Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Polinômios em uma variável: propriedades e operações

Silvana Alves dos Santos

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de Rio Claro.

Orientador
Prof. Dr. Jamil Viana Pereira

Rio Claro
2021

S237p

Santos, Silvana Alves dos

Polinômios em uma variável: propriedades e operações / Silvana Alves dos Santos. -- Rio Claro, 2021

124 p.

Dissertação (mestrado profissional) - Universidade Estadual Paulista (Unesp), Instituto de Geociências e Ciências Exatas, Rio Claro

Orientador: Jamil Viana Pereira

1. Matemática. 2. Álgebra. 3. Polinômios. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

TERMO DE APROVAÇÃO

Silvana Alves dos Santos

Polinômios em uma variável: propriedades e operações

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Prof. Dr. Jamil Viana Pereira
Orientador

Prof. Dr. Thiago de Melo
Departamento de Matemática - IGCE/ UNESP/ Rio Claro (SP)

Profa. Dra. Claudete Matilde Webler Martins
Departamento de Matemática - UEM/ Maringá (PR)

Rio Claro, 29 de outubro de 2021

À minha mãe Célia, que sempre apoiou minhas decisões e está sempre ao meu lado, seja em momentos tristes ou felizes.

AGRADECIMENTOS

Agradeço a Deus, por me dar forças, fé e perseverança para chegar até o fim.

A minha mãe, por me apoiar, animar e compreender a respeito dos momentos de silêncio exigidos para estudos, e por compartilhar comigo os momentos de aflições, os quais me ajudava de sua maneira, por meio de orações a Deus, e me fortalecia.

Aos meus companheiros de trabalho que me ajudaram na compatibilidade de horários de trabalho e curso.

Aos meus colegas de curso, compartilhando das mesmas ansiedades e desafios, mas também muitos momentos felizes.

Aos meus professores do PROFMAT, em especial meu orientador Jamil Viana Pereira, pela dedicação, compreensão e disposição a ajudar fazer um trabalho adequado.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001

Os números governam o mundo.
Pitágoras

Resumo

Esta dissertação aborda o estudo das estruturas algébricas relacionadas aos polinômios. Apresentaremos a estrutura dos anéis de polinômios de forma generalizada, e as operações a eles relacionadas, tais como divisibilidade, fatoração e igualdade. Abordaremos também as propriedades particulares de polinômios, em que seus coeficientes estão no conjunto dos inteiros, racionais, reais e complexos, uma vez que quase toda aplicação matemática na Educação Básica efetua-se sobre tais conjuntos. O trabalho também aborda as equações algébricas e métodos de resolução. Apresentamos algumas análises de atividades propostas em materiais didáticos utilizados na Educação Básica, no que concerne ao estudo de polinômios e finalizamos este trabalho apresentando algumas atividades a serem propostas aos estudantes, relacionadas a aplicações das propriedades dos polinômios e analisamos resultados que esperamos obter a fim de contribuir ao ensino de álgebra.

Palavras-chave: Álgebra, Polinômios.

Abstract

This study approaches the algebraic structures related to polynomials. We will present the structure of polynomial rings, in general, and the operations related to them, such as divisibility, factorization and equality. We will also discuss the particular properties of polynomials, in which their coefficients are in the set of integers, rationals, reals and complexes, since almost every mathematical application in Basic Education is based on such sets. The work also covers algebraic equations and solving methods. We present some analysis of activities proposed in teaching materials, used in Basic Education, regarding the study of polynomials. We end this work by presenting some activities to be proposed to students, related to the application of the properties of polynomials, and we analyze results that we hope to obtain in order to contribute to the teaching of algebra..

Keywords: Algebra, Polynomials.

Lista de Figuras

Lista de Tabelas

Sumário

Introdução

Este trabalho tem por objetivo apresentar as estruturas algébricas relacionadas aos polinômios em uma variável, com ênfase naqueles em que os coeficientes são números reais e complexos. Pretende-se apresentar as operações entre polinômios, tais como as que são relacionadas a divisibilidade, fatoração e igualdade, bem como a aplicação destas em contextos matemáticos ou mesmo em outras áreas.

A motivação deu-se devido a observação, durante o exercício docente na Educação Básica, da forma como são tratadas as temáticas do ensino de Álgebra, em especial as ligadas as propriedades e operações entre polinômios.

Segundo a Base Nacional Comum Curricular - BNCC [3], o estudo dos polinômios faz parte da unidade temática Álgebra, a qual:

> "Tem como finalidade o desenvolvimento de um tipo especial de pensamento – pensamento algébrico – que é essencial para utilizar modelos matemáticos na compreensão, representação e análise de relações quantitativas de grandezas e, também, de situações e estruturas matemáticas, fazendo uso de letras e outros símbolos. Para esse desenvolvimento, é necessário que os alunos identifiquem regularidades e padrões de sequências numéricas e não numéricas, estabeleçam leis matemáticas que expressem a relação de interdependência entre grandezas em diferentes contextos, bem como criar, interpretar e transitar entre as diversas representações gráficas e simbólicas, para resolver problemas por meio de equações e inequações, com compreensão dos procedimentos utilizados. As ideias matemáticas fundamentais vinculadas a essa unidade são: equivalência, variação, interdependência e proporcionalidade."

Ainda segundo a BNCC [3], deve-se assegurar aos estudantes o desenvolvimento de competências, ou seja, a mobilização de conhecimentos e procedimentos, e as habilidades, constituídas através da prática e aspectos cognitivos. Assim, no que concerne ao estudo da Álgebra e mais especificamente aos polinômios são apresentadas algumas habilidades, tais como:

No Ensino Fundamental - Anos Finais

EF07MA16 - Reconhecer se duas expressões algébricas obtidas para descrever a regularidade de uma mesma sequência numérica são ou não equivalentes.

EF08MA09 - Resolver e elaborar, com e sem uso de tecnologias, problemas que possam ser representados por equações polinomiais de $2^{\underline{o}}$ grau do tipo $ax^2 = b$.

> EF09MA09 - Compreender os processos de fatoração de expressões algébricas, com base em suas relações com os produtos notáveis, para resolver e elaborar problemas que possam ser representados por equações polinomiais do 2^{o} grau.

No Ensino Médio

> EM13MAT302 - Construir modelos empregando as funções polinomiais de 1^{o} ou 2^{o} graus, para resolver problemas em contextos diversos, com ou sem apoio de tecnologias digitais.
>
> EM13MAT501 - Investigar relações entre números expressos em tabelas para representá-los no plano cartesiano, identificando padrões e criando conjecturas para generalizar e expressar algebricamente essa generalização, reconhecendo quando essa representação é de função polinomial de 1^{o} grau.

O ensino de álgebra constitui fundamentação importante na aprendizagem matemática. Para Ribeiro e Cury [9] :

> "A álgebra, trabalhada desde os anos iniciais do Ensino Fundamental, pode ser o fio condutor do currículo escolar e o desenvolvimento do pensamento algébrico pode permitir que sejam realizadas abstrações e generalizações que estão na base dos processos de modelagem matemática da vida real."

No entanto, Ribeiro e Cury [9] ainda observa que, os livros-texto de álgebra reforçam os aspectos transformacionais da álgebra. Esses aspectos, são aquelas atividades que incluem reduzir termos semelhantes, simplificar expressões e trabalhar com expressões semelhantes. Com isso observa-se a ênfase em regras a serem seguidas para a manipulação de expressões simbólicas, ao invés de atentar para as noções conceituais que sustentam essas regras.

Considerando a importância do ensino e aprendizagem de álgebra, este trabalho visa abordar o estudo de polinômios em uma variável, explorando suas características e propriedades e significando as operações a eles relacionadas. Para isso, organizamos este trabalho da seguinte forma:

Capítulo 1 Abordamos neste capítulo as características de maneira geral, relacionadas a estrutura de anéis, enfatizando suas propriedades operatórias.

Capítulo 2 Abordamos neste capítulo as características relacionadas aos anéis de polinômios, bem como as propriedades e operações a eles relacionadas, de maneira geral.

Capítulo 3 Abordamos neste capítulo as características dos anéis de polinômios considerando os coeficientes nos conjuntos do números inteiros, racionais, reais e complexos. Enfatizamos aqui como se comportam as operações de divisibilidade e fatoração considerando os coeficientes neste conjuntos.

Capítulo 4 Abordamos neste capítulo os métodos para resolução de equações polinomiais, em geral aquelas que são abordadas na Educação Básica.

Capítulo 5 Abordamos neste capítulo algumas propostas de atividades contextualizando e dando significado às operações entre polinômios.

Capítulo 6 Abordamos neste capítulo as considerações e expectativas a respeito do trabalho apresentado.

Para fundamentação teórica dos capítulos 1, 2, 3 e 4, foram utilizadas as referências [17], [6], [13], [18] , [10] , [1], [14], [8]. Para abordagens referentes à Educação Básica e proposta de atividades foram utilizadas as referências [3], [12], [15], [5], [4], [11].

1 Anéis

Para desenvolvermos este trabalho iniciamos com a apresentação da teoria relacionada às estruturas algébricas, com ênfase nos anéis. Introduziremos aqui o conceito de anel e os tipos de anéis de acordo com as propriedades a eles relacionadas.

1.1 Conjuntos

Nesta Seção vamos apresentar as noções de conjunto e dar exemplos dos conjuntos numéricos, os quais serão o foco das propriedades em anéis as quais iremos abordar.

Definição 1.1. *Um conjunto é uma coleção de objetos, chamados de elementos do conjunto. Quando um elemento x pertence a um conjunto C usamos a notação $x \in C$. A respeito da relação entre conjuntos, se todos os elementos de um conjunto A também são elementos de um conjunto B, dizemos que A está contido em B e usamos a notação $A \subset B$.*

Exemplo 1.2. Estes são os conjuntos numéricos os quais posteriormente estudaremos suas propriedades e caracterizaremos suas estruturas, referentes a anéis, domínios e corpos.

1. Números naturais $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, \ldots\}$.
2. Números inteiros $\mathbb{Z} = \{\ldots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, \ldots\}$.
3. Números racionais $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$.
4. Números reais $\mathbb{R}$.
5. Números complexos $\mathbb{C} = \{z = a + bi : a, b \in \mathbb{R},\ i = \sqrt{-1}\}$. Onde a é chamada de parte real e b de parte imaginária. Se $z = a + 0i$ então z é um número real e se $z = 0 + bi$ então z é imaginário puro.

Ainda considerando os conjuntos numéricos vamos apresentar mais alguns, os quais analisaremos posteriormente.

(i) Conjunto dos múltiplos inteiros de n.

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}, \text{ tal que } n\mathbb{Z} \subset \mathbb{Z}.$$

(ii) Conjunto das classes de equivalência módulo n, $\mathbb{Z}_n$.
Consideremos $J = n \cdot \mathbb{Z}$, e em $\mathbb{Z}$ definimos a relação $\equiv \pmod{n}$ tal que:

$$x, x' \in \mathbb{Z}, \quad x \equiv x' \pmod{n} \Leftrightarrow x - x' \in J.$$

Usaremos a notação $\overline{x} = x + J = \{x + kn : k \in \mathbb{Z}\}$ para a classe de equivalência de x em relação a $\equiv \pmod{n}$, e então:

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Observação 1.3. Os conjuntos apresentam a seguinte relação de inclusão:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

1.2 Anéis

Definição 1.4. *(soma e produto) Seja A um conjunto não vazio e sobre ele definimos operações soma $(+)$ e produto $(\cdot)$, fechadas em A, tais que:*

$$\begin{array}{rcccc} (+) & : & A \times A & \to & A \\ & & (a,b) & \mapsto & a+b \\ (\cdot) & : & A \times A & \to & A \\ & & (a,b) & \mapsto & a \cdot b. \end{array}$$

Para efeitos de notação, consideremos $a \cdot b = ab$.

Dado um conjunto A, munido das operações soma e produto, as seguintes condições podem ser satisfeitas:

A1. Associativa da adição: Para todo x, y, z em A, $(x + y) + z = x + (y + z)$

A2. Existência do elemento neutro da adição : Existe 0 em A tal que, para todo x em A, $0 + x = x$ e $x + 0 = x$.

A3. Existência do elemento inverso relativo à adição: Para todo x em A, existe y em A tal que, $x + y = 0$ e $y + x = 0$.

A4. Comutativa relativa à adição: Para todo x, y em A, $x + y = y + x$.

M1. Associativa da multiplicação: Para x, y, z em A, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

M2. Existência do elemento neutro da multiplicação: Existe 1 em A, tal que, para todo x em A, $1 \cdot x = x$ e $x \cdot 1 = x$.

M3. Comutativa relativa à multiplicação: Para todo x, y em A, $x \cdot y = y \cdot x$.

M4. Distributiva da multiplicação relativa à adição: Para todox, y, z em A, $x \cdot (y+z) = x \cdot y + x \cdot z$ e $(x + y) \cdot z = x \cdot z + y \cdot z$.

Definição 1.5. *(anel) Chamaremos de anel e denotaremos por $(A, +, \cdot)$ o conjunto A, munido das operações soma e produto, se forem satisfeitas as condições $A1$, $A2$, $A3$, $A4$, $M1$, $M4$.*

Definição 1.6. *(anel comutativo) Chamaremos de anel comutativo e denotaremos por $(A, +, \cdot)$ o conjunto A, munido das operações soma e produto, se forem satisfeitas as condições $A1$, $A2$, $A3$, $A4$, $M1$, $M3$, $M4$.*

Definição 1.7. *(anel comutativo com unidade) Chamaremos de anel comutativo com unidade e denotaremos por* $(A, +, \cdot)$ *o conjunto* A*, munido das operações soma e produto, se forem satisfeitas as condições* $A1$*,* $A2$*,* $A3$*,* $A4$*,* $M1$*,* $M2$*,* $M3$*,* $M4$*.*

Definição 1.8. *(domínio de integridade ou domínio) Chamaremos o anel* $(A, +, \cdot)$ *de domínio de integridade, ou simplesmente domínio se, além das condições* $A1$ *a* $A4$ *e* $M1$ *a* $M4$*, for satisfeita também a condição:*

M5 Para todo x, y *em* A *, se* $x \cdot y = 0$*, então* $x = 0$ *ou* $y = 0$*.*

Quando nos referirmos a um domínio, usaremos a notação $(D, +, \cdot)$*.*

Definição 1.9. *(corpo) O domínio* $(D, +, \cdot)$ *será chamado de corpo se, além das condições* $A1$ *a* $A4$ *e* $M1$ *a* $M5$*, for satisfeita a condição:*

M6 Elemento invertível: Para todo x *em* D*,* x *não nulo, ou seja,* $x \neq 0$*, existe* y *em* D*, tal que* $x \cdot y = y \cdot x = 1$ *.*

Quando nos referirmos a um corpo, usaremos a notação $(K, +, \cdot)$*.*

Observação 1.10.

1. Podemos enfatizar pelas Definições 1.8 e 1.9, que todo corpo é domínio de integridade.

2. Ainda a respeito de domínio e corpo podemos afirmar que todo domínio finito é um corpo.

   De fato, sejam D um domínio finito, $x \in D$, $x \neq 0$. Consideremos o conjunto $\{x^n \mid n \in \mathbb{N}\}$. Utilizando a recorrência

   $$x^1 = x, \quad x^2 = x \cdot x, \quad x^3 = x^2 \cdot x, \cdots, x^n = x^{n-1} \cdot x, \quad \forall n \in \mathbb{N},$$

   existem inteiros $n_1 < n_2$ tais que $x^{n_1} = x^{n_2}$ (pois D é finito). Assim temos

   $$\begin{array}{rcl@{\qquad}rcl} x \cdot x^{n_2-n_1-1} & = & a & \Rightarrow & x^{n_2-n_1} & = & a \\ x^{n_2} & = & ax^{n_1} & \Rightarrow & a & = & 1 \end{array}$$

   logo, $x \cdot x^{n_2-n_1-1} = 1$. Assim x possui elemento inverso e portanto D é corpo.

Exemplo 1.11. Dados os conjuntos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, então:

1. $(\mathbb{Z}, +, \cdot)$ é um domínio.

2. $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ são corpos.

3. $(\{a + b\sqrt{n} \,|\, a, b \in \mathbb{Z}\}, +, \cdot)$ e $(\{a + bi\sqrt{n} \,|\, a, b \in \mathbb{Z}\}, +, \cdot)$, para todo $n \in \mathbb{N}^*$, são domínios.

Exemplo 1.12. Considere o conjunto $\mathcal{F}(\mathbb{R})$ de todas as funções $f\colon \mathbb{R} \to \mathbb{R}$. Vamos definir neste conjunto as operações soma $(+)$ e produto $(\cdot)$ sobre duas funções $f\colon \mathbb{R} \to \mathbb{R}$ e $g\colon \mathbb{R} \to \mathbb{R}$, tais que :

$$\begin{array}{rccc} f+g\colon & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & f(x)+g(x) \\ f\cdot g\colon & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & f(x)\cdot g(x)\ . \end{array}$$

Temos que $(\mathcal{F}(\mathbb{R}),+,\cdot)$ é um anel comutativo com unidade, cujo elemento neutro da adição é a função identicamente nula, $f(x)=0$, e o elemento neutro da multiplicação é a função constante igual a 1, $f(x)=1$. Observe que $(\mathcal{F}(\mathbb{R}),+,\cdot)$ não é um domínio pois, se tomarmos as funções: $f\colon \mathbb{R}\times\mathbb{R}$ e $g\colon \mathbb{R}\times\mathbb{R}$ definidas por:

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

temos $f\cdot g=0$, mas $f\neq 0$ e $g\neq 0$ para $x\neq 0$.

Considerando a Definição 1.6 referente a anéis, apresentaremos a seguir algumas propriedades imediatas dos anéis:

Proposição 1.13. *(Propriedades imediatas de um anel) Seja $(A,+,\cdot)$ um anel.*

1. *O elemento neutro do anel, ou seja ,0 (zero do anel) é único.*
2. *O elemento oposto ou simétrico aditivo $-x$ é único.*
3. *Se $x_1,x_2,\ldots,x_n\in A$, então $-(x_1+x_2+\cdots+x_n)=(-x_1)+(-x_2)+\cdots+(-x_n)$.*
4. *Para todo $x\in A$, $-(-x)=x$.*
5. *Para todos a, b, x em A, se $x+a=x+b$ então $a=b$.*
6. *Para todo x em A, $x\cdot 0=0\cdot x=0$.*
7. *Para todos x, y em A, $x\cdot(-y)=(-x)\cdot y=-(x\cdot y)=-(xy)$.*
8. *Para todos x, y em A, $(-x)\cdot(-y)=x\cdot y=xy$.*

Sobre o anel $(A,+,\cdot)$ foram definidas as operações soma e multiplicação. Definiremos então mais algumas operações sobre o anel e sobre alguns elementos do anel.

Definição 1.14. *(diferenças em um anel) Sejam x, y elementos do anel A. Chama-se diferença entre x e y, e indica-se por $x-y$, o elemento $x+(-y)$ de A. Assim $x+(-y)=x-y$. Além disso, temos que para todo a, b, x em A, $x(a-b)=xa-xb$.*

Exemplo 1.15. Sejam A e B anéis e consideremos o produto cartesiano $A\times B$. Se definirmos a soma $(+)$ e o produto $(\cdot)$ sobre $A\times B$ de modo que:

$$\begin{array}{rccc} & A\times B & \to & A\times B \\ (+) & (a_1,b_1)+(a_2,b_2) & \to & (a_1+a_2,b_1+b_2) \\ (\cdot) & (a_1,b_1)\cdot(a_2,b_2) & \to & (a_1\cdot a_2,b_1\cdot b_2). \end{array}$$

Temos que $(A\times B,+,\cdot)$ é um anel.
Então, sejam $u=(a_1,b_1), v=(a_2,b_2)$:

(i)

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

(ii)

$$\begin{aligned} x(u-v) &= (x_1,y_1)\cdot(a_1-a_2,b_1-b_2) \\ &= (x_1(a_1-a_2),y_1(b_1-b_2) \\ &= (x_1a_1-x_1a_2,y_1b_1-y_1b_2) \\ &= (x_1a_1-y_1b_1,-x_1a_2-y_1b_2) \\ &= \ldots \\ &= xu-xv. \end{aligned}$$

Definição 1.16. *(potenciação num anel) Seja $(A,+,\cdot)$ um anel comutativo com unidade. Definindo a potência de um elemento $x \in A$ (usando associatividade do produto), de modo que:*

$$x^0=1, \quad x^1=x, \quad x^2=x\cdot x, \quad x^3=x^2\cdot x, \cdots, x^n=x^{n-1}\cdot x, \quad \forall n\in\mathbb{N}.$$

Vamos mostrar que as seguintes propriedades são válidas para todo $m,n\in\mathbb{N}$:

1. $x^{m+n}=x^mx^n$;
2. *se* $xy=yx$, *então* $(xy)^m=x^my^m$;
3. $(x^m)^n=x^{m\cdot n}$;
4. *Se* $xy=yx$ *então,* $(x+y)^n=\sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i$ *onde* $\binom{n}{i}=\frac{n!}{(n-i)!i!}$.

Demonstração. Mostraremos por indução sobre $n \geqslant 1$, $n\in\mathbb{N}$. Consideremos nas passagens o uso da definição e as propriedades referentes a $\mathbb{N}$:

- $\overset{*}{=}$: hipótese de indução;
- $\overset{1}{=}$: Definição 1.16;
- $\overset{2}{=}$ propriedade associativa;
- $\overset{3}{=}$ propriedade comutativa.

1. Para $n=1$, temos $x^{m+1}\overset{1}{=}x^mx$ e $x=x^1$. Assim, $x^{m+1}=x^mx^1$. Portanto a propriedade é válida para $n=1$. Suponhamos que a propriedade seja válida para $n=k$, ou seja, $x^{m+k}=x^mx^k$. Vamos verificar se é válida para $n=k+1$. De fato, temos que $x^{m+(k+1)}=x^{(m+k)+1}\overset{1}{=}x^{m+k}x^1\overset{*}{=}(x^mx^k)x^1\overset{2}{=}x^m(x^kx^1)=x^mx^{k+1}$.

   Portanto, concluímos que a propriedade é válida para todo expoente $n\in\mathbb{N}$.

2. Para $n=1$, temos $(xy)^n=(xy)^1=xy\overset{1}{=}x^1y^1$. Suponhamos que seja válida para $n=k$, ou seja, $(xy)^k=x^ky^k$. Vamos verificar se é válida para $n=k+1$. De fato, $(xy)^{k+1}\overset{1}{=}(xy)^k(xy)^1\overset{*}{=}x^ky^kx^1y^1\overset{3}{=}(x^kx^1)(y^k\cdot y^1)=x^{k+1}y^{k+1}$.

   Portanto, concluímos que a propriedade é válida para todo expoente $n\in\mathbb{N}$.

3. Para $n = 1$, temos $(x^m)^1 \stackrel{1}{=} x^m = x^{m\cdot 1}$. Suponhamos que seja válida para $n = k$, ou seja, $(x^m)^k = x^{mk}$. Vamos verificar se é válida para $n = k+1$. De fato, temos que $(x^m)^{k+1} \stackrel{1}{=} (x^m)^k x^m \stackrel{*}{=} x^{mk}x^m = x^{mk+m} = x^{m(k+1)} = x^m x^{k+1}$.

   Portanto, concluímos que a propriedade é válida para todo expoente $n \in \mathbb{N}$.

4. Para $n = 1$ temos

$$(x+y)^1 = \binom{1}{0}x^1y^0 + \binom{1}{1}x^0y^1 = x + y.$$

   Suponhamos que seja válida para $n = k$, ou seja,

$$(x+y)^k = \sum_{i=0}^{k}\binom{k}{i}x^{k-i}y^i = \binom{k}{0}x^k + \binom{k}{1}x^{k-1}y^1 + \cdots + \binom{k}{i}x^{k-i}y^i + \cdots + \binom{k}{k}y^k,$$

   e então vamos verificar se é válida para $n = k+1$. Temos que,

$$\begin{aligned}(x+y)^{k+1} = (x+y)(x+y)^k &= (x+y)\left(\sum_{i=0}^{k}\binom{k}{i}\cdot x^{k-i}y^i\right)\\ &= x\left(\sum_{i=0}^{k}\binom{k}{i}\cdot x^{k-i}y^i\right) + \\ &\quad y\left(\sum_{i=0}^{k}\binom{k}{i}\cdot x^{k-i}y^i\right)\\ &= \sum_{i=0}^{k}\binom{k}{i}x^{k-i+1}y^i + \sum_{i=0}^{k}\binom{k}{i}x^{k-i}y^{i+1}.\end{aligned} \tag{1.1}$$

   Desenvolvendo os somatórios obtemos as expressões abaixo:

$$\begin{aligned}\sum_{i=0}^{k}\binom{k}{i}x^{k-i+1}y^i = {} & x^{k+1} + \binom{k}{1}x^ky + \binom{k}{2}x^{k-1}y^2 + \cdots + \\ & + \binom{k}{k-1}x^2y^{k-1} + \binom{k}{k}xy^k.\\ \sum_{i=0}^{k}\binom{k}{i}x^{k-i}y^{i+1} = {} & \binom{k}{0}x^ky + \binom{k}{1}x^{k-1}y^2 + \cdots + \\ & + \binom{k}{k-2}x^2y^{k-1} + \binom{k}{k-1}x^k + y^{k+1}.\end{aligned} \tag{1.2}$$

   Pela Relação de Stifel temos que:

$$\binom{n+1}{i} = \binom{n}{i}\binom{n}{i-1} \tag{1.3}$$

   Assim, considerando o desenvolvimento do somatório em (1.2) e aplicando a este a Relação de Stifel (1.3), concluímos que a expressão obtida em (1.1) é dada por:

$$\begin{aligned}(x+y)^{k+1} &= x^{k+1} + \binom{k+1}{1}x^ky + \cdots + \binom{k+1}{i}x^{(k+1)-i}y^i + \cdots + \\ &\quad + \binom{k+1}{k}xy^k + y^{k+1}\\ &= \sum_{i=0}^{k+1}\binom{k+1}{i}x^{k+1-i}y^i.\end{aligned}$$

   Portanto, concluímos que a propriedade é válida para todo expoente $n \in \mathbb{N}$.

□

Definição 1.17. *(elemento invertível) Seja $(A, +, \cdot)$ um anel comutativo com unidade. Um elemento $x \in (A, +, \cdot)$ é invertível se, e somente se, x é invertível para a multiplicação definida sobre A. Portanto, se x é invertível, então existe um único elemento x^{-1} (denominado inverso de x), tal que: $x \cdot x^{-1} = 1 = x^{-1} \cdot x$, onde 1 é o elemento neutro de A.*

Observação 1.18. O conjunto dos elementos invertíveis de $(A, +, \cdot)$ será indicado por $U(A)$, unidades de A.

Definição 1.19. *(divisor do zero) Um elemento x de $(A, +, \cdot)$, onde A é anel comutativo, é um divisor de zero se, e somente se, existe $y \in A$, $y \neq 0$, tal que $xy = 0$. Além disso, se x é divisor de zero e $x \neq 0$ então x é chamado de divisor próprio de zero.*

Exemplo 1.20. No anel $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ temos que $\overline{2}$ é divisor próprio do zero pois $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$ e $\overline{2} \neq 0$.

Definição 1.21. *(subanel) Seja $(A, +, \cdot)$ um anel. Dizemos que um subconjunto $I \subset A$, $I \neq \varnothing$, é um subanel de A se,*

(i) Para todo x, $y \in I \Rightarrow x + y \in I$.

(ii) Para todo x, $y \in I \Rightarrow xy \in I$.

(iii) $(I, +, \cdot)$ também é um anel com as operações de A.

A proposição a seguir apresenta uma forma de identificar um subanel no conjunto $I \subset A$.

Proposição 1.22. *Um conjunto $I \subset A$, $I \neq \varnothing$ é um subanel de A se, e somente se:*

(i) $0 \in I$ (o elemento neutro de A pertence a I);

(ii) $x, y \in I \Rightarrow x - y \in I$, para todo $x, y \in I$;

(iii) $x, y \in I \Rightarrow xy \in I$, para todo $x, y \in I$.

Demonstração.

($\Rightarrow$) Se $I \subset A$ é um subanel de A então:

(i) Seja $x \in I$, então $-x \in I$, pois pela Definição 1.21, referente a subanel, I é também um anel. Assim $x - x = 0 \in I$;

(ii) Como I é anel, se $y \in I$ então $-y \in I$. Assim $x + (-y) \in I$, mas pela Definição de diferença em um anel (1.14) $x + (-y) = x - y \in I$;

(iii) Imediata pela Definiçao de subanel (1.21).

($\Leftarrow$) Em *(i)* temos que $0 \in I$, então $I \neq \varnothing$. Por *(ii)* e *(iii)* temos que se $x \in I$ então $-x = 0 - x \in I$ e se $x, y \in I$ então $x + y = x - (-y) \in I$ isto é, I é fechado para a soma. Por *(iii)* I é fechado para o produto. Assim, como as propriedades associativa, comutativa e distributiva de I são as propriedades de A, pois $I \subset A$, então I é um subanel de A.

□

Exemplo 1.23. Para representar um subanel B de um anel A, usaremos a notação $B \subset A$. Usando a Proposição 1.22 vamos mostrar que os anéis $n\mathbb{Z}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $n \in \mathbb{N}$ são tais que,

$$n\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}, \quad n \in \mathbb{N}. \tag{1.4}$$

De fato:

1. $n\mathbb{Z} \subset \mathbb{Z}$

   Seja $n\mathbb{Z} = \{nk \,|\, k \in \mathbb{Z}\}$ e $\mathbb{Z} = \{\text{números inteiros}\}$. Temos que:

   (i) $0 \in n\mathbb{Z}$ pois $0 = n \cdot 0 \quad \forall n \in \mathbb{N}$;

   (ii) $a = nk_1$ e $b = nk_2$ então $a - b = n(k_1 - k_2) \in n\mathbb{Z}$;

   (iii) $a = nk_1$ e $b = nk_2$ então $ab = n(nk_1k_2) = nk \in n\mathbb{Z}$.

2. $\mathbb{Z} \subset \mathbb{Q}$

   Seja $\mathbb{Q} = \left\{\frac{a}{b} \,|\, a, b \in \mathbb{Z},\, b \neq 0\right\}$

   (i) $\dfrac{0}{b} = 0 \in \mathbb{Z}$;

   (ii) $a \in \mathbb{Z}, b \in \mathbb{Z}, a - b \in \mathbb{Z}$;

   (iii) $a \in \mathbb{Z}, b \in \mathbb{Z}, ab \in \mathbb{Z}$.

3. $\mathbb{Q} \subset \mathbb{R}$

   (i) $0 \in \mathbb{Q}$;

   (ii) Sejam $r = \dfrac{a}{b}, s = \dfrac{c}{d} \in \mathbb{Q}$, $b, d \neq 0$, temos que $r - s = \dfrac{ad - bc}{bd}$. Como $a, b, c, d \in \mathbb{Z}$ então $(ad - bc) \in \mathbb{Z}, bd \in \mathbb{Z}$. Assim $\dfrac{ad - bc}{bd} = r - s \in \mathbb{Q}$;

   (iii) Sejam $r = \dfrac{a}{b}, s = \dfrac{c}{d} \in \mathbb{Q}$, $b, d \neq 0$, temos que $rs = \dfrac{ac}{bd}$. Como $a, b, c, d \in \mathbb{Z}$ então $(ac) \in \mathbb{Z}, bd \in \mathbb{Z}$. Assim $\dfrac{ac}{bd} = rs \in \mathbb{Q}$.

