \mid b(x)$ e $b(x) \mid a(x)$, então $a(x) = c \cdot b(x)$, onde c é uma constante de F.*

7. *Se $b(x) \mid a(x)$, então $Gr(b(x)) \leq Gr(a(x))$.*

Demonstração. Para mostrar o Item **1**, se $b(x) \mid a(x)$, então $a(x) = b(x) \cdot h(x)$ para algum $h(x) \in F[X]$. Assim temos:

$$a(x) = 1_F \cdot b(x) \cdot h(x) = c \cdot c^{-1} \cdot b(x) \cdot h(x) = c \cdot b(x)[c^{-1} \cdot h(x)].$$

Portanto, $c \cdot b(x) \mid a(x)$.

Para mostrar o Item **2**, se $a(x) \mid b(x)$ e $b(x) \mid c(x)$, então temos o seguinte:

$$b(x) = a(x) \cdot q_1(x), \text{ para algum } q_1(x) \in F[X] \text{ e}$$
$$c(x) = b(x) \cdot q_2(x), \text{ para algum } q_2(x) \in F[X],$$

assim

$$c(x) = a(x) \cdot q_1(x) \cdot q_2(x) \text{ e como } q_1(x) \cdot q_2(x) \in F[X], \text{ então } a(x) \mid c(x).$$

Para mostrar o Item **3**, se $a(x) \mid b(x)$ e $a(x) \mid c(x)$, então temos o seguinte:

$$b(x) = a(x) \cdot q_1(x), \text{ para algum } q_1(x) \in F[X] \text{ e}$$
$$c(x) = a(x) \cdot q_2(x), \text{ para algum } q_2(x) \in F[X],$$

assim

$$b(x) + c(x) = a(x) \cdot (q_1(x) + q_2(x)) \text{ com } q_1(x) + q_2(x) \in F[X], \text{ então}$$
$$a(x) \mid (b(x) + c(x)).$$

Para mostrar o Item **4**, se $a(x) \mid b(x)$, então $b(x) = a(x) \cdot q(x)$ para algum $q(x) \in F[X]$, e para todo $c(x) \in F[X]$, temos o seguinte:

$b(x) \cdot c(x) = a(x) \cdot q(x) \cdot c(x)$ e como $q(x) \cdot c(x) \in F[X]$ então $a(x) \mid b(x) \cdot c(x)$

Para mostrar o Item **5**, se $a(x) \mid b(x)$ e $a(x) \mid c(x)$, então pelo Item **4** temos que:

$$a(x) \mid b(x) \cdot d(x), \text{ para todo } d(x) \in F[X] \text{ e}$$
$$a(x) \mid c(x) \cdot e(x), \text{ para todo } e(x) \in F[X],$$

agora pelo Item **3** temos que:

$$a(x) \mid (b(x) \cdot d(x) + c(x) \cdot e(x)), \text{ para quaisquer } d(x), e(x) \in F[X].$$

Para mostrar o Item **6**, se $a(x) \mid b(x)$ e $b(x) \mid a(x)$, então temos o seguinte:

$$b(x) = a(x) \cdot q_1(x), \text{ para algum } q_1(x) \in F[X],$$
$$a(x) = b(x) \cdot q_2(x), \text{ para algum } q_2(x) \in F[X]$$

e assim

$$a(x) = a(x) \cdot q_1(x) \cdot q_2(x)$$

Assim $Gr(a(x)) = Gr(a(x) \cdot q_1(x) \cdot q_2(x))$, e como $F[X]$ é um domínio de integridade e pelo Teorema 2.1.16, temos que $Gr(a(x)) = Gr(a(x)) + Gr(q_1(x) \cdot q_2(x))$, com isso $Gr(q_1(x) \cdot q_2(x)) = 0$, ou seja, $Gr(q_1(x)) + Gr(q_2(x)) = 0$, o que implica que $Gr(q_1(x)) = 0$ e $Gr(q_2(x)) = 0$. Portanto, $q_2(x) = c$ é um polinômio constante e $a(x) = c \cdot b(x)$.

Para mostrar o Item **7**, suponha $b(x) \mid a(x)$, então $a(x) = b(x) \cdot h(x)$ para algum $h(x) \in F[X]$. Pelo Teorema 2.1.16, $Gr(a(x)) = Gr(b(x)) + Gr(h(x))$. Uma vez que o grau dos polinômios são números naturais, devemos ter $0 \leq Gr(b(x)) \leq Gr(a(x))$. □

Definição 2.1.25. *Sejam F um corpo e $a(x), b(x) \in F[X]$, ambos não nulos. O máximo divisor comum (mdc) entre $a(x)$ e $b(x)$ é o polinômio mônico de maior grau que divide $a(x)$ e $b(x)$.*

Em outras palavras, $d(x)$ é o máximo divisor comum (mdc) de $a(x)$ e $b(x)$ desde que $d(x)$ é mônico, e tenha as seguintes propriedades:

(1) *$d(x) \mid a(x)$ e $d(x) \mid b(x)$;*

(2) *Se $c(x) \mid a(x)$ e $c(x) \mid b(x)$, então o $Gr(c(x)) \leq Gr(d(x))$.*

Teorema 2.1.26. *Sejam F um corpo e $a(x), b(x) \in F[X]$, ambos não nulos. Então, existe um único máximo divisor comum $d(x)$ de $a(x)$ e $b(x)$. Além disso, existem polinômios $u(x)$ e $v(x)$, tal que $d(x) = a(x) \cdot u(x) + b(x) \cdot v(x)$, não necessariamente únicos.*

Demonstração. **(Prova da Existência)**

Seja S o conjunto de todas as combinações lineares de $a(x)$ e $b(x)$, isto é,

$$S = \{a(x) \cdot m(x) + b(x) \cdot n(x); m(x), n(x) \in F[X]\}.$$

Observe que S contém polinômios não nulos, por exemplo, pelos menos $a(x)$ e $b(x)$ pertencem a S, pois, $a(x) = a(x) \cdot 1_F + b(x) \cdot 0_F$ e $b(x) = a(x) \cdot 0_F + b(x) \cdot 1_F$. Assim, o conjunto de todos graus dos polinômios em S é um conjunto não vazio de inteiros não negativos, que tem um menor elemento, pelo Princípio da Boa Ordenação[1]. Assim, existe um polinômio $w(x)$ de menor grau em S. Se d é coeficiente líder de $w(x)$, então $t(x) = d^{-1} \cdot w(x)$ é um polinômio mônico de menor grau em S. Pela definição de S, temos que:

$$\text{existem } u(x), v(x) \in F[X], \text{ tal que } t(x) = a(x) \cdot u(x) + b(x) \cdot v(x).$$

Vamos provar que $t(x)$ é o máximo divisor comum entre $a(x)$ e $b(x)$, ou seja, que $t(x)$ satisfaz as duas propriedades da Definição 2.1.25. Pelo Teorema 2.1.19, existem polinômios $q(x)$ e $r(x)$, tal que $a(x) = q(x) \cdot t(x) + r(x)$, com $r(x) = 0_F$ ou $Gr(r(x)) < Gr(t(x))$. Consequentemente temos o seguinte:

$$r(x) = a(x) - q(x) \cdot t(x)$$

$$r(x) = a(x) - q(x) \cdot [a(x) \cdot u(x) + b(x) \cdot v(x)]$$

$$r(x) = a(x) - q(x) \cdot a(x) \cdot u(x) - q(x) \cdot b(x) \cdot v(x))$$

$$r(x) = a(x) \cdot [1 - q(x) \cdot u(x)] + b(x) \cdot [-q(x) \cdot v(x)$$

Assim, $r(x)$ é uma combinação linear de $a(x)$ e $b(x)$, portanto $r(x) \in S$, e como $t(x)$ é o polinômio mônico de menor grau em S, então não pode ocorrer a possibilidade $Gr(r(x)) < Gr(t(x))$, assim a única possibilidade é $r(x) = 0_F$. Portanto $a(x) = q(x) \cdot t(x) + r(x) = q(x) \cdot t(x) + 0_F = q(x) \cdot t(x)$, de modo que $t(x) \mid a(x)$. Um argumento semelhante mostra que $t(x) \mid b(x)$. Assim provamos a primeira propriedade:

(1) $t(x) \mid a(x)$ e $t(x) \mid b(x)$

Se $c(x) \mid a(x)$ e $c(x) \mid b(x)$, então pelo Item **(5)** do Teorema 2.1.24 $c(x) \mid a(x) \cdot u(x) + b(x) \cdot v(x) = t(x)$, com isso $c(x) \mid t(x)$ e pelo Item **(7)** do Teorema 2.1.24 temos que $Gr(c(x) \leq Gr(t(x))$. Assim provamos a segunda propriedade:

(2) Se $c(x) \mid a(x)$ e $c(x) \mid b(x)$, então o $Gr(c(x)) \leq Gr(t(x))$.

[1]Para uma melhor compreensão desse Princípio, ver [7] p. 10.

Portanto $t(x)$ é o máximo divisor comum de $a(x)$ e $b(x)$.

(Prova da unicidade)

Vamos provar que $t(x)$ é o único máximo divisor comum de $a(x)$ e $b(x)$.

Suponhamos que $d(x)$ seja qualquer máximo divisor comum de $a(x)$ e $b(x)$. Para provar a unicidade, devemos mostrar que $d(x) = t(x)$. Como $d(x)$ é máximo divisor comum, então existem polinômios $f(x), g(x) \in F[X]$, tais que $a(x) = d(x) \cdot f(x)$ e $b(x) = d(x) \cdot g(x)$. Portanto,

$$t(x) = a(x) \cdot u(x) + b(x) \cdot v(x)$$

$$t(x) = [d(x) \cdot f(x)] \cdot u(x) + [d(x) \cdot g(x)] \cdot v(x)$$

$$t(x) = d(x)[f(x) \cdot u(x) + g(x) \cdot v(x)]$$

Pelo Teorema 2.1.16, temos o seguinte:

$$Gr(t(x)) = Gr(d(x)) + Gr([f(x) \cdot u(x) + g(x) \cdot v(x)])$$

Como $t(x)$ e $d(x)$ são máximos divisores comuns, então $Gr(t(x)) = Gr(d(x))$. Consequentemente,

$$Gr([f(x) \cdot u(x) + g(x) \cdot v(x)]) = 0$$

Assim $f(x) \cdot u(x) + g(x) \cdot v(x) = c$ para alguma constante $c \in F$. Portanto, $t(x) = d(x) \cdot c$. Como $d(x)$ e $t(x)$ são polinômios mônicos, o coeficiente líder do lado esquerdo da igualdade é 1_F e o do lado direito é c, então devemos ter $c = 1_F$. Portanto, $d(x) = t(x) = a(x) \cdot u(x) + b(x) \cdot v(x)$ é o único máximo divisor comum de $a(x)$ e $b(x)$. □

Corolário 2.1.27. *Sejam F um corpo e $a(x), b(x) \in F[X]$, ambos não nulos. Um polinômio mônico $d(x) \in F[X]$ é o máximo divisor comum de $a(x)$ e $b(x)$ se, e somente se, $d(x)$ satisfaz as seguintes condições:*

(i) *$d(x) \mid a(x)$ e $d(x) \mid b(x)$.*

(ii) *Se $c(x) \mid a(x)$ e $c(x) \mid b(x)$, então $c(x) \mid d(x)$.*

Demonstração. Primeiramente suponhamos que $d(x)$ é o máximo divisor comum de $a(x)$ e $b(x)$, e provaremos que $d(x)$ satisfaz as condições **(i)** e **(ii)**.

Como $d(x)$ é o máximo divisor comum de $a(x)$ e $b(x)$, então pela definição de máximo divisor comum, $d(x)$ satisfaz a propriedade **(1)**, que é igual a condição **(i)**.

Então $d(x)$ satisfaz a condição **(i)**. Além disso, pelo Teorema 2.1.26 existem polinômios $u(x), v(x) \in F[X]$ tais que $d(x) = a(x) \cdot u(x) + b(x) \cdot v(x)$.

Suponha que $c(x) \in F[X]$ tal que $c(x) \mid a(x)$ e $c(x) \mid b(x)$, então pelo Item **(5)** do Teorema 2.1.24 $c(x) \mid a(x) \cdot u(x) + b(x) \cdot v(x)$.

Assim temos que $c(x) \mid d(x)$, então $d(x)$ satisfaz a condição **(ii)**.

Reciprocamente, suponhamos que $d(x)$ é um polinômio mônico que satisfaz as condições **(i)** e **(ii)**, e provaremos que $d(x)$ é o máximo divisor comum entre $a(x)$ e $b(x)$, ou seja, que $d(x)$ satisfaz as propriedades **(1)** e **(2)** da definição de máximo divisor comum.

Por hipótese $d(x)$ satisfaz a condição **(i)**, que é igual a propriedade **(1)**, portanto $d(x)$ satisfaz **(1)**.

Suponha que $c(x) \in F[X]$ tal que $c(x) \mid a(x)$ e $c(x) \mid b(x)$, então pela hipótese, ou seja, a condição **(ii)**, temos que $c(x) \mid d(x)$. Pelo Teorema 2.1.24, temos que $Gr(c(x)) \leq Gr(d(x))$. Assim $d(x)$ tem a propriedade **(2)**. Portanto $d(x)$ é máximo divisor comum entre $a(x)$ e $b(x)$.

□

Os polinômios $a(x)$ e $b(x)$ são chamados primos entre si, se o máximo divisor comum de $a(x)$ e $b(x)$ é igual a 1_F.

O próximo corolário é uma versão do Lema de Gauss [7] p.82-83 para polinômios com coeficientes em um corpo.

Corolário 2.1.28. *Sejam F um corpo e $a(x), b(x), c(x) \in F[X]$. Se $a(x) \mid b(x) \cdot c(x)$ e $a(x)$ e $b(x)$ são primos entre si, então $a(x) \mid c(x)$.*

Demonstração. Como $a(x) \mid b(x) \cdot c(x)$, então existe $r(x) \in F[X]$ tal que $b(x) \cdot c(x) = a(x) \cdot r(x)$. Como o máximo divisor comum entre $a(x)$ e $b(x)$ é igual a 1_F. Pelo Teorema 2.1.26, existem $u(x), v(x) \in F[X]$ tais que

$$a(x) \cdot u(x) + b(x) \cdot v(x) = 1_F.$$

Multiplicando por $c(x)$ ambos os lados da igualdade acima, temos que

$$c(x) = a(x) \cdot c(x) \cdot u(x) + b(x) \cdot c(x) \cdot v(x).$$

Substituindo $b(x) \cdot c(x)$ por $a(x) \cdot r(x)$ nesta última igualdade, temos que

$$c(x) = a(x) \cdot c(x) \cdot u(x) + a(x) \cdot r(x) \cdot v(x)$$

$$c(x) = a(x) \cdot [c(x) \cdot u(x) + r(x) \cdot v(x)]$$

Portanto, $a(x) \mid c(x)$. $\square$

Definição 2.1.29. *Seja F um corpo e $a(x), b(x) \in F[X]$, ambos não nulos. O mínimo múltiplo comum (mmc) de $a(x)$ e $b(x)$ é o polinômio mônico de menor grau que é múltiplo tanto $a(x)$ e $b(x)$.*

Em outras palavras, $m(x)$ é o mínimo múltiplo comum (mmc) de $a(x)$ e $b(x)$ desde que $m(x)$ é mônico, e tenha as seguintes propriedades:

(I) *$a(x) \mid m(x)$ e $b(x) \mid m(x)$;*

(II) *Se $a(x) \mid c(x)$ e $b(x) \mid c(x)$, então o $Gr(m(x)) \leq Gr(c(x))$.*

Teorema 2.1.30. *Sejam F um corpo e $a(x), b(x) \in F[X]$, ambos não nulos, com o coeficientes líderes a e b respectivamente, e sendo $q(x)$ é o quociente da divisão de $a(x) \cdot b(x)$ pelo $mdc(a(x), b(x))$. Então existe um único mínimo múltiplo comum entre $a(x)$ e $b(x)$, que é*

$$mmc(a(x), b(x)) = q(x) \cdot a^{-1} \cdot b^{-1}.$$

Demonstração. **Prova da Existência**

Primeiramente, denotaremos por $d(x)$ o $mdc(a(x), b(x))$, e como $d(x) \mid a(x)$, pelo Item **(4)** do Teorema 2.1.24, temos que $d(x) \mid a(x) \cdot b(x)$, assim podemos escrever $a(x) \cdot b(x) = d(x) \cdot q(x)$, como $d(x)$ é mônico e o coeficiente líder de $a(x) \cdot b(x)$ é igual a $a \cdot b$, então o coeficiente líder de $q(x)$ é igual a $a \cdot b$. Assim $q(x) \cdot a^{-1} \cdot b^{-1}$ é mônico.

Assim, para provar que $m(x) = q(x) \cdot a^{-1} \cdot b^{-1}$ é o $mmc(a(x), b(x))$, devemos mostrar que $m(x)$ satisfaz as duas propriedades da definição de mínimo múltiplo comum.

Multiplicando os dois lados da igualdade $m(x) = q(x) \cdot a^{-1} \cdot b^{-1}$ por $d(x)$ temos o seguinte:

$$d(x) \cdot m(x) = d(x) \cdot q(x) \cdot a^{-1} \cdot b^{-1},$$
$$d(x) \cdot m(x) = a(x) \cdot b(x) \cdot a^{-1} \cdot b^{-1}.$$

Como $b(x) = d(x) \cdot h(x)$ para algum $h(x) \in F[X]$, temos

$$d(x) \cdot m(x) = a(x) \cdot d(x) \cdot h(x) \cdot a^{-1} \cdot b^{-1}.$$

Além disso, $F[X]$ é um domínio de integridade, então vale a lei do cancelamento da multiplicação, Teorema 1.1.21, com isso

$$m(x) = a(x) \cdot h(x) \cdot a^{-1} \cdot b^{-1}.$$

Portanto $a(x) \mid m(x)$. Um argumento semelhante mostra que $b(x) \mid m(x)$. Assim provamos a primeira propriedade:

$$\textbf{(I)}\ a(x) \mid m(x) \text{ e } b(x) \mid m(x).$$

Seja $c(x) \in F[X]$ tal que

$$a(x) \mid c(x) \text{ e } b(x) \mid c(x)$$

ou seja,

$$c(x) = a(x) \cdot f(x) \text{ para algum } f(x) \in F[X],$$
$$c(x) = b(x) \cdot g(x) \text{ para algum } g(x) \in F[X].$$

Pelo Teorema 2.1.26, existem $u(x), v(x) \in F[X]$ tais que

$$d(x) = a(x) \cdot u(x) + b(x) \cdot v(x)$$

Multiplicando os dois lados da igualdade acima por $c(x)$ temos o seguinte:

$$c(x) \cdot d(x) = c(x) \cdot a(x) \cdot u(x) + c(x) \cdot b(x) \cdot v(x)$$

$$c(x) \cdot d(x) = b(x) \cdot g(x) \cdot a(x) \cdot u(x) + a(x) \cdot f(x) \cdot b(x) \cdot v(x)$$

$$c(x) \cdot d(x) = a(x) \cdot b(x) \cdot [g(x) \cdot u(x) + f(x) \cdot v(x)]$$

$$c(x) \cdot d(x) = d(x) \cdot q(x) \cdot [g(x) \cdot u(x) + f(x) \cdot v(x)]$$

$$c(x) = q(x) \cdot [g(x) \cdot u(x) + f(x) \cdot v(x)]$$

Portanto $q(x) \mid c(x)$, e pelo Item **(1)** do Teorema 2.1.24, temos que $a^{-1} \cdot b^{-1} \cdot q(x) \mid c(x)$, ou seja, $m(x) \mid c(x)$. Agora pelo Item **(7)** temos que $Gr(m(x)) \leq Gr(c(x))$. Assim provamos a segunda propriedade:

$$\textbf{(II)}\ \text{Se } a(x) \mid c(x) \text{ e } b(x) \mid c(x), \text{ então o } Gr(m(x)) \leq Gr(c(x))$$

Portanto $m(x) = q(x) \cdot a^{-1} \cdot b^{-1}$ é mínimo múltiplo comum de $a(x)$ e $b(x)$.

Prova da unicidade

Vamos provar que $m(x)$ é o único mínimo múltiplo comum entre $a(x)$ e $b(x)$.

Suponhamos que $t(x)$ seja qualquer mínimo múltiplo comum entre $a(x)$ e $b(x)$. Para provar a unicidade, devemos mostrar que $m(x) = t(x)$, na demonstração de existência do $mmc(a(x), b(x))$, demonstramos que $m(x)$ divide todos os múltiplos comuns de $a(x)$ e $b(x)$, em particular $m(x) \mid t(x)$, ou seja, $t(x) = m(x) \cdot f(x)$ para algum $f(x) \in F[X]$. Assim pelo Teorema 2.1.16 temos

$$Gr(t(x)) = Gr(m(x)) + Gr(f(x))$$

Como $t(x)$ e $m(x)$ são mínimos múltiplos comuns, então o $Gr(t(x)) = Gr(m(x))$, consequentemente $Gr(f(x)) = 0$.

Assim $f(x) = c$ para alguma constante $c \in F$. Portanto, $t(x) = m(x) \cdot c$. Como $m(x)$ e $t(x)$ são polinômios mônicos, o coeficiente líder do lado esquerdo da igualdade é 1_F e o do lado direito é c, então devemos ter $c = 1_F$. Portanto $t(x) = m(x) = q(x) \cdot a^{-1} \cdot b^{-1}$ é o único mínimo múltiplo comum de $a(x)$ e de $b(x)$.

□

Capítulo 3

Irredutibilidade

Neste capítulo, estudaremos a definição de polinômio irredutível, as raízes dos polinômios e fatoração única.

Quando F é um corpo, o anel de domínio de integridade $F[X]$ apresentam várias semelhanças algébricas com o anel $\mathbb{Z}$ do números inteiros. Por exemplo, o conceito de polinômio irredutível corresponde, no anel do números inteiros, ao número primo.

3.1 Irredutibilidade

Nesta seção, estudaremos um conceito muito importante que é o da irredutibilidade de um polinômio com coeficientes em um corpo, e teremos como referências as obras [10] e [8].

Para o desenvolvimento do presente trabalho precisamos da seguinte definição.

Definição 3.1.1. *Um elemento a em um anel comutativo com identidade A, será chamado de associado de um elemento $b \in A$, se $a = b \cdot u$ para alguma unidade $u \in A$.*

Note que se a é associado a b, então b é associado a a, pois $b = a \cdot u^{-1}$ e u^{-1} é uma unidade. Por exemplo no anel dos números inteiros $\mathbb{Z}$, os únicos associados de um número inteiro n são n e $-n$, porque somente 1 e -1 são as unidades em $\mathbb{Z}$.

Teorema 3.1.2. *Se F é um corpo e $a(x), b(x) \in F[X]$, então $a(x)$ é associado a $b(x)$ se, e somente se, $a(x) = b(x) \cdot c$ para algum polinômio constante não nulo c.*

Demonstração. Primeiramente suponhamos que $a(x)$ é associado a $b(x)$, ou seja, $a(x) = b(x)\cdot u(x)$ onde $u(x)$ é uma unidade de $F[X]$. Pelo Corolário 2.1.17 as unidades em $F[X]$ são os polinômios constantes não nulos, assim $a(x) = b(x) \cdot c$ para algum polinômio não nulo c.

Reciprocamente, se $a(x) = b(x)\cdot c$ para algum polinômio constante não nulo c, então novamente pelo Corolário 2.1.17, c é uma unidade em $F[X]$. Portanto $a(x)$ é associado a $b(x)$. □

No anel dos números inteiros $\mathbb{Z}$, um número diferente de zero p é primo, se não for ± 1, ou seja, p não é uma unidade de $\mathbb{Z}$, e seus únicos divisores são ± 1 (as unidades) e $\pm p$ (os associados de p). Se F é um corpo, então as unidades em $F[X]$ são os polinômios constantes não nulos, assim temos a seguinte definição de polinômio irredutível.

Definição 3.1.3. *Seja F um corpo. Um polinômio não constante $p(x) \in F[X]$ é considerado irredutível se seus únicos divisores são seus associados e os polinômios constantes não nulos (as unidades). Um polinômio não constante que não é irredutível é chamado de redutível.*

Exemplo 3.1.4. *Considere o polinômio $f(x) = 5x+1$ em $\mathbb{R}$, pelo Item **(7)** do Teorema 2.1.24 os divisores de $f(x)$ são de grau 0 ou 1. Os divisores de $f(x)$ de grau 0 são polinômios constantes não nulos. Se $g(x)$ é um divisor de $f(x)$ de grau 1, então, $5x + 1 = g(x) \cdot h(x)$, como isso o $Gr(h(x)) = 0$, de modo que $h(x) = c$, então $g(x) = c^{-1} \cdot (5x + 1)$, assim $g(x)$ é um associado de $f(x)$. Portanto, $f(x)$ é irredutível em $\mathbb{R}[X]$.*

Seja F um corpo, podemos concluir com uma argumentação semelhante do Exemplo 3.1.4 a generalização de que todo polinômio de grau 1 em $F[X]$ é irredutível em $F[X]$, conforme vê-se no Teorema 3.1.5.

Teorema 3.1.5. *Seja F um corpo, então todo polinômio de grau 1 pertencente a $F[X]$ é irredutível em $F[X]$.*

Demonstração. Argumentação semelhante ao do Exemplo 3.1.4 . □

Teorema 3.1.6. *Seja F um corpo. Um polinômio não nulo $f(x)$ é redutível em $F[X]$ se, e somente se, $f(x)$ pode ser escrito como produto de dois polinômios de grau menor.*

Demonstração. Primeiramente, suponha que $f(x)$ é redutível em $F[X]$, então $f(x)$ tem um divisor $g(x) \in F[X]$ que não é associado a $f(x)$ e não é um polinômio constante

não nulo, ou seja, $f(x) = g(x) \cdot h(x)$. Se $g(x)$ ou $h(x)$ tem o mesmo grau de $f(x)$, então pelo Teorema 2.1.16 um deles tem grau igual 0. Como um polinômio de grau 0 é um polinômio constante não nulo em $F[X]$, isso significa que $g(x)$ é um polinômio constante não nulo ou um associado de $f(x)$, ou seja, contrário a hipótese. Portanto tanto $g(x)$ como $h(x)$ tem grau menor que $f(x)$.

Reciprocamente, suponha que $f(x)$ pode ser escrito como produto de dois polinômios de grau menor, ou seja, $f(x) = g(x) \cdot h(x)$, onde $Gr(g(x)) < Gr(f(x))$ e $Gr(h(x)) < Gr(f(x))$, então $Gr(g(x)) \neq 0$ e $Gr(h(x)) \neq 0$, assim $g(x)$ e $h(x)$ são polinômios não constantes não nulos. Se $g(x)$ é um associado de $f(x)$, então pelo Teorema 3.1.2 temos que $g(x) = f(x) \cdot c$ para algum polinômio constante não nulo c, e pelo Teorema 1.1.21 temos o seguinte:

$$\begin{aligned} 1_F \cdot f(x) &= g(x) \cdot h(x) \\ 1_F \cdot f(x) &= f(x) \cdot c \cdot h(x) \\ 1_F &= c \cdot h(x) \end{aligned}$$

Assim $Gr(1_F) = Gr(c) + Gr(h(x))$, e como $Gr(1_F) = Gr(c) = 0$. Com isso $Gr(h(x)) = 0$, o que não pode ocorrer. Portanto $g(x)$ não pode ser associado de $f(x)$, com argumento semelhante $h(x)$ também não pode ser associado de $f(x)$. Portanto $f(x)$ é redutível em $F[X]$. □

Exemplo 3.1.7. *O polinômio $f(x) = x^2 + 1$ é irredutível em $\mathbb{Q}[X]$. Porque se fosse redutível pelo Teorema 3.1.6 teríamos $x^2 + 1 = (ax + b) \cdot (cx + d)$ com $a, b, c, d \in \mathbb{Q}$, então $x^2+1 = acx^2+(ad+bc)x+bd$, e pela igualdade de polinômios teríamos o seguinte sistema:*

$$\begin{cases} ac = 1 \\ ad + bc = 0 \\ bd = 1 \end{cases}$$

Resolvendo o sistema temos que $bc = \sqrt{-1}$, mas $\sqrt{-1} \notin \mathbb{Q}$, logo não existem $b, c \in \mathbb{Q}$, tais que $bc = \sqrt{-1}$. Portanto não existe em $\mathbb{Q}[X]$ dois polinômios de grau menor que $f(x)$, cuja o produto seja igual a $f(x)$.

A irredutibilidade de um polinômio não é absoluta, depende do corpo dos coeficientes dos polinômios que está sendo analisada a sua irredutibilidade. Por exemplo, o polinômio $f(x) = x^2 + 1$ é redutível em $\mathbb{C}[X]$, porque $x^2 + 1 = (x + i)(x - i)$, e como $(x + i)$ e $(x - i)$ não são polinômios constantes e nem associados a $f(x)$, então $f(x)$ é redutível em $\mathbb{C}[X]$. Mas pelo Exemplo 3.1.7 $f(x)$ é irredutível em $\mathbb{Q}[X]$.