4. $\mathbb{R} \subset \mathbb{C}$

   Seja $\mathbb{C} = \{a + bi \,|\, a, b \in \mathbb{R}, i = \sqrt{-1}\}$.

   (i) $0 + 0i = 0 \in \mathbb{R}$;

   (ii) Sejam $a, b \in \mathbb{R}$, $a - b \in \mathbb{R}$;

   (iii) Sejam $a, b \in \mathbb{R}$, $ab \in \mathbb{R}$.

Vamos a seguir definir e apresentar algumas propriedades de subanéis bastante importante na teoria dos anéis.

Definição 1.24. *(ideal) Dado um subconjunto não vazio I, de um anel comutativo $(A, +, \cdot)$, dizemos que este é um ideal de A se, e somente se,*

(i) $x - y \in I$, *para todo* $x, y \in I$;

(ii) $ax \in I$, *para todo* $x \in I$, *para todo* $a \in A$.

Exemplo 1.25. O conjunto $n\mathbb{Z} \subset \mathbb{Z}$, é ideal de $n\mathbb{Z}$. Vamos demonstrar essa afirmação verificando os itens (i) e (ii) da Definição 1.24.

Demonstração.
Sejam x, y em $n\mathbb{Z}$. Então existem k_1, k_2 em $\mathbb{Z}$, tais que $x = nk_1$ e $y = nk_2$.

(i) $nk_1 - nk_2 = n(k_1 - k_2) \in n\mathbb{Z}$;

(ii) $a(nk) = n(ak) \in n\mathbb{Z}, \quad \forall a \in \mathbb{Z}$.

□

Observação 1.26. Considerando a Definição 1.21 e a Proposição 1.22 a respeito de subanel, podemos afirmar que um ideal $I \subset A$, (A um anel comutativo) é também um subanel de A, porém a recíproca não é verdadeira, como por exemplo, $\mathbb{Z}$ é subanel de $\mathbb{Q}$ mas não é ideal de $\mathbb{Q}$. De fato, observe que,

$$1 \in \mathbb{Z}, \frac{1}{2} \in \mathbb{Q} \text{ mas } \frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}.$$

Proposição 1.27. *Seja* I *um ideal de* $(A+, \cdot)$, *onde* A *é um anel comutativo. As seguintes propriedades são válidas:*

(i) O elemento neutro do anel em A *também pertence a* I;

(ii) Se $a \in I$, *então* $-a \in I$;

(iii) Se $a, b \in I$, *então* $a + b \in I$;

(iv) Se o anel possui unidade e se algum elemento invertível do anel A *pertence a* I, *então* $I = A$.

Demonstração.
Pela definição 1.24 temos que $I \subset A$.

(i) Seja $a \in I$, então $a - a \in I$, mas $a - a = 0$, logo $0 \in I$;

(ii) Como $0 \in I$, então $0 - a = -a \in I$;

(iii) Se $a, b \in I$, então $-b \in I$, assim $a - (-b) = a + b \in I$;

(iv) Como $I \subset A$, então vamos mostrar que $A \subset I$. De fato, seja a um elemento do anel A. Temos que $a = a \cdot 1$. Se tomarmos um elemento invertível $x \in I$, então existe algum $y \in A$ tal que $xy = 1$. Seja $a = a \cdot 1 = a(xy) = (ay)x$. Logo $a = (ay)x \in I$ e então todo elemento de A também é elemento de I, assim $A \subset I$.

□

Dentre os ideais de um anel A temos alguns com propriedades específicas os quais definiremos abaixo.

Definição 1.28. *(ideal maximal) Um ideal $I \subset A$, onde A é um anel comutativo com unidade, é chamado de ideal maximal se, $I \neq A$, e os únicos ideais de A que contêm I são I e A.*

Definição 1.29. *(conjunto gerado) Seja A um anel e a um elemento de A. O conjunto $J = a \cdot x$, tal que $x \in A$, é chamado de conjunto gerado por a e denotado por $J = \langle a \rangle$.*

Definição 1.30. *(ideal finitamente gerado) Sejam A um anel e $S = \{a_1, a_2, \ldots, a_n\} \subset A$, com $a_i \in A, 1 \leqslant i \leqslant n$. O subconjunto I tal que,*

$$I = \langle a_1, a_2, \ldots, a_n \rangle = \{x_1a_1 + x_2a_2 + \cdots + x_na_n | x_1, x_2, \ldots, x_n \in A\},$$

é chamado de ideal gerado por S e neste caso ele é dito ideal finitamente gerado.

Definição 1.31. *(ideal principal) Seja A um anel comutativo. Um ideal $I \subset A$ é chamado de ideal principal se $I = \langle a \rangle$, ou seja, I é gerado por a. Um domínio em que todo ideal é principal é chamado domínio principal.*

A Definição 1.9 fornece as condições para as quais $(A, +, \cdot)$ é um corpo. Considerando agora as propriedades de ideal, apresentaremos algumas condições necessárias e suficientes para que um anel seja também definido como um corpo.

Proposição 1.32. *O anel $(A, +, \cdot)$ comutativo com unidade é um corpo, se e somente se, os únicos ideais de $(A, +, \cdot)$ são os triviais $\{0\}$ e A.*

Demonstração.

($\Rightarrow$) Seja $I \neq \{0\}$ um ideal do anel A. Vamos mostrar que $I = A$.
Vamos tomar um elemento $a \in I, a \neq 0$ invertível, pois A é um corpo. Pela Proposição 1.27 temos que $I = A$.

($\Leftarrow$) Vamos mostrar que todo elemento do anel A, não nulo, é invertível.
Seja $a \in A, a \neq 0$ e $I = \langle a \rangle$. Como $I \neq \{0\}$, então $I = A$ e então a unidade do anel A também pertence a I. Assim, existe $x \in A$, tal que $1 = ax$, logo a é invertível.

□

Na Definição 1.1, item (ii), apresentamos a relação de congruência ($\equiv \pmod{n}$) em $\mathbb{Z}$. Agora vamos estender a um anel qualquer.

Definição 1.33. *Seja A um anel e I um ideal de A e sejam $a, b \in A$. Definimos a relação :*

$$a \equiv b \pmod{I} \Leftrightarrow a - b \in I.$$

Esta relação representa uma relação de equivalência em A.

Definição 1.34. *(conjunto quociente). Sejam $(A, +, \cdot)$ um anel comutativo com unidade e I um ideal de A. Definimos a classe de equivalência de um elemento $x \in A$ por $\overline{x} = \{y \in A : y \equiv x \pmod{I}\}$. Assim $\overline{x} = x + I = \{x + z : z \in I\}$. O conjunto $A/I = \{\overline{x} = x + I : x \in A\}$ é chamado de conjunto quociente de A.*

Teorema 1.35. *Seja A um anel comutativo com unidade, $I \subset A$ um ideal e $A/I = \{\overline{x} = x + I : x \in A\}$ o conjunto quociente de A. Se definirmos as operações soma $(+)$ e produto $(\cdot)$ de maneira que:*

$$\begin{array}{rrcl} (+): & A/I \times A/I & \to & A/I \\ & (\overline{x}, \overline{y}) & \mapsto & \overline{x+y} = \overline{x} + \overline{y} \\ (\cdot): & A/I \times A/I & \to & A/I \\ & (\overline{x}, \overline{y}) & \mapsto & \overline{xy} = \overline{x} \cdot \overline{y}. \end{array}$$

Então,

(i) $(A/I, +, \cdot)$ *é um anel, chamado de anel quociente de* A *módulo* I*;*

(ii) Se 1 *é a unidade do anel* A *então* $\overline{1}$ *é unidade de* A/I*.*

Demonstração.

(i) A demonstração é meramente técnica e será omitida. Ver em [13] página 31.

(ii) Seja $x \in A$, $\overline{x} = \{x + I\} \in A/I$, 1 a unidade do anel A. Então,

$$\begin{array}{rcrcrl} 1 \cdot x & = & x \cdot 1 & = & x & \Rightarrow \\ \overline{1 \cdot x} & = & \overline{x \cdot 1} & = & \overline{x} & \Rightarrow \\ \overline{1} \cdot \overline{x} & = & \overline{x} \cdot \overline{1} & = & \overline{x}, & \end{array}$$

logo, $\overline{1}$ é a unidade de A/I.

□

Definição 1.36. *Sejam I e J ideais de um anel comutativo A. Definimos como soma de ideais, e indicamos por $I + J$, o subconjunto de A tal que:*

$$I + J = \{x + y \,|\, x \in I \quad e \quad y \in J\}.$$

Este subconjunto também é um ideal de A, pois:

1. *Como $0 \in I$ e $0 \in J$ então $0 + 0 = 0 \in I + J$;*
2. *Sejam a e b elementos de $I + J$, tais que $a = x_1 + y_1$ e $b = x_2 + y_2$, com $x_1, x_2 \in I$ e $y_1, y_2 \in J$. Então $a - b = (x_1 - x_2) + (y_1 - y_2) \in I + J$ pois $(x_1 - x_2) \in I$ e $(y_1 - y_2)$;*
3. *Seja $c \in A$ e $d = x + y \in I + J$, então $cd = c(x + y) = cx + cy \in I + J$ pois $cx \in I$ e $cy \in J$.*

Lema 1.37. *Sejam I e J ideais de um anel comutativo A, então*

(i) $I + J$ *contém* I *e* J*;*

(ii) Todo ideal em A *que contém* I *e* J *contém* $I + J$*.*

Demonstração.

(i) Seja a um elemento de I. Temos que $a = a + 0$ e como $a + 0 \in I + J$ pois $0 \in J$, logo $I \subset I + J$. Análogamente, seja $b \in I$, e daí temos que $b = b + 0 \in I + J$ e então concluímos que $J \subset I + J$.

(ii) Seja L um ideal de A tal que $I \subset L$ e $J \subset L$. Seja b um elemento de $I + J$, então $b = x + y$ onde $x \in I$ e $y \in J$. Temos que $x \in L$, pois $x \in I$ e $I \subset L$ e, $y \in L$, pois $y \in J$ e $J \subset L$. Logo $b = x + y \in L$.

□

Teorema 1.38. *Seja A um anel comutativo com unidade e $I \subset A$ um ideal de A. Então, I é ideal maximal de A se, e somente se, A/I é um corpo.*

Demonstração.

($\Rightarrow$) Seja $\overline{a} \neq \overline{0} \in A/I$. Vamos mostrar que existe $\overline{b}$ em A/I tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Para isso, vamos considerar um ideal principal $J = A \cdot a$ (gerado por a), $a \in A$. Temos que $I + J = \{x + y\,;\, x \in I,\, y \in J\}$ é um ideal contendo I (Lema 1.37) e como $\overline{a} \neq \overline{0}$ então $a \notin I$. Mas como $a = 1 \cdot a \in J$ e $J \subset I + J$, então $I + J \neq I$. Como I é maximal então $A = I + J$ e $1 \in A = I + J$, logo existe $u \in I,\ \ v \in J$ tais que $1 = u + v$. Do fato de $v \in J$ então $v = b \cdot a,\ \ b \in A$. Podemos assim obter a relação de igualdade:

$$1 = u + b \cdot a \Rightarrow \overline{1} = \overline{u + b \cdot a} = \overline{u} + \overline{b \cdot a}.$$

Assim, como $\overline{u} = \overline{0}$ temos,

$$1 = u + b \cdot a = \overline{1} = \overline{u + b \cdot a} = \overline{u} + \overline{b \cdot a} = \overline{0} + \overline{b} \cdot \overline{a},$$

e do fato de $\overline{b} \cdot \overline{a} = \overline{a} \cdot \overline{b}$ temos que $\overline{b} \cdot \overline{a} = \overline{1}$.

($\Leftarrow$) Pela hipótese de $\overline{A} = A/I$ ser um corpo, então $\overline{0}, \overline{1} \in \overline{A}$, logo $I \neq A$. Seja M um ideal de A, $M \neq I$ tal que $I \subset M \subset A$. Daí temos que existe um $a \in M$, $a \notin I$. Como $a \notin I$, então $\overline{a} \neq \overline{0}$, $a \in \overline{A}$. Novamente, pela hipótese de $\overline{A}$ ser um corpo, então existe um $\overline{b} \in \overline{A}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$, ou seja, pela Definição 1.34 referente a classe de equivalência, temos que para a e b em A,

$$ab \equiv 1 \pmod{I} \Leftrightarrow ab - 1 \in I,$$

e então existe $u \in I$ tal que,

$$1 = ab - u.$$

Como $a \in M$, um ideal de A, e $\overline{b} \in A/I$, então $b \in A$, logo $ab \in M$. Temos ainda que, sendo $u \in I \subset M$, então $u \in M$ e daí, $1 = ab - u \in M$, logo concluímos que $M = A$ e portanto, o único ideal que contem I é o próprio A. Assim, concluímos que I é ideal maximal.

□

Definição 1.39. *(corpo de frações de um domínio) Seja D um domínio e $D^* = D\backslash\{0\}$. Consideremos a relação de equivalência definida no conjunto $D \times D^* = \{(a,b); a \in D, b \in D^*\}$, tal que:*

$$(a,b) \backsim (c,d) \Leftrightarrow ad = bc.$$

Utilizamos a notação $\frac{a}{b} = \frac{c}{d}$ para representar $(a,b) \backsim (c,d)$ e também $\frac{a}{b}$ para representar a classe de equivalência de (a,b) em $D \times D^*$. Sobre o os elementos de $D \times D^*$definimos as operações soma $(+)$ e produto $(\cdot)$ tal que:

$$\begin{array}{rccc} (+): & (D \times D^*) \times (D \times D^*) & \to & (D \times D^*) \\ & \frac{a}{b} + \frac{c}{d} & \mapsto & \frac{ad+bc}{bd} \end{array}$$

$$\begin{array}{rccc} (\cdot): & (D \times D^*) \times (D \times D^*) & \to & (D \times D^*) \\ & \frac{a}{b} \cdot \frac{c}{d} & \mapsto & \frac{ac}{bd}. \end{array}$$

Temos que $(D \times D^*, +, \cdot)$ é um corpo, chamado de corpo das frações do domínio D.

Observação 1.40. No corpo de frações de domínio, podemos observar que estão definidos o zero de K, sendo 0 a classe de equivalência $\frac{0}{1}$ e 1 a classe de equivalência $\frac{1}{1}$.

A teoria apresentada neste Capítulo teve como objetivo abordar de forma mais generalizada as propriedades referentes aos anéis. No capítulo seguinte enfatizaremos as propriedades relacionadas aos anéis de polinômios e as operações a eles relacionadas.

2 Polinômios em uma variável

Considerando os resultados apresentados no Capítulo 1 em especial na Seção 1.2, a respeito de anéis, vamos neste capítulo apresentar os resultados referentes aos polinômios com coeficientes em anéis, bem como as propriedades relacionadas as estes, tais como a igualdade, divisibilidade, decomposição, funções polinomiais e raízes de funções polinomiais.

2.1 Anéis de polinômios

Seja A um anel. Um símbolo x não pertencente ao anel A será chamado de uma *indeterminada sobre* A.

Definição 2.1. *Seja $(A, +, \cdot)$ um anel. Um polinômio numa indeterminada sobre A é uma sequência $(a_0, a_1, a_2, \dots, a_n, \dots)$ onde $a_i \in A$ para todo i em $\mathbb{N}$ e $a_i \neq 0$ apenas para um número finito de índices, ou seja, existe um $n \in \mathbb{N}$ tal que $a_i = 0$, para todo $i > n$.*

Seja $\mathcal{A}$ o conjunto dos polinômios numa indeterminada sobre A. Em $\mathcal{A}$ definimos as operações soma $(+)$ e produto $(\cdot)$:

$$\begin{array}{rccc} (+): & \mathcal{A} \times \mathcal{A} & \to & \mathcal{A} \\ & (a_0, a_1, \dots), (b_0, b_1, \dots) & \mapsto & (a_0 + b_0, a_1 + b_1, \dots) \\ (\cdot): & \mathcal{A} \times \mathcal{A} & \to & \mathcal{A} \\ & (a_0, a_1, \dots), (b_0, b_1, \dots) & \mapsto & (d_0, d_1, \dots) \end{array} \tag{2.1}$$

sendo

$$\begin{cases} d_0 & = a_0 b_0 \\ d_1 & = a_0 b_1 + a_1 b_0 \\ \vdots & = \vdots \\ d_i & = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0 \\ \vdots & = \vdots \\ d_{n+m} & = a_n b_m. \end{cases}$$

Podemos observar que sendo $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$, então consideramos $a_n \neq 0$, $b_m \neq 0$. Assim, temos que $d_{n+m} \neq 0$. Além disso, para $k \geqslant 1$, $k \in \mathbb{N}$, temos

$$d_{n+m+k} = a_0 b_{n+m+k} + \cdots + a_n b_{m+k} + \cdots + a_{n+k} b_m + \cdots + a_{n+m+k} b_0 = 0$$

pois, para todo $i > n$, $j > m$, temos $a_i = 0$ e $b_j = 0$. Considerando a soma $(+)$ e produto $(\cdot)$ em (2.1) e pelas propriedades do anel A, temos:

- *O elemento neutro relativo à soma* $(+)$ *é* $(0,0,0,\ldots)$*;*
- *O elemento neutro relativo ao produto* $(\cdot)$ *é* $(1,0,0,\ldots)$*;*
- *O inverso relativo à soma* $(+)$ *é* $(-a_0,-a_1,\cdots,-a_n,\ldots)$.

Para efeitos de simplificação de notações, faremos nos elementos do anel $\mathcal{A}$ *(sequências), as seguintes associações:*

1. *Um elemento do anel* $(a_0,0,0,0,\ldots)$ *será denotado simplesmente por* a_0.
2. *Denotaremos uma indeterminada* x *pelo elemento do anel* $(0,1,0,0,\ldots)$ *e daí temos*

$$\begin{array}{rcccl} x^2 & = & (0,1,0,0,\ldots)\cdot(0,1,0,0,\ldots) & = & (0,1,0,0,\ldots)^2 = (0,0,1,0,\ldots); \\ x^3 & = & (0,1,0,0,\ldots)^2\cdot(0,1,0,0,\ldots) & = & (0,1,0,0,\ldots)^3 = (0,0,0,1,0,\ldots); \\ \vdots & & & & \\ x^n & = & (0,1,0,0,\ldots)^{n-1}\cdot(0,1,0,0,\ldots) & = & (0,1,0,0,\ldots)^n = (0,0,0,\ldots,0,\underbrace{1}_{n+1},0,\ldots). \end{array}$$

3. *Aplicando as operações soma e produto em* $\mathcal{A}$*, obtemos as expressões:*

$$\begin{array}{rcll} a_0 & = & (a_0,0,0,\ldots); & \\ a_0+a_1x & = & (a_0,0,0,\ldots) & +[(a_1,0,0,0,0,\ldots)\cdot(0,1,0,0,\ldots)]; \\ & & \vdots & \\ a_0+a_1x+\cdots+a_nx^n & = & (a_0,0,0,\ldots) & +[(a_1,0,0,\ldots)\cdot(0,1,0,0,\ldots)] \\ & & & +[(a_1,0,0,\cdots)\cdot(0,1,0,0,\ldots)^2] \\ & & \vdots & \\ & & & +[(a_n,0,0,\ldots)\cdot(0,1,0,0,\ldots)^n]. \end{array}$$

Assim,

$$\begin{array}{rcl} a_0 & = & (a_0,0,0,\ldots) \\ a_0+a_1x & = & (a_0,a_1,0,\ldots) \\ a_0+a_1x+a_2x^2 & = & (a_0,a_1,a_2,0,\ldots) \\ & \vdots & \\ a_0+a_1x+a_2x^2+\cdots+a_nx^n & = & (a_0,a_1,a_2,\ldots,a_n,0,\ldots). \end{array}$$

Considerando as notações acima e as operações de soma e produto, podemos escrever os elementos do anel da forma

$$\mathcal{A}=\left\{\sum_{i=0}^{n}a_ix^i \,|\, n\in\mathbb{N}\, e\, a_i\in A\right\}.$$

Provaremos na Proposição 2.7 que $\mathcal{A}$ *é um anel. O anel* $(\mathcal{A},+,\cdot)$ *será chamado de anel de polinômios em uma indeterminada e para o representar usaremos a notação* $A[x]$*. Assim, dada a indeterminada* $x=(0,1,0,0,0,\ldots)$*,*

$$A[x]=\{a_0+a_1x+a_2x^2+\cdots+a_nx^n;\quad a_j\in A,\quad 0\leqslant j\leqslant n,\quad n\in\mathbb{N}\}. \tag{2.2}$$

Definição 2.2. *(polinômio constante) Seja* A *um anel, e* $a\in A$*. Chamamos de polinômio constante, o polinômio* $p(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n+\cdots$*, onde* $a_0=a$ *e* $a_i=0$ *para todo* $i\geqslant 1$*. O polinômio constante será denotado por*

$$p(x) = a \text{ onde } a \in A.$$

Definição 2.3. *(polinômio nulo) Seja A um anel. Chamamos de polinômio nulo, o polinômio $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$, onde $a_i = 0$ para todo $i \in \mathbb{N}$. O polinômio nulo será denotado por*

$$p(x) = 0.$$

A seguir enunciaremos algumas propriedades que irão melhor caracterizar os anéis de polinômios com coeficientes no anel A.

Proposição 2.4. *A soma de dois polinômios em A é também um polinômio em A isto é, $A[x]$ é fechado em relação à adição.*

Demonstração. Sejam $p(x)$ e $g(x)$ dois polinômios sobre o anel A tais que

$$p(x) = \sum_{i=0}^{n} a_ix^i \quad , \quad g(x) = \sum_{i=0}^{m} b_ix^i.$$

Considerando a operação soma apresentada em (2.1), seja $c_i = a_i + b_i$. Pela Definição 2.1 temos que $a_i = 0$ para todo $i > n$ e $b_i = 0$ para todo $i > m$. Tomando $r = \max\{m, n\}$, temos então que $c_i = 0$, para $i > r$. Logo, a operação $p(x) + g(x)$ também define um polinômio em A. □

Proposição 2.5. *O produto de dois polinômios sobre A é também um polinômio, ou seja, $A[x]$ é fechado em relação à multiplicação.*

Demonstração. Sejam $p(x)$ e $g(x)$ dois polinômios sobre o anel A tais que

$$p(x) = \sum_{i=0}^{n} a_ix^i \quad , \quad g(x) = \sum_{i=0}^{m} b_ix^i.$$

Considerando a operação produto apresentada em (2.1), seja d_i o coeficiente do termo x^i. Pela Definição 2.1 temos $a_i = 0$ para todo $i > n$ e $b_i = 0$ para todo $i > m$. Então para todo $i \geqslant (n + m) + 1$, $d_i = 0$. Logo, $p(x) \cdot g(x)$ é um polinômio sobre o anel A. □

Exemplo 2.6. Sejam $p(x) = x^n - 1$ e $q(x) = x^n + 1$ polinômios em um anel $A[x]$, então:

1. $p(x) + q(x) = (x^n - 1) + (x^n + 1) = 2x^n = g(x) \in A[x]$.
2. $p(x) \cdot q(x) = (x^n - 1) \cdot (x^n + 1) = x^{2n} - 1 = h(x) \in A[x]$.

Proposição 2.7. *Se A é um anel comutativo com unidade, então $A[x]$ também é anel comutativo com unidade.*

Demonstração. Sejam $p(x) = \sum_{i=0}^{n} a_ix^i$, $q(x) = \sum_{i=0}^{m} b_ix^i$, $t(x) = \sum_{i=0}^{l} e_ix^i$ polinômios sobre A na indeterminada x, e consideremos as operações soma e produto como na Definição 2.1, representada em (2.1). Sem perda de generalidade, sejam $n > m > l \in \mathbb{N}$. Então,

(i) $p(x) + (q(x) + t(x)) = (p(x) + q(x)) + t(x)$.

De fato:

$$\begin{aligned}\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} (b_i + e_i)x^i &= \sum_{i=0}^{n} (a_i + b_i + e_i)x^i \\ &= \sum_{i=0}^{n} ((a_i + b_i) + e_i)x^i \\ &= \sum_{i=0}^{n} (a_i + b_i)x^i + \sum_{i=0}^{n} e_i x^i.\end{aligned}$$

(ii) $p(x) + q(x) = q(x) + p(x)$.

De fato:

$$\begin{aligned}\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i &= \sum_{i=0}^{n} (a_i + b_i)x^i \\ &= \sum_{i=0}^{n} (b_i + a_i)x^i \\ &= \sum_{i=0}^{n} b_i x^i + \sum_{i=0}^{n} a_i x^i.\end{aligned}$$

(iii) $p(x) + 0 = 0 + p(x) = p(x)$.

De fato, tomando o polinômio nulo , temos:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} 0x^i = \sum_{i=0}^{n} (a_i + 0)x^i = \sum_{i=0}^{n} a_i x^i.$$

(iv) Existe $\tilde{p}(x)$ tal que $p(x) + \tilde{p}(x) = 0$.

De fato, no anel A, existe $\tilde{a} = -a$ tal que, $a + \tilde{a} = a + (-a) = 0$. Fazendo $\tilde{p}(x) = -p(x)$, onde $-p(x)$ representa o inverso relativo a soma, ou seja,

$$-p(x) = -\sum_{i=0}^{n} (-a_i)x^i,$$

conforme Definição 2.1, então:

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

(v) $p(x) \cdot (q(x) \cdot t(x)) = (p(x) \cdot q(x)) \cdot t(x)$.

Sejam $p(x) \cdot q(x)$ e $q(x) \cdot t(x)$ definidos por:

- $p(x) \cdot q(x)$

$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{n+m} \left(\sum_{i=\lambda+\gamma} a_\lambda \cdot b_\gamma \right) x^i,$$

- $q(x) \cdot t(x)$

$$\sum_{i=0}^{m} b_i x^i \cdot \sum_{i=0}^{l} e_i x^i = \sum_{i=0}^{m+l} \left(\sum_{i=\gamma+\mu} b_\gamma \cdot e_\mu \right) x^i.$$

Usando a propriedade comutativa do anel A e a operação de produto, temos que:

$$\begin{aligned}
\sum_{i=0}^{n} a_i x^i \cdot \left(\sum_{i=0}^{m} b_i x^i \cdot \sum_{i=0}^{l} e_i x^i \right) &= \sum_{i=0}^{n} a_i x^i \sum_{i=0}^{m+l} \left(\sum_{i=\gamma+\mu} b_\gamma \cdot e_\mu \right) x^i \\
&= \sum_{i=0}^{n+m+l} \left(\sum_{i=\lambda+\mu+\gamma} a_\lambda \cdot b_\gamma \cdot e_\mu \right) x^i \\
&= \sum_{i=0}^{n+m} \left(\sum_{i=\lambda+\gamma} a_\lambda \cdot b_\gamma \right) x^i \cdot \sum_{i=0}^{l} e_i x^i \\
&= \left(\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{m} b_i x^i \right) \cdot \sum_{i=0}^{l} e_i x^i.
\end{aligned}$$

(vi) $p(x) \cdot (q(x) + t(x)) = p(x) \cdot q(x) + p(x) \cdot t(x)$.

De fato, usando a propriedade distributiva do anel A e a operação de produto conforme a expressão (2.1), temos:

$$\begin{aligned}
\sum_{i=0}^{n} a_i x^i \cdot \left(\sum_{i=0}^{m} (b_i + e_i) x^i \right) &= \sum_{i=0}^{n+m} \left(\sum_{i=\lambda+\mu} a_\lambda \cdot (b_\mu + e_\mu) x^i \right) \\
&= \sum_{i=0}^{n+m} \left(\sum_{i=\lambda+\mu} a_\lambda \cdot b_\mu + a_\lambda \cdot e_\mu \right) x^i \\
&= \sum_{i=0}^{n+m} \left(\sum_{i=\lambda+\mu} a_\lambda \cdot b_\mu \right) x^i + \sum_{i=0}^{n+m} \left(\sum_{i=\lambda+\mu} a_\lambda \cdot e_\mu \right) x^i.
\end{aligned}$$

(vii) $p(x) \cdot q(x) = q(x) \cdot p(x)$.

De fato,

$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n+m} \left(\sum_{i=0}^{n} a_\lambda \cdot b_\mu \right) x^i = \sum_{i=0}^{n+m} \left(\sum_{i=0}^{n} b_\mu \cdot a_\lambda \right) x^i.$$

(viii) $p(x) \cdot 1 = 1 \cdot p(x) = p(x)$.

Tomando $h(x) = 1$ (polinômio constante), temos:

$$\left(\sum_{i=0}^{n} a_i x^i \right) \cdot 1 = 1 \cdot \left(\sum_{i=0}^{n} a_i x^i \right) = \sum_{i=0}^{n} (a_i \cdot 1) x^i = \sum_{i=0}^{n} a_i x^i.$$

□

Proposição 2.8. *Se D é um domínio de integridade, então $D[x]$ também é um domínio de integridade .*

Demonstração. Sejam $p(x) = \sum_{i=0}^{n} a_i x^i$, $q(x) = \sum_{i=0}^{m} b_i x^i$, polinômios não nulos de $D[x]$, com $a_n \neq 0$ e $b_m \neq 0$. Considerando a operação de produto como na Definição 2.1 temos que o coeficiente do termo $d_{n+m} = a_n \cdot b_m$. Como a_n e $b_m \in D$ são não nulos, então $a_n \cdot b_m \neq 0$. Assim, $p(x) \cdot q(x) \neq 0$. Dai concluímos que $D[x]$ é domínio pois, para $p(x) \cdot q(x) = 0$ devemos ter $p(x)$ ou $q(x)$ nulo.

□

Os elementos dos anéis A e $A[x]$ são de natureza distinta. No entanto, se considerarmos as propriedades de isomorfismo, podemos supor que $A \subset A[x]$. Assim, as proposições e definições abaixo nos darão a imersão de A em $A[x]$.

Proposição 2.9. *Se A é um anel, então $I = \{(a, 0, 0, 0, \ldots, 0, \ldots) \,|\, a \in A\}$ é um subanel de $A[x]$.*

Demonstração. Usando as condições de subanel da Proposição 1.22, temos que:

(i) $I \neq \varnothing$ pois $0 = (0, 0, 0, 0, \ldots, 0, \ldots) \in I$;

(ii) Seja $p = (a, 0, 0, \ldots, 0, \ldots)$ e $q = (b, 0, 0, \ldots, 0, \ldots)$, então $p - q = (a - b, 0, 0, \ldots, 0, \ldots) \in I$;

(iii) Seja $p = (a, 0, 0, \ldots, 0, \ldots)$ e $q = (b, 0, 0, \ldots, 0, \ldots)$, então $p \cdot q = (a \cdot b, 0, 0, \ldots, 0, \ldots) \in I$.

□

Proposição 2.10. *Seja A um anel e $I = \{(a, 0, 0, \ldots, 0, \ldots) \,|\, a \in A\}$ um subanel de $A[x]$. Temos que A é isomorfo a I.*

Demonstração. Para demonstrar esta Proposição, vamos considerar a aplicação $F\colon A \to I$ dada por $F(x) = (x, 0, 0, \ldots, 0, \ldots)$. Provemos que F é um isomorfismo. De fato, considerando as propriedades de um isomorfismo temos:

(i) $F(a + b) = (a + b, 0, 0, \ldots, 0, \ldots) = (a, 0, 0, \ldots, 0, \ldots) + (b, 0, 0, \ldots, 0, \ldots) = F(a) + F(b)$, para todo $a, b \in A$;

(ii) $F(a \cdot b) = (a \cdot b, 0, 0, \ldots, 0, \ldots) = (a, 0, 0, \ldots, 0, \ldots) \cdot (b, 0, 0, \ldots, 0, \ldots) = F(a) \cdot F(b)$, para todo $a, b \in A$;

(iii) $F(a) = F(b)$ então $(a, 0, 0, \ldots, 0, \ldots) = (b, 0, 0, \ldots, 0, \ldots)$, logo $a = b$, para todo $a, b \in A$. Portanto F é injetora.

(iv) Dados $(x, 0, 0, \ldots, 0, \ldots) \in I$, temos que $(x, 0, 0, \ldots, 0, \ldots) = F(x)$. Portanto F é sobrejetora.

□

Devido ao isomorfismo entre A e I podemos identificar cada $a \in A$ ao polinômio $(a, 0, 0, \ldots, 0, \ldots) \in I$. Assim,

$$a = (a, 0, 0, \ldots, 0, \ldots).$$

Considerando válida essa igualdade e considerando ainda $0 = (0, 0, 0, \ldots, 0, \ldots)$ e $1 = (1, 0, 0, \ldots, 0, \ldots)$ podemos abusar da notação $A \subset A[x]$.

O conceito de polinômio sobre o anel A foi apresentado conforme a Definição 2.1. Vamos agora enfatizar as propriedades e operações dos polinômios considerando o anel dos coeficientes e definir alguns elementos referentes aos polinômios.

2.2 Propriedades sobre anéis e corpos de polinômios

Definição 2.11. *(grau de polinômio) Seja A um anel e $p(x)$ um polinômio em $A[x]$, tal que,*

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

com $a_n \neq 0$ e $a_j = 0$ para todo $j > n$. Dizemos que o número natural n é o grau de $p(x)$ e indicamos por $\partial p(x) = n$. O coeficiente a_n é chamado de coeficiente líder de $p(x)$. Se o coeficiente líder for $a_n = 1$, chamamos polinômio mônico.

O grau de um polinômio, $\partial p(x) = n$, pode ser interpretado como uma função do conjunto de todos os polinômios não nulos no conjunto $\mathbb{N}$ da seguinte maneira:

$$\begin{array}{rccc} \partial\colon & A[x]\backslash\{0\} & \to & \mathbb{N} \\ & p(x) & \mapsto & \partial p(x). \end{array}$$

Observação 2.12. Embora pareça natural definir o polinômio nulo como sendo um polinômio de grau zero, tal definição acarretaria um problema entre a relação grau e raízes de uma função polinomial (a ser abordada posteriormente).

Exemplo 2.13. Sejam $p(x), q(x) \in \mathbb{R}[x]$, $p(x) = x^5 + x^4 - 1$, $q(x) = x^7 - x^8$.

- $\partial p(x) = 5$ e $p(x)$ é polinômio mônico.
- $\partial q(x) = 8$.

Os resultados a serem apresentados abaixo nos permitem analisar melhor as características do grau de um polinômio, considerando as operações de soma e produto de polinômios.

Teorema 2.14. *Sejam $p(x)$ e $q(x)$ polinômios com coeficientes no anel A, tais que $p(x) + q(x) \neq 0$ e $p(x) \cdot q(x) \neq 0$ então,*

(i) $\partial\,(p(x) + q(x)) \leqslant \max\{\partial p(x), \partial q(x)\}$;

(ii) $\partial\,(p(x) \cdot q(x)) \leqslant \partial p(x) + \partial q(x)$.

Demonstração. Sejam

$$p(x) = \sum_{i=0}^{n} a_ix^i \quad , \quad q(x) = \sum_{i=0}^{m} b_ix^i,$$

com $a_n \neq 0$, $b_m \neq 0$ e $c_i = a_i + b_i$, $i \in \mathbb{N}$. Vamos supor, sem perda de generalidade que $n \geqslant m$.

(i) $p(x)+q(x)=\sum_{i=0}^{n} c_i x^i$.

- Se $n>m$ temos $\partial(p(x)+q(x))=n$ pois como $a_n\neq 0$ então $c_n=a_n+0=a_n$.
- Se $n=m$ podemos ter
  - $a_n+b_n=0$ e então $\partial(p(x)+q(x))<n$.
  - $a_n+b_n\neq 0$ e então $\partial(p(x)+q(x))=n$.

(ii) $p(x)\cdot q(x)=\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{n+m}\left(\sum_{i=\lambda+\gamma} a_\lambda \cdot b_\gamma\right) x^i$.

Seja d_i o coeficiente do termo x^i, e então o coeficiente líder do produto é dado por:

$$d_{n+m}=a_n\cdot b_m.$$

- Se $a_n b_m\neq 0$, considerando-os não divisores do zero, temos $\partial(p(x)\cdot q(x))=\partial p(x)+\partial q(x)$.

- Se a_n ou b_m, são divisores dos zero então podemos ter $a_n b_m=0$ e então $\partial(p(x)\cdot q(x))<\partial p(x)+\partial q(x)$.

Portanto $\partial(p(x)\cdot q(x))\leqslant \partial p(x)+\partial q(x)$.

□

Exemplo 2.15. Sejam em $\mathbb{Z}_6$, os polinômios $p(x)$ e $g(x)$ tais que,

$$\begin{aligned} p(x) &= \overline{2}x^2+\overline{1}x+\overline{3},\\ g(x) &= \overline{3}x^2+\overline{5}. \end{aligned}$$

Então,

$p(x)+g(x)=\overline{5}x^2+\overline{1}x+\overline{2}$,

$p(x)\cdot g(x)=\overline{3}x^3+\overline{1}x^2+\overline{5}x+\overline{3}$.

Assim temos:

- $\partial(p(x)+g(x))=\max\{\partial p(x),\partial g(x)\}=2$.
- $\partial(p(x)\cdot g(x))<\partial p(x)+\partial g(x)$.

Pelas considerações feitas na demonstração do Teorema 2.14 item *(ii)*, enunciamos o seguinte corolário.

Corolário 2.16. *Se D é um domínio, então $\partial\left(p(x)\cdot q(x)\right)=\partial p(x)+\partial q(x)$.*

Demonstração. Para que $\partial\left(p(x)\cdot q(x)\right)<\partial p(x)+\partial q(x)$ devemos ter o produto entre os coeficientes dominantes $a_n b_m=0$, com $a_n, b_m\neq 0$, o que é impossível considerando as propriedades de um domínio. Logo $\partial\left(p(x)\cdot q(x)\right)=\partial p(x)+\partial q(x)$. □

Exemplo 2.17. Sejam em $\mathbb{R}[x]$ os polinômios $p(x) = -x^4+x^3-1$ e $q(x) = x^4+3x^3+x^2$.

- $\partial(p(x) + q(x)) = 3 < \max\{\partial p(x), \partial q(x)\}$,
- $\partial(p(x) \cdot q(x)) = 8 = \partial p(x) + \partial q(x)$.

Para prosseguirmos e apresentarmos as operações em polinômios sobre anéis e corpos e definirmos propriedades referentes a divisibilidade e fatoração, definiremos a notação de elementos invertíveis e divisores de zero em anéis. Assim, seja A um anel comutativo com unidade e o anel de polinômio $A[x]$. Indicaremos por $U(A)$ e $U(A[x])$ o conjuntos dos elementos invertíveis de A e $A[x]$, respectivamente.

Teorema 2.18. *Se D é um domínio, então os únicos elementos invertíveis de $D[x]$, são os elementos invertíveis de D.*

Demonstração. Seja $p(x) \in D[x]$ um elemento invertível no anel de polinômios sobre D, ou seja, $p(x) \in U(D[x])$. Então existe $g(x) \in D[x]$ tal que $p(x) \cdot g(x) = 1$ e então $\partial(p(x) \cdot g(x)) = 0$, logo, pelo Corolário 2.16 devemos ter $p(x) = c$ e $g(x) = k$, onde $c, k \in D$. Pelo fato de $p(x) \cdot q(x) = 1$, então $c \cdot k = 1$, ou seja, são elementos invertíveis de D. Assim, $p(x)$ e $g(x)$ são polinômios em $D[x]$ e elementos invertíveis em D, logo, $p(x)$, $g(x) \in U(A)$, $U(A[x]) \subseteq U(A)$. □

Teorema 2.19. *Seja A um anel comutativo com unidade. Se um polinômio $p(x)$ em $A[x]$, é um divisor próprio do zero, então existe $c \in A, c \neq 0$ tal que $cp(x) = 0$.*

Demonstração. Seja $g(x) \in A[x]$ tal que $g(x) \cdot p(x) = 0$. Vamos mostrar que $\partial g(x) = 0$, ou seja, $g(x) = c \in A$. Para isso, consideremos o polinômio de grau mínimo e coeficiente dominante c, definido por $g(x) = c_0 + c_1x + \cdots + cx^r$, e seja $p(x) = a_0 + a_1x + \cdots + a_nx^n$. Vamos supor por absurdo que $\partial g(x) > 0$ e analisar as seguintes situações:

(i) Se $a_ig(x) = 0$, $0 \leqslant i \leqslant n$ teremos $a_ic = 0$, $(0 \leqslant i \leqslant n)$ e então $c \cdot p(x) = 0$. Com isso teremos $\partial g(x) = 0$, contrariando a hipótese sobre o $\partial g(x)$.

(ii) Se existe um certo índice s tal que $a_sg(x) \neq 0, 0 \leqslant s \leqslant n$ e $a_sg(x) = 0, s+1 \leqslant i \leqslant n$ e pelo fato de $g(x) \cdot p(x) = 0$ então $g(x)a_0 + g(x)a_1x + \cdots + g(x)a_nx^n = 0$ ou $g(x) \cdot (a_0 + a_1x + \cdots + a_sx^s) = 0$ e assim, $ca_s = 0$. Seja $h(x) = a_sg(x)$. Temos que $h(x)$ é não nulo e $\partial h(x) < \partial g(x)$ e ainda $h(x) \cdot p(x) = a_sg(x) \cdot p(x) = 0$, ou seja, $h(x) \cdot p(x) = 0$ com $\partial h(x) < \partial g(x)$, contrariando o fato de $g(x)$ ser de grau mínimo.

Assim, de (i) e (ii) concluímos que $\partial g(x) = 0$.

□

Corolário 2.20. *Se um polinômio não nulo $p(x) \in A[x]$ é um divisor próprio do zero em $A[x]$, então todos os coeficientes não nulos de $p(x)$ são divisores próprios do zero em A. Se pelo menos um dos coeficientes é regular então $p(x)$ é regular em $A[x]$.*

Demonstração. Pelo Teorema 2.19, existe $c \neq 0$, $c \in A$ tal que $cp(x) = 0$. Assim, considerando $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, então temos $ca_n = ca_{n-1} = \cdots = ca_1 = ca_0$. Logo, todo coeficiente a_i não nulo, com $i = \{0, 1, 2, \ldots, n\}$ é divisor do zero. □

Apresentaremos outras definições e propriedades referentes a polinômios e funções polinomiais relacionados a estrutura de anéis e em alguns casos explicitaremos que a estrutura considerada será a de corpos.

Definição 2.21. *(função polinomial) Seja $(D, +, \cdot)$ um domínio infinito. Chama-se função polinomial sobre D, determinada pelo polinômio $f(x) \in D[x]$ com coeficientes $a_0, a_1, ..., a_n$, a aplicação:*

$$\begin{array}{rccl} f & : & D[x] & \to & D[x] \\ & & p(x) & \mapsto & f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n. \end{array}$$

Observação 2.22. A respeito de polinômios e funções polinomiais, fazemos as seguintes considerações:

(i) Dado um elemento $(a_0, a_1, \ldots, a_n, 0, \ldots)$ de $D[x]$, pode-se definir, utilizando seus coeficientes, a função polinomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Isto implica na existência de uma correspondência entre os elementos de $D[x]$ e as funções polinomiais com coeficientes em D.

(ii) Se D não for domínio infinito, não podemos considerar essa identificação: polinômio e função polinomial. Para melhor compreender isso, consideremos o anel de polinômios $\mathbb{Z}_5[x]$ e a função polinomial:

$$\begin{array}{rcl} \mathbb{Z}_5 & = & \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}; \\ p(x) & = & x^5 + \overline{4}x. \end{array}$$

Considerando o polinômio $p(x)$, podemos observar que não é um polinômio nulo, no entanto, seja $f(x) = x^5 + \overline{4}x$. Temos que $f(\overline{0}) = f(\overline{1}) = f(\overline{2}) = f(\overline{3}) = f(\overline{4}) = \overline{0}$, ou seja, para todo elemento u de $\mathbb{Z}_5$, temos $f(u) = \overline{0}$, que corresponde à função nula. Daí temos que não existe uma correspondência biunívoca entre $p(x)$ e $f(x)$ pois $p(x)$ não é polinômio nulo.

(iii) Observe que a diferença entre polinômio e função polinomial é sutil. Conforme Definição 2.1, um polinômio é uma sequência de elementos $(a_0, a_1, \ldots, a_n, 0, \ldots)$, com uma quantidade finita de elementos não nulos e nomeando $x = (0, 1, 0, \ldots)$ uma indeterminada em $A[x]$, pode-se denotar o polinômio $(a_0, a_1, \ldots, a_n, 0, \ldots)$ por $a_0 + a_1x + \cdots + a_nx^n$, expressão que coincide com a expressão da função polinomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Assim, embora sejam elementos de conjuntos distintos, $a_0 + a_1x + \cdots + a_nx^n \in A[x]$ e $f(x) = a_0 + a_1x + \cdots + a_nx^n$, no subconjunto das funções de D em D, costumeiramente se refere a ambos como sendo 'o mesmo' elemento.

(iv) Em domínios infinitos toma-se a liberdade de referir-se ao polinômio para falar de elementos de $D[x]$ e de funções polinomiais. A distinção entre um e outro fica dependendo do contexto onde é citado.

Exemplo 2.23. Sejam as funções polinomiais, definidas em $D[x]$ um domínio infinito.

- O polinômio nulo $p(x) = 0$ determina a função $f(x) = 0$.
- Todo polinômio constante $p(x) = a$ determina uma função constante $f(x) = a$.

Definição 2.24. *(raiz de função polinomial) Seja $(D, +, \cdot)$ domínio e $f(x)$ uma função polinomial sobre D. Um elemento $u \in D$ é chamado de raiz de $f(x)$ se $f(u) = 0$ (zero do domínio).*

Observação 2.25. Se a função polinomial é da forma $f(x) = c$, para todo $x \in D$ sendo $c \neq 0$ uma constante, então não há raiz desta função polinomial. Por outro lado, se para todo x em D tem-se $f(x) = 0$, então todo elemento x em D é raiz do polinômio $f(x)$. Sendo assim, esse polinômio tem infinitas raízes se D é infinito.

Exemplo 2.26. Seja $f(x) \in \mathbb{C}[x]$ definido por $f(x) = -1 + x - x^2 + x^3$, temos que $f(1) = f(i) = f(-i) = 0$. Portanto $\{1, \ i, \ -i\}$ são raízes de $f(x)$.

Definição 2.27. *(derivada de função polinomial) Seja A um anel comutativo com unidade e $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n \in A[x]$, definimos como derivada de $f(x)$, usando a notação $f'(x)$ para derivada de ordem 1 e $f^{(n)}$ para derivada de ordem n maior que 1, a função polinomial:*

$$\begin{aligned} f'(x) &= a_1 + 2a_2x^1 + 3a_3x^2 + \cdots + na_nx^{n-1}, \\ f^{(2)}(x) &= (f'(x))' \\ &\vdots \\ f^{(n)}(x) &= (f^{(n-1)})'(x). \end{aligned}$$

Para quaisquer $f(x), g(x) \in A[x]$ temos:

(a) $(f(x) + g(x))' = (f(x))' + (g(x))'$;

(b) $(f(x) \cdot (g(x))' = (f(x))' \cdot g(x) + f(x) \cdot (g(x))'$;

(c) $((x - a)^n)' = n(x - a)^{n-1}$, $a \in K$.

Exemplo 2.28. Sobre o corpo $\mathbb{C}$, consideremos a função polinomial $f\colon \mathbb{C} \to \mathbb{C}$, definida por $f(x) = x^4 - \sqrt{5}x$. A derivada desta função é dada por:

1. $f'(x) = 4x^3 - \sqrt{5}$.
2. $f^{(2)}(x) = 12x^2$.

Na Definição 2.24 apresentamos o conceito de raiz. Vamos apresentar alguns resultados e propriedades obtidas a partir desta definição.

Para isso consideremos que, para $u \in D$, em $D[x]$ é válida a igualdade, facilmente verificada por indução finita,

$$x^n - u^n = (x - u)(x^{n-1} + ux^{n-2} + \cdots + u^{n-2}x + u^{n-1}). \tag{2.3}$$

Proposição 2.29. *Seja D um domínio e $u \in D$ raiz de um polinômio $p(x)$ não constante pertencente a $D[x]$, definido por*

$$p(x) = a_0 + a_1x^1 + \cdots + a_nx^n,$$

então

$$p(x) = (x - u)q(x),$$

onde $q(x) \in D[x]$ e

$$q(x) = b_0 + b_1(x) + \cdots + b_{n-1}x^{n-1},$$

com $b_j \in D$, para $j = \{0, 1, \ldots, n-2\}$ e $b_{n-1} = a_n$.

Demonstração. Como u é raiz de $p(x)$, então:

$$p(x) - p(u) = (a_0 + a_1x + \cdots + a_nx^n) - (a_0 + a_1u + \cdots + a_nu^n)$$
$$p(x) - p(u) = a_1(x-u) + a_2(x^2 - u^2) + \cdots + a_n(x^n - u^n)$$

Considerando a igualdade (2.3) e colocando $(x-u)$ em evidência temos

$$p(x) - p(u) = (x-u)[(a_1 + a_2u + \cdots + a_nu^{n-1}) + (a_2 + a_3u + \cdots + a_nu^{n-2})x + \cdots + a_nx^{n-1}]$$
$$p(x) - p(u) = (x-u)q(x).$$

Como $p(u) = 0$ (zero do anel), então:

$$p(x) = (x-u)q(x).$$

□

Corolário 2.30. *Seja D um domínio. Se $u_1, u_2, \cdots, u_m$ são raízes distintas de um polinômio não nulo $p(x) \in D[x]$, definido por $p(x) = a_0 + a_1x^1 + \cdots + a_nx^n$, então*

$$p(x) = (x-u_1)(x-u_2)\cdots(x-u_m)q_m(x)$$

onde $q_m \in D[x]$, $m \leqslant n$ e

$$q_m(x) = a_nx^{n-m} + b_{m+1}x^{n-(m+1)} + \cdots + b_0,$$

para todo $x \in D$.

Demonstração. Seja $p(x) = a_0 + a_1x^1 + \cdots + a_nx^n$

- Se u_1 é raiz de $p(x)$, pela Proposição 2.29 temos

  $$p(x) = (x-u_1)q_1(x),$$

  sendo
  $$q_1(x) = a_nx^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0.$$

- Se u_2 é raiz de $p(x)$, e $u_2 \neq u_1$, u_2 também é raiz de $q_1(x)$, então temos $q_1(x) = (x-u_2)q_2(x)$, logo
  $$p(x) = (x-u_1)\cdot(x-u_2)q_2(x),$$

  sendo
  $$q_2(x) = a_nx^{n-2} + b_{n-3}x^{n-3} + \cdots b_0.$$

Seguindo raciocínio análogo sobre as raízes $u_3, .., u_m$ temos que para algum $q_m = a_nx^{n-m} + \cdots + b_0$,

$$p(x) = (x-u_1)(x-u_2)\cdots(x-u_m)q_m(x),$$

onde $q_m \in D[x]$ e temos

$$q_m(x) = a_nx^{n-m} + bx^{n-(m+1)} + \cdots + b_0,$$

para todo $x \in D$. □

Corolário 2.31. *Seja D domínio, $D[x]$ o anel de polinômios sobre D e $p(x) = a_0 + a_1x^1 + \cdots + a_nx^n$ não nulo. Então, o número de raízes distintas de $p(x)$ em D é no máximo igual a $\partial p(x) = n$*

Demonstração. Se m é o número de raízes distintas e $m > n$, então $m = n+k$, para algum $k \geqslant 1$. Assim, na notação do Corolário 2.30, teríamos ao menos $u_1, u_2, \cdots, u_n, u_{n+1}$ raízes distintas. Logo, aplicando-se às raízes $u_1, u_2, \cdots, u_n$ teríamos

$$p(x) = (x - u_1)(x - u_2)\cdots(x - u_n)q_n(x),$$

com $q_n(x) = a_n$, isto é,

$$p(x) = a_n(x - u_1)(x - u_2)\cdots(x - u_n).$$

Porém, u_{n+1} seria raiz de $p(x)$ e como $(u_{n+1} - u_i) \neq 0$, para $i = 1, 2, \ldots, n$, isso implicaria em $a_n = 0$, uma contradição. Assim, o número de raízes é no máximo igual a n. □

Exemplo 2.32. Seja em $\mathbb{R}[x]$ o polinômio $p(x) = x^4 + 3x^2 - 4$. Temos que 1 e -1 são raízes de $p(x)$, então:

$$p(x) = (x - 1) \cdot (x + 1) \cdot (x^2 + 4).$$

Proposição 2.33. *Sejam $p(x)$ e $q(x)$ polinômios sobre o domínio $D[x]$, tal que $p(x) = a_0 + a_1x^1 + \cdots + a_nx^n$ e $q(x) = b_0 + b_1x^1 + \cdots + b_mx^m$, com $a_n \neq 0$, $b_m \neq 0$. Então $p(x) = q(x)$ se, e somente se, $m = n$ e $a_i = b_i$, para todo i em $\{0, 1, 2, \ldots, n\}$.*

Demonstração.

($\Rightarrow$) Como $p(x) = q(x)$ então $p(x) - q(x) = 0$. Assim,

(i) vamos supor que $m < n$. Então,

$$(a_0 - b_0) + (a_1 - b_1)x^1 + \cdots + (a_m - b_m)x^m + \cdots + a_nx^n = 0,$$

logo,

$$\begin{aligned} a_0 - b_0 = 0 &\Rightarrow a_0 = b_0 \\ a_1 - b_1 = 0 &\Rightarrow a_1 = b_1 \\ &\vdots \\ a_m - b_m = 0 &\Rightarrow a_m = b_m \\ &\vdots \\ a_n - 0 = 0 &\Rightarrow a_n = 0, \end{aligned}$$

o que é absurdo pois $a_n \neq 0$.

(ii) vamos supor então que $m > n$. Analogamente ao item (i) obtemos $b_m = 0$, o que é absurdo.

Portanto, de (i) e (ii) concluímos que $m = n$ e daí,

$$\begin{aligned} a_0 - b_0 = 0 &\Rightarrow a_0 = b_0 \\ a_1 - b_1 = 0 &\Rightarrow a_1 = b_1 \\ &\vdots \\ a_n - b_n = 0 &\Rightarrow a_n = b_m \end{aligned}$$

Logo, $a_i = b_i$ para $i = \{0, 1, 2, \ldots, n\}$.

($\Leftarrow$) Como $m = n$ e $a_i = b_i$, então $a_i - b_i = 0$, para $i = \{0, 1, \ldots, n\}$, logo

$$\sum_{i=0}^{n}(a_i - b_i)x^i = 0 \Rightarrow p(x) - q(x) = 0 \Rightarrow p(x) = q(x).$$

□

Na Seção 2.2 enunciamos alguns resultados sobre os polinômios, relacionadas com as raízes e os elementos do anel de polinômio. Vamos agora definir algumas propriedades referentes a divisibilidade, irredutibilidade e decomposição, considerando os polinômios sobre anéis e corpos.

2.3 Divisibilidade em polinômios

Nesta seção apresentaremos algumas propriedades que caracterizam a divisibilidade em polinômios. Para introduzir este conceito, utilizamos as propriedades da divisão euclidiana em $\mathbb{Z}$, generalizando para anéis de polinômios.

Definição 2.34. *(domínio euclidiano) Um domínio euclidiano $(D, +, \cdot, \partial)$ é um domínio $(D, +, \cdot)$ com uma função:*

$$\begin{array}{rccl} \partial: & D\backslash\{0\} & \to & \mathbb{N} = \{0, 1, 2, \cdots\} \\ & a & \mapsto & \partial(a) \end{array},$$

que satisfaz as seguintes propriedades:

- *Para todo $a, b \in D, b \neq 0$, existem $t, r \in D$ tais que:*

$$a = bt + r \ com \begin{cases} \partial(r) < \partial(b) \\ ou\ r = 0 \end{cases};$$

- $\partial(a) \leqslant \partial(ab)$, *para todo a, $b \in D\backslash\{0\}$.*

Exemplo 2.35. Seja a função valor absoluto definida por:

$$\begin{array}{rccl} |\ |: & \mathbb{Z} & \to & \mathbb{N} \\ & a & \to & |a| = \begin{cases} a & \text{se } a \geqslant 0 \\ -a & \text{se } a \leqslant 0 \end{cases}. \end{array}$$

Temos que $(\mathbb{Z}, +, \cdot, |\ |)$ é um domínio euclidiano.

Solução. Sendo $(\mathbb{Z}, +, \cdot)$ um domínio, segue do algoritmo da divisão euclidiana, que para todo a, b em $\mathbb{Z}$, $b \neq 0$, existem t e r em $\mathbb{Z}$ tais que,

$$a = bt + r \text{ com } \begin{cases} |r| < |b| \\ \text{ou } r = 0 \end{cases} \text{ e } |a| \leqslant |ab|.$$

Vamos agora estender a definição de domínio euclidiano a polinômios sobre anéis e corpos.

Teorema 2.36. *Seja $(A,+,\cdot)$ um anel comutativo com unidade e seja $A[x]$ o anel de polinômios sobre A. Seja $p(x) \in A[x]$ e $g(x) \in A[x]$ um polinômio em que o coeficiente líder é invertível em A. Então existem e são únicos $q(x), r(x) \in A[x]$ tais que:*

$$p(x) = g(x)\cdot q(x) + r(x) \text{ com } \begin{cases} \partial(r(x)) < \partial(g(x)) \\ ou\ r(x) = 0 \end{cases} ;$$

Demonstração. Sejam,

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \text{ sendo } \partial p(x) = n$$
$$g(x) = b_0 + b_1x + \cdots + b_mx^m \text{ sendo } \partial g(x) = m.$$

Sem perda de generalidade, vamos assumir $n \geqslant m$. Como o coeficiente líder b_m é invertível, então existe em A o elemento b_m^{-1} (inverso de b_m), e assim o polinômio $h(x) = a_nb_m^{-1}x^{n-m}$ pertence a $A[x]$. Multiplicando $g(x)$ por $h(x)$ obtemos a expressão:

$$\begin{aligned} p(x) \;=\; & a_nb_m^{-1}x^{n-m}g(x) + [a_{n-1} - a_nb_m^{-1}b_{m-1}]x^{n-1} + \cdots + \\ & [a_{n-m} - a_nb_m^{-1}b_{m-1}]x^{n-m} + \cdots + a_1x + a_0. \end{aligned}$$

Vamos chamar de $p_1(x)$ a expressão

$$[a_{n-1} - a_nb_m^{-1}b_{m-1}]x^{n-1} + \cdots + [a_{n-m} - a_nb_m^{-1}b_{m-1}]x^{n-m} + \cdots + a_1x + a_0,$$

observe que $\partial p_1(x) \leqslant n-1$, e então podemos escrever

$$p(x) = a_nb_m^{-1}x^{n-m}g(x) + p_1(x). \tag{2.4}$$

A partir desta expressão, podemos considerar que:

(i) Se $\partial p_1(x) < \partial g(x)$, ou $p_1(x) = 0$ então podemos tomar $q(x) = a_nb_m^{-1}x^{n-m}$ e $r(x) = p_1(x)$.

(ii) Se $\partial p_1(x) > \partial g(x)$, seja

$$p_1(x) = c_px^p + c_{p-1}x^{p-1} + \cdots + c_1(x) + c_0$$

onde $c_p \neq 0$, e $m \leqslant p \leqslant n-1$. De forma análoga a que foi feita na expressão de $p(x)$ em (2.4) , multiplicamos $g(x)$ por $c_pb_m^{-1}x^{p-m}$ obtemos a expressão

$$p_1(x) = c_pb_m^{-1}x^{p-m}g(x) + p_2(x), \tag{2.5}$$

com $\partial p_2(x) \leqslant n-2$.

A partir desta expressão podemos escrever o polinômio $p(x)$ como

$$p(x) = [a_nb_m^{-1}x^{n-m} + c_pb_m^{-1}x^{p-m}]g(x) + p_2(x). \tag{2.6}$$

e analisar as seguintes situações:

- Se $\partial p_2(x) < \partial g(x)$, ou $p_2(x) = 0$, tomamos $q(x) = a_nb_m^{-1}x^{n-m} + c_pb_m^{-1}x^{p-m}$ e $r(x) = p_2(x)$;
- Se $\partial p_2(x) > \partial g(x)$ repetimos o processo como em (2.4) e obtemos uma expressão semelhante a (2.6).

Observe que nestes processos, ao obtermos os polinômios $p_i(x)$, com $\partial(p_i(x)) \leqslant n-i$, em algum momento teremos $p_i(x) = 0$ ou $\partial p_i(x) < \partial g(x)$ pois, $m \leqslant n$. Assim, podemos obter os polinômios $q(x)$ e $r(x)$ nas condições enunciadas.

Vamos mostrar que são únicos. Para isso, sejam $q_1(x), q_2(x), r_1(x), r_2(x)$ tais que,

$$p(x) = g(x) \cdot q_1(x) + r_1(x) = g(x) \cdot q_2(x) + r_2(x),$$

onde $r_i(x) = 0$ ou $\partial r_i(x) < \partial g(x)$, para $i = 1, 2$ e daí temos

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

Da igualdade acima, podemos verificar que se $q_1(x) \neq q_2(x)$ temos $\partial((q_1(x) - q_2(x))g(x)) \geqslant \partial g(x)$ e ao mesmo tempo $\partial(r_2(x) - r_1(x)) < \partial g(x)$, obtendo uma contradição. Assim $q_1(x) = q_2(x)$ e daí consequentemente verificamos que $r_2(x) = r_1(x)$. Assim, demonstramos a unicidade. □

Corolário 2.37. *(algoritmo da divisão) Seja $(K, +, \cdot)$ um corpo e $K[x]$ o anel de polinômios sobre K. Os resultados do Teorema anterior são válidos para quaisquer polinômios em $K[x]$, pois os coeficientes serão invertíveis.*

No Teorema 2.36 e Corolário 2.37 apresentamos a divisão de polinômios em anéis e corpos. Vamos agora definir as condições a respeito da divisibilidade em polinômios.