Teorema 3.1.8. *Sejam F um corpo e $p(x)$ um polinômio não constante em $F[X]$. Então, as seguintes condições são equivalentes:*

(1) *$p(x)$ é irredutível.*

(2) *Se $b(x)$ e $c(x)$ são polinômios tais que $p(x) \mid b(x) \cdot c(x)$, então $p(x) \mid b(x)$ ou $p(x) \mid c(x)$.*

(3) *Se $r(x)$ e $s(x)$ são polinômios tais que $p(x) = r(x) \cdot s(x)$, então $r(x)$ ou $s(x)$ é um polinômio constante não nulo.*

Demonstração. Vamos provar que a condição **(1)** implica a condição **(2)**, suponhamos que $p(x)$ é irredutível, como $mdc(p(x), b(x))$ é um divisor de $p(x)$, então as únicas possibilidades são $mdc(p(x), b(x)) = c$ para algum polinômio constante não nulo c ou $mdc(p(x), b(x)) = f(x)$ com $f(x)$ sendo um associado de $p(x)$. Se $mdc(p(x), b(x)) = c$ para algum polinômio constante não nulo c, como por definição o máximo divisor comum é mônico, com isso $mdc(p(x), b(x)) = 1_F$ e como por hipótese $p(x) \mid b(x) \cdot c(x)$, então pelo Corolário 2.1.28 $p(x) \mid c(x)$. Se $mdc(p(x), b(x)) = f(x)$ com $f(x)$ sendo um associado de $p(x)$, como $f(x) \mid b(x)$, então $b(x) = f(x) \cdot g(x)$ para algum $g(x) \in F[X]$, como pelo Teorema 3.1.2 temos que $f(x) = p(x) \cdot c$ para algum polinômio constante não nulo c, com isso $b(x) = p(x) \cdot c \cdot g(x)$, assim $p(x) \mid b(x)$. Portanto em todo caso $p(x) \mid b(x)$ ou $p(x) \mid c(x)$.

Vamos provar que a condição **(2)** implica a condição **(3)**, se $p(x) = r(x) \cdot s(x)$, então pela condição **(2)** $p(x) \mid r(x)$ ou $p(x) \mid s(x)$. Se $p(x) \mid r(x)$, logo $r(x) = p(x) \cdot v(x)$ para algum $v(x) \in F[X]$, então $p(x) = r(x) \cdot s(x) = p(x) \cdot v(x) \cdot s(x)$. Como $F[X]$ é um domínio de integridade, podemos pelo Teorema 1.1.21 cancelar $p(x)$ e concluir que $v(x) \cdot s(x) = 1_F$. Assim $s(x)$ é uma unidade, e pelo Corolário 2.1.17 é um polinômio constante não nulo. Um argumento semelhante mostra que se $p(x) \mid s(x)$, então $r(x)$ é um polinômio constante não nulo.

Vamos provar que a condição **(3)** implica a condição **(1)**, seja $c(x)$ qualquer divisor de $p(x)$, ou seja, $p(x) = c(x) \cdot d(x)$ para algum $d(x) \in F[X]$, então pela condição **(3)**, $c(x)$ ou $d(x)$ é um polinômio constante não nulo. Se $d(x) = d \neq 0_F$, então $p(x) = c(x) \cdot d$, agora multiplicando os dois lados da igualdade por d^{-1}, temos que $c(x) = d^{-1} \cdot p(x)$, como d^{-1} é uma unidade temos que $c(x)$ é um associado de $p(x)$. Assim em todo caso, $c(x)$ é um polinômio constante não nulo ou um associado de $p(x)$. Portanto, $p(x)$ é irredutível. □

Corolário 3.1.9. *Sejam F um corpo e $p(x)$ irredutível em $F[X]$. Se $p(x) \mid a_1(x) \cdot a_2(x) \cdots a_n(x)$, então $p(x)$ divide pelo menos um dos $a_i(x)$.*

Demonstração. Se $p(x) \mid a_1(x) \cdot (a_2(x) \cdots a_n(x))$, então pelo Teorema 3.1.8, $p(x) \mid a_1(x)$ ou $p(x) \mid a_2(x) \cdot (a_3(x) \cdots a_n(x))$. Se $p(x) \mid a_1(x)$ nós terminamos aqui. Se $p(x) \mid a_2(x) \cdot (a_3(x) \cdots a_n(x))$, então pelo Teorema 3.1.8 novamente, $p(x) \mid a_2(x)$ ou $p(x) \mid a_3(x) \cdot (a_4(x) \cdots a_n(x))$. Se $p(x) \mid a_2(x)$ nós terminamos aqui. Caso contrário, continuemos esse processo, usando o Teorema 3.1.8 repetidamente. Após no máximo n etapas, deve haver um $a_i(x)$ que seja divisível por $p(x)$. □

3.2 Raízes de Polinômios

Nesta seção, estudaremos o conceito de raiz de um polinômio e sua relação com a redutibilidade ou irredutibilidade do polinômio, e teremos como referências as obras [10], [8] e [2].

Seja R um anel comutativo, a função polinomial associada ao polinômio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_2 x^2 + a_1 x + a_0 \in R[X]$ é a função $f : R \to R$ com a seguinte regra:

$$f(r) = a_n r^n + a_{n-1} r^{n-1} + \cdots a_2 r^2 + a_1 r + a_0 \text{ para todo } r \in R.$$

Definição 3.2.1. *Sejam R um anel comutativo e $f(x) \in R[X]$. Se $\alpha \in R$ é tal que $f(\alpha) = 0_R$, ou seja, α anula a função polinomial associada ao polinômio $f(x)$, então α é dita uma raiz de $f(x)$ em R.*

Exemplo 3.2.2. *As raízes do polinômio $f(x) = 5x + 1 \in \mathbb{Q}[X]$, são os números racionais, tal que $f(r) = 0$ onde $r \in \mathbb{Q}$, ou seja, solução da equação $5x + 1 = 0$, que é o número racional $-\frac{1}{5}$. Assim, uma raiz de $f(x)$ é $-\frac{1}{5}$.*

Com argumento semelhante ao do Exemplo 3.2.2, podemos provar que se F é um corpo e $f(x) = ax + b \in F[X]$, ou seja, é um polinômio de grau 1 em $F[X]$, então sempre terá uma única raiz em F. De fato, como $a, b \in F$ com $a \neq 0_F$, então $-\frac{b}{a} \in F$ é a única raiz, pois, $f(-\frac{b}{a}) = a(-\frac{b}{a}) + b = 0_F$.

Exemplo 3.2.3. *O polinômio $f(x) = x^2 + 1 \in \mathbb{R}$ não tem raízes em $\mathbb{R}$ porque não existem soluções reais da equação $x^2 + 1 = 0$. No entanto, se $f(x) = x^2 + 1$ for considerado como um polinômio em $\mathbb{C}[X]$, então tem raízes, porque i e $-i$ são soluções em $\mathbb{C}$ da equação $x^2 + 1 = 0$.*

Teorema 3.2.4. *Sejam F um corpo, $f(x) \in F[X]$ e $a \in F$. O resto da divisão de $f(x)$ por $x - a$ é o valor de $f(a)$.*

Demonstração. Pelo algoritmo da divisão, $f(x) = (x-a)\cdot q(x)+r(x)$, onde o polinômio do resto $r(x)$ é igual a 0_F ou possui grau menor que o divisor $x-a$, ou seja, $Gr(r(x) = 0$ ou $r(x) = 0_F$. Em ambos os casos, $r(x) = c$ para algum $c \in F$. Portanto, $f(x) = (x - a) \cdot q(x) + c$, de modo que $f(a) = (a - a) \cdot q(x) + c = 0_F + c = c$. □

Exemplo 3.2.5. *Vamos encontrar o resto da divisão de $f(x) = x^{100} + 2x^{74} + 3x^{36} + 5$ por $x - 1$, para isso basta aplicar o Teorema 3.2.4 com $a = 1$. Portanto o resto é*

$$f(1) = 1^{100} + 2 \cdot 1^{74} + 3 \cdot 1^{36} + 5 = 11.$$

Teorema 3.2.6. *Sejam F um corpo, $f(x) \in F[X]$ e $a \in F$. Então a é uma raiz do polinômio $f(x)$ se, e somente se, $x - a$ é um fator de $f(x)$ em $F[X]$.*

Demonstração. Primeiramente, suponhamos que a é uma raiz de $f(x)$. Então, temos pelo algoritmo da divisão que $f(x) = (x - a) \cdot q(x) + r(x)$, e pelo Teorema 3.2.4 temos que $f(x) = (x - a) \cdot q(x) + f(a)$, e como a é uma raiz de $f(x)$, então $f(a) = 0_F$, assim $f(x) = (x - a) \cdot q(x)$. Portanto, $x - a$ é um fator de $f(x)$.

Reciprocamente, suponhamos que $x - a$ é um fator de $f(x)$, ou seja, $f(x) = (x - a) \cdot g(x)$ para algum $g(x) \in F[X]$. Então, a é uma raiz de $f(x)$, porque $f(a) = (a - a) \cdot g(x) = 0_F \cdot g(x) = 0_F$. □

Corolário 3.2.7. *Sejam F um corpo e $f(x)$ um polinômio não nulo de grau n em $F[X]$. Então $f(x)$ tem no máximo n raízes em F.*

Demonstração. Se $f(x)$ tem uma raiz a_1 em F, então pelo Teorema 3.2.6, $f(x) = (x - a_1) \cdot h_1(x)$ para algum $h_1(x) \in F[X]$. Se $h_1(x)$ tem uma raiz a_2 em F, então novamente pelo Teorema 3.2.6 , $f(x) = (x-a_1)\cdot(x-a_2)\cdot h_2(x)$ para algum $h_2(x) \in F[X]$. Se $h_2(x)$ tem uma raiz a_3 em F, repetimos o procedimento e continuamos fazendo o procedimento até chegar a uma dessas situações:

(1) $f(x) = (x - a_1) \cdot (x - a_2) \cdots (x - a_n) \cdot h_n(x)$

(2) $f(x) = (x - a_1) \cdot (x - a_2) \cdots (x - a_k) \cdot h_k(x)$ e $h_k(x)$ não tem raiz em F.

No caso **(1)**, pelo Teorema 2.1.16, temos

$$\begin{aligned} Gr(f(x)) &= Gr(x-a_1) + Gr(x-a_2) + \cdots + Gr(x-a_n) + Gr(h_n(x)) \\ n &= 1 + 1 + \cdots + 1 + Gr(h_n(x)) \\ n &= n + Gr(h_n(x)) \end{aligned}$$

Assim, $Gr(h_n(x)) = 0$, então $h_n(x) = c$ para alguma constante $c \in F$ e $f(x)$ tem como fatores

$$f(x) = c \cdot (x - a_1) \cdot (x - a_2) \cdots (x - a_n).$$

Claramente, os n números $a_1, a_2, \ldots, a_n$ são as únicas raízes de $f(x)$ em F.

No caso **(2)**, argumentando da mesma forma, somente substituindo n por k, chegaremos a seguinte conclusão:

$$n = Gr(f(x) = k + Gr(h_k(x)).$$

Portanto o número de raízes é k, que é menor ou igual a n.

□

Corolário 3.2.8. *Sejam F um corpo e $f(x) \in F[X]$, com $Gr(f(x)) \geq 2$. Se $f(x)$ é irredutível em $F[X]$, então $f(x)$ não tem raízes em F.*

Demonstração. Se $f(x)$ é irredutível, então não possui fator da forma $x - a$ em $F[X]$. Portanto, pelo Teorema 3.2.6, $f(x)$ não tem raízes em F. □

A reciproca do Corolário 3.2.8 geralmente não é verdadeira, por exemplo, $f(x) = x^2 + 5x + 6$ é redutível em $\mathbb{R}[X]$, pois temos

$$f(x) = x^4 + 5x^2 + 6 = (x^2 + 2)(x^2 + 3).$$

Mas as raízes de $x^2 + 2$ e $x^2 + 3$ não são números reais, ou seja, $f(x)$ não tem raízes em $\mathbb{R}$.

No entanto, a reciproca é verdadeira para polinômios de graus 2 e 3, conforme o Corolário 3.2.9.

Corolário 3.2.9. *Sejam F um corpo e $f(x) \in F[X]$ um polinômio de grau 2 ou 3. Então $f(x)$ é irredutível em $F[X]$ se, e somente se, $f(x)$ não tiver raízes em F.*

Demonstração. Primeiramente, suponhamos que $f(x)$ é irredutível. Então pelo Corolário 3.2.8, $f(x)$ não tem raízes em F.

Reciprocamente, suponhamos que $f(x)$ não tenha raízes em F. Então $f(x)$ não tem fator de primeiro grau em $F[X]$, porque todo polinômio de primeiro grau $ax + b$ em

$F[X]$ tem uma raiz em F. Portanto, se $f(x) = r(x) \cdot s(x)$, nem $r(x)$ e nem $s(x)$ possui grau 1, pelo Teorema 2.1.16, $Gr(f(x)) = Gr(r(x)) + Gr(s(x))$. Como o grau de $f(x)$ é 2 ou 3, então as únicas possibilidades para $(Gr(r(x)), Gr(s(x)))$, são $(2,0)$ ou $(0,2)$ e $(3,0)$ ou $(0,3)$. Portanto, $r(x)$ ou $s(x)$ devem ter grau 0, ou seja, $r(x)$ ou $s(x)$ é um polinômio constante não nulo, e pelo Teorema 3.1.8, $f(x)$ é irredutível.

□

Exemplo 3.2.10. *Vamos mostrar que $f(x) = x^3 + x + 1$ é irredutível em $\mathbb{Z}_2[X]$, pelo o Corolário 3.2.9, temos que verificar se $[0], [1] \in \mathbb{Z}_2$ é raiz de $f(x)$, como $f([0]) = [0]^3 + [0] + [1] = [1]$ e $f([1]) = [1]^3 + [1] + [1] = [1]$, então $f(x)$ é irredutível em $\mathbb{Z}_2[X]$.*

Corolário 3.2.11. *Seja F um corpo e $f(x) \in F[X]$, com $Gr(f(x)) \geq 2$. Se $f(x)$ tiver uma raiz em F, então $f(x)$ é redutível em $F[X]$.*

Demonstração. Se $a \in F$ é uma raiz de $f(x)$, então pelo Teorema 3.2.6, $x - a$ divide $f(x)$, ou seja, $f(x) = (x-a) \cdot g(x)$ para algum $g(x) \in F[X]$, pelo Teorema 2.1.16 temos que:

$$Gr(f(x)) = Gr(x - a) + Gr(g(x))$$

$$Gr(f(x)) = 1 + Gr(g(x))$$

Mas $Gr(f(x)) \geq 2$, então $Gr(g(x)) \geq 1$, assim $f(x)$ pode ser escrito como produto de dois polinômios de grau menor. Portanto pelo Teorema 3.1.6, $f(x)$ é redutível.