Definição 2.38. *(divisibilidade) Seja A um anel comutativo com unidade e $A[x]$ o anel de polinômios sobre A. Sejam $p(x), g(x) \in A[x]$, $g(x) \neq 0$. Dizemos que $g(x)$ é divisor de $p(x)$ em $A[x]$, se existe $h(x) \in A[x]$, tal que:*

$$p(x) = h(x) \cdot g(x).$$

Usamos a notação $g(x) \mid p(x)$ em $A[x]$ e dizemos que $p(x)$ é divisível por $g(x)$.

A divisibilidade em $A[x]$ apresenta algumas propriedades imediatas.

Proposição 2.39. *(Propriedades imediatas da divisibilidade em $A[x]$) Sejam $p(x)$, $g(x)$, $h(x)$ polinômios em $A[x]$. Considerando a Definição 2.38 obtemos as propriedades imediatas:*

(i) $p(x) \mid p(x)$ *(reflexiva).*

(ii) *se* $p(x) \mid g(x)$ *e* $g(x) \mid h(x)$ *então* $p(x) \mid h(x)$ *(transitiva).*

(iii) *se* $p(x) \mid g_1(x)$ *e* $p(x) \mid g_2(x)$ *então* $p(x) \mid (g_1(x)h_1(x) + g_2(x)h_2(x))$, *para todo* $h_1(x), h_2(x) \in A[x]$.

Demonstração.

(i) $p(x) = 1 \cdot p(x)$. Assim, considerando $h(x) = 1$ temos que $p(x) \mid p(x)$.

(ii) Sejam $p_1(x), p_2(x) \in A[x]$ tais que:
$p(x) \mid g(x) \Rightarrow g(x) = p_1(x) \cdot p(x)$;
$g(x) \mid h(x) \Rightarrow h(x) = p_2(x) \cdot g(x)$.
Então $h(x) = p_2(x) \cdot g(x) = p_2(x) \cdot p_1(x) \cdot p(x)$.
Logo, $p(x) \mid h(x)$.

(iii) Sejam $q_1(x), q_2(x) \in A[x]$ tais que:

$$g_1(x) = p(x) \cdot q_1(x) \quad \text{e} \quad g_2(x) = p(x) \cdot q_2(x).$$

Daí

$$\begin{aligned} g_1(x)h_1(x) + g_2(x)h_2(x) &= p(x)q_1(x)h_1(x) + p(x)q_2(x)h_2(x) \\ &= p(x)(q_1(x)h_1(x) + q_2(x)h_2(x)). \end{aligned}$$

Então $p \mid (g_1(x)h_1(x) + g_2(x)h_2(x)$.

□

Teorema 2.40. *(Teorema do resto) Seja $p(x) \in A[x]$, um polinômio, com $\partial p(x) \geqslant 1$. Se A é um subanel, com unidade, do domínio de integriade D e $u \in D$, então o resto da divisão de $p(x)$ por $(x-u)$ em $D[x]$ é $p(u)$.*

Demonstração. Sejam $q(x)$ e $r(x)$, respectivamente, o quociente e resto da divisão de $p(x)$ por $(x-u)$, então:

$$p(x) = (x-u) \cdot q(x) + r(x) \text{ com } \begin{cases} \partial(r(x)) < \partial(x-u) \\ \text{ou } r(x) = 0 \end{cases}.$$

Se $r(x) \neq 0$ então $\partial r(x) = 0$, ou seja $r(x)$ é constante. Fazendo $x = u$ temos:

$$p(u) = (u-u) \cdot q(u) + r(u),$$

como $r(x)$ é constante, então $r(x) = p(u)$. Se $r(x) = 0$, então,

$$\begin{aligned} p(x) &= (x-u)q(x) \\ p(u) &= (u-u)q(u) \\ p(u) &= 0. \end{aligned}$$

Logo, $r(x) = p(u)$. □

Como consequência da Definição 2.24, Definição 2.38, do Teorema 2.37, Corolário 2.37 e Teorema 2.40, apresentados até este momento a respeito da divisão e divisibilidade em polinômios, apresentaremos algumas definições e proposições:

Proposição 2.41. *Seja $p(x) \in A[x]$ um polinômio tal que $\partial p(x) \geqslant 1$. Se A é um subanel com unidade, do domínio D, e u um elemento de D, então $(x-u) \mid p(x)$, $(p(x) \in D[x])$ se, e somente se $p(u) = 0$.*

Demonstração.

($\Rightarrow$) Se $(x-u) \mid p(x)$ então o resto da divisão de $p(x)$ por $(x-u)$ é 0. Mas, pelo Teorema 2.40, esse resto é $p(u)$. Logo $p(u) = 0$.

($\Leftarrow$) Como $p(u)$ é o resto da divisão de $p(x)$ por $(x-u)$ e $p(u) = 0$, então $p(x) = (x-u)q(x)$, $q(x) \in D[x]$. Logo $(x-u) \mid p(x)$.

□

Definição 2.42. *(multiplicidade de uma raiz) Seja A um anel, $p(x) \in A[x]$, um polinômio de grau n, $u \in A$ e seja $s \geqslant 1$ um inteiro. Dizemos que u é uma raiz de multiplicidade s de $p(x)$ se, $(x-u)^s$ divide $p(x)$ mas $(x-u)^{s+1}$ não divide $p(x)$.*

Lema 2.43. *Seja A um anel comutativo com unidade e $A[x]$ o anel de polinômios sobre A. Se $(x-u)^s g(x) = 0$, para $u \in A$, então $g(x) = 0$.*

Demonstração. Suponhamos que $(x-u)^s g(x) = 0$ e $g(x) \neq 0$. De $(x-u)^s g(x) = 0$, temos que o coeficiente líder do produto é nulo. Tal coeficiente é o produto dos coeficientes líderes x^s e $a_n x^n$, que é $a_n \cdot 1 = a_n$, o que é uma contradição, pois teríamos $a_n = 0$. Logo, $g(x) = 0$. □

Proposição 2.44. *Sejam $p(x) \in A[x]$, $u \in A$, e seja $s \geqslant 1$ um inteiro. As afirmações seguintes são equivalentes:*

(i) u é raiz de multiplicidade s de $p(x)$.

(ii) Existe $g(x) \in A[x]$ tal que $p(x) = (x-u)^s g(x)$, com $g(u) \neq 0$.

Demonstração.

$(i) \Rightarrow (ii)$ Suponhamos que $g(u) = 0$, então $g(x) = (x-u)\tilde{g}(x)$. Daí, $p(x) = (x-u)^s(x-u)\tilde{g}(x)$, o que é uma contradição pois neste caso u seria raiz de multiplicidade $s+1$. Logo u é raíz de multiplicidade s e $g(u) \neq 0$.

$(ii) \Rightarrow (i)$ Considerando a Definição 2.42, vamos mostrar que $(x-u)^{s+1} \nmid p(x)$. Suponhamos por absurdo que $(x-u)^{s+1} \mid p(x)$. Então,

$$p(x) = (x-u)^{s+1} h(x) \text{ com } h(x) \in A[x].$$

Assim,

$$(x-u)^s g(x) = (x-u)^{s+1} h(x),$$

e então,

$$(x-u)^s [g(x) - (x-u)h(x)] = 0.$$

Como $(x-u)^s$ é um polinômio mônico, pelo Lema 2.43, temos que

$$g(x) - (x-u)h(x) = 0,$$

e então,

$$g(x) = (x-u)h(x).$$

Assim, $g(u) = 0$, o que é uma contradição, pois $g(u) \neq 0$. Logo $(x-u)^s$ é raiz de multiplicidade s de $p(x)$.

□

Corolário 2.45. *Sejam D um domínio e $p(x) \in D[x]$, $p(x) \neq 0$, tal que $\partial p(x) = n$ Então:*

(i) Se $u_1, \ldots, u_k$ são todas as raízes com multiplicidades respectivamente $e_1, \ldots, e_k$, temos

$$p(x) = (x - u_1)^{e_1} \cdots (x - u_k)^{e_k} g(x),$$

onde $g(x) \in D[x]$ é um polinômio que não tem raiz em D.

(ii) O número de raízes de $p(x)$ em $D[x]$ é no máximo igual ao grau de $p(x)$, ou seja, se s é o número de raízes de $p(x)$, então $s \leqslant n$.

Demonstração.

(i) Consideremos

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Dividindo $p(x)$ por $(x - u_1)^{e_1} \cdots (x - u_k)^{e_k} g(x)$ tem-se

$$p(x) = \underbrace{(x - u_1)^{e_1} \cdots (x - u_k)^{e_k}}_{\tilde{p}(x)} g(x) + r(x),$$

com grau de $r(x)$ menor que $e_1 + e_2 + \cdots + e_k$.

Observe também que $(x - u_1)^{e_1}$ divide $p(x)$ e divide $\tilde{p}(x)$. Logo, divide $r(x)$ ou $r \neq 0$. Se $r \neq 0$ temos,

$$p(x) = \tilde{p}(x) + (x - u_1)^{e_1} r_1(x),$$

com $r_1(x) \neq 0$(pois $r \neq 0$). Agora, $(x - u_2)^{e_2}$ divide $p(x)$ e divide $\tilde{p}(x)$. Logo, divide $r_1(x)$, que fornece $r_1(x) = (x - u_2^{e_2}) r_2(x)$ com $r_2(x) \neq 0$ e consequentemente,

$$p(x) = \tilde{p}(x) + (x - u_1)^{e_1} (x - u_2)^{e_2} r_2(x),$$

com $r_2(x) \neq 0$ (pois $r \neq 0$).

Procedendo desta forma, obtemos

$$r(x) = (x - u_1)^{e_1} \cdots (x - u_k)^{e_k} r_k(x),$$

com $r_k \neq 0$, o que contradiz o grau de $r(x)$ ser menor que $e_1 + e_2 + \cdots + e^k$. Portanto, não pode acontecer $r \neq 0$. Com $r(x) = 0$ temos

$$p(x) = (x - u_1)^{e_1} \cdots (x - u_k)^{e_k} g(x). \tag{2.7}$$

Segue da expressão (2.7) que $g(x)$ não pode ter raiz distinta de $u_1, u_2, \ldots, u_k$, pois ela seria raiz de $p(x)$. Além disso, se fizermos

$$g_1(x) = (x - u_2)^{e_2} \cdots (x - u_k)^{e_k} g(x),$$

temos

$$p(x) = (x - u_1)^{e_1} g_1(x),$$

e a Proposição 2.44 fornece $g_1(u_1) \neq 0$, o que implica $g(u_1) \neq 0$.

Procedendo desta forma, $g(u_i) \neq 0$, para $i = 1, 2, 3, \ldots, k$ e portanto $g(x)$ não possui raízes em D.

(ii) Temos da expressão (2.7) que

$$p(x) = (x - u_1)^{e_1} \cdots (x - u_k)^{e_k} g(x),$$

o que implica que $s = e_1 + e_2 + \cdots + e_k \leqslant n$. Logo, o número de raízes contada a multiplicidade não excede ao valor de n.

□

2.4 Maior Divisor Comum - M.D.C.

Nesta seção apresentaremos a definição e propriedades do maior divisor comum (M.D.C.) entre polinômios. Para isso, vamos considerar essa definição em anéis e posteriormente estender aos anéis de polinômios.

Definição 2.46. *(elemento primo) Um elemento $p \in D$, onde D é um domínio, é primo se:*

(i) $p \neq 0$.

(ii) p *não é invertível.*

(iii) Para todo $a, b \in D$, *se* $p \mid ab$ *então* $p \mid a$ *ou* $p \mid b$.

Definição 2.47. *Sejam a, b em D, onde D é domínio. Dizemos que o elemento a é associado ao elemento b, usando a notação $a \sim b$, se $a \mid b$ e $b \mid a$.*

Definição 2.48. *(elemento irredutível) Um elemento $p \in D$, onde D é domínio, é irredutível se:*

(i) $p \neq 0$.

(ii) p *não é invertível.*

(iii) Para todo $a, b \in D$, *se* $p \mid ab$, *então* a *é invertível e então temos que* b *é associado de* p, *ou* b *é invertível e então* a *é associado de* p.

A Definição 2.46 e a Definição 2.48 nos levam a seguinte Proposicão:

Proposição 2.49. *Todo elemento primo de um domínio D é também irredutível.*

Demonstração. Seja $p = ab$ com $a, b \in D$, então $p \mid a$ ou $p \mid b$. Sem perda de generalidade, vamos usar a divisibilidade em a. Então existe um elemento c em D, tal que $a = pc$ e daí podemos reescrever a igualdade

$$p = ab \Rightarrow p = pcb.$$

Daí temos $bc = 1$. Logo b é invertível e a é associado de p. Analogamente, considerando $p \mid b$ temos que a é invertível e associado a b. □

Definição 2.50. *(polinômio primo) Seja D um domínio, $D[x]$ o anel de polinômios em D. Um polinômio não nulo e não constante $p(x) \in D[x]$ é chamado de primo se, ao representarmos $p(x) = g(x) \cdot h(x)$, então $p(x) \mid g(x)$ ou $p(x) \mid h(x)$, sendo $g(x), h(x) \in D[x]$.*

Proposição 2.51. *Seja D um domínio, $D[x]$ o anel de polinômios sobre D, e $p(x) \in D[x]$ um polinômio não nulo e de grau maior ou igual a 1. Dizemos que um polinômio $g(x) \in D[x]$ é associado de $p(x)$ se, e somente se, $g(x) = c \cdot p(x)$, onde c é um elemento invertível de $D[x]$.*

Demonstração.

($\Rightarrow$) Como são associados, pela Definição 2.47 $g(x) \mid p(x)$ e $p(x) \mid g(x)$ e, pela Definição 2.38, existem polinômios $g_1(x)$ e $p_1(x)$, ambos em $D[x]$, tais que,

$$g(x) = p(x) \cdot g_1(x) \quad \text{e} \quad p(x) = g(x) \cdot p_1(x).$$

Assim,

$$p(x) = p(x) \cdot (g_1(x)p_1(x)).$$

Com isso, temos que $g_1(x)p_1(x) = 1$, ou seja, $g_1(x)$ é elemento invertível em $D[x]$ e então, pelo Teorema 2.18, $g_1(x) = c$, onde $c \in D$ é um elemento invertível.

($\Leftarrow$) Seja $g(x) = c \cdot p(x)$ com $c \in D$ invertível. Temos que $p(x) \mid g(x)$. Além disso, como c é invertível, então existe c^{-1} e daí obtemos $p(x) = c^{-1}g(x)$. Logo, $g(x) \mid p(x)$. Com isso, temos que $p(x) \mid g(x)$ e $g(x) \mid p(x)$, portanto, são associados em $D[x]$.

□

Exemplo 2.52. Consideremos os polinômios sobre $D[x]$, onde D é um domínio, tais que $p(x) = 1 + x$ e $g(x) = a + ax$, sendo $a \in D$ é um elemento invertível. Temos que

- $a + ax = a \cdot (1 + x) \Rightarrow 1 + x \mid a + ax$.
- $1 + x = \frac{1}{a}(a + ax) \Rightarrow a + ax \mid 1 + x$.

Logo, concluímos que são associados em $D[x]$.

Definição 2.53. *(maior divisor comum - M.D.C.) Um elemento $d \in D$, sendo D um domínio, é maior divisor comum - M.D.C., de $a, b \in D$ se:*

(i) $d \mid a$ *e* $d \mid b$*;*

(ii) todo divisor de a, b é divisor de d.

Definição 2.54. *(primos entre si) Se o M.D.C. de a e b, ambos em D é igual a* 1 *(unidade do anel), então eles são considerados primos entre si.*

Teorema 2.55. *Seja D um domínio e consideremos em D os elementos $a_1, a_2, \ldots, a_n$. Seja o ideal I de D, gerado por $a_1, a_2, \ldots, a_n$, ou seja $I = D \cdot a_1 + D \cdot a_2 + \cdots + D \cdot a_n$. Se I é ideal principal, ou seja, se existe $d \in D$ tal que $I = D \cdot d$, então;*

(i) Existem $r_1, r_2, \ldots, r_n$ em D, tais que

$$d = r_1 \cdot a_1 + r_2 \cdot a_2 + \cdots + r_n \cdot a_n;$$

(ii) O elemento d é o M.D.C.$\{a_1, a_2, \ldots, a_n\}$.

Demonstração. (i) Como $I = D \cdot d$ então

$$D \cdot d = D \cdot a_1 + D \cdot a_2 + \cdots + D \cdot a_n.$$

(ii) Seja

$$D \cdot d = D \cdot a_1 + D \cdot a_2 + \cdots + D \cdot a_n.$$

Então, para cada $a_i \in D$, $i = \{1, 2, \ldots n\}$, temos que $a_i \in D \cdot a_1 + D \cdot a_2 + \cdots + D \cdot a_n = D \cdot d$. Assim existem $r_i \in D$, $i = \{1, 2, \ldots, n\}$ tais que $a_i = r_i \cdot d$. Logo d é divisor comum de $a_1, a_2, \ldots, a_n$. Além disso, se existir $d' \in D$ tal que d' é divisor de a_i, então $a_i = r_i \cdot d'$. Assim, $D \cdot d \subset D \cdot d'$, logo d' divide d e então d é o M.D.C$\{a_1, a_2, \ldots, a_n\}$.

□

Teorema 2.56. *Seja $(D, +, \cdot, \partial)$ um domínio euclidiano como na Definição 2.34. Então:*

(i) D é um domínio principal;

(ii) Para todo $a, b \in D\backslash\{0\}$ pode-se encontrar efetivamente $e, f \in D$ tal que,

$$M.D.C.\ \{a, b\} = ea + fb,$$

se a divisão em D for efetiva, ou seja, existe o M.D.C de a e b em D.

Demonstração.

(i) Seja I um ideal, D um domínio e $I \subset D$. Vamos mostrar que $I = \langle a \rangle$ ou seja, para todo $x \in I$, $x = ay$, $a \in I$, $y \in D$. Para isso, consideremos o conjunto

$$\partial(I\backslash\{0\}) = \{\partial(\alpha) \,|\, \alpha \in I,\ \alpha \neq 0\} \subseteq \mathbb{N}.$$

Esse conjunto possui um menor elemento, pois $\mathbb{N}$ é bem ordenado. Seja $a \in I$ o elemento cuja imagem é esse menor elemento. Como D é euclidiano e $I \subset D$, então existe $y, r \in D$ tal que

$$x = ay + r \text{ com } \begin{cases} \partial(r) < \partial(a) \\ \text{ou } \ r = 0 \end{cases}.$$

Do fato de $x = ay + r$ e I ser um ideal temos que $-ay \in I$ e então podemos considerar que

$$r = x - ay,$$

e daí temos que $r \in I$. Assim, $\partial(r) < \partial(a)$ ou $r = 0$. Como a é o menor elemento do conjunto $I\backslash\{0\}$, então não podemos ter $\partial(r) < \partial(a)$, logo $r = 0$ e então concluímos que $x = ay$, ou seja, todo elemento de I é gerado por a. Assim, temos que I é ideal principal e então os ideais de D são principais, logo, D é um domínio principal.

(ii) Como D é euclidiano, então existem r_1, t_1 tais que para $a \in D$,

$$a = bt_1 + r_1 \ \text{ com } \ \begin{cases} \partial(r_1) < \partial(b) \\ \text{ou } \ r_1 = 0 \end{cases}. \tag{2.8}$$

Daí consideremos que

1. Sobre r_1 temos as seguintes situações:
   - Se $r_1 = 0$ então
   $$a = bt_1.$$
   Assim, O M.D.C. existe e é igual a b e podemos escrever
   $$\text{M.D.C.}\{a, b\} = 0 \cdot a + 1 \cdot b.$$
   - Se $r_1 \neq 0$ vamos considerar um elemento $c \in D$. Então c divide a e b se, e somente se, divide b e r_1. Assim
   $$d = \text{M.D.C.}\{a.b\} = \text{M.D.C.}\{b, r_1\}.$$

   Considerando b e r_1, existem $r_2, t_2 \in D$ tais que
   $$b = r_1 t_2 + r_2 \text{ com } \begin{cases} \partial(r_2) < \partial(t_2) \\ \text{ou } r_2 = 0 \end{cases}. \tag{2.9}$$

2. Sobre r_2 temos as seguintes situações.
   - Se $r_2 = 0$ então
   $$b = r_1 t_2.$$
   Assim, o M.D.C.$\{b, r_1\}$ existe e é igual r_1 e podemos escrever
   $$\text{M.D.C.}\{b, r_1\} = 1a + (-t_1)b.$$
   - Se $r_2 \neq 0$ vamos considerar um elemento $c \in D$. Esse elemento c divide b e r_1, se, e somente se, c divide r_1 e r_2. Assim,
   $$d = \text{M.D.C.}\{b, r_1\} = \text{M.D.C.}\{r_1, r_2\}.$$

   Agora considerando r_1, r_2, existem $t_3, r_3 \in D$ tais que
   $$r_1 = r_2 t_3 + r_3 \text{ com } \begin{cases} \partial(r_3) < \partial(r_2) \\ \text{ou } r_3 = 0 \end{cases}.$$

3. Sobre r_3 temos as seguintes situações:
   - Se $r_3 = 0$ então
   $$r_1 = r_2 t_3.$$
   Assim, o M.D.C. existe e podemos escrever
   $$\text{M.D.C.}\{a, b\} = (-t_2)a + (t_1 t_2 + 1)b.$$
   - Se $r_3 \neq 0$ e continuando o processo, obtem-se um r_{i+1} tal que
   $$\begin{cases} \partial(r_{i+1}) < \partial(r_i) \\ \text{ou } r_{i+1} = 0 \end{cases}.$$

Como a função ∂ toma valores em $\mathbb{N}$ então vai existir um n tal que não teremos $\partial(r_{n+1}) < \partial(r_n)$ sendo então $r_{n+1} = 0$. Com isso, temos

$$\text{M.D.C.}\{a, b\} = \cdots = \text{M.D.C.}\{r_{n-1}, r_n\} = r_n,$$

o que mostra que e e f podem ser efetivamente calculados, sendo M.D.C. escrito como combinação linear de a e b.

□

Corolário 2.57. *Sejam K um corpo e $p_1(x), p_2(x) \in K[x]$ dois polinômios primos entre si, ou seja, M.D.C.$\{p_1(x), p_2(x)\} = 1$. Seja $p(x) \in K[x]$. Então:*

(i) É possível calcular efetivamente $g_1(x)$ e $g_2(x)$ em $K[x]$ tais que

$$p(x) = g_1(x)p_1(x) + g_2(x)p_2(x);$$

(ii) Se $\partial p(x) < \partial p_1(x) + \partial p_2(x)$ então os polinômios e $g_1(x)$, $g_2(x)$ são tais que:

$$\partial g_1(x) < \partial p_2(x) \text{ ou } g_1 = 0;$$
$$\partial g_2(x) < \partial p_1(x) \text{ ou } g_2 = 0.$$

Demonstração.

(i) Pelo Corolário 2.37 $(K, +, \cdot, \partial)$ é domínio euclidiano, então a divisão em K é efetiva. Como $p_1(x)$ e $p_2(x)$ são primos entre si, pelo Teorema 2.56, podemos encontrar $e_1(x), e_2(x)$ tais que

$$1 = e_1(x)p_1(x) + e_2(x)p_2(x)$$

e daí podemos obter $p(x)$ tal que:

$$p(x) = p(x)e_1(x)p_1(x) + p(x)e_2(x)p_2(x).$$

Assim podemos considerar $g_1(x)$ e $g_2(x)$ efetivamente calculados e tais que:

$$g_1(x) = p(x)e_1(x) \text{ e } g_2(x) = p(x)e_2(x).$$

(ii) Pelo Corolário 2.37 existem $q(x)$ e $r(x)$ em $K[x]$ tais que:

$$g_1(x) = p_2(x)q(x) + r(x) \text{ com } \begin{cases} \partial r(x) < \partial p_2(x) \\ \text{ou } r(x) = 0 \end{cases}.$$

Assim temos,

$$p(x) = r(x)p_1(x) + [p_1(x)q(x) + g_2(x)]\, p_2(x),$$

com

$$\partial(r(x)p_1(x)) < \partial p_1(x) + \partial p_2(x) \text{ ou } r(x) = 0,$$

e então,

$$\partial\,[p_1(x)q(x) + g_2(x)]\, p_2(x) < \partial p_1(x) + \partial p_2(x) \text{ ou } p_1(x)q(x) + g_2(x) = 0.$$

Portanto $p_1(x)q(x) + g_2(x)$ tem grau menor que $p_1(x)$ ou é igual a zero. Assim, $r(x)$, $p_1(x)q(x) + g_2(x)$, satisfazem as propriedades referentes ao grau.

□

O Teorema abaixo dará as condições necessárias para que um polinômio seja o maior divisor comum - M.D.C..

Teorema 2.58. *Sejam sobre o corpo* $K[x]$

- $p_1(x), \ldots, p_m(x) \in K[x] \backslash \{0\}$;
- $I = K[x] \cdot p_1(x) + \cdots + K[x] \cdot p_m(x)$ *um ideal de gerado pelos polinômios não nulos* $p_1(x), \ldots, p_m(x)$.

Se existe $d(x) \in K[x]$ *tal que* $I = K[x] \cdot d(x)$, *então são válidas as seguintes propriedades:*

(i) Existem, $r_1(x), \ldots, r_m(x) \in K[x]$ *tais que,*

$$d(x) = r_1(x) \cdot p_1(x) + \cdots + r_m(x) \cdot p_m(x).$$

(ii) $d(x)$ *é um divisor comum de* $p_1(x), \ldots, p_m(x)$.

(iii) Se $d'(x)$ *é um divisor comum de qualquer* $p_1(x), \ldots, p_m(x)$ *então* $d'(x) \mid d(x)$.

(iv) $d(x)$ *é o M.D.C de* $p_1(x), \ldots, p_m(x) \in K[x] \backslash \{0\}$.

Demonstração.

(i) O resultado segue da igualdade

$$K[x] \cdot d(x) = K[x] \cdot p_1(x) + \cdots + K[x] \cdot p_m(x).$$

(ii) Seja $i \in \{1, \ldots, m\}$ e $K[x] \cdot d(x) = K[x]\, p_1(x) + \cdots + K[x] \cdot p_m(x)$. Então,

$$p_i(x) \in K[x] \cdot p_i(x) \subset K[x] \cdot p_1(x) + \cdots + K[x] \cdot p_m(x) = K[x] \cdot d(x).$$

Assim, podemos considerar que existe $r_i(x) \in K[x]$ tal que $p_i(x) = r_i(x) \cdot d(x)$, isto é, $d(x)$ é divisor de cada $p_i(x)$, $i = \{1, 2, \ldots, m\}$.

(iii) Seja $d'(x)$ um divisor comum de $p_1(x), \ldots, p_m(x)$ em $K[x]$. Então existe um $r_i(x)$ em $K[x]$ tal que $p_i(x) = r_i(x) \cdot d'(x)$ para $i = \{1, 2, \ldots, m\}$. Assim,

$$K[x] \cdot p_i(x) \subset K[x] \cdot d'(x), \quad \forall i \in \{1, 2, \ldots, m\}.$$

Daí temos $K[x] \cdot d(x) \subset d'(x)K[x]$ ou seja, existe $r(x) \in K[x]$ tal que $d(x) = r(x) \cdot d'(x)$.

□

Observação 2.59. Se o M.D.C. $\{p_1(x), \ldots, p_m(x)\} = 1$, então eles são primos entre si ou relativamente primos.

Teorema 2.60. *Seja* K *um corpo,* $p(x), g(x) \in K[x]$. *Se* $r(x)$ *é o resto da divisão de* $p(x)$ *por* $g(x)$, *então* $M.D.C\{p(x), g(x)\} = M.D.C\{g(x), r(x)\}$.

Demonstração. Seja $p(x) = q(x) \cdot g(x) + r(x)$ e $M.D.C\{p(x), g(x)\} = d(x)$. Temos pela Definição 2.38 que $d(x) \mid p(x)$ e $d(x) \mid g(x)$ e então podemos escrever:

$$p(x) = d(x) \cdot q_1(x); \tag{2.10}$$

$$g(x) = d(x) \cdot q_2(x). \tag{2.11}$$

Por outro lado temos,

$$r(x) = p(x) - q(x) \cdot g(x). \tag{2.12}$$

Substituindo as expressões (2.10) e (2.11) em (2.12) obtemos:

$$\begin{aligned} r(x) &= d(x) \cdot q_1(x) - d(x) \cdot q_2(x) \cdot q(x) \\ &= d(x) \cdot [q_1(x) - q_2(x) \cdot q(x)], \end{aligned}$$

e assim podemos verificar que $d(x)$ é divisor de $r(x)$.

Seja $M.D.C\{g(x), r(x)\} = d_1(x)$. Pelo item (iii) do Teorema 2.58 $d(x) \mid d_1(x)$ e pela Definição 2.38 escrevemos:

$$g(x) = d_1(x) \cdot q_3(x); \tag{2.13}$$

$$r(x) = d_1(x) \cdot q_4(x). \tag{2.14}$$

Substituindo em $p(x)$ as expressões (2.13) e (2.14), então:

$$\begin{aligned} p(x) &= q(x) \cdot g(x) + r(x) \\ &= q(x) \cdot d_1(x) \cdot q_3(x) + d_1(x) \cdot q_4(x) \\ &= d_1(x) \cdot [q(x) \cdot q_3(x) + q_4(x)]. \end{aligned}$$

Dai, $d_1(x)$ é divisor de $p(x)$. Como também é divisor de $g(x)$, então $d_1(x) \mid d(x)$. Assim, pelo fato de $d(x) \mid d_1(x)$ e $d_1(x) \mid d(x)$, então $d_1(x) = d(x)$. Logo, $M.D.C\{p(x), g(x)\} = M.D.C\{g(x), r(x)\}$. □

2.5 Fatoração de polinômios

Vamos introduzir sobre os polinômios o conceito análogo aos números inteiros, referente a primalidade, irredutibilidade e fatoração. Para isso apresentaremos algumas definições e propriedades que caracterizam a fatoração em polinômios e quando estes são irredutíveis.

Definição 2.61. *Seja D um domínio e $p(x), g(x)$ polinômios não nulos de $D[x]$. Um polinômio $m(x)$ é um mínimo múltiplo comum, ou M.M.C. de $p(x)$ e $g(x)$ se:*

(i) $m(x)$ é múltiplo de $p(x)$ e também de $g(x)$;

(ii) Se existir outro polinômio $h(x)$ múltiplo de $p(x)$ e também de $g(x)$, então $h(x)$ é múltiplo de $m(x)$.

Nosso objetivo será apresentar as condições necessárias sobre os polinômios sobre as quais poderemos escrever um polinômio como produto de elementos irredutíveis, ou em outras palavras, dizer se esse polinômio é redutível ou não.

Definição 2.62. *(polinômio irredutível) Um polinômio $p(x)$ de grau maior ou igual a um, é irredutível em:*

(i) $D[x]$, *onde* D *é um domínio, se ao representarmos* $p(x) = g(x) \cdot q(x)$, *então* $g(x)$ *é invertível em* D *ou* $q(x)$ *é invertível em* D, *o que equivale a dizer, pelo Teorema 2.18 que* $g(x) = c$, *onde* c *é constante e invertível em* D, *ou* $q(x) = d$, *onde* d *é constante invertível em* D.

(ii) $K[x]$, *onde* K *é um corpo, se ao representarmos* $p(x) = g(x) \cdot q(x)$, *com* $g(x), q(x) \in K[x]$ *então* $g(x) = a$ *ou* $q(x) = b$, *onde* a *e* b *são constantes pertencentes a* K.

Definição 2.63. *(domínio de fatoração única) Um domínio* D *é fatorial se, todo a não nulo em* D, *e não-invertível, se escreve de maneira única, como produto de elementos irredutíveis de* D, *isto é:*

(i) $a = p_1 \cdot p_2 \cdots p_r$, *com* p_i *primos, para* $1 \leqslant i \leqslant r$.

(ii) Se $\{p_i\}_{1 \leqslant i \leqslant r}$ *e* $\{q_j\}_{1 \leqslant j \leqslant s}$ *são elementos irredutíveis de* D *tais que* $p_1 \cdots p_r = q_1 \cdots q_s$ *então:*

- $r = s$;
- *A menos da ordem,* p_i *é associado a* q_i *ou seja,* $p_i = uq_i$ *onde* $u_i \in D$ *é invertível, isto é, existe uma bijeção* $\sigma(i)$ *de* $\{1, \ldots, r\}$ *sobre* $\{1, \ldots, r\}$ *tal que* p_i *é associado a* $q_{\sigma(i)}$.

Definição 2.64. *(polinômio primitivo) Seja* D *um domínio fatorial e seja um polinômio não nulo* $p(x) = a_0 + a_1x + \cdots + a_nx^n$ *em* $D[x]$. *Nestas condições,* $p(x)$ *é primitivo se os coeficientes* $a_0, a_1, a_2, \ldots, a_n$ *são primos entre si.*

Definição 2.65. *(conteúdo de p(x)) Seja* D *um domínio fatorial e seja um polinômio não nulo* $p(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x]$. *Chamaremos de conteúdo de* $p(x)$, *o elemento* c *de* D, *tal que* c *é o M.D.C. de* $\{a_0, ..., a_n\}$. *Esse elemento será denotado por* $c = c(p(x))$.

O lema abaixo nos apresentará as condições necessárias e suficientes para que um elemento $c \in D$, seja o conteúdo de $p(x)$.

Lema 2.66. *Seja* D *um domínio fatorial e seja um polinômio não nulo e não primitivo* $p(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x]$. *Um elemento* $c \in D$ *é o conteúdo de* $p(x)$ *se, e somente se, existe um polinômio primitivo* $p_1(x) \in D[x]$ *tal que* $p(x) = c \cdot p_1(x)$.

Demonstração.

($\Rightarrow$) Suponhamos que c seja o M.D.C $\{a_0, a_1, \ldots, a_n\}$, ou seja, o conteúdo de $p(x)$. Sejam $a_i = cb_i$, com $i = 0, 1, \ldots, n$. Temos que os coeficientes b_i são primos entre si, pois qualquer divisor comum entre eles seria divisor de a_i. Escrevendo o polinômio

$$p_1(x) = b_0 + b_1x + \cdots + b_nx^n,$$

temos que este é um polinômio primitivo. Assim, temos que o polinômio $p(x)$ é tal que, $p(x) = c \cdot p_1(x)$.

($\Leftarrow$) Suponhamos que exista um polinômio primitivo $p_1(x)$ tal que $p(x) = c \cdot p_1(x)$. Seja c_1 o M.D.C. dos coeficientes de $p(x)$. Como c é divisor comum dos coeficientes de $p(x)$, então $c \mid c_1$ e então podemos escrever $c_1 = k \cdot c$, com $k \in D$. Por outro

lado, como $p(x)$ não é primitivo, então existe um polinômio primitivo $p_2(x)$ de $D[x]$ tal que $p(x) = c_1 \cdot p_2(x)$ e daí

$$\begin{cases} p_1(x) = k \cdot p_2(x) \\ p(x) = c \cdot p_1(x) \end{cases} \quad \text{então} \quad c \cdot p_1(x) = c_1 p_2(x),$$

logo, $c_1 \mid c$ ou $c_1 \mid p(x)$ em $D[x]$. E daí, se $c_1 \mid c$ e como $c \mid c_1$ então eles são associados e c é o conteúdo de $p(x)$. Se $c_1 \mid p(x)$ então c_1 divide os coeficientes de $p_1(x)$, logo $c_1 = 1$ e $p(x)$ é primitivo, o que nos traz uma contradição, pois $p(x)$ não é primitivo.

□

Observação 2.67. Considerando a Definição 2.64, a Definição 2.65 e o Lema 2.66, $p(x)$ é um polinômio primitivo em $D[x]$ se o conteúdo de $p(x)$ é um elemento invertível de $D[x]$.

Lema 2.68. *O produto entre dois polinômios primitivos é um polinômio primitivo.*

Demonstração. Seja D um domínio fatorial, e sejam em $D[x]$ os polinômios primitivos e não nulos:

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$
$$g(x) = b_0 + b_1 x + \cdots + b_m x^m.$$

Consideremos $h(x) = p(x) \cdot g(x)$, com $h(x) \in D[x]$ tal que,

$$h(x) = c_0 + c_1 x + \cdots + c_k x^k + \cdots + c_{n+m} x^{n+m},$$

com $c_k = \sum_{i+j=k} a_i b_j$. Suponhamos por absurdo que $h(x)$ não seja primitivo. Então existe um elemento irredutível $d \in D$ tal que $d \mid c_k$ para $0 \leqslant k \leqslant n+m$. Mas, como $p(x)$ e $g(x)$ são primitivos, então d não divide todos os coeficientes de $p(x)$ e $g(x)$. Assim, existem índices r e s onde $0 \leqslant r \leqslant n$ e $0 \leqslant s \leqslant m$, tais que, $d \nmid a_r$ e $d \nmid b_s$ e $d \mid a_i$ para $i < r$ e $d \mid b_j$ para $j < s$. Daí, considerando o coeficiente c_{r+s} de $h(x)$ então $d \mid a_r$ ou $d \mid b_s$ contra a definição de a_r e b_s pois são primos entre si. Assim concluímos que $h(x) = p(x) \cdot g(x)$ é também um polinômio primitivo. □

Lema 2.69. *Todo polinômio não nulo $p(x) \in K[x]$ pode ser representado na forma*

$$p(x) = \left(\frac{c}{d}\right) p_1(x),$$

com $c, d \in D$ onde D é um domínio e $p_1(x) \in D[x]$ é primitivo.

Demonstração. Seja D um domínio, K o corpo das frações de D, $D[x]$, $K[x]$ o anel de polinômios sobre eles, e consideremos o polinômio $p(x) = \sum_{i=0}^{n} a_i x^i$ de $K[x]$, onde $a_i \in K$ para $0 \leqslant i \leqslant n$. Vamos escrever $a_i = \left(\frac{c_i}{d_i}\right)$, onde $c_i, d_i \in D$ e $d_i \neq 0$. Considerando que podemos ter $d = d_0 d_1 \cdots d_n$ então,

$$p(x) = \left(\frac{1}{d}\right) g(x),$$

onde $g(x) \in D[x]$. Pelo Lema 2.66 existe um polinômio primitivo $p_1(x)$ tal que

$$g(x) = c \cdot p_1(x),$$

com $c \in D$. Logo, podemos escrever

$$p(x) = \left(\frac{c}{d}\right) p_1(x),$$

obtendo assim a representação onde temos um polinômio primitivo. □

Considerando as definições e propriedades apresentadas, a respeito de elementos primos, primitivos, redutíveis e irredutíveis, vamos analisar as condições para as quais os polinômios apresentam tais propriedades.

Teorema 2.70. *Seja D um domínio e $D[x]$ o anel de polinômios em D. Para todo $a \in D$, o polinômio mônico $(x - a)$ é irredutível em $D[x]$.*

Demonstração. Sejam $g(x), q(x) \in D[x]$ tais que $x - a = g(x) \cdot q(x)$.
Como $\partial(x - a) = 1$, então pelo Corolário 2.16 temos $\partial g(x) + \partial q(x) = 1$, e daí temos que as seguintes condições:

(i) $\partial g(x) = 1$ e $\partial q(x) = 0 \Rightarrow q(x) = c$ uma constante de D, ou

(ii) $\partial g(x) = 0$ e $\partial q(x) = 1 \Rightarrow g(x) = c$ uma constante de D.

Suponhamos válida a primeira condição (a outra é análoga). Podemos escrever

$$x - a = c \cdot g(x).$$

Logo, $x - a$ só pode ser escrito como um produto de polinômios se um deles for polinômio constante, logo, é um polinômio irredutível em $D[x]$. Convém observar que pela hipótese de ser um polinômio mônico em um domínio, então, seja $g(x) = a_1x + a_0$ um polinômio de grau 1. Daí temos

$$x - a = ca_1x + ca_0 \Rightarrow ca_1 = 1$$

ou seja, c é um elemento invertível do domínio D. □

Corolário 2.71. *Todo polinômio de grau 1 sobre um corpo K é irredutível.*

Demonstração. Considerando $p(x) = a_1x + a_0$, a demonstração é análoga a feita no Teorema 2.70. □

Proposição 2.72. *Seja D um domínio, $D[x]$ o anel de polinômios em D. Todo polinômio primo em $D[x]$ é irredutível.*

Demonstração. Seja $p(x) \in D[x]$ um polinômio primo tal que $p(x) = g(x) \cdot h(x)$, onde $g(x)$ e $h(x)$ são polinômios não nulos de $D[x]$. Pela Definição 2.50 $p(x) \mid g(x)$ ou $p(x) \mid h(x)$. Vamos supor, sem perda de generalidade que $p(x) \mid g(x)$ (o outro caso é análogo). Daí temos que $g(x) = p(x) \cdot t(x)$, com $t(x) \in D[x]$ e então obtemos

$$p(x) = g(x) \cdot h(x) = p(x) \cdot t(x) \cdot h(x).$$

Com isso, temos que que $t(x) \cdot h(x) = 1$, o que nos diz que $h(x)$ é um elemento invertível de $D[x]$, ou seja, $h(x) = h \in D$ (Teorema 2.18). Logo, temos que $p(x) = h \cdot g(x)$ e então, pela Definição 2.62, concluímos que $p(x)$ é irredutível em $D[x]$. □

Proposição 2.73. *Seja K um corpo, $K[x]$ o anel de polinômios em K. Um polinômio $p(x)$, não nulo e não constante, de $K[x]$ é primo se, e somente se, $p(x)$ é irredutível em $K[x]$.*

Demonstração.

($\Rightarrow$) Imediata pela Proposição 2.72.

($\Leftarrow$) Seja $p(x) \in K[x]$ um polinômio não nulo e não constante e sejam $g(x), h(x) \in K[x]$, tais que, $p(x) \mid g(x) \cdot h(x)$ mas $p(x) \nmid g(x)$. Vamos mostrar que $p(x) \mid h(x)$. Pelo Teorema 2.58, existem polinômios $r_1(x), r_2(x) \in K[x]$ tais que,

$$d(x) = r_1(x)p(x) + r_2(x)g(x),$$

onde $d(x) \in K[x]$ é o M.D.C $\{p(x), g(x)\}$. Como $d(x) \mid p(x)$ e $p(x)$ é irredutível, então $d(x) = a \in K$, ou $d(x) = a \cdot p(x)$. No entanto, observemos que, se $d(x) = a \cdot p(x)$ e como $d(x)$ é divisor de $g(x)$, então teríamos $g(x) = a \cdot p(x) \cdot g_1(x)$, com $g_1(x) \in K[x]$, e portanto $p(x) \mid g(x)$, o que é absurdo pois $p(x) \nmid g(x)$. Logo, temos $d(x) = a$ e daí,

$$a = r_1(x)p_1(x) + r_2(x)g(x).$$

Multiplicando ambos lados por $h(x) \cdot a^{-1}$ obtemos

$$h(x) = r_1(x)p(x)h(x)a^{-1} + r_2(x)g(x)h(x)a^{-1}.$$

Podemos observar que $p(x)$ divide ambos lados da soma (pois $p(x) \mid g(x)h(x)$), e então $p(x) \mid h(x)$.

□

Teorema 2.74. *Seja D um domínio e $D[x]$ o anel de polinômios em D. Se $p \in D$ é um elemento irredutível em D, então o polinômio constante $p(x) = p \in D[x]$ é irredutível em $D[x]$.*

Demonstração. Sejam $g(x), q(x) \in D[x]$ tais que $p(x) = g(x) \cdot q(x) = p$.
Pelo Corolário 2.16 temos $\partial g(x) + \partial q(x) = 0$, e então $\partial g(x) = 0$ e $\partial q(x) = 0$. Daí concluímos que $g, q \in D$, e $p = g \cdot q$. Como p é irredutível em D , então pela Definição 2.48 g ou q são invertíveis e assim $p(x) = p$ é irredutível em $D[x]$.

□

Definição 2.75. *(algebricamente fechado) Seja K um corpo infinito. Se todo polinômio não constante de $K[x]$ tem pelo menos uma raiz em K, então dizemos que K é algebricamente fechado.*

Proposição 2.76. *Um polinômio $p(x)$ sobre um corpo K algebricamente fechado é irredutível em $K[x]$ se, e somente se, $\partial p(x) = 1$, ou seja, é da forma $p(x) = ax + b$ com $a \neq 0$.*

Demonstração.

($\Rightarrow$) Seja $p(x)$ um polinômio irredutível. Como K é algebricamente fechado, então existe $u \in K$ tal que $p(u) = 0$. Logo, pelo Corolário 2.41 $(x-u) \mid p(x)$ e portanto, pela Proposição 2.44 existe $g(x) \in K[x]$ tal que $p(x) = (x-u) \cdot g(x)$, com $g(x) \neq 0$. Novamente, como $p(x)$ é irredutível, então $g(x) = a$ onde a é constante pertencente a K e $a \neq 0$, pois caso contrário, $p(x)$ seria o polinômio nulo. Assim $p(x) = a \cdot (x-u) = ax - au$. Fazendo $b = (-au)$, temos que $b \in K$ e então podemos escrever $p(x) = ax + b$. Logo podemos concluir que $\partial p(x) = 1$ (pois $b = (-au)$ é constante).

($\Leftarrow$) Imediata pela Proposição 2.71, uma vez que a Proposição diz respeito a um corpo K qualquer.

□

Teorema 2.77. *Seja K um corpo e $K[x]$ o anel de polinômios com coeficientes em K. Todo ideal de $K[x]$ é principal.*

Demonstração. Seja $I \subset K[x]$ um ideal de $K[x]$ e $p(x)$ um polinômio de I.

- Se $I = \{0\}$, então I é gerado por 0.
- Se $I \neq 0$, vamos tomar em $K[x]$ um polinômio $p(x)$ de grau mínimo.Tal polinômio existe, pois o grau de um polinômio é um número natural, e o conjunto dos números naturais é bem ordenado. Daí,

  1. Se $p(x) = a$, $a \in I$, $a \neq 0$, então $a \cdot a^{-1} = 1 \in I$ e então, $I = K[x]$ é gerado por 1.
  2. Se $p(x)$ é de grau maior ou igual a 1, consideremos o ideal $K[x] \cdot p(x)$. Temos que $p(x) \in I$, e então $K[x] \cdot p(x) \subset I$. Agora, vamos mostrar que $I \subset K[x] \cdot p(x)$. Para isso, seja $h(x) \in I$. Pelo Teorema 2.37 existem polinômios $r(x)$ e $q(x)$ em $K[x]$ tais que

     $$h(x) = q(x) \cdot p(x) + r(x) \text{ com } \partial r(x) < \partial p(x) \text{ ou } r(x) = 0.$$

     Assim, $r(x) = h(x) - q(x) \cdot p(x)$ e como $h(x), q(x) \in I$ então $r(x) \in I$. Por outro lado, observemos que $p(x)$ é de grau mínimo, daí $r(x) = 0$ e então $h(x) = q(x) \cdot p(x)$. Logo $h(x) \in K[x] \cdot p(x)$ e do fato de $h(x) \in I$, então $I \subset K[x] \cdot p(x)$.

□

Teorema 2.78. *Sejam K um corpo e $p(x) \in K[x]$, as seguintes condições são equivalentes:*

(i) $p(x)$ *é irredutível sobre* $K[x]$.

(ii) $I = K[x] \cdot p(x)$ *é um ideal maximal em* $K[x]$.

(iii) $K[x]/I$ *é um corpo em que* $I = K[x] \cdot p(x)$.

Demonstração. Vamos mostrar que:

(i) $\Rightarrow$ (ii) Seja $p(x) \in K[x]$ um polinômio irredutível em $K[x]$, então $\partial p(x) \geqslant 1$. Consideremos o ideal

$$I = K[x] \cdot p(x) = \{g(x) \cdot p(x); \quad g(x) \in K[x]\}.$$

Pelo fato de $p(x)$ ser um polinômio de grau maior ou igual a 1, então podemos concluir que $I \neq K[x]$. Vamos mostrar que se existir em $K[x]$ outro ideal principal J, tal que $I \subset J \subset K[x]$, definido por

$$J = K[x] \cdot h(x) = \{k(x) \cdot h(x); \quad k(x) \in K[x]\},$$

então $I = J$ ou $J = K[x]$. De fato, como

$$p(x) \in K[x] \cdot p(x) \subset K[x] \cdot h(x)$$

existe um polinômio $g(x) \in K[x]$ tal que,

$$p(x) = g(x) \cdot h(x).$$

Como $p(x)$ é irredutível em $K[x]$ então, $g(x) = a$, $a \in K$, $a \neq 0$ ou $h(x) = b$, $b \in K$, $b \neq 0$. E daí temos que:

Se $g(x) = a$ então $h(x) = a^{-1}p(x)$ e portanto $J \subset I$, mas $I \subset J$, então $I = J$.

Se $h(x) = b$ temos $J = K[x]h(x) = K[x]$.

Assim, concluímos que I é ideal maximal em $K[x]$.

(ii) $\Rightarrow$ (i) Suponhamos que $p(x) = g(x) \cdot h(x)$ com $g(x), h(x) \in K[x]$ e seja

$$I = K[x] \cdot p(x) = \{g(x) \cdot p(x); \quad g(x) \in K[x]\},$$

um ideal maximal em $K[x]$. Como I é maximal, então $I \neq K[x]$ e portanto $\partial p(x) \geqslant 1$. Considerando em $K[x]$ outro ideal principal $J = K[x] \cdot h(x) = \{k(x) \cdot h(x); \quad k(x) \in K[x]\}$ temos que $p(x) \in J$, logo $I \subset J$. Novamente, pelo fato de I ser maximal então:

- Se $I = J$, temos que $h(x) \in I$ e então $h(x) = k(x) \cdot p(x)$. Por outro lado $p(x) \in J$ pois $I = J$ e então $p(x) = g(x) \cdot h(x)$. Assim, $p(x) = g(x) \cdot k(x) \cdot p(x)$ e então temos que $g(x) \cdot k(x) = 1$, logo $g(x) = a$ e $k(x) = b$, onde a e b são elementos invertíveis de K. Assim, $p(x) = a \cdot h(x)$ ou $p(x) = b \cdot g(x)$. Portanto $p(x)$ é irredutível em $K[x]$.
- Se $J = K[x]$ temos que $h(x) = b$ e então $p(x)$ é irredutível em $K[x]$.

(ii)$\Leftrightarrow$ (iii) Imediata pelo Teorema 1.38.

□

Considerando o conceito de polinômio irredutível, apresentado na Definição 2.62, vamos dar a caracterização de tais polinômios. Para isso, apresentamos as definições e proposições que seguem.

O teorema abaixo nos mostra as condições sobre as quais um polinômio pode ser representado na forma fatorada. Embora a estrutura apresentada seja sobre corpos, posteriormente apresentaremos alguns resultados que podem ser aplicados também em domínios.

Teorema 2.79. *Seja K um corpo, $u \in K\backslash\{0\}$. Todo polinômio não nulo $p(x) \in K[x]$ pode ser escrito de forma única (a menos da ordem) na forma*

$$p(x) = u \cdot p_1(x) \cdots p_m(x),$$

sendo $p_1(x), ..., p_m(x)$ polinômios mônicos e irredutíveis sobre $K[x]$ (não necessariamente distintos) e $u \in K\backslash\{0\}$ o coeficiente dominante de $p(x)$.

Demonstração. Vamos mostrar por indução sobre $\partial p(x) = n$.

- Se $n = 0$ então $p(x) = u$.
- Vamos supor que todo polinômio não nulo, de grau entre 1 e $n-1$ possa ser escrito nessa expressão e vamos demonstrar que $p(x)$ de grau igual a n pode ser escrito dessa maneira. Para isso, seja $p(x) = g(x) \cdot h(x)$, com $\partial p(x) = \partial(g(x)) + \partial(h(x))$.
  - Se $p(x)$ é irredutível, então pela Definição 2.62, temos que $g(x) = u$, $u \in K$. Daí, tomando $h(x) = p_1(x)$, podemos escrever $p(x) = u \cdot p_1(x)$ com $u \in K$ e $p_1(x)$ irredutível em $K[x]$.
  - Se $p(x)$ é redutível então, pela hipótese de indução, temos que todo polinômio pode ser escrito com produto de fatores irredutíveis. Daí, tomando $g(x) = a \cdot p_1(x) \cdots p_r(x)$ e $h(x) = b \cdot p_{r+1}(x) \cdots p_m(x)$, com p_i, $1 \leqslant i \leqslant m$ irredutíveis sobre K e $u = ab$, obtemos $p(x) = u \cdot p_1(x) \cdots p_m(x)$.

Para demonstrar a unicidade desta fatoração suponhamos que existam em $K[x]$ polinômios mônicos e irredutíveis, $q_1(x), q_2(x), \ldots, q_r(x)$, com $m \leqslant n$, tais que

$$p(x) = u \cdot p_1(x) \cdots p_m(x) = u' \cdot q_1(x) \cdots q_m(x) q_{m+1}(x) \cdots q_r(x),$$

onde $u' \in K$. Como u é o coeficiente líder de $p(x)$ então $u = u'$. Assim, obtemos

$$p_1(x) \cdots p_m(x) = q_1(x) \cdots q_m(x) q_{m+1}(x) \cdots q_r(x).$$

Podemos observar que $p_1(x)$ divide $q_1(x) \cdots q_m(x) q_{m+1}(x) \cdots q_r(x)$. Como $p_1(x)$ é primo (pois num corpo, todo elemento irredutível é primo), então $p_1(x)$ divide algum $q_i(x), i = 1, \ldots, r$. Assim, $ap_1(x) = q_i(x)$, de onde vem, que $a = 1$, pois ambos possuem coeficiente líder igual a 1, e então $p_1(x) = q_i(x)$. Vamos supor, sem perda de generalidade que $p_1(x) = q_1(x)$. Logo,

$$p_2(x) \cdots p_m(x) = q_2(x) \cdots q_r(x).$$

Assim, temos que $p_2(x)$ divide algum $q_i(x)$. Sem perda de generalidade, suponhamos que $p_2(x) \mid q_2(x)$. Daí temos que $p_2(x) = q_2(x)$ (análogo a $p_1(x) = q_1(x)$). Com isso temos,

$$p_3(x) p_4(x) \cdots p_m(x) = q_3(x) q_4(x) \cdots q_m(x) q_{m+1}(x) \cdots q_r(x).$$

Seguindo este processo obtemos, $p_m(x) = q_m(x)$ e então

$$1 = q_{m+1}(x) \cdots q_r(x). \tag{2.15}$$

Como $q_1(x), q_2(x), \ldots, q_r(x)$ são irredutíveis, não pode acontecer $r > m$ pois gera contradição com a expressão (2.15). Portanto a decomposição é única. □

Corolário 2.80. *Seja K um corpo algebricamente fechado e seja $p(x) \in K[x]$ polinômio sobre K. Todo polinômio não constante de grau maior que zero, pode ser representado de modo único (a menos da ordem) na forma,*

$$p(x) = a\,(x - x_1)^{\alpha_1}\,(x - x_2)^{\alpha_2} \cdots (x - x_r)^{\alpha_r}\,,$$

onde a é o coeficiente líder de $p(x)$, α_i natural, $x_i \in K$ são raízes de $p(x)$, e $x_i \neq x_j$ se $i \neq j$, com $1 \leqslant i, j \leqslant r$.

Demonstração. Suponhamos que $\partial p(x) = n$. Como K é algebricamente fechado, existe $x_1 \in K$, raiz de $p(x)$. Logo, pela Proposição 2.29,

$$p(x) = (x - x_1)q_1(x), \text{ com } \partial q_1(x) = n - 1.$$

Se $\partial q_1(x) \geqslant 1$ então $q_1(x)$ possui raiz $x_2 \in K$. Daí,

$$p(x) = (x - x_1)(x - x_2)q_2(x), \text{ com } \partial q_2(x) = n - 2.$$

Este processo continua até obtermos $\partial q_n = 0$.

$$\begin{aligned} p(x) &= (x - x_1)(x - x_2) \cdots (x - x_n)q_n(x) \\ &= a(x - x_1)(x - x_2) \cdots (x - x_n). \end{aligned}$$

Agrupando as raízes coincidentes segue o resultado.

□

A seguir apresentaremos um teorema, definição e lema que constituem importantes resultados para apresentarmos um critério para verificar se polinômios são irredutíveis.

Teorema 2.81. *Seja D um domínio fatorial e K seu corpo de frações. Se $p(x)$ e $g(x)$ são polinômios primitivos de $D[x]$, então eles são associados em $D[x]$ se, e somente se, forem associados em $K[x]$.*

Demonstração.

($\Rightarrow$) Sendo $p(x)$ e $g(x)$ associados em $D[x]$, então, pela Proposição 2.51 temos que $p(x) = a \cdot g(x)$ e $g(x) = b \cdot p(x)$, sendo a e b elementos invertíveis de D (Teorema 2.18). Logo são associados em $K[x]$ pois $a, b \in K$.

($\Leftarrow$) Suponhamos $p(x)$ e $g(x)$ primitivos e associados em $K[x]$. Assim, $p(x) = c \cdot g(x)$ com c invertível em $K[x]$. Vamos mostrar que $p(x)$ e $g(x)$ são associados em $D[x]$. De fato, sendo K o corpo das frações de D, podemos escrever $c = \dfrac{a}{b}$, com $a, b \in D$, $b \neq 0$ e então,

$$p(x) = c \cdot g(x) = \left(\frac{a}{b}\right) g(x) \Rightarrow b \cdot p(x) = a \cdot g(x)$$

Assim, pela Proposição 2.51, a e b são elementos associados em D e daí $c = \dfrac{a}{b}$ é invertível em D. Logo $p(x)$ e $g(x)$ são associados em D.

□

Teorema 2.82. *(Lema de Gauss) Seja D um domínio fatorial e K seu corpo de frações. Se $p(x) \in D[x]$ é tal que $\partial p(x) \geqslant 1$, então $p(x)$ é irredutível em $D[x]$ se, e somente se, $p(x)$ é primitivo em $D[x]$ e irredutível em $K[x]$.*

Demonstração.

($\Rightarrow$) Suponhamos que $p(x)$ é irredutível em $D[x]$ e provemos inicialmente que é primitivo. De fato, se $p(x)$ não fosse primitivo, existiria o M.D.C. entre os coeficientes de $p(x)$ denotado por d tal que $d \neq 1$. Assim,poderíamos escrever $p(x) = d \cdot p_1(x)$ implicando em $p(x)$ redutível em $D[x]$, o que é uma contradição. Logo $p(x)$ é primitivo em $D[x]$. Suponhamos agora que $p(x)$ é redutível em $K[x]$. Logo, existem polinômios $g(x), h(x)$ em $K[x]$, ambos de grau maior ou igual a 1, tais que $p(x) = g(x) \cdot h(x)$. Pelo Lema 2.69 existem constantes a, b, c e d em D, e polinômios primitivos $g_1(x), h_1(x)$ em $D[x]$, tais que

$$g(x) = \left(\frac{a}{b}\right) g_1(x) \quad ; \quad h(x) = \left(\frac{c}{d}\right) h_1(x).$$

Daí,

$$p(x) = \left(\frac{ac}{bd}\right) g_1(x)h_1(x). \tag{2.16}$$

Pelo Lema 2.68 o produto $(g_1(x)h_1(x))$ resulta em um polinômio primitivo. Aplicando o conteúdo aos dois lados da expressão (2.16), utilizando o fato de $p(x)$, $g_1(x)h_1(x)$ serem primitivos, temos:

$$\begin{aligned} 1 = c(p(x)) &= c\left(\left(\frac{ac}{bd}\right) g_1(x)h_1(x)\right) \\ &= \frac{ac}{bd} c(g_1(x)h_1(x)) \\ &= \frac{ac}{bd}. \end{aligned}$$

Portanto, $p(x) = g_1(x)h_1(x)$, com $g_1(x), h_1(x) \in D[x]$, ambos com grau maior ou igual a um, o que é absurdo, pois $p(x)$ é irredutível em $D[x]$. Portanto, $p(x)$ é irredutível em $K[x]$.

($\Leftarrow$) Suponhamos por absurdo que $p(x)$ é redutível em $D[x]$, então $p(x) = g(x) \cdot h(x)$, sendo $g(x), h(x)$ polinômios em $D[x]$ e ambos diferentes de 1. Suponhamos, sem perda de generalidade, que grau de $g(x)$ seja menor ou igual ao grau de $h(x)$. Se o grau de $g(x)$ é zero, então $g(x)$ é constante e $g(x) \neq 1$ divide $p(x)$, o que contradiz $p(x)$ ser primitivo. Se o grau de $g(x)$ é maior ou igual a 1, temos $p(x)$ redutível em $K[x]$, o que também é uma contradição.

□

Teorema 2.83. *Seja D um domínio fatorial. Então $D[x]$ é um domínio fatorial.*

Demonstração. Seja $D[x] \subseteq K[x]$, onde $D[x]$ é um domínio e $K[x]$ o corpo das frações de $D[x]$. Vamos mostrar que $D[x]$ é fatorial. Para isso, seja $p(x) \in D[x]$, um polinômio de grau maior ou igual a 1. Pelo Lema 2.66, temos que existe um polinômio primitivo $p_1(x)$ em $D[x]$, tal que $p(x) = d \cdot p_1(x)$, onde $d \in D$ é o conteúdo de $p(x)$. Como D é fatorial, e $d \in D$, então, pela Definição 2.63, existem elementos $p_1, \ldots, p_s$, irredutíveis em D, tais que, $d = p_1 \cdots p_s$ e então, pelo Teorema 2.74, são também irredutíveis em $D[x]$. Por outro lado, como $p_1(x) \in D[x] \subset K[x]$, então $p_1(x)$ pode ser escrito como produto de fatores irredutíveis de $K[x]$, ou seja,

$$p_1(x) = q_1(x)\cdots q_r(x), \quad q_i(x) \in K[x], \quad 1 \leqslant i \leqslant r.$$

Como $q_1(x)\cdots q_r(x) \in K[x]$, pelo Lema 2.69, existem elementos $a_i, b_i \in D$, $b_i \neq 0$, e polinômios primitivos $\tilde{q}_i(x)$ em $D[x]$, com $1 \leqslant i \leqslant r$, tais que $q_i(x) = (a_i/b_i)\tilde{q}_i(x)$. Temos ainda que, como $q_i(x)$ é irredutível em $K[x]$, pelo Lema 2.82, $\tilde{q}_i(x)$ é irredutível em $D[x]$. Com isso temos

$$p_1(x) = q_1(x)\cdots q_r(x) = (a_1\cdots a_r/b_1\cdots b_r)\tilde{q}_1(x)\cdots\tilde{q}_r(x),$$

e então

$$b_1\cdots b_r p_1(x) = a_1\cdots a_r\tilde{q}_1(x)\cdots\tilde{q}_r(x).$$

Temos que em ambos lados os polinômios são primitivos e então o conteúdo do lado esquerdo é $b_1\cdots b_r$ e do lado direito $a_1\cdots a_r$. Com isso temos que eles são associados em D e daí $(a_1\cdots a_r/b_1\cdots b_r)$ é invertível em D.