□

3.3 Fatoração única

Nesta seção, estudaremos a fatoração única dos polinômios com coeficientes em um corpo F em polinômios irredutíveis. Apresentaremos uma forma para o cálculo do máximo divisor comum e do mínimo múltiplo comum de dois polinômios. Utilizaremos como referências as obras [10], [8] e [7].

Teorema 3.3.1. *Seja F um corpo. Cada polinômio não constante em $F[X]$ é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $F[X]$. Esta escrita é única no seguinte sentido: Se*

$$f(x) = p_1(x) \cdot p_2(x) \cdots p_r(x) \text{ e } f(x) = q_1(x) \cdot q_2(x) \cdots q_s(x).$$

com cada $p_i(x)$ e $q_i(x)$ irredutível, então $r = s$, ou seja, o número de polinômios irredutíveis é o mesmo. Após, se necessário, os $q_i(x)$ serem reordenados e remarcados, temos

$$p_i(x) \text{ é um associado a } q_i(x) \ (i = 1, 2, 3, \ldots, r).$$

Demonstração. Vamos provar que $f(x) \in F[X]$ sendo um polinômio não constante é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $F[X]$, considere $Gr(f(x)) = n$, temos que $n \geq 1$, faremos a demonstração por indução completa sobre n.

No caso de $n = 1$, pelo Teorema 3.1.5, $f(x)$ é irredutível, portanto a propriedade é válida.

Suponhamos que a propriedade é válida para todo polinômio de grau menor que n, ou seja, nossa hipótese de indução é que qualquer polinômio em $F[X]$ de grau menor que n é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $F[X]$. Se $f(x)$ é irredutível em $F[X]$, nada temos que fazer. Caso contrário, $f(x)$ é redutível em $F[X]$, portanto pelo Teorema 3.1.6, $f(x)$ pode ser escrito com produto de dois polinômios de grau menor, ou seja, $f(x) = g(x) \cdot h(x)$ onde $Gr(g(x)) < n$ e $Gr(h(x)) < n$. Agora, aplicamos a hipótese de indução em $g(x)$ e $h(x)$, ou seja, que $g(x)$ ou $h(x)$ é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $F[X]$. Assim $f(x)$ é irredutível ou pode ser escrito como produto de polinômios irredutíveis em $F[X]$, então a propriedade é válida para n.

Portanto pelo princípio da indução completa a propriedade é válida para todo $n \geq 1$.

Vamos provar que está fatoração é única, a menos da ordem de fatores, suponhamos que $f(x) = p_1(x) \cdot p_2(x) \cdots$
$p_r(x) = q_1(x) \cdot q_2(x) \cdots q_s(x)$ com $p_i(x)$ e $q_j(x)$ irredutíveis. Como $p_1(x) \cdot [p_2(x) \cdots p_r(x)]$ $= q_1(x) \cdot q_2(x) \cdots q_s(x)$, logo $p_1(x) \mid q_1(x) \cdot q_2(x) \cdots q_s(x)$, e pelo Corolário 3.1.9 temos que $p_1(x) \mid q_j(x)$ para algum j. Após reorganização e renumeração dos $q_j(x)'s$, se for necessário, podemos assumir que $p_1(x) \mid q_1(x)$. Como $q_1(x)$ é irredutível, então $p_1(x)$ deve ser um polinômio constante ou um associado de $q_1(x)$. No entanto, $p_1(x)$ é irredutível, e pela definição de polinômio irredutível não pode ser um polinômio constante. Portanto, $p_1(x)$ é um associado de $q_1(x)$, com $p_1(x) = c_1 \cdot q_1(x)$ para algum polinômio constante c_1. Portanto

$$q_1(x) \cdot [c_1 \cdot p_2(x) \cdot p_3(x) \cdots p_r(x)] = p_1(x) \cdot p_2(x) \cdots p_r(x) = q_1(x) \cdot q_2(x) \cdots q_s(x)$$

Pelo Teorema 1.1.21 podemos cancelar $q_1(x)$, temos

$$p_2(x) \cdot [c_1 \cdot p_3(x) \cdots p_r(x)] = q_2(x) \cdot q_3(x) \cdots q_s(x)$$

Usando o mesmo argumento com relação a $p_2(x)$, teremos

$$p_3(x) \cdot [c_1 \cdot c_2 \cdot p_4(x) \cdots p_r(x)] = q_3(x) \cdot q_4(x) \cdots q_s(x)$$

Continuamos dessa maneira, usando repetidamente o mesmo argumento e eliminando um polinômio irredutível de cada lado da igualdade a cada etapa. Se $r = s$, então esse processo prova a unicidade da escrita. Então para completar a demonstração do teorema, devemos mostrar que $r = s$. Provaremos por contradição que $r = s$, vamos assumir que $r \neq s$, ou seja, $r < s$ ou $r > s$, e mostraremos que essa suposição leva a uma contradição.

Primeiro, suponha que $r > s$, após as etapas do processo anterior, todas os $q_j(x)'s$ serão eliminados e teremos o seguinte

$$c_1 \cdot c_2 \cdots c_s \cdot p_{s+1}(x) \cdot p_{s+2}(x) \cdots p_r(x) = 1_F$$

Isto mostra que $p_r(x) \mid 1_F$, pelo Item **(7)** do Teorema 2.1.24, então $Gr(p_r(x)) \leq Gr(1_F) = 0$, assim $Gr(p_r(x)) = 0$, mas $p_r(x)$ é irredutível e pela definição de polinômio irredutível, temos que $Gr(p_r(x) \geq 1$, logo chegamos a uma contradição. Portanto, $r > s$ não pode ocorrer. Um argumento semelhante mostra que a suposição $r < s$ também leva a uma contradição e, portanto não pode ocorrer. Portanto, $r = s$ é a única possibilidade.

□

Corolário 3.3.2. *Sejam F um corpo e $f(x) \in F[X]$ um polinômio não constante. Então, existem polinômios mônicos irredutíveis $p_1(x), p_2(x), \ldots, p_r(x)$ distintos, $a \in F$ não nulo e números naturais $n_1 \geq 1, n_2 \geq 1, \ldots, n_r \geq 1$, tais que*

$$f(x) = a \cdot p_1(x)^{n_1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r}$$

Essa expressão é única, a menos da ordem dos fatores.

Demonstração. Pelo Teorema 3.3.1, existem polinômios irredutíveis $q_1(x), q_2(x), \ldots, q_s(x)$ tais que $f(x) = q_1(x) \cdot q_2(x) \cdots q_s(x)$. Sejam $a_1, a_2, \ldots, a_s$ os coeficientes líderes de $q_1(x), q_2(x), \ldots, q_s(x)$ respectivamente, e $p_1(x) = a_1^{-1} \cdot q_1(x), p_2(x) = a_2^{-1} \cdot q_2(x), \ldots, p_s(x) = a_s^{-1} \cdot q_s(x)$, assim os $p_i(x)$ são polinômios mônicos irredutíveis. Como $q_i(x) = a_i \cdot p_i(x)$ temos

$$f(x) = a_1 \cdot p_1(x) \cdot a_2 \cdot p_2(x) \cdots a_s \cdot p_s(x)$$

Fazendo $a = a_1 \cdot a_2 \cdots a_s$ e agrupando os $p_i(x)$ iguais, temos

$$f(x) = a \cdot p_1(x)^{n_1} \cdot p_2(x)^{n_2} \cdots p_r(x)^{n_r} \text{ com } r \leq s.$$

A unicidade da expresão, a menos da ordem dos fatores, decorre da unicidade do Teorema 3.3.1. □

Proposição 3.3.3. *Seja F um corpo e $p(x), q(x) \in F[X]$ polinômios mônicos irredutíveis distintos. Então*

$$mdc(p(x), q(x)) = 1_F$$

Demonstração. Sendo $p(x)$ e $q(x)$ irredutíveis, como $mdc(p(x), q(x))$ é um divisor de $p(x)$ e de $q(x)$, então as únicas possibilidades são $mdc(p(x), q(x)) = c$ para algum polinômio constante não nulo c ou $mdc(p(x), q(x)) = f(x)$ com $f(x)$ sendo um associado de $p(x)$ e de $p(x)$. Se $mdc(p(x), q(x)) = c$ para algum polinômio constante não nulo c, como por definição o máximo divisor comum é mônico, então $mdc(p(x), q(x)) = 1_F$. Se $mdc(p(x), q(x)) = f(x)$ com $f(x)$ sendo um associado de $p(x)$ e de $p(x)$, pelo Teorema 3.1.2 temos que $f(x) = p(x) \cdot c$ para algum polinômio constante não nulo c e $f(x) = q(x) \cdot d$ para algum polinômio constante não nulo d, como por definição de máximo divisor comum $f(x)$ é mônico e por hipótese $p(x)$ e $q(x)$ são mônicos distintos, então temos que $c = d = 1$, assim, $p(x) = q(x)$ o que contradiz a hipótese. Portanto, a única possibilidade é $mdc(p(x), q(x)) = 1_F$. □

Quando estivermos lidando com a fatoração em polinômios mônicos irredutíveis de dois, ou mais, polinômios não constantes, usaremos o recurso de acrescentar fatores da forma $p_i(x)^0 = 1_F$, onde $p_i(x)$ é um polinômio mônico irredutível qualquer. Assim, dados $f(x), g(x) \in F[X]$ polinômios não constantes quaisquer, podemos escrever

$$f(x) = a \cdot p_1(x)^{\alpha_1} \cdots p_n(x)^{\alpha_n} \text{ e } g(x) = b \cdot p_1(x)^{\beta_1} \cdots p_n(x)^{\beta_n} \text{ com } a, b \in F$$

usando o mesmo conjunto de polinômios mônicos irredutíveis $p_1(x), \ldots, p_n(x)$, desde que permitimos que os expoentes $\alpha_1, \alpha_2, \ldots, \alpha_n$ e $\beta_1, \beta_2, \ldots, \beta_n$ variem em $\mathbb{N}$.

Proposição 3.3.4. *Sejam F um corpo e $f(x) = a \cdot p_1(x)^{\alpha_1} \cdots p_n(x)^{\alpha_n} \in F[X]$ um polinômio não constante escrito na forma acima. Se $f^1(x) \in F[X]$ é um divisor de $f(x)$, então*

$$f^1(x) = b \cdot p_1(x)^{\beta_1} \cdots p_n(x)^{\beta_n}$$

onde $0 \leq \beta_i \leq \alpha_i$ para $i = 1, \ldots n$ e $b \in F$.

Demonstração. Seja $f^1(x)$ um divisor de $f(x)$ e seja $p(x)^\beta$ a potência de um polinômio mônico irredutível $p(x)$ que esteja na decomposição de $f^1(x)$ em polinômios mônicos irredutíveis na forma do Corolário 3.3.2. Então $p(x)^\beta \mid f(x)$, segue que $p(x)^\beta$ divide algum $p_i(x)^{\alpha_i}$, por ser primo com os demais $p_j(x)^{\alpha_j}$, conforme Proposição 3.3.3, e, consequentemente, $p(x) = p_i(x)$ e $0 \leq \beta \leq \alpha_i$, e como $p_i(x)^\beta \mid f(x)$ então pelo Item **(1)** do Teorema 2.1.24 para todo $b \in F$, temos que $b \cdot p_i(x)^\beta \mid f(x)$. □

Se denotarmos por $d_m(f(x))$ o número dos polinômios mônicos que divide $f(x)$, com uma contagem fácil utilizando a Proposição 3.3.4, temos que

$$d_m(f(x)) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1).$$

Podemos usar um método semelhante ao algoritmo de Euclides para determinar o máximo divisor comum mas a fatoração única em polinômios mônicos irredutíveis de um polinômio não constante em $F[X]$, onde F é um corpo, nos permite determinar facilmente o máximo divisor comum e o mínimo múltiplo comum de dois polinômios não constantes.

Teorema 3.3.5. *Seja F um corpo e seja $f(x), g(x) \in F[X]$ polinômios não constantes, então $f(x) = a \cdot p_1(x)^{\alpha_1} \cdot p_2(x)^{\alpha_2} \cdots p_n(x)^{\alpha_n}$ e $g(x) = b \cdot p_1(x)^{\beta_1} \cdot p_2(x)^{\beta_2} \cdots p_n(x)^{\beta_n}$ com $p_i(x) \in F[X]$ polinômios mônicos irredutíveis, $a, b \in F$ não nulos e $\alpha_i, \beta_i \geq 0$. Pondo*

$$\gamma_i = min\{\alpha_i, \beta_i\},\ \delta_i = max\{\alpha_i, \beta_i\},\ i = 1, 2, \ldots, n,$$

tem-se que

$$mdc(f(x), g(x)) = p(x)_1^{\gamma_1} \cdots p(x)_n^{\gamma_n} \text{ e } mmc(f(x), g(x)) = p(x)_1^{\delta_1} \cdots p(x)_n^{\delta_n}.$$

Demonstração. É claro, pela Proposição 3.3.4, que $p(x)_1^{\gamma_1} \cdots p(x)_n^{\gamma_n}$ é divisor comum de $f(x)$ e $g(x)$, e, é um polinômio mônico. Se $c(x)$ é um divisor comum de $f(x)$ e $g(x)$, então $c(x) = c \cdot p_1(x)^{\epsilon_1} \cdots p_n(x)^{\epsilon_n}$, onde $\epsilon_i \leq min\{\alpha_i, \beta_i\}$ e $c \in F$ e, portanto, $c(x) \mid p(x)_1^{\gamma_1} \cdots p(x)_n^{\gamma_n}$ e pelo Corolário 2.1.27, $mdc(f(x), g(x)) = p(x)_1^{\gamma_1} \cdots p(x)_n^{\gamma_n}$.