Seja $\eta = (a_1\cdots a_r/b_1\cdots b_r)$, então

$$p(x) = \eta p_1 \cdot p_2\cdots p_t \cdot \tilde{q}_1(x)\cdots\tilde{q}_r(x)$$

é uma fatoração de $p(x)$ com elementos irredutíveis em $D[x]$. Logo, $D[x]$ é fatorial. □

Teorema 2.84. *(critério de Eisenstein) Seja D um domínio fatorial e $p(x) = a_0 + a_1x + \cdots + a_nx^n \in D[x]$, $\partial p(x) \geqslant 1$. Se existe um elemento irredutível d em D tal que:*

(i) $d \nmid a_n$

(ii) $d \mid a_i, \quad \forall i \leqslant n-1$

(iii) $d^2 \nmid a_0$

então $p(x)$ é irredutível em $K[x]$, sendo K o corpo das frações de D.

Demonstração. Suponhamos que $p(x)$ é redutível em $K[x]$, ou seja, existem polinômios não constantes $g(x), h(x) \in D[x]$ tais que $p(x) = g(x)\cdot h(x)$.
Onde

- $g(x) = \sum_{j=0}^{m} b_jx^j = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$, $b_m \neq 0$, $m \geqslant 1$.
- $h(x) = \sum_{j=0}^{k} c_kx^k = c_kx^k + c_{k-1}x^{k-1} + \cdots + c_1x + c_0$, $c_k \neq 0$, $k \geqslant 1$.
- $g(x)\cdot h(x) = \sum_{i=0}^{n} a_ix^i$, sendo $a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1 + b_ic_0$, e $n = m + k$.

Temos que

$$\left.\begin{array}{r} a_0 = b_0c_0 \\ d \mid a_0 \\ d^2 \nmid a_0 \end{array}\right\} \overbrace{\text{como D é fatorial}}^{\Longrightarrow} \begin{cases} d \mid b_0 \text{ e } d \nmid c_0 \\ \text{ou} \\ d \mid c_0 \text{ e } d \nmid b_0. \end{cases}$$

Vamos considerar o caso onde $d \mid b_0$ e $d \nmid c_0$. Então

$$\left.\begin{array}{r} a_n = b_mc_k \\ d \nmid a_n \end{array}\right\} \Longrightarrow \begin{cases} d \nmid b_m \\ \text{e} \\ d \nmid c_k. \end{cases}$$

Como $d \nmid b_m$ então existe um menor índice i com $i < m < n-1$ tal que $d \nmid b_i$. Consideremos o coeficiente a_i de $p(x)$ onde

$$a_i = b_0c_i + b_1c_{i-1} + \cdots + b_{i-1}c_1 + b_ic_0.$$

Então, pela condição de $d \nmid b_i$ temos que $d \nmid a_i$, o que contraria a hipótese de que $d \mid a_i$. Logo, $p(x)$ não pode ser o produto de dois polinômios não constantes, portanto, $p(x)$ é irredutível em $D[x]$ e pelo Lema 2.82 é irredutível em $K[x]$. □

3 Polinômios sobre os anéis $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$

Nos Capítulos 1 e 2 introduzimos definições e propriedades dos anéis, corpos e polinômios quaisquer. Vamos agora apresentar as propriedades dos polinômios, quanto a existência de raízes, divisibilidade e fatoração, levando em consideração as propriedades específicas dos coeficientes em $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

3.1 Polinômios sobre os inteiros $\mathbb{Z}$

Consideremos o domínio $(\mathbb{Z}, +, \cdot)$ e o anel de polinômios com coeficientes em $\mathbb{Z}$, denotado por $(\mathbb{Z}[x], +, \cdot)$. Considerando as definições, teoremas e demais propriedades apresentadas nos capítulos anteriores, apresentaremos a tabela abaixo, que traz uma síntese das propriedades deste anel.

Propriedade	$(\mathbb{Z}, +, \cdot)$	$(\mathbb{Z}[x], +, \cdot)$	**Justificativa**
Domínio	sim	sim	Proposição 2.8
Corpo	não	não	Teorema 2.18 $U(Z) = U(\mathbb{Z}[x]) = \{-1\,,\,1\}$
Domínio Principal	sim	não	Ver observação abaixo, item 1.
Domínio Fatorial	sim	sim	$\mathbb{Z}$ é fatorial, então $(\mathbb{Z}[x], +, \cdot)$ também é fatorial (Teorema 2.83)
Domínio Euclidiano	sim	não	Ver observação abaixo, item 2
Ideais	sim	sim	Triviais ($\{0\}$, $\mathbb{Z}$, $\mathbb{Z}_n$ e $\mathbb{Z}[x]$)

Tabela 3.2: Propriedades sobre $\mathbb{Z}$ e $\mathbb{Z}[x]$.

Observação 3.1. A respeito das propriedades apresentadas na Tabela 3.2 temos

1. Seja $I \subset \mathbb{Z}[x]$ um ideal de $\mathbb{Z}[x]$ gerado por a, $a \neq \pm 1$, e x, ou seja $I = \{a \cdot p(x) + x \cdot q(x) \,|\, p(x), q(x) \in \mathbb{Z}[x]\}$. Suponhamos por absurdo que $\mathbb{Z}[x]$ é domínio principal, ou seja, todo ideal de $\mathbb{Z}[x]$ é ideal principal. Assim, existe um elemento $d(x) \in \mathbb{Z}[x]$ tal que $\mathbb{Z}[x] \cdot d(x) = I$. Com isso temos que $\mathbb{Z}[x] \cdot a + \mathbb{Z}[x] \cdot x = \mathbb{Z}[x] \cdot d(x)$ e então $d(x)$ é o M.D.C. $\{a, x\}$. Por outro lado, observemos que $a \nmid x$

e então M.D.C. $\{a, x\} = \pm 1$, assim, $\mathbb{Z}[x] \cdot a + \mathbb{Z}[x] \cdot x = \mathbb{Z}[x]$. Daí temos que existem $p(x)$ e $q(x)$ em $\mathbb{Z}[x]$ tais que $1 = a \cdot p(x) + x \cdot q(x)$, pois $\mathbb{Z}[x]$ é gerado por a e x. Escrevendo $p(x) = a_n x^n + \cdots + a_1 x + a_0$, deve-se ter $a \cdot a_0 = 1$, o que é um absurdo pois $a \neq \pm 1$.

2. Pelo Teorema 2.56 um domínio euclidiano é um domínio principal. No entanto, mostramos no item anterior que $(\mathbb{Z}[x], +, \cdot)$ não é domínio principal, assim não é euclidiano.

Proposição 3.2. *Seja $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Z}[x]$. Se um número $u \in \mathbb{Q}$, $u = \frac{r}{s}$ com r, s primos entre si, é raiz de $p(x)$, então $r \mid a_0$ e $s \mid a_n$.*

Demonstração. Como $p(u) = 0$ então temos

$$a_0 + a_1(\frac{r}{s}) + a_2(\frac{r}{s})^2 + \cdots + a_n(\frac{r}{s})^n = 0.$$

Multiplicando a expressão por s^n obtemos

$$a_0 s^n + a_1 r s^{n-1} + a_2 r^2 s^{n-2} + \cdots + a_{n-1} r^{n-1} s + a_n r^n = 0. \tag{3.1}$$

A partir dessa expressão podemos obter a seguinte igualdade:

$$s(a_0 s^{n-1} + a_1 r s^{n-2} + a_2 r^2 s^{n-3} + \cdots + a_{n-1} r^{n-1}) = -a_n r^n.$$

Assim, temos que $s \mid a_n r^n$. Como r, s são primos entre si, então , $s \mid a_n$. De forma semelhante, podemos concluir que $s \mid a_0$, pois a partir da expressão (3.1), colocando r em evidência e passando para o outro membro o termo $a_0 s^n$ obtemos a igualdade

$$-a_0 s^n = r(a_1 s^{n-2} + a_2 r s^{n-3} + \cdots + a_{n-1} r^{n-2} s + a_n r^{n-1}).$$

Assim, temos que $r \mid a_0 s^n$. Como r, s são primos entre si, então , $r \mid a_0$. □

Corolário 3.3. *Seja $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + x^n \in \mathbb{Z}[x]$, um polinômio mônico. As raízes racionais de $p(x)$ são os inteiros divisores de a_0.*

Demonstração. Se $u = \frac{r}{s} \in \mathbb{Q}$ é raiz de $p(x)$, com r, s primos entre si, então $s \mid 1$ e portanto $s = \pm 1$. Assim $\frac{r}{s} = \pm r$ e então $r \in \mathbb{Z}$. Pela Proposição 3.2, $r \mid a_0$ e então $-r \mid a_0$. Assim concluímos que $u \mid a_0$. □

Lema 3.4. *Sejam $p(x), g(x) \in \mathbb{Z}[x]$ polinômios primitivos. Se para algum par de inteiros $c, d \in \mathbb{Z}\backslash\{0\}$ tivermos a igualdade $c \cdot p(x) = d \cdot g(x)$ então c e d são associados em $\mathbb{Z}$ e $p(x), g(x)$ são associados em $\mathbb{Z}[x]$.*

Demonstração. Sejam $a_0, a_1, ..., a_n$ coeficientes de $p(x)$. Como o polinômio é primitivo, o $M.D.C.\{a_0, a_1, ..., a_n\} = 1$. Então, existem inteiros $b_0, b_1, ..., b_n$ tais que, $a_0 b_0 + a_1 b_1 + \cdots + a_n b_n = 1$. Como $c \cdot p(x) = d \cdot g(x)$, então $d \mid c \cdot a_i$, $i = 0, 1, 2, ..., n$ e então divide $\sum_{i=0}^{n} c \cdot a_i b_i = c \cdot \sum_{i=0}^{n} a_i b_i = c$. Analogamente mostramos que $c \mid d$. Assim, $d = \pm c$ e então $p(x) = \pm g(x)$. □

Vamos apresentar alguns exemplos de aplicação das propriedades referentes aos anéis $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Z}[x], +, \cdot)$

3.1.1 Exemplos

Exemplo 3.5. Seja D um domínio que não é um corpo e seja $\alpha \neq 0$ um elemento não invertível de D. Seja $D[x]$ o anel de polinômios em uma indeterminada com coeficientes em D.

a) Mostre que o maior divisor comum entre α e x existe em $D[x]$ e é igual a 1.

b) Mostre que não existem $g(x), h(x) \in D[x]$ tais que $g(x) \cdot \alpha + h(x) \cdot x = 1$

c) Mostre que o ideal $\langle \alpha, x \rangle$ de $D[x]$ não é principal.

Solução.

(a) Temos que x é irredutível em D sendo $x = 1 \cdot x$ e além disso $x \nmid \alpha$. Daí temos que o único elemento que divide α e x é 1.

(b) Sejam os polinômios $g(x)$ e $h(x)$ tais que $g(x) = b_r x^r + b_{r-1}x^{r-1} + \cdots + b_1 x + b_0$ e $h(x) = c_s x^s + c_{s-1}x^{s-1} + \cdots + c_1 x + c_0$. Suponhamos então que estes polinômios satisfaçam a igualdade $g(x) \cdot \alpha + h(x) \cdot x = 1$. Com isso devemos ter $c_i = 0$, para todo $i = 0, 1, \ldots, s$ e $b_i = 0$ para $i = 1, 2, \ldots, r$, mas $b_0 \neq 0$. No entanto, dessa igualdade temos que $b_0 \cdot \alpha = 1$, ou seja, $b_0 = \alpha^{-1}$, o que é um absurdo pois α é não invertível. Logo concluímos que tais polinômios não existem.

(c) Seja $I \subset D[x]$ um ideal gerado por α e x, ou seja,

$$I = \langle \alpha, x \rangle = \{\alpha \cdot g(x) + h(x) \cdot x; g(x), h(x) \in D[x]\}.$$

Vamos supor que I é ideal principal, ou seja, existe o elemento $h(x)$ de I tal que $I = \langle h(x) \rangle$. Consideremos em I os elementos α e x. Temos que:

(i) $\alpha = h(x) \cdot h_1(x)$, sendo $h_1(x) \in D[x]$. Como α é constante, temos que $\partial(h(x)) = \partial(h_1(x)) = 0$ e então, podemos observar que $h(x) = c \in D$. Com isso, temos que $c \mid \alpha$.

(ii) $x = h(x) \cdot h_2(x) = c \cdot h_2(x)$, logo $c \mid x$. Tendo (i) e (ii), segue do item (a) que $c = 1$. Assim, pelo Teorema 2.56, temos:

$$1 = \alpha \cdot g(x) + x \cdot h(x),$$

o que é absurdo, conforme demonstrado no item (*b*). Logo I não é ideal principal.

Exemplo 3.6. Seja $p \in \mathbb{Z}$ primo. Então $q(x) = x^{p-1} - x^{p-2} + x^{p-3} - \cdots - x + 1$ é irredutível em $\mathbb{Z}[x]$.

Solução. Vamos supor que $q(x)$ é redutível em $\mathbb{Z}[x]$ e daí temos que $q(x) = g(x) \cdot h(x)$, com $g(x)$ e $h(x)$ polinômios de $\mathbb{Z}[x]$ e ambos de grau maior ou igual a 1. Com isso, temos que $q(1-x) = g(1-x) \cdot h(1-x)$. Vamos verificar se esse polinômio é redutível. Observemos que

$$q(1-x) = (1-x)^{p-1} - (1-x)^{p-2} + (1-x)^{p-3} - \cdots - (1-x) + 1.$$

Daí,

(i) Se $p = 2$, então
$$q(1-x) = (1-x) - 1 + 1 = -x + 1.$$

(ii) Se p é primo e $p > 2$, então p é ímpar. Logo, podemos escrever
$$q(x) = \sum_{k=0}^{p-1} (-x)^k.$$

Daí,
$$q(x) = \frac{(-x)^p - 1}{-x - 1},$$

$$\begin{aligned} q(x-1) &= \frac{(1-x)^p - 1}{-x+1-1} = \frac{(1-x)^p - 1}{-x} \\ &= \frac{1-(1-x)^p}{x} = \frac{1-(1-C_p^1(x) + C_p^2(x)^2 - C_p^3x^3 + \cdots - x^p)}{x} \\ &= \frac{px - C_p^2x^2 + C_p^3x^3 + \cdots + x^p}{x} = \\ &= x^{p-1} - C_p^{p-1}x^{p-2} + C_p^{p-2}x^{p-3} - \cdots - C_p^2x + p. \end{aligned}$$

Denotando
$$q(1-x) = a_n x^{p-1} + a_{n-1}x^{p-2} + \cdots + a_0,$$
temos $a_{p-1} = 1$, $a_i = (-1)^{p-1}C_p^{p-1}$ e $a_0 = p$. Sendo p irredutível em $\mathbb{Z}$, $p \nmid a_{p-1}$, $p^2 \nmid a_0$, $p \mid a_i$, para $i = 1, 2, \ldots, p-2$, o Critério de Eisenstein (Teorema 2.84) garante que $q(1-x)$ é irredutível, o que contradiz o fato de $q(x)$ ser redutível.

Exemplo 3.7. Demonstrar que se o domínio fatorial D não é um corpo, então $D[x]$ não é anel euclidiano.

Demonstração. Vamos demonstrar considerando um contra-exemplo. De fato, considerando a Definição 2.34, em $D[x]$, dado um polinômio $p(x) = x^2$ e $g(x) = bx$, sendo b não invertível, devem existir polinômios $q(x)$ e $r(x)$ tais que,
$$p(x) = g(x) \cdot q(x) + r(x), \quad \text{com} \quad \partial(r(x)) < \partial(g(x)) \quad \text{ou} \quad r(x) = 0.$$
Assim, devemos ter $q(x) = ax + b$ e $r(x) = c$. Com isso devemos ter $a \cdot b = 1$, o que é impossível. □

3.2 Polinômios sobre os racionais $\mathbb{Q}$

Consideremos o corpo $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{Q}[x], +, \cdot)$ o anel de polinômios com coeficientes em $\mathbb{Q}$. A respeito das propriedades apresentadas nos capítulos anteriores referentes aos anéis, apresentamos a tabela abaixo para melhor caracterização destes anéis.

Propriedade	$(\mathbb{Q}, +, \cdot)$	$(\mathbb{Q}[x], +, \cdot)$	**Justificativa**
Domínio	sim	sim	Proposição **??**
Corpo	sim	sim	Teorema **??**.
Domínio Principal	sim	sim	Teorema 2.56.
Domínio Fatorial	sim	sim	Teorema 2.79
Domínio Euclidiano	sim	sim	Proposição 2.36
Ideais	sim	sim	Triviais ($\{0\}$, $\mathbb{Q}$ e $\mathbb{Q}[x]$)

Tabela 3.4: Propriedades sobre $\mathbb{Q}$ e $\mathbb{Q}[x]$.

Proposição 3.8. *Seja $p(x) \in (\mathbb{Z}[x], +, \cdot)$ irredutível em $\mathbb{Z}[x]$. Então $p(x)$ é irredutível em $\mathbb{Q}[x]$.*

Demonstração. Suponhamos por absurdo que $p(x)$ não é irredutível em $\mathbb{Q}[x]$. Daí, existem polinômios $g(x), h(x)$ em $\mathbb{Q}[x]$, tais que $p(x) = g(x) \cdot h(x)$, com $\partial g(x) \geqslant 1$, e $\partial(g(x) + h(x)) = \partial p(x)$. Como os coeficientes de $p(x)$ são racionais, então existe um inteiro positivo m tal que

$$m \cdot p(x) = g_1(x) \cdot h_1(x), \tag{3.2}$$

sendo $g_1(x), h_1(x)$ polinômios de $\mathbb{Z}[x]$ e com graus iguais aos de $g(x)$ e $h(x)$, respectivamente. Sejam b, c e d o conteúdo de $p(x), g_1(x)$ e $h_1(x)$ respectivamente. Pelo Lema 2.65, existem polinômios primitivos $p_1(x), h_2(x), g_2(x)$ em $\mathbb{Z}[x]$ e de graus iguais aos graus de $p(x), g_1(x)$ e $h_1(x)$, respectivamente, tais que:

$$p(x) = bp_1(x), \tag{3.3}$$
$$g_1(x) = cg_2(x), \tag{3.4}$$
$$h_1(x) = dh_2(x). \tag{3.5}$$

Com isso, considerando a igualdade entre as expressões obtidas em (3.2), (3.3), (3.4) e (3.5), obtemos

$$(m \cdot b)p_1(x) = (c \cdot d)(g_2(x) \cdot h_2(x))$$

e então, pelo Lema 3.4 temos

$$m \cdot b = \pm(c \cdot d),$$

e

$$p_1(x) = \pm(g_2(x) \cdot h_2(x)).$$

Como os polinômios $g_2(x)$ e $h_2(x)$ tem graus iguais aos graus de $g_1(x)$ e $h_1(x)$, respectivamente, e estes são maiores ou iguais a 1, então $p_1(x)$ é redutível em $\mathbb{Z}[x]$, mas isso é absurdo pois se $p_1(x)$ for redutível, então $p(x) = bp_1(x)$ é também redutível, contrariando a afirmação de $p(x)$ ser irredutível. Logo $p(x)$ é irredutível em $\mathbb{Q}[x]$. □

Definição 3.9. *Seja $K \subset \mathbb{C}$ um corpo e $p(x) = ax^2 + bx + c \in K[x]$. Chamamos de discriminante Δ a expressão dada por:*

$$\Delta = b^2 - 4ac.$$

Proposição 3.10. *Um polinômio quadrático $p(x) = ax^2 + bx + c \in \mathbb{Q}[x]$ com $a \neq 0$ é redutível em $\mathbb{Q}[x]$ se, e somente se, o discriminante $\Delta = b^2 - 4ac$ é um quadrado perfeito em $\mathbb{Q}$.*

Demonstração.

($\Rightarrow$) Como $p(x)$ é redutível em $\mathbb{Q}$, então pelo Teorema 2.29 e Corolário 2.30, existem $x_1, x_2 \in \mathbb{Q}$ tais que $p(x) = a(x - x_1)(x - x_2)$. Com isso obtemos $b = -a(x_1 + x_2)$ e $c = x_1 \cdot x_2$ e temos então $\Delta = a^2(x_1 - x_2)^2$.

($\Leftarrow$) Se $\Delta = \Delta_0^2$, com $\Delta_0 \in \mathbb{Q}$ temos então

$$p(x) = a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right] \Rightarrow p(x) = a\left(x + \frac{b + \Delta_0}{2a}\right) \cdot \left(x + \frac{b - \Delta_0}{2a}\right),$$

concluindo que $p(x)$ é redutível em $\mathbb{Q}[x]$.

□

Corolário 3.11. *O polinômio quadrático $p(x) = ax^2 + bx + c \in \mathbb{Q}[x]$ com $a \neq 0$ é irredutível em $\mathbb{Q}[x]$ se, e somente se, o discriminante $\Delta = b^2 - 4ac$ não é um quadrado perfeito em $\mathbb{Q}$.*

3.2.1 Exemplos

Exemplo 3.12. Prove que se p é um número primo e n é inteiro maior que 1, então o polinômio $x^n - p$ é irredutível em $\mathbb{Q}[x]$.

Demonstração. Como p é primo, então pela Proposição 2.49 é irredutível. Analisando as condições de divisibilidade segundo o Critério de Einsenstein (Teorema 2.84), aplicando a $x^n - p$ ($a_n = 1$, $a_0 = -p$ e $a_i = 0$, $i = 1, 2, \ldots, n-1$), temos :

- $p \nmid a_n$;
- $p \mid a_i$ para $i = \{0, 1, \ldots, n-1\}$;
- $p^2 \nmid a_0$.

Assim, concluímos que $x^n - p$ é irredutível em $\mathbb{Z}[x]$ e consequentemente irredutível em $\mathbb{Q}[x]$, segundo a Proposição 3.8. □

Exemplo 3.13. Verifique se $\mathbb{Z}[x]$ é ideal de $\mathbb{Q}[x]$.

Demonstração. Sejam em $\mathbb{Z}[x]$ os polinômios $p(x) = \sum_i^n a_i x^i$ e $g(x) = \sum_i^m b_i x^i$, com $m \leqslant n$. Considerando a Definição 1.24, podemos verificar que:

(i) Seja $h(x) = p(x) - g(x)$, onde

$$p(x) - g(x) = \sum_{i=0}^{m}(a_i - b_i)x^i + a_{m+1}x^{m+1} + \cdots + a_n x^n.$$

Como a_i e b_i são elementos de $\mathbb{Z}$, então $c_i = a_i - b_i$ também é elemento de $\mathbb{Z}$ e portanto, considerando $h(x) = p(x) - g(x)$, podemos concluir que é um polinômio de $\mathbb{Z}[x]$;

(ii) Seja $t(x) = p(x) \cdot g(x)$ um polinômio de $\mathbb{Q}[x]$, onde $t(x) = \sum_{i}^{n+m} d_i x^i$. Considerando a Definição 2.1 e a expressão que representa o produto de polinômios em (2.1) podemos observar que d_i não é necessariamente um elemento de $\mathbb{Z}[x]$, logo, o item (ii) da Definição 1.24 não pode ser satisfeito, e daí concluímos que $\mathbb{Z}[x]$ não é ideal de $\mathbb{Q}[x]$. Podemos ainda verificar que dados os polinômios $p(x) = 2x^2$ em $\mathbb{Z}[x]$ e $g(x) = \frac{3}{5}x$ em $\mathbb{Q}[x]$, temos:

$$p(x) \cdot g(x) = 2x^2 \cdot \frac{3}{5}x = \frac{6}{5}x^3,$$

e este polinômio não pertence a $\mathbb{Z}[x]$.

□

3.3 Polinômios sobre os reais $\mathbb{R}$

Consideremos $(\mathbb{R}, +, \cdot)$ anel comutativo com unidade e $(\mathbb{R}[x], +, \cdot)$ o anel de polinômios com coeficientes em $\mathbb{R}$. A respeito das propriedades apresentadas nos capítulos anteriores referentes aos anéis, apresentamos a tabela abaixo:

Propriedade	$(\mathbb{R}, +, \cdot)$	$(\mathbb{R}[x], +, \cdot)$	**Justificativa**
Domínio	sim	sim	Proposição 2.8
Corpo	sim	sim	Teorema 2.18.
Domínio Principal	sim	sim	Teorema 2.56.
Domínio Fatorial	sim	sim	Teorema 2.79
Domínio Euclidiano	sim	sim	Proposição 2.36
Ideais	sim	sim	Triviais ($\{0\}$, $\mathbb{R}$, $\mathbb{R}[x]$)

Tabela 3.6: Propriedades sobre $\mathbb{R}$ e $\mathbb{R}[x]$.

Teorema 3.14. *Seja o polinômio* $p(x) = x^2 + bx + c \in \mathbb{R}[x]$, $b, c \in \mathbb{R}$. *O polinômio* $p(x)$ *é irredutível em* $\mathbb{R}[x]$, *se, e somente se,*

$$\Delta = b^2 - 4c < 0.$$

Demonstração. Temos que $p(x)$ é redutível se, e somente se, existem x_1 e x_2 em $\mathbb{R}$, tais que

$$p(x) = (x - x_1)(x - x_2),$$

o que é equivalente a

$$\Delta = (x_1 - x_2)^2.$$

Logo, é redutível se, e somente se, $\Delta \geqslant 0$. □

Observação 3.15. Considerando o Teorema 2.70 e o Teorema 3.14, temos que os binômios da forma $p(x) = u(x-a)$ e os trinômios da forma $g(x) = v(x^2+bx+c)$, com $\Delta = b^2 - 4ac < 0$ são irredutíveis em $\mathbb{R}[x]$, onde $u, v \neq 0$ são os coeficientes líderes de $p(x)$ e $g(x)$, respectivamente. Mais adiante mostraremos que estes são os únicos polinômios irredutíveis em $\mathbb{R}[x]$.

Teorema 3.16. *Seja o polinômio não nulo e não constante $p(x) \in \mathbb{R}[x]$. Suponhamos que existam a e b números reais, $a < b$ tais que $p(a) \cdot p(b) < 0$. Então, existe um elemento $c \in \mathbb{R}$ tal que $p(c) = 0$, ou seja, c é raiz de $p(x)$.*

Demonstração. Ver em [17] página 436. □

Lema 3.17. *Seja o polinômio não constante $p(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \in \mathbb{R}[x]$. Sejam*

$$M = \max\{-a_0, -a_1, \ldots, -a_{n-1}, 0\}$$

$$m = \max\{(-1)^{n-1}a_0, (-1)^{n-2}a_2, \ldots, -a_{n-2}, a_{n-1}, 0\}.$$

Para todo a e b em $\mathbb{R}$ temos:

(1) Se $b > M+1$ então $p(b) > 0$;

(2) $(-1)^n p(a) > 0$, se $a < -(m+1)$.

Demonstração.

(1) Podemos observar que $-M \leqslant a_i, i = 0, 1, \ldots, n-1$, logo, para $b > 1$, temos

$$\begin{aligned} p(x) &= x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 \\ &\geqslant -M(x^{n-1} + x^{n-2} + \cdots + x + 1) + \frac{x^n(x-1)}{x-1} \\ &= -M\left(\frac{x^n - 1}{x-1}\right) + \frac{x^n(x-1)}{x-1} \\ &= \frac{-M(x^n-1) + x^{n+1} - x^n}{x-1} \\ &= \frac{[x-(M+1)]x^n + M}{x-1}, \end{aligned}$$

e então $p(b) > 0$ para todo $b > M+1$.

(2) Consideremos o polinômio

$$\begin{aligned} g(x) &= (-1)^n p(-x) \\ &= (-1)^n a_0 + (-1)^{n+1}a_1x + \cdots + (-1)^{2n-1}a_{n-1}x^{n-1} + x^n, \end{aligned}$$

logo,

$$\begin{aligned} max\{-(-1)^n a_0, -(-1)^{n+1}a_1, \ldots, (-1)^{2n-1}a_{n-1}, 0\} &= \\ max\{(-1)^{n-1}a_0, (-1)^{n-2}a_1, \ldots, -a_{n-2}, a_{n-1}, 0\} &= m. \end{aligned}$$

Assim, de acordo como o item (1) temos que se $a > m+1$ então $g(a) > 0$, ou seja, $a > m+1$ e $(-1)^n p(-a) > 0$. Com isso temos que se $a < -(m+1)$ então $(-1)^n p(a) > 0$.

□

Teorema 3.18. *Todo polinômio não nulo,* $p(x) \in \mathbb{R}[x]$ *de grau ímpar, possui pelo menos uma raiz real.*

Demonstração. Seja

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Denotemos

$$g(x) = a_n^{-1} \cdot p(x),$$
$$M = \max\{-a_0, -a_1, \ldots, -a_{n-1}, 0\},$$

e

$$m = \max\{(-1)^{n-1}a_0, (-1)^{n-2}a_2, \ldots, -a_{n-2}, a_{n-1}, 0\}.$$

Pelo Lema 3.17, existem a e b reais, com $a < -(m+1)$ e $b > M+1$ tais que $g(a) < 0$ e $g(b) > 0$. Utilizando então o Teorema 3.16, segue que existe um elemento c de $\mathbb{R}$ tal que, para $a < c < b$, $g(c) = 0$. Assim para $p(x) = a_n \cdot g(x)$ temos que $p(c) = 0$. Logo, o elemento c de $\mathbb{R}$ é raiz de $p(x)$.

□

3.3.1 Exemplos

Exemplo 3.19. Seja $p(x) \in K[x] \subset \mathbb{C}[x]$ um polinômio de grau 2 ou 3, onde K é um corpo ($\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$). Mostre que $p(x)$ é redutível em $K[x]$ se, e somente se, $p(x)$ tem raiz em K.

Demonstração. ($\Rightarrow$) Como $p(x)$ redutível em $K[x]$, então existem polinômios não constantes, $g(x)$ e $h(x)$ em $K[x]$ tais que

$$p(x) = g(x) \cdot h(x),$$

e com isso temos que,

(i) se $p(x)$ é um polinômio de grau 2, então $\partial g(x) + \partial h(x) = 2$ e como não são constantes, $\partial g(x) = \partial h(x) = 1$. Assim, $p(x)$ é o produto de dois polinômios de grau 1. Pela Proposição 2.71 tais polinômios são irredutíveis em $K[x]$ e pelo Teorema 2.79, (como estes polinômios são irredutíveis), podemos escrever

$$p(x) = u \cdot (x-a) \cdot (x-b),$$

com a, b constantes de K. Portanto a e b são raízes de $p(x)$.

(ii) se $p(x)$ é um polinômio de grau 3, então $\partial g(x) + \partial h(x) = 3$ e como são não constantes,podemos ter $\partial g(x) = 1$ e $\partial h(x) = 2$ ou $\partial g(x) = 2$ e $\partial h(x) = 1$. Suponhamos, sem perda de generalidade, que ocorra a primeira situação. Assim temos que $p(x) = u \cdot (x-a)(x^2+bx+c)$, onde u é o coeficiente líder de $p(x)$, a, b, c constantes de K. Assim, podemos observar que $a \in K$ é raiz de $p(x)$.

($\Leftarrow$) Se existe $a \in K$ tal que a é raiz de $p(x)$, então pelo Corolário 2.41, $(x-a)$ divide $p(x)$ e assim podemos escrever $p(x) = (x-a)g(x)$, com $g(x) \neq 0$. Daí podemos observar que, como o grau de $p(x)$ é maior ou igual a 2, o grau de $g(x)$ deve ser maior ou igual a 1, portanto $p(x)$ é redutível.

□

3.4 Polinômios sobre os complexos $\mathbb{C}$

Consideremos $(\mathbb{C}, +, \cdot)$ anel comutativo com unidade e $(\mathbb{C}[x], +, \cdot)$ o anel de polinômios com coeficientes em $\mathbb{C}$. A respeito das propriedades apresentadas nos capítulos anteriores referentes aos anéis, apresentamos a tabela abaixo:

Propriedade	$(\mathbb{C}, +, \cdot)$	$(\mathbb{C}[x], +, \cdot)$	**Justificativa**
Domínio	sim	sim	Proposição 2.8
Corpo	sim	sim	Teorema 2.18.
Domínio Principal	sim	sim	Teorema 2.56.
Domínio Fatorial	sim	sim	Teorema 2.79
Domínio Euclidiano	sim	sim	Proposição 2.36
Ideais	sim	sim	Triviais ($\{0\}$, $\mathbb{C}$ e $\mathbb{C}[x]$)

Tabela 3.8: Propriedades sobre $\mathbb{C}$ e $\mathbb{C}[x]$.

Para melhor compreendermos as propriedades dos polinômios sobre o anel dos complexos, vamos apresentar as definições e propriedades abaixo, referente aos números complexos e suas propriedades operatórias.

Definição 3.20. *(Conjugado de um número complexo) Seja $z = a + bi \in \mathbb{C}$. Definimos como conjugado de z o número complexo $\overline{z} = a - bi$.*

A respeito das propriedades de um número complexo, vamos apresentar algumas propriedades, importantes para a posterior compreensão dos polinômios sobre os complexos.

Teorema 3.21. *Sejam os números complexos $z = a + bi$, $w = c + di$ e seus respectivos conjugados $\overline{z} = a - bi$ e $\overline{w} = c - di$. Então:*

(i) $\overline{z + w} = \overline{z} + \overline{w}$;

(ii) $\overline{z - w} = \overline{z} - \overline{w}$;

(iii) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$;

(iv) Se z é um número real, então $z = \overline{z}$;

(v) Se n é um inteiro positivo, $\overline{z}^n = \overline{z^n}$.

Demonstração.

(i) Temos que

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$$

e então,

$$\begin{aligned} \overline{z + w} &= (a + c) - (b + d)i \\ &= (a - bi) + (c - di) \\ &= \overline{z} + \overline{w}. \end{aligned}$$

(ii) Temos que

$$z - w = (a + bi) - (c + di) = (a - c) + (b - d)i$$

e então,

$$\begin{aligned} \overline{z - w} &= (a - c) - (b - d)i \\ &= (a - bi) - (c - di) \\ &= \overline{z} - \overline{w}. \end{aligned}$$

(iii) Temos que,

$$z \cdot w = (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i,$$

e então,

$$\begin{aligned} \overline{z \cdot w} &= (ac - bd) - (ad + bc)i \\ &= ac - adi - bd - bci \\ &\overset{*}{=} a(c - di) - bi(c - di) \\ &= (a - bi) \cdot (c - di) \\ &= \overline{z} \cdot \overline{w}. \end{aligned}$$

Observe que em $(\overset{*}{=})$ utilizamos o fato de que $-bd = (-b)(-d)i^2 = (-bi)(-di)$.

(iv) Seja $z = a + 0i = a$ então $\overline{z} = a - 0i = a$, o que mostra a igualdade de z e $\overline{z}$.

(v) Pelo item (*iii*) temos $\overline{z} \cdot \overline{z} = \overline{z \cdot z}$. Assim, aplicando recursivamente essa propriedade, temos $\underbrace{\overline{z} \cdots \overline{z}}_{n} = \overline{z^n}$.

□

Definição 3.22. *Seja* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *um polinômio em* $\mathbb{C}[x]$. *Definimos como polinômio conjugado de* $p(x)$, *denotado por* $\overline{p}(x)$ *o polinômio*

$$\overline{p}(x) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0},$$

onde $\overline{a_i}$ *é o conjugado de* a_i, *para* $i = 0, 1, \ldots, n$.

Os polinômios conjugados apresentam as propriedades a serem mostradas na proposição abaixo.

Proposição 3.23. *Sejam os polinômios sobre* $\mathbb{C}[x]$ *dados por:*

- $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *e* $\overline{p}(x) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0}$ *o conjugado de* $p(x)$;
- $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ *e* $\overline{g}(x) = \overline{b_n}x^n + \overline{b_{n-1}}x^{n-1} + \cdots + \overline{b_1}x + \overline{b_0}$ *o conjugado de* $g(x)$;
- $h(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + a_0$ *e* $\overline{h}(x) = \overline{c_n}x^n + \overline{c_{n-1}}x^{n-1} + \cdots + \overline{c_1}x + \overline{c_0}$ *o conjugado de* $h(x)$.

Os polinômios conjugados apresentam as seguintes propriedades:

(i) Se $p(x) = g(x) + h(x)$, *então* $\overline{p}(x) = \overline{g}(x) + \overline{h}(x)$;

(ii) Se $p(x) = g(x) \cdot h(x)$, *então* $\overline{p}(x) = \overline{g}(x) \cdot \overline{h}(x)$;

(iii) $p(x) = \overline{p}(x)$ *se, e somente se,* $p(x) \in \mathbb{R}[x]$*;*

(iv) $\overline{p}(\overline{z}) = \overline{p(z)}$*, para* $z \in \mathbb{C}$*.*

Demonstração.

(i) Pela Definição 2.1 referente a soma de polinômios, temos $a_i = b_i + c_i$, para $i = 0, 1, \ldots, n$. Daí, $\overline{a_i} = \overline{b_i + c_i}$. Pelo Teorema 3.21, item *(i)*, $\overline{b_i + c_i} = \overline{b_i} + \overline{c_i}$. Logo $\overline{a_i} = \overline{b_i} + \overline{c_i}$ e então, $\overline{p}(x) = \overline{g}(x) + \overline{h}(x)$.

(ii) Pela Definição 2.1 referente ao produto de polinômios, temos $a_i = \sum_{\gamma+\mu=i} b_\gamma c_\mu$, para $i = 0, 1, \ldots, n$. Daí, $\overline{a_i} = \sum_{\gamma+\mu=i} \overline{b_\gamma c_\mu}$. Pelo Teorema 3.21, item *(iii)*, $\overline{b_\gamma c_\mu} = \overline{b_\gamma} \cdot \overline{c_\mu}$. Logo $\overline{a_i} = \sum_{\gamma+\mu=i} \overline{b_\gamma} \cdot \overline{c_\mu}$ e então, $\overline{p}(x) = \overline{g}(x) \cdot \overline{h}(x)$.

(iii) Se $p(x) = \overline{p}(x) \Leftrightarrow a_i = \overline{a_i}$. Pelo Teorema 3.21, item *(iv)* isso ocorre se $a_i \in \mathbb{R}$. Logo, nestas condições, verificamos a igualdade.

(iv) Temos que

$$\overline{p}(\overline{z}) = \overline{a_n}(\overline{z})^n + \overline{a_{n-1}}(\overline{z})^{n-1} + \cdots + \overline{a_1}(\overline{z}) + \overline{a_0}$$

Aplicando as propriedades do Teorema 3.21, itens *(iii)* e *(v)* verificamos que

$$\begin{aligned} \overline{p}(\overline{z}) &= \overline{a_n z^n} + \overline{a_{n-1} z^{n-1}} + \cdots + \overline{a_1 z} + \overline{a_0} \\ &= \overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0} \\ &= \overline{p(z)}. \end{aligned}$$

□

Ainda a respeito de conjugado e considerando as propriedades da Proposição 3.23 apresentamos o resultado abaixo:

Teorema 3.24. *Se* $p(x)$ *é um polinômio com coeficientes reais, então* $p(\overline{z}) = \overline{p(z)}$*, onde* $\overline{z}$ *é o conjugado do número complexo de* z*.*

Demonstração. Seja $p(x) = \sum_{i=0}^{n} a_i x^i$. Aplicando os itens (i), (iii) e (iv) do Teorema 3.21, temos

$$p(\overline{z}) = \sum_{i=0}^{n} a_i (\overline{z})^i = \sum_{i=0}^{n} \overline{a_i}(\overline{z})^i = \sum_{i=0}^{n} \overline{a_i z^i} = \overline{\sum_{i=0}^{n} a_i z^i} = \overline{p(z)}.$$

□

Teorema 3.25. *Se* $z \in \mathbb{C}$ *é raiz de multiplicidade* m *de um polinômio* $p(x) \in \mathbb{R}[x]$*, então* $\overline{z}$ *também é raiz de multiplicidade* m *de* $p(x)$*.*

Demonstração. Sejam $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, $z = a + bi$ e $\overline{z} = a - bi$. Temos que

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0, \tag{3.6}$$

e daí, aplicando as propriedades do Teorema 3.21 referente ao conjugado do número complexo e da Proposição 3.23 referente a conjugação de polinômios temos:

$$\begin{aligned} p(\overline{z}) &= a_n\overline{z}^n + a_{n-1}\overline{z}^{n-1} + \cdots + a_1\overline{z} + a_0 \\ &= \overline{a_n z^n + a_{n-1}z^{n-1}} + \cdots + a_1\overline{z} + a_0 \\ &= \overline{a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0} \\ &= \overline{0} = 0. \end{aligned}$$

Além disso, podemos observar que um número complexo z_0 é raiz de multiplicidade m de um polinômio $p(z) \in \mathbb{C}[x]$, se e só se, existe um polinômio $q(z)$ tal que

$$p(z) = (z - z_0)^m q(z),$$

com $q(z) \in \mathbb{C}[x]$ e $q(z) \neq 0$. Se $p(z) = (z-z_0)^m q(z)$, então $\overline{p}(z) = (z-\overline{z_0})^m \overline{q}(z)$. Como $p(x)$ tem coeficientes reais, então pela Proposição 3.21 item *(iii)*, $p(z) = \overline{p}(z)$, e daí, $p(z) = (z - \overline{z_0})^m \overline{q}(z)$. Além disso, temos $\overline{q}(\overline{z_0}) = \overline{q(z_0)} \neq \overline{0} = 0$. Logo,

$$p(z) = (z - \overline{z_0})^m \overline{q}(z), \text{ com } \overline{q}(\overline{z}) \neq 0,$$

implicando que $\overline{z_0}$ é raiz de multiplicidade m de $p(x)$. □

A Observação 3.15 nos diz sobre alguns tipos de polinômios que são irredutíveis em $\mathbb{R}[x]$. Vamos agora apresentar um Teorema que melhor caracteriza quais polinômios são irredutíveis em $\mathbb{R}[x]$.

Teorema 3.26. *Um polinômio $p(x) \in \mathbb{R}[x]$ é irredutível em $\mathbb{R}[x]$ se, e somente se, $\partial p(x) = 1$ ou $p(x)$ é um trinômio da forma $(x^2 + bx + c)$, com $\Delta = b^2 - 4c < 0$. Além disso, estes são os únicos polinômios irredutíveis em $\mathbb{R}[x]$.*

Demonstração.

(⇒) Consideremos um elemento $b \in \mathbb{C}$ que seja raiz de $p(x)$ em $\mathbb{C}[x]$ (lembrando que os coeficientes de $p(x)$ são reais). Daí temos as seguintes situações:

(i) Se $b \in \mathbb{R}$ então, pelo Teorema 2.70 temos que $p(x) = (x - b)q(x)$, e como estamos considerando $p(x)$ irredutível, então $q(x) = c$, uma constante real e daí, $p(x)$ é um polinômio de grau 1.

(ii) Se b não for real, então pela Proposição 3.25 o elemento conjugado de b, ou seja $\overline{b}$, também é raiz de $p(x)$. Seja $b = \alpha + \beta i$ e $\overline{b} = \alpha - \beta i$. Então, pelo Corolário 2.30 temos

$$p(x) = (x - b)(x - \overline{b})q(x),$$

com $q(x) \in \mathbb{C}[x]$e $\partial q(x) = n - 2$. Assim, podemos escrever

$$p(x) = [x^2 - 2\alpha x + (\alpha^2 + \beta^2)]q(x).$$

Analisando essa decomposição de $p(x)$ podemos observar que $x^2 - 2\alpha x + (\alpha^2 + \beta^2)$ é um polinômio de $\mathbb{R}[x]$ pois seus coeficientes são reais, e $q(x)$ é um polinômio de $\mathbb{C}[x]$. Pela Definição 2.3 temos que $x^2 - 2\alpha x + (\alpha^2 + \beta^2)$

é divisor de $p(x)$ em $\mathbb{R}[x]$ pois $[x^2 - 2\alpha x + (\alpha^2 + \beta^2)] \in \mathbb{R}[x]$. Assim, pelo Teorema 2.36 existem $q_1(x)$ e $r(x)$ em $\mathbb{R}[x]$ tais que :

$$p(x) = (x^2 - 2\alpha x + (\alpha^2 + \beta^2))q_1(x) + r(x).$$

Pela unicidade de $q_1(x)$ e $r(x)$ em $\mathbb{R}[x]$ concluímos que $q_1(x) = q(x) \in \mathbb{R}[x]$ e $r(x) = 0$ e então:

$$p(x) = (x^2 - 2\alpha x + (\alpha^2 + \beta^2))q(x).$$

Daí, podemos concluir que:

(a) Se $q(x) = c$ onde c é constante não nula, então

$$p(x) = c(x^2 - 2\alpha x + (\alpha^2 + \beta^2)),$$

é um polinômio de grau 2 e seu discriminante é dado por:

$$\Delta = (2\alpha)^2 - 4(\alpha^2 + \beta^2)c^2 = -4\beta^2c^2 < 0;$$

(b) Se $\partial q(x) \geqslant 1$ então $\partial p(x) > 2$ e $p(x)$ é redutível em $\mathbb{R}[x]$ o que nos mostra que qualquer polinômio de grau maior que 2 é redutível em $R[x]$.

Assim, pelos itens (a) e (b) acima concluímos as condições sobre as quais um polinômio é irredutível em $\mathbb{R}[x]$.

($\Leftarrow$) Imediata, considerando a Proposição 2.71 e o Teorema 3.14.

□

Corolário 3.27. *Todo polinômio não nulo e não constante $p(x)$, de grau n e coeficiente líder a, cujos coeficientes são números reais, pode ser representado, a menos da ordem dos fatores, da seguinte forma:*

(i) Se todas as raízes de $p(x)$ são reais então:

$$p(x) = a(x - u_1)^{\alpha_1}(x - u_2)^{\alpha_2} \cdots (x - u_r)^{\alpha_r},$$

onde α_i representa a multiplicidade da raiz u_i e tais que $\alpha_1 + \alpha_2 + \cdots + \alpha_r = n$.

(ii) Se todas as raízes de $p(x)$ são números complexos não reais, então;

$$p(x) = a(x^2 + b_1x + c_1)^{\beta_1}(x^2 + b_2x + c_2)^{\beta_2} \cdots (x^2 + b_sx + c_s)^{\beta_s},$$

onde cada elemento β_j corresponde à multiplicidade do polinômio quadrático $(x^2 + b_jx + c_j)$ com coeficientes reais b_j e c_j tais que $b_j^2 - 4c_j < 0$, para $1 \leqslant j \leqslant s$.

(iii) Se as raízes forem reais e complexas não reais, então:

$$p(x) = a(x - u_1)^{\alpha_1} \cdots (x - u_r)^{\alpha_r}(x^2 + b_1x + c_1)^{\beta_1} \cdots (x^2 + b_sx + c_s)^{\beta_s},$$

com $\alpha_i, \beta_j, b_j, c_j$ reais não nulos e $b_j^2 - 4c_j < 0$.

Demonstração. Este resultado segue imediatamente do Teorema 2.80 e Teorema 3.26

□

Teorema 3.28. *(Teorema Fundamental da Álgebra) O corpo* $\mathbb{C}$ *é algebricamente fechado.*

Demonstração. A demonstração deste Teorema exige abordagens de Análise Real, e portanto vamos omitir tal demonstração. Pode ser encontrada nas referências [17], páginas 435 a 443 ou [1] página 154 a 157. □

Considerando o Teorema 2.41 e o Teorema 2.80 podemos reescrever o Teorema Fundamental da Álgebra 3.28 da seguinte forma:

Teorema 3.29. *Todo polinômio não constante* $p(x) \in \mathbb{C}[x], \partial p(x) = n$*, se escreve de maneira única, a menos da ordem dos fatores como*

$$p(x) = a\,(x - x_1)^{r_1}\,(x - x_2)^{r_2} \cdots (x - x_s)^{r_s}$$

com $x_1, \ldots, x_n \in \mathbb{C}, a \in \mathbb{C}\backslash\{0\}$ *e* $r_1 + \cdots + r_s = n$

Demonstração. Imediata considerando o Teorema 3.28 e o Corolário 2.80. □

4 Equações algébricas

Neste Capítulo abordaremos equações algébricas, representadas por polinômios em uma variável. Enfatizaremos as propriedades das equações polinomiais cujos coeficientes pertencem aos anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.

Definição 4.1. *Seja A um anel. Uma equação polinomial é uma expressão matemática representada por um polinômio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$ tal que:*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0. \tag{4.1}$$

Ao abordarmos as equações polinomiais, conforme a Definição 2.24, queremos encontrar $u \in A$ tal que $p(u) = 0$.

Exemplo 4.2. São equações polinomiais as expressões:

1. $x^3 + 3x^2 + 2x = 0$.
2. $x^4 + (3 - 2i)x^3 = 0$.

Observação 4.3. O grau da equação polinomial corresponde ao grau do polinômio que a representa. Assim, sejam $a_i \in \mathbb{C}$, $0 \leqslant i \leqslant n$, temos:

- $a_1 x + a_0 = 0$ é equação do primeiro grau, desde que $a_1 \neq 0$;
- $a_2 x^2 + a_1 x + a_0$ é equação do segundo grau, desde que $a_2 \neq 0$;

$\vdots$

- $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ é equação de grau n, desde que $a_n \neq 0$.

Para discutir a resolubilidade de equações polinomiais, ou seja, encontrar as raízes dessa equação considere a Definição 2.24 referente à raiz, a Definição 2.42 referente à multiplicidade de uma raiz, e a Proposição 2.31 referente a quantidade de raízes da equação polinomial.

Vamos apresentar algumas propriedades relacionadas às raízes comuns dos polinômios, e sua relação com os coeficientes da equação polinomial.

4.1 Raízes múltiplas

Teorema 4.4. *Sejam $K \subset \mathbb{C}$, onde K é um dos anéis $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, $p(x) \in K[x]$, tal que $p(x) = q(x) \cdot g(x) + r(x)$. Se u é raiz de $p(x)$ e $g(x)$, então u é raiz de $r(x)$.*

Demonstração. Sendo $p(x) = q(x) \cdot g(x) + r(x)$ então $r(x) = p(x) - q(x) \cdot g(x)$. Daí temos:

$$r(u) = p(u) - q(u) \cdot g(u) \Rightarrow 0 - q(u) \cdot 0 = 0$$

Logo, u é raiz de $r(x)$. □

Teorema 4.5. *Sejam $K \subset \mathbb{C}$, onde K é um dos anéis $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, $p(x) \in K[x]$ tal que $p(x) = q(x) \cdot g(x) + r(x)$. Se u é raiz de $g(x)$ e $r(x)$ então u é raiz de $p(x)$.*

Demonstração. Como $p(x) = q(x) \cdot g(x) + r(x)$ então, $p(u) = q(u) \cdot g(u) + r(u) = q(u) \cdot 0 + 0 = 0$ Logo, u é raiz de $p(x)$. □

Proposição 4.6. *Sejam $K \subset \mathbb{C}$, onde K é um dos anéis $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, $p(x) \in K[x]$ com $\partial p(x) \geqslant 1$ e seja $u \in \mathbb{C}$ tal que $p(u) = 0$. Então:*

(i) u é raiz simples[1] de $p(x)$ se, e somente se, $p(u) = 0$ e $p'(u) \neq 0$, onde $p'(x)$ é a derivada de $p(x)$ (Definição 2.27);

(ii) Se $p(x)$ é irredutível em K, então todas as raízes de $p(x)$ são simples.

Demonstração.

(*i*) Seja $p(x) \in K[x]$.

(⇒) Se u é raiz simples de $p(x)$ então pela Proposição 2.44 temos que $p(x) = (x - u) \cdot g(x)$, $g(u) \neq 0$. Consequentemente, considerando a Definição 2.27, item (*b*), a respeito da derivada de produto, temos,

$$p'(x) = (x - u)' \cdot g(x) + (x - u)g'(x) = g(x) + (x - u)g'(x),$$

e daí $p'(u) = g(u)$. Como $g(u) \neq 0$, então $p'(u) \neq 0$.

(⇐) De $p(u) = 0$ temos pelo Teorema 2.41 que $(x - u) \mid p(x)$ ou seja $p(x) = (x - u)g(x)$. Suponhamos que u seja raiz de multiplicidade $s \geqslant 1$. Então pela Proposição 2.44 temos que:

$$p(x) = (x - u)^s \cdot h(x),\ h(u) \neq 0,$$

e pela regra da derivada do produto, temos

$$p'(x) = s \cdot (x - u)^{s-1} \cdot h(x) + (x - u)^s \cdot h'(x).$$

Como $h(u) \neq 0$ então $p'(u) = 0$ implica em $s = 1$. Logo, u é raiz de multiplicidade 1 de $p(x)$.

(*ii*) Seja $p(x) \in K[x]$ irredutível sobre K, $u \in \mathbb{C}$ raiz de multiplicidade s de $p(x)$. Vamos mostrar que $s = 1$.

Seja $g(x)$ o polinômio mônico de menor grau tal que $g(u) = 0$. Considerando o Teorema 2.37 sobre $p(x)$, existem $q(x), r(x) \in K[x]$ tal que:

$$p(x) = q(x) \cdot g(x) + r(x), \text{ com } r(x) = 0 \text{ ou } \partial r(x) < \partial g(x).$$

[1] multiplicidade 1

Como $r(u) = p(u) - q(u) \cdot g(u) = 0$, então $r(u) = 0$. Como $g(x)$ é o de menor grau tal que $g(u) = 0$, temos $r(x) = 0$, logo,

$$p(x) = q(x) \cdot g(x).$$

Mas pela irredutibilidade de $p(x)$, conforme a Definição 2.62, temos

$$p(x) = c \cdot g(x), c \in K.$$

Assim, se $s > 1$ então, pelo item (i), $p'(u) = 0$, e consequentemente $g'(u) = 0$, contrariando o fato de $g(x)$ ter grau mínimo. Logo $s = 1$.

□

Teorema 4.7. *Seja $K \subset \mathbb{C}$, onde K é um dos anéis $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, $u \in K$ e $p(x) \in K[x]$. Se u é raiz de multiplicidade s de $p(x)$ então u é raiz de multiplicidade $s-1$ de $p'(x)$.*

Demonstração. Como u é raiz de multiplicidade s de $p(x)$ então, pela Proposição 2.44 temos

$$p(x) = (x-u)^s \cdot g(x), g(u) \neq 0,$$

e pela regra da derivada do produto (Definição 2.27), temos:

$$\begin{aligned} p'(x) &= s \cdot (x-u)^{s-1} \cdot g(x) + (x-u)^s \cdot g'(x) \\ &= s \cdot (x-u)^{s-1} \cdot g(x) + (x-u)^{s-1} \cdot (x-u) \cdot g'(x) \\ &= (x-u)^{s-1} \cdot [s \cdot g(x) + (x-u) \cdot g'(x)] \\ &= (x-u)^{s-1} \cdot h(x). \end{aligned}$$

Como $g(u) \neq 0$ então $h(u) \neq 0$, logo, u é raiz de multiplicidade $s-1$ de $p'(x)$. □

Corolário 4.8. *Seja $K \subset \mathbb{C}$, onde K é um dos anéis $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, $u \in K$ e $p(x) \in K[x]$. Então, se u é raiz de multiplicidade s de $p(x)$, vale*

$$p(u) = 0, p'(u) = 0, \ldots, p^{s-1}(u) = 0 \text{ e } p^s(u) \neq 0,$$

onde p^i, $1 \leqslant i \leqslant s$, representa as ordens das derivadas de $p(x)$, sendo $p^1(x) = p'(x)$.

Exemplo 4.9. Seja $p(x) = x^3 - x^2 - x + 1 \in \mathbb{R}[x]$. Temos que 1 é raiz de multiplicidade $s = 2$ de $p(x)$, pois:

$$\begin{array}{rcllcl} p(x) & = & x^3 - x^2 - x + 1 & \Rightarrow & p(1) & = & 0; \\ p'(x) & = & 3x^2 - 2x - 1 & \Rightarrow & p(1) & = & 0; \\ p^2(x) & = & 6x - 2 & \Rightarrow & p(1) & = & 4 \neq 0. \end{array}$$

De fato,

$$p(x) = x^3 - x^2 - x + 1 = (x-1)^2(x+1).$$

Os resultados do Teorema 4.7 e Corolário 4.8 nos trazem informações importantes a respeito das raízes de um polinômio. Vamos agora verificar uma forma de encontrar as multiplicidades das raízes de um polinômio, considerando ser este polinômio fatorial.

Corolário 4.10. *Sejam $K \subset \mathbb{C}$, onde K é um dos anéis $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, $p(x) \in K[x]$, tal que*

$$p(x) = (x-\alpha_1)^{\beta_1}(x-\alpha_2)^{\beta_2}\cdots(x-\alpha_r)^{\beta_r},$$

onde $\alpha_1, \alpha_2, \ldots, \alpha_r$ *são raízes de* $p(x)$, $\beta_1, \beta_2, \ldots, \beta_r$ *as respectivas multiplicidades e* $p'(x)$ *a derivada de* $p(x)$. *Pelo Corolário 4.8* $\alpha_1, \alpha_2, \ldots, \alpha_r$ *são raízes de multiplicidade* $\beta_1 - 1, \beta_2 - 1, \ldots, \beta_r - 1$ *de* $p'(x)$. *Daí temos que* $p(x)$ *e* $p'(x)$ *são divisíveis por*

$$d(x) = (x-\alpha_1)^{\beta_1-1}(x-\alpha_2)^{\beta_2-1}\cdots(x-\alpha_r)^{\beta_r-1}$$

e $d(x)$ *é o M.D.C*$\{p(x), p'(x)\}$.

Observação 4.11. Vamos agora deduzir um método prático para encontrar a fatoração de $p(x)$, quando conhecermos $p(x)$ e $p'(x)$, e admitindo que $p(x)$ é fatorável, como no Corolário 4.10. Fazendo a divisão de $p(x)$ por $p'(x)$, obtêm-se:

$$p(x) = p'(x)q(x) + r(x),$$

com $\partial r(x) < \partial p'(x)$. Ao dividirmos $p'(x)$ por $r(x)$, obtemos,

$$p'(x) = r(x)q_1(x) + r_1(x),$$

com $\partial r_1(x) < \partial r(x)$. Continua-se o processo até obter $r_k(x)$ nulo, e isto irá acontecer, pois consideramos que os polinômios são fatoráveis. Assim,

$$\begin{aligned}
p(x) = p'(x)q(x) + r(x) &\Rightarrow \text{M.D.C.}\{p(x), p'(x)\} = \text{M.D.C.}\{p'(x), r(x)\};\\
p'(x) = r(x)q_1(x) + r_1(x) &\Rightarrow \text{M.D.C.}\{p'(x), r(x)\} = \text{M.D.C.}\{r(x), r_1(x)\};\\
r(x) = r_1(x)q_2(x) + r_2(x) &\Rightarrow \text{M.D.C.}\{r(x), r_1(x)\} = \text{M.D.C.}\{r_2(x), r_1(x)\};\\
&\vdots\\
r_{k-2}(x) = r_{k-1}(x)q_k(x) &\Rightarrow \text{M.D.C.}\{r_{k-3}(x), r_{k-2}(x)\} = \text{M.D.C.}\{r_{k-2}(x), r_{k-1}(x)\}.
\end{aligned}$$

Com este processo, encontram-se $d(x) = \text{M.D.C.}\{p(x), p'(x)\}$, que terá raízes iguais as do último resto não nulo. Encontra-se assim um fator da decomposição de $p(x)$, que pode auxiliar na busca da fatoração de $p(x)$. Considerando $p(x) = p_1(x)d(x)$, fatorar $d(x)$ e $p_1(x)$ pode ser mais simples que fatorar $p(x)$. Vejamos no exemplo abaixo:

Exemplo 4.12. Verificar as multiplicidades das raízes de $p(x) = x^3 - 3x^2 - 9x + 27$.

Soluçáo. Sejam, $p(x) = x^3 - 3x^2 - 9x + 27$ e $p'(x) = 3x^2 - 6x - 9$.

$$\begin{aligned}
p(x) &= p'(x)\left(\frac{1}{3}x - \frac{1}{3}\right) + (-8x + 24)\\
p'(x) &= (-8x + 24)\left(-\frac{3}{8}x - \frac{3}{8}\right) + 0.
\end{aligned}$$

Logo, M.D.C.$\{p(x), p'(x)\} = (-8x + 24)$, implicando que $x = 3$ é raiz de $p(x)$. Assim, divide-se $p(x)$ por $x - 3$, obtendo-se

$$p(x) = (x-3)(x^2 - 9).$$

Fatora-se $x^2 - 9 = (x + 3)(x - 3)$ obtendo-se

$$p(x) = (x+3)(x-3)^2.$$

Com isso, verificamos que $x = 3$ é raiz de multiplicidade 2 e $x = -3$ é raiz de multiplicadde 1 de $p(x)$.

Analisaremos agora algumas formas de resolver equações, de acordo com o grau do polinômio que a representa. Para isso, vamos considerar as equações polinomiais com coeficientes em $\mathbb{C}$, fazendo a devida distinção nos casos em que os coeficientes estiverem em $\mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$.

4.2 Resolução de equações

Para abordarmos as equações consideremos sobre o corpo $\mathbb{C}$ as seguintes equações:

1. Equação do primeiro grau, com $a \neq 0$

$$ax + b = 0.$$

2. Equação do segundo grau, com $a \neq 0$

$$ax^2 + bx + c = 0.$$

3. Equação do terceiro grau, com $a_3 \neq 0$

$$a_3x^3 + a_2x^2 + a_1x + a_0 = 0.$$

4. Equação do quarto grau, com $a_4 \neq 0$

$$a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0.$$
$$\vdots$$

5. Equação de grau n, com $a_n \neq 0$

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0.$$

4.2.1 Equação do primeiro grau

Consideremos a equação do primeiro grau, dada por:

$$ax + b = 0,\ a \neq 0. \tag{4.2}$$

A equação possui solução:

(i) Em $\mathbb{Z}$, se $a \mid b$;

(ii) Em $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, para todo a e b pertencentes a estes anéis, sendo $a \neq 0$.