Seja $q(x)$ o quociente da divisão de $f(x) \cdot g(x)$ por $mdc(f(x), f(x))$, e como foi provado anteriormente $mdc(f(x), g(x)) = p(x)_1^{\gamma_1} \cdots p(x)_n^{\gamma_n}$, logo $q(x) = a \cdot b \cdot p(x)_1^{\delta_1} \cdots p(x)_n^{\delta_n}$. Pelo Teorema 2.1.30, o $mmc(f(x), g(x)) = q(x) \cdot a^{-1} \cdot b^{-1}$. Portanto, temos que

$$mmc(f(x), g(x)) = a \cdot b \cdot p(x)_1^{\delta_1} \cdots p(x)_n^{\delta_n} \cdot a^{-1} \cdot b^{-1} = p(x)_1^{\delta_1} \cdots p(x)_n^{\delta_n}.$$

□

Exemplo 3.3.6. *Vamos calcular o máximo divisor comum e o mínimo múltiplo comum dos polinômios* $f(x) = 2x^3 - 10x^2 + 16x - 8$ *e* $g(x) = 4x^2 - 20x + 24$ *pertencentes a* $\mathbb{Q}[X]$.

Fatorando em polinômios mônicos irredutíveis temos que

$$f(x) = 2(x-2)^2(x-1) \text{ e } g(x) = 4(x-3)(x-2)$$

Reescrevendo $f(x)$ *e* $g(x)$ *usando o mesmo conjunto de polinômios mônicos irredutíveis* $(x-2), (x-1)$ *e* $(x-3)$ *temos*

$$f(x) = 2(x-3)^0(x-2)^2(x-1)^1 \text{ e } g(x) = 4(x-3)^1(x-2)^1(x-1)^0.$$

Pelo Teorema 3.3.5 temos que

$$\begin{aligned} mdc(f(x), g(x)) = &\quad (x-3)^0(x-2)^1(x-1)^0 = (x-2) \\ mmc(f(x), g(x)) = &\quad (x-3)^1(x-2)^2(x-1)^1 = x^4 - 8x^3 + 23x^2 - 28x + 12 \end{aligned}$$

3.4 Critérios de Irredutibilidade

Nesta seção, estudaremos alguns dos critérios de irredutibilidade dos polinômios com os coeficientes nos corpos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

Veremos que os critérios de irredutibilidade podem variar de acordo com o corpo dos coeficientes dos polinômios que está sendo estudado, os quais possuem características específicas.

3.4.1 Irredutibilidade em $\mathbb{Q}[X]$

Nesta subseção estudaremos alguns dos testes e alguns dos critérios para determinação da irredutibilidade de algum polinômio em $\mathbb{Q}[X]$, e teremos como referências as obras [10], [8] e [2].

Primeiramente, devemos observar um fato muito importante, que será muito utilizado nesta seção.

Se $f(x) \in \mathbb{Q}[X]$, então $c \cdot f(x)$ tem como coeficientes números inteiros, para algum número inteiro $c \neq 0$.

Exemplo 3.4.1. *Seja o polinômio*

$$f(x) = \tfrac{1}{6}x^6 + \tfrac{1}{4}x^3 + \tfrac{5}{3}x + 2$$

O mínimo múltiplo comum dos denominadores dos coeficiente de $f(x)$ *é* 12*, assim os coeficientes de* $12 \cdot f(x)$ *são números inteiros, pois*

$$12 \cdot f(x) = 12 \cdot [\tfrac{1}{6}x^6 + \tfrac{1}{4}x^3 + \tfrac{5}{3}x + 2] = 2x^6 + 3x^3 + 20x + 24.$$

Pelo Teorema 3.2.6 para encontrar os fatores de grau 1 de um polinômio $f(x) \in \mathbb{Q}[X]$ é equivalente a encontrar as raízes de $f(x)$ em $\mathbb{Q}$. Agora, $f(x)$ tem as mesmas raízes de $c \cdot f(x)$, para qualquer $c \neq 0 \in \mathbb{Q}$. Quando c é escolhido para que $c \cdot f(x)$ tenha como coeficientes números inteiros, podemos encontrar as raízes de $f(x)$ em $\mathbb{Q}$, utilizando o seguinte teste.

Teorema 3.4.2. (Teste da Raiz Racional)

Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *um polinômio com coeficientes de números inteiros e* $\alpha = \frac{r}{s}$ *com* $mdc(r, s) = 1$*. Se* α *for uma raiz de* $f(x)$*, então* $r \mid a_0$ *e* $s \mid a_n$*.*

Demonstração. Como $\alpha = \frac{r}{s}$ é raiz de $f(x)$, segue que

$$a_n(\tfrac{r}{s})^n + a_{n-1}(\tfrac{r}{s})^{n-1} + \cdots + a_1(\tfrac{r}{s}) + a_0 = 0$$

Multiplicando ambos os lados da igualdade por s^n temos

$$a_n r^n + a_{n-1}r^{n-1}s + \cdots a_1 r s^{n-1} + a_0 s^n = 0$$

Logo

$$a_0 s^n = -r(a_n r^{n-1} + a_{n-1}r^{n-2}s + \cdots + a_1 s^{n-1})$$

Portanto, $r \mid a_0 s^n$.

Como $mdc(r, s) = 1$, então $mdc(r, s^n) = 1$, e pelo Lema de Gauss (para uma melhor compreensão desse lema, ver [7] p.82-83), temos que $r \mid a_0$.

Um processo análogo nos fornece a seguinte igualdade

$$a_n r^n = -s(a_{n-1}r^{n-1} + \cdots + a_1 r s^{n-2} + a_0 s^{n-1}).$$

Portanto, $s \mid a_n r^n$.

Como $mdc(r, s) = 1$, então $mdc(r^n, s) = 1$, e pelo Lema de Gauss, temos que $s \mid a_n$. □

Exemplo 3.4.3. *Vamos mostrar que o polinômio* $f(x) = x^3 + 6x^2 + 7x - 1$ *é irredutível em* $\mathbb{Q}[X]$*. Pelo Teorema 3.4.2 temos que* r *é um divisor de* -1 *e* s *é um divisor de* 1*. Logo as possibilidades para* $\alpha = \frac{r}{s}$ *é* 1 *e* -1*.*

Desta forma temos que 1 *e* -1 *são as únicas possíveis raízes de* $f(x)$ *em* $\mathbb{Q}$. *Mas é fácil verificar que* 1 *e nem* -1 *são raízes de* $f(x)$. *Portanto pelo Corolário 3.2.9* $f(x)$ *é irredutível em* $\mathbb{Q}[X]$.

Se $f(x) \in \mathbb{Q}[X]$, então $c \cdot f(x)$ possui coeficientes inteiros, para algum número número inteiro não nulo c. Qualquer fatoração de $c \cdot f(x)$ em $\mathbb{Z}[X]$ leva à fatoração de $f(x)$ em $\mathbb{Q}[X]$. Então parece que testes de irredutibilidade em $\mathbb{Q}[X]$ podem ser restritos a polinômios com coeficientes inteiros. No entanto, devemos primeiro excluir a possibilidade de que um polinômio com coeficientes inteiros pode ser fatorado em $\mathbb{Q}[X]$ mas não pode ser fatorado em $\mathbb{Z}[X]$.

Lema 3.4.4. *Seja* $f(x), g(x), h(x) \in \mathbb{Z}[X]$ *com* $f(x) = g(x) \cdot h(x)$. *Se* p *é um número primo que divide todos os coeficientes de* $f(x)$, *então* p *divide todos os coeficientes de* $g(x)$ *ou* p *divide todos os coeficientes de* $h(x)$.

Demonstração. Seja $f(x) = a_k x^k + \cdots + a_1 x + a_0, g(x) = b_m x^m + \cdots + b_1 x + b_0$, e $h(x) = c_n x^n + \cdots + c_1 x + c_0$. A prova será por contradição. Se o lema é falso, então p não divide algum coeficiente de $g(x)$ e também não divide algum coeficiente de $h(x)$. Seja b_r o primeiro coeficiente de $g(x)$ que não é divisível por p, e seja c_s o primeiro coeficiente de $h(x)$ que não é divisível por p. Então $p \mid b_i$ para $i < r$ e $p \mid c_j$ para $j < s$. Considere o coeficiente a_{r+s} do $f(x)$. Como $f(x) = g(x) \cdot h(x)$ temos

$$a_{r+s} = b_0 c_{r+s} + \cdots + b_{r-1} c_{s+1} + b_r c_s + b_{r+1} c_{s-1} + \cdots b_{r+s} c_0$$

Consequentemente,

$$b_r c_s = a_{r+s} - [b_0 c_{r+s} + \cdots + b_{r-1} c_{s+1}] - [b_{r+1} c_{s-1} + \cdots b_{r+s} c_0].$$

Agora, por hipótese $p \mid a_{r+s}$. Além disso, p divide cada termo do primeiro colchete porque $p \mid b_i$ para $i < r$, e p divide cada termo do segundo colchete porque $p \mid c_j$ para $j < s$. Como p divide cada termo do lado direito, então $p \mid b_r c_s$. Portanto como p é um número primo, então $p \mid b_r$ ou $p \mid c_s$. Isso contradiz o fato de que nem b_r e nem c_s é divisível por p.

□

Teorema 3.4.5. *Seja* $f(x)$ *um polinômio com coeficientes inteiros. Então* $f(x)$ *pode ser fatorado em produto de polinômios de graus* m *e* n *em* $\mathbb{Q}[X]$ *se, e somente se,* $f(x)$ *pode ser fatorado em produto de polinômios de graus* m *e* n *em* $\mathbb{Z}[X]$.

Demonstração. Obviamente, se $f(x)$ pode ser fatorado em $\mathbb{Z}[X]$, então pode ser fatorado em $\mathbb{Q}[X]$. Por outro lado, suponhamos que $f(x) = g(x) \cdot h(x)$ em $\mathbb{Q}[X]$. Seja c e d números inteiros diferentes de zero, de modo que $cg(x)$ e $dh(x)$ tenha coeficientes inteiros. Então $cdf(x) = cg(x) \cdot dh(x)$ em $\mathbb{Z}[X]$ com $Gr(cg(x)) = Gr(g(x))$ e $Gr(dh(x)) = Gr(h(x))$. Seja p qualquer número primo divisor de cd, ou seja, $cd = pt$ para algum $t \in \mathbb{Z}$. Então p divide todos os coeficientes de $cdf(x)$. Pelo Lema 3.4.4, p divide todos os coeficientes de $cg(x)$ ou todos os coeficientes de $dh(x)$, digamos que seja os coeficientes de $cg(x)$, então $cg(x) = pk(x)$ com $k(x) \in \mathbb{Z}[X]$ e $Gr(k(x)) = Gr(g(x))$. Portanto,

$$ptf(x) = cdf(x) = [cg(x)] \cdot [dh(x)] = [pk(x)] \cdot [dh(x)]$$

Cancelando p temos

$$tf(x) = k(x) \cdot [dh(x)] \text{ em } \mathbb{Z}[X].$$

Agora repetindo o mesmo argumento com qualquer divisor primo de t e cancelando esse número primo em ambos lados da igualdade. Continuando esse processo até cada fator primo de cd for cancelado. Então do lado esquerdo da igualdade teremos $\pm f(x)$ e do lado direito teremos um produto de dois polinômios em $\mathbb{Z}[X]$, um com o mesmo grau de $g(x)$ e outro com o mesmo grau de $h(x)$.

□

Seja $f(x) \in \mathbb{Q}[X]$, se multiplicamos $f(x)$ pelo mínimo múltiplo comum dos coeficientes de $f(x)$ obtemos $f_1(x) \in \mathbb{Z}[X]$. O Teorema 3.4.5 nos diz que a irredutibilidade de $f(x)$ em $\mathbb{Q}[X]$ é equivalente a irredutibilidade de $f_1(x)$ em $\mathbb{Z}[X]$.

Exemplo 3.4.6. *Vamos mostrar que* $f(x) = \frac{1}{10}x^4 - x^2 + \frac{1}{10}$ *é irredutível em* $\mathbb{Q}[X]$.

Como $mmc(10, 1) = 10$, *temos que* $10 \cdot f(x) = 10[\frac{1}{10}x^4 - x^2 + \frac{1}{10}] = x^4 - 10x^2 + 1$. *Como consequência do Teorema 3.4.5, se* $10 \cdot f(x)$ *é irredutível em* $\mathbb{Z}[X]$, *então* $10 \cdot f(x)$ *é irredutível em* $\mathbb{Q}[X]$ *e portanto* $f(x)$ *é irredutível em* $\mathbb{Q}[X]$. *Assim é suficiente provar que* $10 \cdot f(x)$ *é irredutível em* $\mathbb{Z}[X]$. *A prova será por contradição. Se* $10 \cdot f(x)$ *é redutível em* $\mathbb{Z}[X]$, *então a fatoração de* $10 \cdot f(x)$ *somente pode ser de dois tipos: o produto de um polinômio de grau* 1 *com outro de grau* 3 *ou o produto de dois polinômios de grau* 2.

Se existe um polinômio de grau 1 *que divide* $10 \cdot f(x)$, *isso que dizer que* $10 \cdot f(x)$ *tem uma raiz racional. Pelo Teorema 3.4.2, as únicas possíveis raízes racionais de* $10 \cdot f(x)$ *são* ± 1, *podemos ver facilmente que nem* 1 *e nem* -1 *são raízes de* $10 \cdot f(x)$.

Logo uma possível fatoração de $10 \cdot f(x)$ *é o produto de polinômios de grau* 2. *Seja* $10 \cdot f(x) = (ax^2 + bx + c)(dx^2 + ex + f)$ *com* $a, b, c, d, e, f \in \mathbb{Z}$. *Fazendo a distributiva e comparando os coeficientes, temos que*

$$ad = 1 \quad ae + bd = 0 \quad af + be + cd = -10 \quad bf + ce = 0 \quad cf = 1$$

Como $ae + bd = 0$ *e* $bf + ce = 0$, *então* $ae = -bd$ *e* $bf = -ce$. *Agora, como* $ad = 1$ *e* $cf = 1$, *então* $a = d = 1$ *ou* $a = d = -1$ *e* $c = f = 1$ *ou* $c = f = -1$. *Em todo caso temos que* $e = -b$, *assim temos que*

$$\begin{aligned} -10 = &\quad af + be + cd \\ -10 = &\quad af - b^2 + cd \\ b^2 = &\quad 10 + af + cd \end{aligned}$$

Agora temos quatro situações a considerar:

Se $a = d = 1$ *e* $c = f = 1$, *então temos*

$$\begin{aligned} b^2 = &\quad 10 + 1 + 1 \\ b^2 = &\quad 12 \end{aligned}$$

Se $a = d = 1$ *e* $c = f = -1$, *então temos*

$$\begin{aligned} b^2 = &\quad 10 - 1 - 1 \\ b^2 = &\quad 8 \end{aligned}$$

Se $a = d = -1$ *e* $c = f = 1$, *então temos*

$$\begin{aligned} b^2 = &\quad 10 - 1 - 1 \\ b^2 = &\quad 8 \end{aligned}$$

Se $a = d = -1$ *e* $c = f = -1$, *então temos*

$$\begin{aligned} b^2 = &\quad 10 + 1 + 1 \\ b^2 = &\quad 12 \end{aligned}$$

Como não existe um número inteiro cujo o quadrado é 8 *ou* 12. *Assim, a fatoração em produto de dois polinômios de grau* 2 *é impossível. Portanto,* $10 \cdot f(x)$ *é irredutível em* $\mathbb{Z}[X]$, *e consequentemente,* $f(x)$ *é irredutível em* $\mathbb{Q}[X]$.

Outro critério de irredutibilidade muito útil é o seguinte:

Teorema 3.4.7. (Critério de Eisenstein)

Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *um polinômio não constante com coeficientes inteiros. Se houver um número* p *primo, tal que* p *divide cada um dos* $a_0, a_1, \ldots, a_{n-1}$, *mas* p *não divide* a_n *e* p^2 *não divide* a_0, *então* $f(x)$ *é irredutível em* $\mathbb{Q}[X]$.

Demonstração. A prova é por contradição. Se $f(x)$ é redutível em $\mathbb{Q}[X]$, então pelo Teorema 3.4.5, $f(x)$ redutível em $\mathbb{Z}[X]$, digamos

$$f(x) = (b_0 + b_1x + \cdots + b_rx^r) \cdot (c_0 + c_1x + \cdots + c_sx^s)$$

Com $b_i, c_j \in \mathbb{Z}, r \geq 1$, e $s \geq 1$, além disso $n = r + s$. Note que $a_0 = b_0c_0$. Por hipótese $p \mid a_0$, pelo Lema de Gauss, temos que $p \mid b_0$ ou $p \mid c_0$. Como p^2 não divide a_0 segue que p divide apenas um dos inteiros b_0, c_0. Vamos admitir sem perda de generalidade, que $p \mid b_0$ e p não divide c_0.

Temos que $a_n = b_rc_s$, e como p não divide a_n, então p não divide b_r. Como podemos ter outros b_i que não seja divisível por p também. Seja b_k o primeiro dos b_i que não seja divisível por p, então $0 < k \leq r < n$ e $p \mid b_i$ para $i < k$ e p não divide b_k.

Pela regra de multiplicação do polinômios,

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0,$$

De forma que

$$b_kc_0 = a_k - b_0c_k - b_1c_{k-1} - \cdots - b_{k-1}c_1.$$

Como $p \mid a_k$ e $p \mid b_i$ para $i < k$, vemos que p divide cada termo do lado direito da igualdade. Assim, $p \mid b_kc_0$, e pelo Lema de Gauss, temos que $p \mid b_k$ ou $p \mid c_0$. Isso contradiz o fato de que nem b_k e nem c_0 é divisível por p. Portanto $f(x)$ é irredutível em $\mathbb{Z}[X]$, e consequentemente $f(x)$ é irredutível em $\mathbb{Q}[X]$.

□

Exemplo 3.4.8. *Vamos mostrar que o polinômio* $f(x) = x^{50} + 9x^{37} + 15x^{24} + 12x^{15} + 6x + 3$ *é irredutível em* $\mathbb{Q}[X]$.

Considere $p = 3$, *observe que* $p \mid 9, p \mid 0, p \mid 15, p \mid 12, p \mid 6$ *e* $p \mid 3$, *além disso* p *não divide* 1, *e* p^2 *não divide* 3. *Logo, utilizando o Teorema 3.4.7, ou seja, o Critério de Eisenstein, temos que* $f(x) = x^{50} + 9x^{37} + 15x^{24} + 12x^{15} + 6x + 3$ *é irredutível em* $\mathbb{Q}[X]$.

Exemplo 3.4.9. *Vamos mostrar que o polinômio da forma* $x^n + p$, *onde* p *é um número inteiro primo, é irredutível em* $\mathbb{Q}[X]$.

Observe que $p \mid p$ *e* $p \mid 0$, *além disso* p *não divide* 1, *e* p^2 *não divide* p. *Logo, utilizando o Teorema 3.4.7, ou seja, o Critério de Eisenstein, temos que* $x^n + p$ *é irredutível em* $\mathbb{Q}[X]$.

O Exemplo 3.4.9 mostra que existem polinômios de todos os graus, exceto de grau 0, que são irredutíveis em $\mathbb{Q}[X]$.

Um dos métodos para provar que um polinômio é irredutível sobre $\mathbb{Z}[x]$, e logo sobre $\mathbb{Q}[X]$ também, é considerá-lo módulo p, para algum primo p conveniente e usar a fatoração única de $\mathbb{Z}_p[X]$, pois $\mathbb{Z}_p$ é um corpo. Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0$ um polinômio com coeficientes inteiros, denotaremos por $\bar{f}(x)$ o polinômio $[a_n]x^n + \cdots + [a_1]x + [a_0]$ em $\mathbb{Z}_p[X]$. Por exemplo, se $f(x) = 5x^6 + 9x^5 + 16x^4 + 7x^2 + 1x + 4$ em $\mathbb{Z}[X]$, então em $\mathbb{Z}_3[X]$,

$$\begin{aligned} \bar{f}(x) &= [5]x^6 + [9]x^5 + [16]x^4 + [7]x^2 + [1]x + [4] \\ \bar{f}(x) &= [2]x^6 + [0]x^5 + [1]x^4 + [1]x^2 + [1]x + [1] \\ \bar{f}(x) &= [2]x^6 + [1]x^4 + [1]x^2 + [1]x + [1] \end{aligned}$$

Teorema 3.4.10. *Seja $f(x) = a_k x^k + \cdots + a_1 x + a_0$ um o polinômio com coeficientes inteiros, e seja p um primo positivo que não divide a_k. Se $\bar{f}(x)$ for irredutível em $\mathbb{Z}_p[X]$, então $f(x)$ é irredutível em $\mathbb{Q}[X]$.*

Demonstração. A prova será por contradição, suponhamos que $f(x)$ é redutível em $\mathbb{Q}[X]$. Então pelo Teorema 3.4.5, $f(x) = g(x) \cdot h(x)$ com $g(x)$ e $h(x)$ polinômios não constantes em $\mathbb{Z}[X]$. Como p não divide a_k, que é o coeficiente líder de $f(x)$, então p não divide os coeficientes líderes de $g(x), h(x)$, pois a_k é igual ao produto deles. Consequentemente, $Gr(\bar{g}(x)) = Gr(g(x))$ e $Gr(\bar{h}(x)) = Gr(h(x))$. Em particular nem $\bar{g}(x)$ e nem $\bar{h}(x)$ são polinômios constantes em $\mathbb{Z}_p[X]$.

É fácil verificar que $f(x) = g(x) \cdot h(x)$ em $\mathbb{Z}[X]$ implica que $\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$ em $\mathbb{Z}_p[X]$, isso decorre da definição da multiplicação das classes residuais módulo p. Assim $\bar{f}(x)$ seria redutível em $\mathbb{Z}_p[X]$, uma contradição, pois, por hipótese $\bar{f}(x)$ é irredutível em $\mathbb{Z}_p[X]$. Portanto $f(x)$ deve ser irredutível em $\mathbb{Q}[X]$. □

Exemplo 3.4.11. *Vamos mostrar que o polinômio $f(x) = x^3 + 27x^2 + 17x + 4$ é irredutível em $\mathbb{Q}[X]$.*

Primeiramente, considere $p = 3$ e $\mathbb{Z}_3 = \{[0], [1], [2]\}$, então $\bar{f}(x) = [1]x^3 + [2]x + [1] \in \mathbb{Z}_3[X]$.

Como 3 não divide 1, então pelo Teorema 3.4.10 é suficiente provar que $\bar{f}(x)$ é irredutível $\mathbb{Z}_3[X]$.

Agora, pelo Corolário 3.2.9, basta verificar se $\bar{f}(x)$ não tem raízes em $\mathbb{Z}_3$, como $\bar{f}([0]) = [1][0]^3 + [2][0] + [1] = [1]$, $\bar{f}([1]) = [1][1]^3 + [2][1] + [1] = [1]$ e $\bar{f}([2]) =$

$[1][2]^3 + [2][2] + [1] = [1]$, *com isso* $\bar{f}(x)$ *não tem raízes em* $\mathbb{Z}_3$. *Portanto é* $\bar{f}(x)$ *é irredutível em* $\mathbb{Z}_3[X]$.

Exemplo 3.4.12. *Vamos mostrar que o polinômio* $f(x) = x^4 + 50x^3 + 34x^2 + 25x + 22$ *é irredutível em* $\mathbb{Q}[X]$.

Primeiramente, considere $p = 5$ *e* $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$, *então* $\bar{f}(x) = [1]x^4 + [4]x^2 + [2] \in \mathbb{Z}_5[X]$.

Como 5 *não divide* 1, *então pelo Teorema 3.4.10 é suficiente provar que* $\bar{f}(x)$ *é irredutível em* $\mathbb{Z}_5[X]$.

Primeira observação que fazemos é que $\bar{f}(x) = [1]x^4 + [4]x^2 + [2]$ *não possui raízes em* $\mathbb{Z}_5$. *Assim, se* $\bar{f}(x)$ *é redutível em* $\mathbb{Z}_5[X]$, *então a única forma possível de fatoração de* $\bar{f}(x)$ *é o produto de polinômios de grau* 2, *como* $\bar{f}(x)$ *é mônico, então se existir essa fatoração os polinômios de grau* 2 *são mônicos. Logo temos*

$$(x^2 + ax + b)(x^2 + cx + d) = [1]x^4 + [4]x^2 + [2]$$

com $a, b, c, d \in \mathbb{Z}_5$. *Fazendo a distributiva e comparando os coeficientes, temos*

$$a + c = [0] \quad ac + b + d = [4] \quad bc + ad = [0] \quad bd = [2]$$

Como $a + c = 0$, *então* $a = -c$, *assim temos*

$$[4] = ac + b + d = -c^2 + b + d$$

Como $[1]$ *é o elemento simétrico da adição de* $[4]$ *em* $\mathbb{Z}_5$, *temos o que*

$$c^2 = [1] + b + d$$

Agora, como $bd = [2]$, *temos quatro situação a considerar:*

Se $b = [1]$, *então* $d = [2]$, *assim temos*

$$c^2 = [1] + [1] + [2]$$

$$c^2 = [4]$$

Se $b = [2]$, *então* $d = [1]$, *assim temos*

$$c^2 = [1] + [2] + [1]$$

$$c^2 = [4]$$

Se $b = [3]$, *então* $d = [4]$, *assim temos*

$$c^2 = [1] + [3] + [4]$$

$$c^2 = [3]$$

Se $b = [4]$, *então* $d = [3]$, *assim temos*

$$c^2 = [1] + [4] + [3]$$

$$c^2 = [3]$$

Como em $\mathbb{Z}_5$ *não existe uma classe resídual que elevada ao quadrado é igual a classe do* $[3]$ *e* $[2]^2 = [4]$. *Assim, temos que* $c = [2]$, *então* $a = -[2] = [3]$. *Com isso temos duas possibilidades para* b *e* d, *ou seja,* $b = [1]$ *e* $d = [2]$ *ou* $b = [2]$ *e* $d = [1]$. *Agora usando a igualdade* $bc + ad = [0]$, *a qual implica que* $bc = -ad$, *mas essa igualdade é impossível, pois se* $b = [1]$, *então* $d = [2]$, *assim temos que* $bc = [1][2] = [2]$ *que é diferente de* $-ad = -[3][2] = [-6] = [4]$, *e se* $b = [2]$, *então* $d = [1]$, *assim temos que* $bc = [2][2] = [4]$ *que é diferente de* $-ad = -[3][1] = [-3] = [2]$. *Assim, é impossível a fatoração de* $\bar{f}(x)$ *em um produto de dois polinômios de grau* 2. *Portanto* $\bar{f}(x)$ *é irredutível em* $\mathbb{Z}_5[X]$.

3.4.2 Irredutibilidade em $\mathbb{R}[X]$ e em $\mathbb{C}[X]$

Nesta subseção estudaremos os critérios de irredutibilidade em $\mathbb{R}[X]$ e em $\mathbb{C}[X]$, e teremos como referências as obras [10], [8] e [2].

Diferentemente da situação que ocorre em $\mathbb{Q}[X]$, é possível fornecer uma descrição explicita de todos os polinômios irredutíveis em $\mathbb{C}[X]$ e $\mathbb{R}[X]$. Consequentemente, podemos dizer imediatamente se um polinômio em $\mathbb{C}[X]$ e $\mathbb{R}[X]$ é irredutível sem testes ou critérios elaborados. Esses fatos são uma consequência do seguinte teorema, que foi provado pela primeira vez por Gauss em 1799.

Teorema 3.4.13. O Teorema Fundamental da Álgebra

Todo polinômio não constante em $\mathbb{C}[X]$ *tem uma raiz em* $\mathbb{C}$.

Demonstração. Todas as demonstrações do Teorema Fundamental da Álgebra envolvem Análise, não sendo conhecida nenhuma prova puramente algébrica dele. Portanto, não demonstraremos aqui, uma demonstração pode ser encontrada em [8].

□

Corolário 3.4.14. *Um polinômio é irredutível em* $\mathbb{C}[X]$ *se, e somente se, tiver grau* 1.

Demonstração. O polinômio $f(x)$ de grau maior ou igual a 2 em $\mathbb{C}[X]$ tem uma raiz a em $\mathbb{C}$ pelo Teorema 3.4.13, e como pelo Teorema 3.2.6 o polinômio $x - a$ é um fator de $f(x)$. Portanto, $f(x)$ é redutível em $\mathbb{C}[X]$.

Reciprocamente, pelo Teorema 3.1.5 todo polinômio de grau 1 em $\mathbb{C}[X]$ é irredutível.

□

Portanto, pelo Corolário 3.4.14, que é uma consequência do Teorema Fundamental da Álgebra, os únicos polinômios irredutíveis em $\mathbb{C}[X]$ são os polinômios de grau 1.

Corolário 3.4.15. *Todo polinômio não constante $f(x)$ de grau n em $\mathbb{C}[X]$ pode ser escrito na forma de $c(x-a_1)(x-a_2)\cdots(x-a_n)$ para certos $c, a_1, a_2, \ldots, a_n \in \mathbb{C}$. Essa fatoração é única, exceto pela ordem dos fatores.*

Demonstração. Pelo Teorema 3.3.1, $f(x)$ é um produto de polinômios irredutíveis em $\mathbb{C}[X]$. Como pelo Corolário 3.4.14 os polinômios irredutíveis em $\mathbb{C}[X]$ são de grau 1, e pelo Teorema 2.1.16 há exatamente n polinômios de grau 1. Portanto,

$$\begin{aligned} f(x) = &\quad (r_1x+s_1)(r_2x+s_2)\cdots(r_nx+s_n) \\ f(x) = &\quad r_1(x-(-r_1^{-1}s_1))r_2(x-(-r_2^{-1}s_2))\cdots r_n(x-(-r_n^{-1}s_n)) \\ f(x) = &\quad c(x-a_1)(x-a_2)\cdots(x-a_n) \end{aligned}$$

Onde $c = r_1r_2\cdots r_n$ e $a_i = -r_i^{-1}s_i$. A unicidade decorre do Teorema 3.3.1.

□

Para obter um descrição de todos polinômios irredutíveis em $\mathbb{R}[X]$ precisamos do seguinte lema.

Lema 3.4.16. *Sejam $f(x)$ um polinômio em $\mathbb{R}[X]$ e $a+bi$ uma raiz de $f(x)$ em $\mathbb{C}$, então $a-bi$ também é uma raiz de $f(x)$.*

Demonstração. Se $c = a+bi \in \mathbb{C}$ com $a, b \in \mathbb{R}$, e utilizando $\overline{c}$ para denotar $a-bi$. É fácil verificar que para qualquer $c, d \in \mathbb{C}$ temos:

$$\overline{(c+d)} = \overline{c} + \overline{d} \text{ e } \overline{cd} = \overline{c}\,\overline{d}.$$

Observe também que $\overline{c} = c$ se, e somente se, c for um número real. Agora, se $f(x) = a_nx^n + \cdots + a_1x + a_0$ com $a_i \in \mathbb{R}$ e c é uma raiz de $f(x)$, então $f(c) = 0$, de modo que

$$\begin{aligned} 0 = \overline{0} = \overline{f(c)} = &\quad \overline{a_nc^n + \cdots + a_1c + a_0} \\ = &\quad \overline{a_n}\,\overline{c^n} + \cdots + \bar{a_1}\bar{c} + \overline{a_0} \\ = &\quad a_n\overline{c}^n + \cdots + a_1\overline{c} + a_0 \\ = &\quad f(\overline{c}) \end{aligned}$$

Portanto $\overline{c} = a - bi$ também é uma raiz de $f(x)$.

□

Teorema 3.4.17. *Um polinômio $f(x)$ é irredutível em $\mathbb{R}[X]$ se, e somente se, $f(x)$ é um polinômio de grau 1 ou*

$$f(x) = ax^2 + bx + c \text{ com } b^2 - 4ac < 0.$$

Demonstração. Primeiramente, suponhamos que, $f(x)$ é irredutível em $\mathbb{R}[X]$. Pelo Teorema 3.4.13, $f(x)$ tem uma raiz $\alpha \in \mathbb{C}$. Há duas possibilidades para α, ou seja, $\alpha \in \mathbb{R}$ ou $\alpha \notin \mathbb{R}$. No primeira possibilidade $\alpha \in \mathbb{R}$. Neste caso, $(x - \alpha) \mid f(x)$ pelo Teorema 3.2.6, logo $f(x) = (x - \alpha) \cdot q(x)$ para algum $q(x) \in \mathbb{R}[X]$. Como $f(x)$ é irredutível, assim $q(x)$ é um polinômio constante não nulo, digamos $q(x) = k$ para algum $k \in \mathbb{R}$, assim teremos

$$f(x) = (x - \alpha) \cdot k = kx - k\alpha$$

Portanto, $Gr(f(x)) = 1$.

Na segunda possibilidade $\alpha \notin \mathbb{R}$, ou seja, $\alpha = r + si$, com $s \neq 0$. Neste caso, pelo Lema 3.4.16, $\overline{\alpha}$ também é raiz de $f(x)$. Então $f(x)$ é divisível em $\mathbb{C}[X]$ por $(x - \alpha)$ e $(x - \overline{\alpha})$ e, como

$$\begin{aligned}(x - \alpha)(x - \overline{\alpha}) = &\quad (x - (r + si))(x - (r - si)) \\ (x - \alpha)(x - \overline{\alpha}) = &\quad x^2 - 2rx + (r^2 + s^2)\end{aligned}$$

que é um polinômio com coeficientes reais. Então existe um $g(x) \in \mathbb{C}[X]$ tal que

$$f(x) = [x^2 - 2rx + (r^2 + s^2)] \cdot g(x).$$

Por outro lado, como $x^2 - 2rx + (r^2 + s^2) \in \mathbb{R}[X]$, podemos usar o algoritmo da divisão euclideana em $\mathbb{R}[X]$ para dividir $f(x)$ por $x^2 - 2rx + (r^2 + s^2)$. Se $q(x)$ e $r(x)$ são respectivamente o quociente e o resto, então

$$f(x) = [x^2 - 2rx + (r^2 + s^2)] \cdot q(x) + r(x)$$

Mas, lembrando do fato que $q(x)$ e $r(x)$ também pertence a $\mathbb{C}[X]$ e a unicidade do quociente e resto da divisão euclideana, concluímos que $q(x) = g(x)$ e $r(x) = 0$, e assim $g(x) \in \mathbb{R}[X]$. Então, como $f(x)$ é irredutível em $\mathbb{R}[X]$, portanto $g(x)$ é um polinômio constante não nulo, seja $g(x) = k$ para algum $k \in \mathbb{R}$. Assim obtemos que

$$\begin{aligned} f(x) = &\quad [x^2 - 2rx + (r^2 + s^2)] \cdot g(x) \\ f(x) = &\quad [x^2 - 2rx + (r^2 + s^2)] \cdot k \\ f(x) = &\quad kx^2 - 2rkx + (r^2 + s^2)k. \end{aligned}$$

Mostrando que $Gr(f(x)) = 2$. Além disso, fazendo $a = k, b = -2rk$ e $c = (r^2+s^2)k$ em $f(x)$ temos que

$$b^2 - 4ac = (-2rk)^2 - 4k(r^2 + s^2)k = -4s^2k^2 < 0$$

Uma vez que $s \neq 0$ e $k \neq 0$.

Reciprocamente, se $Gr(f(x)) = 1$, então pelo Teorema 3.1.5, $f(x)$ é irredutível em $\mathbb{R}[X]$. Se $Gr(f(x)) = 2$, e como $b^2 - 4ac < 0$, então $f(x)$ não tem raiz em $\mathbb{R}$. Portanto, pelo Corolário 3.2.9, $f(x)$ é irredutível em $\mathbb{R}[X]$. □

Exemplo 3.4.18. *O polinômio $f(x) = 2x^2 - 4x + 4$ é irredutível em $\mathbb{R}[X]$, pois, $b^2 - 4ac = (-4)^2 - 4 \cdot 2 \cdot 4 = -16 < 0$, conforme Teorema 3.4.17.*

Portanto, não existem polinômios irredutíveis de grau maior que 2 em $\mathbb{R}[X]$. Uma consequência do Teorema 3.4.17, é o próximo corolário, que nós diz que os polinômios de grau ímpar tem pelos menos uma raiz em $\mathbb{R}$.

Corolário 3.4.19. *Todo polinômio $f(x)$ de grau ímpar em $\mathbb{R}[X]$ possui uma raiz em $\mathbb{R}$.*

Demonstração. Pelo Teorema 3.3.1, $f(x) = p_1(x) \cdot p_2(x) \cdots p_k(x)$ com cada $p_i(x)$ irredutível em $\mathbb{R}[X]$. Pelo Teorema 3.4.17 cada p_i possui grau 1 ou 2. Pelo Teorema 2.1.16 temos que

$$Gr(f(x)) = Gr(p_1(x)) + Gr(p_2(x)) + \cdots + Gr(p_k(x)).$$

Como $f(x)$ possui grau ímpar, pelo menos um dos $p_i(x)$ deve ter grau 1. Assim, $f(x)$ possui um fator de primeiro grau em $\mathbb{R}[X]$. Portanto, $f(x)$ tem uma raiz em $\mathbb{R}$. □

Exemplo 3.4.20. *Os polinômios da forma $f(x) = x^3 - a \in \mathbb{R}[X]$, possui uma raiz em $\mathbb{R}$, conforme Corolário 3.4.19. Portanto, todos os números reais possui uma raiz cúbica real.*

Capítulo 4

Algumas Sugestões de Aplicações de Polinômios no Ensino Médio

Neste capítulo, apresentaremos algumas sugestões de aplicações de polinômios e dos conceitos desenvolvidos no presente trabalho que podem ser aplicadas em sala de aula do ensino médio.

Existe muitas abordagem que podem ser feitas sobre o estudo dos polinômios no ensino médio, mas a que é mais utilizada é na resolução de problemas de uma situação problema que consiste em representar o problema por um polinômio e em seguida resolver uma equação algébrica. Outra é utilizar a função polinomial associado ao polinômio que represente o problema é analisar seu gráfico.

Vamos estudar algumas sugestões com diferentes enfoques que podemos dar ao trabalharmos com o conceito de polinômios no ensino médio.

4.1 Estudo da racionalidade de um número

Nesta seção, apresentaremos uma sugestão de aplicação dos polinômios, que é pouca explorada no ensino médio, que é a sua utilização para determinar a racionalidade ou não de um número, e teremos como referência a obra [2]. Assim, temos uma opção de abordagem que pode deixar mais claro para os alunos o conceito de número racional.

Em [2] p.66 menciona que "Muitos alunos tem dificuldade quanto a determinar se

um dado número é racional ou não apenas por uma análise visual"

A aplicação do conceito de polinômio para determinar a racionalidade ou não de um número, consiste em determinar um polinômio $f(x) \in \mathbb{Q}[X]$ de modo que o número α seja raiz e utilizando o Teorema 3.4.2 para determinar se α é ou não uma das possíveis raízes racionais de $f(x)$. Assim, determinando se α é um número racional. Observe os exemplos a seguir:

Exemplo 4.1.1. *Vamos verificar que o número* $\sqrt[6]{11} \notin \mathbb{Q}$.

Tomando $\alpha = \sqrt[6]{11}$ *e elevando ambos os lados da igualdade a* 6, *obtemos* $\alpha^6 = 11$, *assim essa igualdade pode ser escrita como*

$$\alpha^6 - 11 = 0$$

Assim obtemos o polinômio $f(x) = x^6 - 11 \in \mathbb{Q}[X]$ *com coeficientes de números inteiros, sendo que* α *é raiz de* $f(x)$.

Agora utilizando o Teorema 3.4.2, temos que as possíveis raízes racionais de $f(x)$ *são* ± 1 *e* ± 11, *mas é fácil verificar que nenhum destes números são raízes de* $f(x)$, *e como* α *é raiz, então* $\alpha \notin \mathbb{Q}$. *Portanto,* $\sqrt[6]{11} \notin \mathbb{Q}$.

O próximo exemplo mostra que em alguns casos não é tão trivial determinar se um é racional ou não.

Exemplo 4.1.2. *Vamos verificar se o número* $\sqrt[3]{9+4\sqrt{5}} + \sqrt[3]{9-4\sqrt{5}} \in \mathbb{Q}$.

Seja $\alpha = \sqrt[3]{9+4\sqrt{5}} + \sqrt[3]{9-4\sqrt{5}}$. *Elevando ambos os lados da igualdade ao cubo obtemos*

$$\alpha^3 = (\sqrt[3]{9+4\sqrt{5}} + \sqrt[3]{9-4\sqrt{5}})^3 = (\sqrt[3]{9+4\sqrt{5}})^3 + 3(\sqrt[3]{9+4\sqrt{5}})^2(\sqrt[3]{9-4\sqrt{5}}) + 3(\sqrt[3]{9+4\sqrt{5}})(\sqrt[3]{9-4\sqrt{5}})^2 + (\sqrt[3]{9-4\sqrt{5}})^3$$

que podemos reescrever como

$$\alpha^3 = 9 + 4\sqrt{5} + 3(\sqrt[3]{9+4\sqrt{5}} + \sqrt[3]{9-4\sqrt{5}}) \cdot (\sqrt[3]{9+4\sqrt{5}})(\sqrt[3]{9-4\sqrt{5}}) + 9 - 4\sqrt{5}$$

$$\alpha^3 = 18 + 3(\sqrt[3]{9+4\sqrt{5}} + \sqrt[3]{9-4\sqrt{5}}) \cdot (\sqrt[3]{81-80})$$

$$\alpha^3 = 18 + 3(\sqrt[3]{9+4\sqrt{5}} + \sqrt[3]{9-4\sqrt{5}})$$

Agora observando que a soma entre parênteses é o que definimos como sendo α, *assim obtemos*

$$\alpha^3 = 18 + 3\alpha$$
$$\alpha^3 - 3\alpha - 18 = 0$$

Assim obtemos o polinômio $f(x) = x^3 - 3x - 18 \in \mathbb{Q}[X]$ *com coeficientes de números inteiros, para o qual* α *é raiz. Utilizando o Teorema 3.4.2 temos que as possíveis raízes racionais de* $f(x)$ *são* $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9,$ *e* ± 18.

Verificamos que $f(3) = 0$, *ou seja,* 3 *é raiz de* $f(x)$.

Aplicando o algoritmo da divisão de polinômios, vamos obter $q(x) \in \mathbb{Q}[X]$ *tal que* $f(x) = (x-3) \cdot q(x)$.

$$\begin{array}{rl|l} x^3 - 3x - 18 & & x - 3 \\ \cline{3-3} -x^3 + 3x^2 & & x^2 + 3x + 6 \\ \cline{1-1} \quad 3x^2 - 3x - 18 & & \\ -3x^2 + 9x & & \\ \cline{1-1} \quad 6x - 18 & & \\ -6x + 18 & & \\ \cline{1-1} \quad 0 & & \end{array}$$

Obtemos assim $q(x) = x^2 + 3x + 6$, *que nos permite reescrever* $f(x)$ *da seguinte forma*

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

Temos que as raízes de $f(x)$ *são as raízes de* $(x-3)$ *e de* $q(x) = (x^2 + 3x + 6)$, *a raiz de* $x - 3$ *é* 3, *mas* $q(x) = x^2 + 3x + 6$ *não tem raízes reais, pois* $b^2 - 4ac = 3^2 - 4 \cdot 1 \cdot 6 = -15 < 0$, *então pelo Teorema 3.4.17,* $q(x)$ *é irredutível em* $\mathbb{R}[X]$, *e pelo Corolário 3.2.8,* $q(x)$ *não tem raízes em* $\mathbb{R}$. *Como* α *é raiz de* $f(x)$ *e sabemos que* $\alpha \in \mathbb{R}$, *assim temos que*

$$\sqrt[3]{9 + 4\sqrt{5}} + \sqrt[3]{9 - 4\sqrt{5}} = 3$$

Portanto, $\sqrt[3]{9 + 4\sqrt{5}} + \sqrt[3]{9 - 4\sqrt{5}} \in \mathbb{Q}$.

Exemplo 4.1.3. *Vamos verificar que o número* $\sqrt[4]{7 + \sqrt{33}} + \sqrt[4]{7 - \sqrt{33}} \notin \mathbb{Q}$.

Seja $\alpha = \sqrt[4]{7 + \sqrt{33}} + \sqrt[4]{7 - \sqrt{33}}$. *Elevando ambos os lados da igualdade a* 4 *obtemos*

$$\alpha^4 = (\sqrt[4]{7 + \sqrt{33}} + \sqrt[4]{7 - \sqrt{33}})^4$$

desenvolvendo temos

$$\alpha^4 = (\sqrt[4]{7+\sqrt{33}})^4 + 4(\sqrt[4]{7+\sqrt{33}})^3(\sqrt[4]{7-\sqrt{33}}) + 6(\sqrt[4]{7+\sqrt{33}})^2(\sqrt[4]{7-\sqrt{33}})^2 + 4(\sqrt[4]{7+\sqrt{33}})(\sqrt[4]{7-\sqrt{33}})^3 + (\sqrt[4]{7-\sqrt{33}})^4$$

sabendo que

$$4(\sqrt[4]{7+\sqrt{33}})^3(\sqrt[4]{7-\sqrt{33}}) + 4(\sqrt[4]{7+\sqrt{33}})(\sqrt[4]{7-\sqrt{33}})^3 = 4(\sqrt[4]{7+\sqrt{33}} + \sqrt[4]{7-\sqrt{33}})^2 - 8(\sqrt[4]{7+\sqrt{33}})^2(\sqrt[4]{7-\sqrt{33}})^2$$

assim podemos reescrever como

$$\alpha^4 = 7 + \sqrt{33} + 4(\sqrt[4]{7+\sqrt{33}} + \sqrt[4]{7-\sqrt{33}})^2 - 2(\sqrt[4]{7+\sqrt{33}})^2(\sqrt[4]{7-\sqrt{33}})^2 + 7 - \sqrt{33}$$
$$\alpha^4 = 14 + 4(\sqrt[4]{7+\sqrt{33}} + \sqrt[4]{7-\sqrt{33}})^2 - 2(\sqrt[4]{49-33})^2$$
$$\alpha^4 = 14 + 4(\sqrt[4]{7+\sqrt{33}} + \sqrt[4]{7-\sqrt{33}})^2 - 2(\sqrt[4]{16})^2$$
$$\alpha^4 = 14 + 4(\sqrt[4]{7+\sqrt{33}} + \sqrt[4]{7-\sqrt{33}})^2 - 8$$
$$\alpha^4 = 6 + 4(\sqrt[4]{7+\sqrt{33}} + \sqrt[4]{7-\sqrt{33}})^2$$

A igualdade acima, observando que a soma que está entre parênteses é o que definimos como α, pode ser escrita da seguinte forma

$$\alpha^4 = 6 + 4\alpha^2$$
$$\alpha^4 - 4\alpha^2 - 6 = 0$$

Assim obtemos o polinômio $f(x) = x^4 - 4x^2 - 6 \in \mathbb{Q}[X]$ com coeficientes inteiros, para o qual α é raiz. Agora observando que $2 \mid 4, 2 \mid 0$ e $2 \mid 6$, ou seja, 2 é o máximo divisor comum dos coeficientes de $f(x)$ diferentes do coeficiente líder, além disso 2 não divide 1, e 2^2 não divide 6. Logo, utilizando o Teorema 3.4.7, ou seja, o Critério de Eisenstein, temos que $f(x)$ é irredutível em $\mathbb{Q}[X]$, e pelo Corolário 3.2.8, $f(x)$ não tem raízes em $\mathbb{Q}$ e como α é raiz de $f(x)$. Portanto, $\sqrt[4]{7+\sqrt{33}} + \sqrt[4]{7-\sqrt{33}} \notin \mathbb{Q}$.

4.2 Resolução de problemas

Nesta seção, apresentaremos uma sugestão de aplicação dos polinômios que é mais utilizada no ensino médio, que é a resolução de problemas, e teremos como referência a obra [2].

Em [2] p.69 menciona que "Na resolução de situações problemas pode-se fazer necessário o uso da função polinomial definida por um polinômio p(X) para analisar e resolver o problema de acordo com os dados utilizados e que desejamos alcançar", mas

nem sempre as funções obtidas são as de segundo grau, as quais estamos acostumados a trabalhar e calcular suas raízes.

Nestes casos, que obtemos funções polinomiais de grau maior que 2, e como a resolução geralmente consiste em determinar as raízes do polinômio, assim podemos utilizar a fatoração dos polinômios (Teorema 3.3.1) para poder investigar melhor suas raízes, podemos utilizando o teste da raiz racional (Teorema 3.4.2) determinar uma raíz do polinômio e como isso poder reduzir o grau do polinômio, utilizando o algoritmo da divisão de polinômios (Teorema 2.1.19), até que seja possível utilizar alguma das técnicas conhecidas para o cálculo das raízes.

Exemplo 4.2.1. *Queremos construir um poço que tenha o volume igual a* 80.000 *metros cúbicos e que tenha a mesma largura e a mesma profundidade, o qual será construído ao redor de um castelo quadrado que tem* 30 *metros de lado, conforme Figura 4.1. Assim, queremos responder a seguinte pergunta: qual deve ser a menor medida da largura e da profundidade deste poço?*

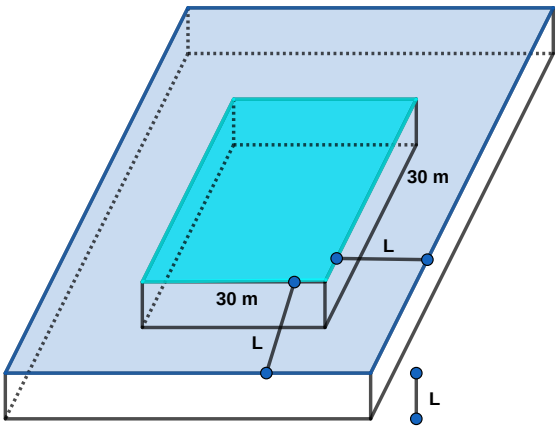


Figura 4.1: *Poço*

Fonte: Própria, 2020.

Para resolução deste problema denotaremos a largura e a profundidade do poço por L.

Podemos determinar o volume deste poço em função de L, ou seja, primeiro calculamos a área do fundo do poço, que é igual a área de quatro retângulos, sendo que dois tem área igual a $(30 + 2 \cdot L) \cdot L$ e os outros dois tem área igual a $30 \cdot L$, e em seguida multiplicamos a área do fundo do poço pela profundidade L para obter o volume do poço. Assim, utilizando a representação polinomial temos que

$$\begin{aligned} V(L) = &\quad ((30 + 2 \cdot L) \cdot L \cdot 2 + 30 \cdot L \cdot 2) \cdot L \\ V(L) = &\quad (60L + 4L^2 + 60L) \cdot L \\ V(L) = &\quad (4L^2 + 120L) \cdot L \\ V(L) = &\quad 4L^3 + 120L^2 \end{aligned}$$

Sabemos que o volume desejado é 80.000 m^3, assim obtemos a seguinte igualdade

$$4L^3 + 120L^2 = 80.000$$

que é equivalente a

$$L^3 + 30L^2 - 20.000 = 0$$

Conforme o enunciado do problema, o que nos interessa é determinar a menor medida que resolve a equação algébrica acima, mais isso é equivante a determinar a menor raiz positiva do polinômio $V_1(x) = x^3 + 30x^2 - 20.000$. Como $V_1 \in \mathbb{Q}[X]$ e tem coeficientes inteiros, aplicaremos o Teorema 3.4.2 que nos diz que as possíveis raízes racionais desse polinômio são os divisores e os simétricos da adição dos divisores de 20.000. Fazendo o teste com os menores divisores positivos de 20.000, que são os números $1, 2, 4, 5, 8, 10, 16, 20, \ldots$, obtemos que $V_1(20) = 0$, logo 20 é raiz, mas o polinômio $V_1(x)$ pode possui até 3 raízes reais pelo fato de $Gr(V_1(x)) = 3$, assim aplicaremos o Teorema 2.1.19 para reduzirmos o seu grau e assim podemos estudar as demais raízes.

$$\begin{array}{rl|l} x^3 + 30x^2 - 20000 & & x - 20 \\ \cline{3-3} -x^3 + 20x^2 & & x^2 + 50x + 1000 \\ \cline{1-1} 50x^2 - 20000 & & \\ -50x^2 + 1000x & & \\ \cline{1-1} 1000x - 20000 & & \end{array}$$

$$\begin{array}{r|l} -1000x + 20000 & \\ \hline 0 & \end{array}$$

Assim, obtemos que $V_1(x) = (x-20)(x^2+50x+1000)$, temos que as raízes de $V_1(x)$ são as raízes de $(x-20)$ e de $x^2+50x+1000$, a raiz de $x-20$ é 20, mas $x^2+50x+1000$ não tem raízes reais, pois $b^2-4ac = 50^2-4\cdot 1\cdot 1000 = -1500 < 0$, então pelo Teorema 3.4.17, $x^2+50x+1000$ é irredutível em $\mathbb{R}[X]$, e pelo Corolário 3.2.8, $x^2+50x+1000$ não tem raízes em $\mathbb{R}$. Logo, a única raíz real de $V_1(x)$ é 20.

Portanto, a menor medida da largura e da profundidade L para que o volume do poço seja igual a 80.000 m^3 é 20 metros.

Considerações finais

O presente trabalho desenvolvido, fornece ao professor do Ensino Médio um material para o seu aprimoramento e sugestões de aplicação em sala de aula. Claro que não é viável a abordagem com o formalismo que foi expostas as teorias desenvolvidas neste trabalho no ensino médio, mas é possível uma abordagem com menos formalidade, a qual daria mais condições para o aluno ter melhor aproveitamento tanto na sala de aula como no Ensino Superior.

A abordagem que foi realizada neste trabalho sobre o conceito de polinômio, usando uma definição de polinômio utilizando o conceito de sequência que é diferente da definição normalmente utilizada no ensino médio, nos possibilita compreender melhor o conceito de polinômio, entender o significado da incógnita x, que é um elemento que não pertence ao anel dos coeficientes do polinômio, e a partir dessa definição mostramos que podemos obter a definição de polinômio normalmente utilizada no ensino médio e entender melhor toda a estrutura algébrica dos polinômios.

Umas das sugestões de aplicações que culminou este trabalho é muito útil para superar a dificuldade que os alunos tem em compreender se um número é racional ou não, em situações que não são tão óbvias, que é a utilização do teste de raiz racional em um polinômio, sabendo que um dado número é raiz deste polinômio, e assim determinar se esse número é racional ou não. Isso, deve provocar a curiosidade dos alunos, pois números que visualmente não demonstravam ser racionais o são.

Por fim, outra sugestão de aplicação que resultou este trabalho, que de maneira geral é aplicável ao cotidiano do aluno, foi a resolução de situações problemas, sabemos que muitas das situações que envolvem um problema no cotidiano podem ser expressas por uma equação polinomial. Nestes casos, na maioria das vezes, para resolver o problema devemos encontrar as raízes do polinômio, assim utilizando a redutibilidade do polinômio com coeficientes em um corpo é possível encontrar suas raízes o que nos permite analisar os possíveis resultados e sua pertinência como solução da situação

problema.

Portanto, os resultados obtidos no nosso trabalho permitem que os professores realizem abordagens interessantes para desenvolvimento do estudo sobre polinômios em sala de aula do ensino médio, como o estudo da racionalidade dos números e resolução de situações problemas.

Para a continuação do presente trabalho podemos estudar outros métodos para o cálculo das raízes de um polinômio. Por exemplo, os métodos de Newton, os critérios de Gauss para a existência de raízes inteiras, etc.

Referências Bibliográficas

[1] Baiocco, J. C., *Relação entre a Álgebra aprendida na Licenciatura e a Álgebra ensinada na Educação Básica*, 2010. 37f. Monografia de graduação. Universidade Regional Integrada do Alto Uruguai e das Missões, Erechim, 2010.

[2] Biazzi, R. N., *Polinômios Irredutíveis: Critérios e Aplicações*, 2014. 76f. Dissertação de Mestrado. Universidade Estadual Paulista "Júlio de Mesquita Filho", Rio Claro, 2014.

[3] Boyer, C. B., *História da Matemática*. Tradução de Elza F. Gomide, Edgard Blucher, São Paulo, 1974.

[4] BRASIL, Secretaria de Educação Média e Tecnológica. *PCN + Ensino Médio: Orientações Educacionais Complementares aos Parâmetros Curriculares Nacionais. Ciências da Natureza, Matemática e suas Tecnologias*. Brasília: Ministério da Educação/Secretaria de Educação Média e Tecnológica, 2002.

[5] Dierings, A. R., *Ensino de Polinômios no Ensino Médio - Uma Nova Abordagem*, 2014. 70f. Dissertação de Mestrado. Universidade Federal de Santa Maria, Santa Maria, 2014.

[6] Guimarães, A. M. S., *Estudo de Anéis de Polinômios aos Elos de Níveis de Ensino*, 2016. 76f. Dissertação de Mestrado. Universidade Federal da Bahia, Cruz das almas, 2016.

[7] Hefez, Abramo., *Aritmética*, SBM, Coleção PROFMAT, Volume único, 2ª Edição, Rio de Janeiro, 2016.

[8] Hefez, A.; Villela, M. L. T., *Polinômios e Equações Algébricas*, SBM, Coleção PROFMAT, Volume único, 2ª Edição, Rio de Janeiro, 2018.

[9] Herstein, I. N., *Topics in Algebra*, Ginn and Company, Chicago, 1964.

[10] Hungerford, Thomas W., *Abstract Algebra, An Introduction*, BROOKS/COLE, CENGAGE Leaming, 3ª Edição, Boston, 2014.

[11] Roque, T.; Pitombeira, J. B., *Tópicos de História da Matemática*, SBM, Coleção PROFMAT, Volume único, 1ª Edição, Rio de Janeiro, 2012.

[12] Milies, C. P., *Breve História da Álgebra Abstrata*, II Bienal da SBM, 2004. Disponível em: <http://www.bienasbm.ufba.br/M18.pdf>. Acesso em: 01/06/2020.

[13] Santos, C. A. M.; Gentil, N.; Greco, S. E., *Matemática*, Série Novo Ensino Médio, Volume único, 7ª edição, Ática, São Paulo, 2003.