A solução ou raiz desta equação é $x = -\dfrac{b}{a}$.

Exemplo 4.13. Quais as raízes inteiras e reais da equação

$$3x - 17 = 0$$

Não temos raízes inteiras, e a raiz real é dada por $x = \dfrac{17}{3}$

4.2.2 Equação do segundo grau

Consideremos a equação do segundo grau dada por:

$$ax^2 + bx + c = 0,\ a \neq 0, \tag{4.3}$$

então,

(i) Considerando os coeficientes em $\mathbb{Z}$, a equação possui solução em $\mathbb{Z}$, se $2a \mid b$ e $2a \mid \sqrt{\Delta}$, onde $\Delta = b^2 - 4ac$.

(ii) Considerando os coeficientes em $\mathbb{Q}$, a equação possui solução em $\mathbb{Q}$ se Δ é quadrado perfeito. Observemos que aqui estamos considerando a Proposição 3.10 a respeito de Δ, Teorema 2.79 a respeito da forma fatorada de $p(x)$ e Proposição 2.41 a respeito das raízes e divisibilidade.

(iii) Seja $\Delta = b^2 - 4ac$, o discriminante desta equação, conforme Definição 3.9. Considerando os coeficientes em $\mathbb{R}$, a equação possui solução em $\mathbb{R}$, se $\Delta \geqslant 0$ de modo que:

Se $\Delta > 0$, temos duas raízes reais distintas;

Se $\Delta = 0$, temos duas raízes reais idênticas;

(iv) A equação possui solução em $\mathbb{C}$ para todo $a, b, c \in \mathbb{C}$, considerando que $\mathbb{C}$ é algebricamente fechado.

A expressão obtida para cálculo da raiz é dada por

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

sendo

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a}$$

e

$$x_2 = \frac{-b\ - \sqrt{\Delta}}{2a}.$$

Exemplo 4.14. Vamos verificar a existência de raízes inteiras ou reais na equação $2x^2 - 6x + 4 = 0$.

1. Calculando o discriminante Δ obtemos:

$$\Delta = b^2 - 4ac = 6^2 - 4 \cdot 2 \cdot 4 = 4.$$

Como Δ é um quadrado perfeito então a equação possui raízes racionais, além disso, como $\Delta > 0$ então as raízes são distintas.

Exemplo 4.15. Vamos verificar a existência de raízes inteiras ou reais na equação $x^2 - 4x + 7 = 0$.

1. Calculando o discriminante Δ obtemos:

$$\Delta = b^2 - 4ac = (-4)^2 - 4 \cdot 1 \cdot 7 = -12$$

Como $\Delta < 0$ então a equação não possui raízes reais. Mas, como os coeficientes são números reais, então a equação possui raízes complexas conjugadas.

4.2.3 Equação do terceiro grau

Vamos considerar a equação do terceiro grau com coeficientes em $\mathbb{C}$,

$$a'_3x^3 + a'_2x^2 + a'_1x + a'_0 = 0, \quad \text{com} \quad a'_3 \neq 0. \tag{4.4}$$

A respeito das soluções desta equação, podemos afirmar que, se os coeficientes forem números reais, de acordo com o Teorema 3.18, ela possui pelo menos uma raiz real e além disso, pelo Teorema 3.25, se ela possui uma raiz complexa z, então o conjugado de z, $\overline{z}$ também é raiz desta equação. Sendo $\mathbb{C}$ algebricamente fechado, se estivermos considerando os coeficientes no anel $\mathbb{C}$ é evidente que ela possua raízes complexas.

Para encontrar as soluções desta equação, a partir da expressão (4.4) obtemos a equação,

$$x^3 + a_2x^2 + a_1x + a_0 = 0$$

onde $a_2 = \dfrac{a'_2}{a'_3}$, $a_1 = \dfrac{a'_1}{a'_3}$, $a_0 = \dfrac{a'_0}{a'_3}$.

Vamos encontrar as raízes da equação do terceiro grau na forma

$$x^3 + a_2x^2 + a_1x + a_0 = 0. \tag{4.5}$$

Para isso, efetuamos algumas alterações na equação da seguinte forma:

(i) Com o objetivo de obtermos uma expressão onde não apareça o termo de grau 2, na expressão (4.5) fazemos uma mundança de variável, substituindo x por $y + d$. Com isso obtemos a expressão

$$y^3 + (3d + a_2)y^2 + (3d^2 + 2da_2 + a_1)y + (d^3 + d^2a_2 + da_1 + a_0). \tag{4.6}$$

Fazendo $d = -\dfrac{a_2}{3}$, substituímos x por $y - \dfrac{a_2}{3}$, ou seja,

$$x = y - \frac{a_2}{3}, \tag{4.7}$$

obtemos a expressão da equação:

$$y^3 + py + q = 0, \tag{4.8}$$

onde

$$p = a_1 - \frac{a_2^2}{3} \quad e \quad q = \frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0. \tag{4.9}$$

(ii) Na expressão (4.8) fazemos a substituição

$$y = u + v, \tag{4.10}$$

obtendo a expressão

$$u^3 + v^3 + (p + 3uv) \cdot (u + v) + q = 0.$$

Nesta igualdade consideremos

$$p + 3uv = 0 \Rightarrow uv = -\frac{p}{3},$$

e daí obtemos um sistema de equações definido por

$$\begin{cases} u^3 + v^3 &= -q \\ u \cdot v &= -\dfrac{p}{3}. \end{cases} \tag{4.11}$$

Continuando o processo, elevando ao cubo os termos da segunda equação do sistema (4.11), obtemos o sistema

$$\begin{cases} u^3 + v^3 &= -q \\ u^3 \cdot v^3 &= -\dfrac{p^3}{27}. \end{cases} \tag{4.12}$$

(iii) Para continuarmos o processo, temos que observar que as equações do sistema (4.12) correspondem a soma e produto das raízes u^3 e v^3 de uma equação do segundo grau, da forma

$$t^2 + qt - \frac{p^3}{27} = 0.$$

Resolvendo essa equação do segundo grau obtemos as raízes

$$\begin{aligned} t_1 &= -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}; \\ t_2 &= -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}. \end{aligned} \tag{4.13}$$

Assim, considerando $u^3 = t_1$ e $v^3 = t_2$ que satisfaça as condições do sistema (4.12) e definindo a expressão

$$w = \frac{-1 + i\sqrt{3}}{2},$$

os possíveis valores de u e v são dados por:

$$\begin{aligned} u_1 &= \sqrt[3]{t_1} \quad , \quad v_1 = \sqrt[3]{t_2}; \\ u_2 &= w\sqrt[3]{t_1} \quad , \quad v_2 = w^2\sqrt[3]{t_2}; \\ u_3 &= w^2\sqrt[3]{t_1} \quad , \quad v_3 = w\sqrt[3]{t_2}. \end{aligned} \tag{4.14}$$

(iv) Agora com as soluções u e v obtidas, conforme as relações apresentadas em (4.14), e substituindo-as na expressão (4.10), obtemos as relações chamadas de fórmula

de Cardano, definidas da seguinte forma:

$$\begin{aligned}
y_1 &= u_1 + v_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}};\\
y_2 &= u_2 + v_2 = w\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + w^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}; \qquad (4.15)\\
y_3 &= u_3 + v_3 = w^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + w\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.
\end{aligned}$$

(v) Para finalizar o processo, substituímos o valores y_1, y_2, y_3 da fórmula de Cardano (4.15) na expressão (4.7) e, fazendo as substituições dos valores p e q da expressão (4.9), encontramos os valores x_1, x_2, x_3 que são raízes da equação cúbica expressa em (4.5), de modo que:

$$\begin{aligned}
x_1 &= \sqrt[3]{-\frac{\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0}{2} + \sqrt{\frac{\left(\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0\right)^2}{4} + \frac{\left(a_1 - \frac{a_2^2}{3}\right)^3}{27}}}\\
&\quad + \sqrt[3]{-\frac{\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0}{2} - \sqrt{\frac{\left(\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0\right)^2}{4} + \frac{\left(a_1 - \frac{a_2^2}{3}\right)^3}{27}}}\\
&\quad - \frac{a_2}{3};\\
x_2 &= \frac{-1 + i\sqrt{3}}{2}\sqrt[3]{-\frac{\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0}{2} + \sqrt{\frac{\left(\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0\right)^2}{4} + \frac{\left(a_1 - \frac{a_2^2}{3}\right)^3}{27}}}\\
&\quad + \left(\frac{-1 + i\sqrt{3}}{2}\right)^2\sqrt[3]{-\frac{\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0}{2} - \sqrt{\frac{(\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0)^2}{4} + \frac{\left(a_1 - \frac{a_2^2}{3}\right)^3}{27}}}\\
&\quad - \frac{a_2}{3};\\
x_3 &= \left(\frac{-1 + i\sqrt{3}}{2}\right)^2\sqrt[3]{-\frac{\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0}{2} + \sqrt{\frac{\left(\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0\right)^2}{4} + \frac{\left(a_1 - \frac{a_2^2}{3}\right)^3}{27}}}\\
&\quad + \frac{-1 + i\sqrt{3}}{2}\sqrt[3]{-\frac{\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0}{2} - \sqrt{\frac{(\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0)^2}{4} + \frac{\left(a_1 - \frac{a_2^2}{3}\right)^3}{27}}}\\
&\quad - \frac{a_2}{3}.
\end{aligned}$$

Exemplo 4.16. Vamos encontrar as raízes complexas da equação

$$x^3 - 9x^2 - 9x - 15 = 0.$$

Solução. Fazendo a substituição da variável x conforme a expressão (4.7) e encontrando os valores p e q conforme a expressão (4.9), obtemos a equação cúbica na variável y, como na expressão (4.8) da seguinte forma:

$$y^3 - 36y - 96 = 0,$$

onde $x = y + 3$.
Na equação cúbica na variável y, fazemos a mudança de variável em y, conforme a expressão (4.10) e consequentemente obtemos um sistema de equações como na expressão (4.12), onde as soluções desse sistema correspondem a soma e produto das raízes da equação do segundo grau da forma

$$z^2 + 96z + 1728 = 0.$$

Resolvendo essa equação obtemos as raízes: $z_1 = -24$ e $z_2 = -72$.
Assim, sendo $u^3 = z_1$, $v^3 = z_2$ e $w = \dfrac{-1 + i\sqrt{3}}{2}$ obtemos o valores:

$$u_1 = \sqrt[3]{-24} = -2\sqrt[3]{3} \quad , \quad v_1 = \sqrt[3]{-72} = -2\sqrt[3]{3}\sqrt[3]{3};$$

$$u_2 = w\sqrt[3]{-24} = -2w\sqrt[3]{3} \quad , \quad v_2 = w^2\sqrt[3]{-72} = -2w^2\sqrt[3]{3}\sqrt[3]{3};$$

$$u_3 = w^2\sqrt[3]{-24} = -2w^2\sqrt[3]{3} \quad , \quad v_3 = w\sqrt[3]{-72} = -2w\sqrt[3]{3}\sqrt[3]{3}.$$

A partir desses valores encontramos os valores y_1, y_2, y_2 dados por:

$$y_1 = u_1 + v_1 = -2\sqrt[3]{3} - 2\sqrt[3]{3}\sqrt[3]{3} = -2\sqrt[3]{3}(1 + \sqrt[3]{3});$$

$$y_2 = u_2 + v_2 = -2w\sqrt[3]{3} - 2w^2\sqrt[3]{3}\sqrt[3]{3} = -2\sqrt[3]{3}(w + w^2\sqrt[3]{3});$$

$$y_3 = u_3 + v_3 = -2w^2\sqrt[3]{3} - 2w\sqrt[3]{3}\sqrt[3]{3} = -2\sqrt[3]{3}(w^2 + w\sqrt[3]{3}).$$

A partir dos valores y_1, y_2, y_3 encontramos as raízes x_1, x_2, x_3 da forma:

$$x_1 = y_1 + 3 = -2\sqrt[3]{3}(1 + \sqrt[3]{3}) + 3;$$

$$x_2 = y_2 + 3 = -2\sqrt[3]{3}(w + w^2\sqrt[3]{3}) + 3;$$

$$x_3 = y_3 + 3 = -2\sqrt[3]{3}(w^2 + w\sqrt[3]{3}) + 3.$$

4.2.4 Equação do quarto grau

Vamos considerarar a equação do quarto grau na forma

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

Considerando os coeficientes, em quaisquer anéis $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, então podemos ter:

(i) Duas raízes reais e duas complexas conjugadas;

(ii) Quatro raízes reais;

(iii) Quatro raízes complexas, sendo dois pares de duas complexas conjugadas.

Para encontrarmos as raízes ou soluções desta equação, utilizaremos uma forma de resolução denominado método de Ferrari. Para isso seguimos os seguintes passos:

1. A equação $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ será escrita na forma

$$x^4 + a_3x^3 = -(a_2x^2 + a_1x + a_0). \tag{4.16}$$

2. Na expressão (4.16) completamos o quadrado no primeiro membro, mantendo a equivalência da igualdade e então obtemos a expressão

$$\left(x^2 + \frac{1}{2}a_3x\right)^2 = \left(\frac{1}{4}a_3^2 - a_2\right)x^2 - a_1x - a_0. \tag{4.17}$$

3. Para transformar o segundo membro da expressão (4.17) em um quadrado perfeito, adicionamos a ambos membros a expressão

$$y^2 + 2y(x^2 + \tfrac{1}{2}a_3x),$$

e obemos a expressão

$$\left[\left(x^2 + \frac{1}{2}a_3x\right) + y\right]^2 = \left(2y + \frac{1}{4}a_3^2 - a_2\right)x^2 + (ya_3 - a_1)\,x + \left(y^2 - a_0\right). \tag{4.18}$$

O segundo membro da expressão (4.18) corresponde a uma equação do segundo grau na variável x e esta somente poderá ser reduzida a um quadrado perfeito se as raízes forem idênticas, ou seja, se tivermos o discriminante $\Delta = 0$, conforme mostrado na resolução da equação do segundo grau. Assim, devemos ter

$$(ya_3 - a_1)^2 - 4\left(2y + \frac{1}{4}a_3^2 - a_2\right)\left(y^2 - a_0\right) = 0. \tag{4.19}$$

4. Assumindo que o y corresponde a uma das raízes da expressão (4.19), então a expressão (4.18) pode ser escrita na forma

$$\left[\left(x^2 + \frac{1}{2}a_3x\right) + y\right]^2 = (ax + b)^2. \tag{4.20}$$

5. Resolvendo a equação obtida na expressão (4.20) obtemos:

$$\left(x^2 + \frac{1}{2}a_3x\right) + y = (ax + b); \tag{4.21}$$

$$\left(x^2 + \frac{1}{2}a_3x\right) + y = -(ax + b). \tag{4.22}$$

com a e b convenientes.

6. A partir das expressões (4.21) e (4.22) obtemos:

$$x^2 + \left(\frac{a_3}{2} - a\right)x + (y - b) = 0; \tag{4.23}$$

$$x^2 + \left(\frac{a_3}{2} + a\right)x + (y + b) = 0. \tag{4.24}$$

7. Resolvendo as equações (4.23) e (4.24) encontramos x_1, x_2, x_3 e x_4 sendo:

$$x_1 = \frac{-\left(\frac{a_3}{2} - a\right) + \sqrt{\left(\frac{a_3}{2} - a\right)^2 - 4 \cdot (y - b)}}{2};$$
$$x_2 = \frac{-\left(\frac{a_3}{2} - a\right) - \sqrt{\left(\frac{a_3}{2} - a\right)^2 - 4 \cdot (y - b)}}{2};$$
$$x_3 = \frac{-\left(\frac{a_3}{2} - a\right) + \sqrt{\left(\frac{a_3}{2} - a\right)^2 - 4 \cdot (y + b)}}{2};$$
$$x_4 = \frac{-\left(\frac{a_3}{2} - a\right) - \sqrt{\left(\frac{a_3}{2} - a\right)^2 - 4 \cdot (y + b)}}{2}.$$

com a e b convenientes e y a raiz da equação (4.19).

Exemplo 4.17. Vamos encontrar as raízes complexas da equação

$$x^4 + 2x^3 + x^2 + 4x - 2 = 0.$$

A equação pode ser escrita na forma

$$x^4 + 2x^3 = -x^2 - 4x + 2.$$

Completando quadrado no primeiro termo e mantendo a equivalência da expressão, obtemos

$$(x^2 + x)^2 = -4x + 2.$$

Para transformar o segundo membro em um quadrado perfeito, mantendo a equivalência da expressão, adicionamos a ambos membros a expressão $y^2 + 2y\,(x^2 + x)$ e obtemos a expressão

$$[(x^2 + x) + y]^2 = 2yx^2 + (2y - 4)x + (y^2 + 2)$$

Para que o segundo membro seja quadrado perfeito, devemos ter o discriminante $\Delta = 0$, conforme a expressão (4.19). Encontrando o valor que satisfaz essa condição, obtemos $y = \dfrac{1}{2}$ e com esse valor escrevemos a expressão na seguinte forma:

$$\left[(x^2 + x) + \frac{1}{2}\right]^2 = \left(x - \frac{3}{2}\right)^2.$$

Assim, as soluções da equação são dadas por:

1. $(x^2 + x) + \dfrac{1}{2} = x - \dfrac{3}{2}$.

   onde, efetuando os devidos cálculos, obtemos

   (a) $x_1 = \sqrt{2}i$;

   (b) $x_2 = -\sqrt{2}i$.

2. $(x^2+x)+\dfrac{1}{2}=-x+\dfrac{3}{2}$),

   onde, efetuando os devidos cálculos, obtemos:

   (a) $x_3=-1+\sqrt{2}$;

   (b) $x_4=-1-\sqrt{2}$.

Logo, as soluções da equação são dadas por

$$S=\{-\sqrt{2}i,\sqrt{2}i,-1-\sqrt{2},-1+\sqrt{2}\}.$$

4.3 Relação entre coeficientes e raízes

Definição 4.18. *Sejam $K\subset\mathbb{C}$ um corpo, onde K é um dos anéis $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, x uma indeterminada, $\alpha_1,\alpha_2,\ldots,\alpha_n$ elementos de K e $p(x)$ tal que,*

$$p(x)=\prod_{i=1}^{n}(x-\alpha_i)=(x-\alpha_1)\cdot(x-\alpha_2)\cdots(x-\alpha_n). \tag{4.25}$$

Vamos definir as seguintes somas relacionadas a $\alpha_1,\alpha_2,\ldots,\alpha_n$.

$$\begin{aligned}
s_1 &= \sum_{i=1}^{n}\alpha_i=\alpha_1+\alpha_2+\cdots+\alpha_n;\\
s_2 &= \sum_{i_1<i_2}^{n}\alpha_{i_1}\cdot\alpha_{i_2}=\alpha_1\alpha_2+\alpha_1\alpha_3+\cdots+\alpha_1\alpha_n+\cdots+\alpha_{n-1}\alpha_n;\\
s_3 &= \sum_{i_1<i_2<i_3}^{n}\alpha_{i_1}\cdot\alpha_{i_2}\cdot\alpha_{i_3}\\
&= \alpha_1\alpha_2\alpha_3+\cdots+\alpha_1\alpha_2\alpha_n+\cdots+\alpha_{n-2}\alpha_{n-1}\alpha_n;\\
&\vdots\\
s_{n-1} &= \sum_{i_1<i_2<\cdots<i_{n-1}}^{n}\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_{n-1}}\\
&= \alpha_1\alpha_2\cdots\alpha_{n-1}+\cdots+\alpha_2\alpha_3\cdots\alpha_n;\\
s_n &= \alpha_1\alpha_2\cdots\alpha_n.
\end{aligned} \tag{4.26}$$

Proposição 4.19. *Considerando o polinômio* (4.25) *e as somas* (4.26) *apresentadas na Definição 4.18, é válida a seguinte igualdade:*

$$\begin{aligned}
\prod_{i=1}^{n}(x-\alpha_i) &= (x-\alpha_1)\cdot(x-\alpha_2)\cdots(x-\alpha_n)\\
&= x^n-s_1x^{n-1}+\cdots+(-1)^ns_n.
\end{aligned}$$

Demonstração. Faremos por indução sobre $n\geqslant 2$.

Para $n=2$ o resultado é válido pois

$$\begin{aligned}
(x-\alpha_1)\cdot(x-\alpha_2) &= x^2-\alpha_2x-\alpha_1x+\alpha_1\alpha_2\\
&= x^2-(\alpha_1+\alpha_2)x+\alpha_1\alpha_2\\
&= x^2-s_1x+(-1)^2s_2.
\end{aligned}$$

Suponhamos que o resultado é válido para n, ou seja,

$$(x-\alpha_1)\cdot(x-\alpha_2)\cdots(x-\alpha_n) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n.$$

Vamos mostrar que é válido para $n+1$. De fato, multiplicando ambos lados da expressão por $(x-\alpha_{n+1})$ obtemos a expressão

$$\begin{aligned}(x-\alpha_1)\cdot(x-\alpha_2)\cdots(x-\alpha_n)(x-\alpha_{n+1}) &= [x^n - s_1x^{n-1} + \cdots + (-1)^n s_n](x-\alpha_{n+1}) \\ &= x^{n+1} - [s_1+\alpha_{n+1}]x^n + \\ &\quad [s_2x^{n-1} + \alpha_{n+1}s_1]x^{n-1} + \cdots + \\ &\quad (-1)^{n+1}\alpha_{n+1}s_n \\ &= x^{n+1} - s_1x^n + \cdots + (-1)^n s_n x + (-1)^{n+1}s_{n+1}.\end{aligned}$$

Este resultado nos diz que a igualdade é valida para todo n. □

Proposição 4.20. *Seja $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ um polinômio com coeficientes no corpo K, $\alpha_1, \alpha_2, \ldots, \alpha_n$ raízes de $p(x)$ (não necessariamente distintas), s_i, $1 \leqslant i \leqslant n$ as somas (4.26) representadas na Definição 4.18. Então:*

$$s_i = (-1)^i \frac{a_{n-i}}{a_n}, 1 \leqslant i \leqslant n.$$

Demonstração. Pelo Teorema 2.79 podemos escrever

$$p(x) = a_n[(x-\alpha_1)\cdot(x-\alpha_2)\cdots(x-\alpha_n)].$$

Então, pela Proposição 4.19,

$$p(x) = a_n[x^n - s_1x^{n-1} + \cdots + (-1)^{n-1}s_{n-1}x + (-1)^n s_n].$$

Para obter o resultado basta igualar os coeficientes dos termos de mesmo grau.

□

Exemplo 4.21. Vamos resolver a equação polinomial $x^4 - 2x^3 + 4x^2 + 6x - 21 = 0$ sabendo que existem duas raízes simétricas.

Sejam $\alpha_1, \alpha_2, \alpha_3$ e α_4 as raízes. Vamos considerar $\alpha_1 + \alpha_2 = 0$ (condição do problema). Temos então:

(1) $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 2$;
(2) $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 = 4$;
(3) $\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4\alpha_2\alpha_3\alpha_4 = -6$;
(4) $\alpha_1\alpha_2\alpha_3\alpha_4 = -21$;
(5) $\alpha_1 + \alpha_2 = 0$.

Para resolver efetuamos as operações:

Substituindo (5) em (1) temos:

(6) $(\alpha_1 + \alpha_2) + \alpha_3 + \alpha_4 = 2 \Rightarrow \alpha_3 + \alpha_4 = 2$

Substituindo (5) em (3) temos:

(7) $\alpha_1\alpha_2\underbrace{(\alpha_3+\alpha_4)}_{2} + (\alpha_3\alpha_4)\underbrace{(\alpha_1+\alpha_2)}_{0} = -6 \Rightarrow \alpha_1\alpha_2 = -3.$

Substituido (7) em (4) temos:

(8) $(\alpha_1\alpha_2)\alpha_3\alpha_4 = -21 \Rightarrow \alpha_3\alpha_4 = 7$.

Temos então,

(9) $\alpha_1 + \alpha_2 = 0$ e $\alpha_1\alpha_2 = -3 \Rightarrow \alpha_1 = \sqrt{3}$, $\alpha_2 = -\sqrt{3}$.

(10) $\alpha_3 + \alpha_4 = 2$ e $\alpha_3\alpha_4 = 7 \Rightarrow \alpha_3 = 1 - \sqrt{6}i$, $\alpha_4 = 1 + \sqrt{6}i$.

Assim o conjunto solução $S = \{\sqrt{3}, -\sqrt{3}, 1 - \sqrt{6}i, 1 + \sqrt{6}i\}$.

5 Aplicação na Educação Básica

Antes de apresentarmos as atividades propostas a respeito de polinômios, a serem trabalhadas na Educação Básica, faremos uma breve síntese de como este assunto é tratado em alguns livros didáticos ou materiais de apoio.

O estudo de polinômios é apresentado no Ensino Fundamental, conforme mencionado na Introdução, sob a abordagem de expressões algébricas e funções do primeiro e segundo graus. Neste segmento, a abordagem mais específica e relacionada aos estudos de polinômios se dá por meio da habilidade da BNCC [3]:

> (EF09MA09)- Compreender os processos de fatoração de expressões algébricas, com base em suas relações com os produtos notáveis, para resolver e elaborar problemas que possam ser representados por equações polinomiais do 2^{o} grau.

Nesta abordagem são apresentados alguns tópicos relacionados a polinômios, conforme vemos no livro didático *A Conquista da Matemática* [15] e de forma semelhante no livro didático *Araribá Mais Matemática* [12].

Definição de polinômio: Denomina-se monômio ou termo algébrico toda expressão algébrica representada apenas por um número, ou apenas por uma variável, ou por uma multiplicação de números e variáveis em que esta não esteja no denominador nem no radical. A adição algébrica de monômios formam um polinômio.

Fatoração de polinômios: Fatorar um polinômio, quando possível, significa escrever esse polinômio como uma multiplicação de dois ou mais polinômios.

Feitas essas considerações a respeito de polinômios e fatoração, são abordadas operações envolvendo equações algébricas, em particular, a equação do segundo grau, onde são abordadas: existência de raízes, cálculo de raízes por meio de processos como o de completar quadrados, ou aplicação da fórmula resolutiva, conhecida em sua maioria, por fórmula de *Bháskara*, relação entre coeficientes e raízes.

A abordagem exclusiva de polinômios, suas propriedades e operações, dá-se no 3^{o} ano do Ensino Médio, conforme as habilidades da BNCC [3]:

1. Conhecer as relações entre os coeficientes e as raízes de uma equação algébrica;

2. Saber reduzir a ordem de uma equação a partir do conhecimento de uma raiz.

Na Secretaria da Educação do Estado de São Paulo, segundo o *Material de apoio ao aluno* (veja em [5]), e com base nas habilidades da BNCC [3], o estudo de polinômios é abordado conforme a grade curricular abaixo:

Currículo Oficial - BNCC-SP		**Currículo Paulista - E.M.**
Tema/Conteúdo	**Habilidades**	**Competência Geral**
Números Equações algébricas e números complexos. Equações polinomiais; Números complexos: operações e representação geométrica; Teorema sobre as raízes de uma equação polinomial; Relações de Girard.	Compreender a história das equações, com o deslocamento das atenções das fórmulas para as análises qualitativas. Conhecer as relações entre os coeficientes e as raízes de uma equação algébrica; Saber reduzir a ordem de uma equação a partir do conhecimento de uma raiz; Saber expressar o significado dos números complexos por meio do plano de Argand-Gauss.	Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.

Tabela 5.1: Grade curricular da 3ª série do Ensino Médio

Nestas habilidades são apresentadas definições, propriedades e operações tais como:

- No *Caderno do aluno - SP faz escola* [5], após abordar números complexos e trabalhar resolução de equações algébricas por meio da relação com raízes, entre outros métodos, somente ao final desta abordagem é apresentada a seguinte definição de polinômio:

  > Como se sabe, um polinômio de grau n é uma expressão algébrica do tipo:
  >
  > $$P(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + a_3x^{n-3} + \cdots + a_{n-1}x + a_n = 0$$
  >
  > com $a_0 \neq 0$. Então, uma equação algébrica também pode ser chamada uma equação polinomial, uma vez que ela pode ser escrita na forma $P(x) = 0$, sendo $P(x)$ um polinômio. Dessa forma, se o valor de$P(x)$ para $x = k$, que indicaremos por $P(k)$, for igual a zero, ou seja $P(k) = 0$, então isso significa que k é uma raiz da equação polinomial $P(x) = 0$.

- No livro didático *Matemática - contexto e aplicações* [4], apresenta-se a seguinte definição de polinômios:

  > Chamamos expressão polinomial ou polinômio na variável x toda expressão na forma
  >
  > $$a_nx^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0.$$

Acrescenta-se ainda a seguinte definição: "Toda função definida por $p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ para todo x complexo, é denominado função polinomial de grau n, em que n é um número inteiro positivo ou nulo e a_n é diferente de 0". Feita esta definição, são apresentadas propriedades referentes à igualdade de polinômios, valor numérico, seguindo-se para cálculo de raízes e fatoração. São abordadas propriedades do Teorema Fundamental da Álgebra 3.28, Teorema 2.79, Corolário 2.70. Considerando o anel do complexos, somente no segmento do Ensino Médio os polinômios são abordados por meio de suas propriedades.

Tanto no Ensino Fundamental, quanto no Ensino Médio, há maior foco nas propriedades e operações relacionadas às funções polinomiais e equações algébricas (em geral as de grau no máximo quatro). Ressaltamos que tais equações e funções polinomiais são representadas por polinômios com coeficientes reais ou complexos, o que segundo a Observação 2.22 nos permite considerar tais conceitos aparentes.

5.1 Análise de atividades dos materiais didáticos

Vamos inicialmente analisar e resolver atividades propostas nos livros didáticos e materiais de apoio, tais como [15, 12, 5, 4, 11], referentes ao estudo de polinômios no Ensino Básico.

Exemplo 5.1. Atividade proposta em *A conquista da matemática* [15], página 85, exercício 13: A área de um retângulo é expressa pelo polinômio $x^2 - 9$, em que $x > 3$. Fatorando-o, temos as medidas de seus lados. Se o perímetro do retângulo é 32 cm, qual é a área desse retângulo?

Habilidade BNCC: EF09MA09

Público alvo: Alunos a partir do $9^{\underline{o}}$ ano do Ensino Fundamental

Objetivo: Compreender a fatoração entre polinômios e equações polinomiais relacionadas a área e perímetro de polígonos.

Resposta/Resolução A área de um retângulo de lados $x + 3$ e $x - 3$ é representada pelo polinômio $x^2 - 9$, ou seja,

$$x^2 - 9 = (x - 3) \cdot (x + 3).$$

Esses são polinômios irredutíveis em um corpo, e por ausência de se explicitar o anel de coeficientes, consideremos em $\mathbb{R}$. Observando a forma fatorada, podemos considerar que se trata de um retângulo de lados $x + 3$ e $x - 3$, logo o perímetro é dado pela expressão

$$2(x + 3) + 2(x - 3) = 32 \Leftrightarrow x = 8.$$

Assim, a área dada pela expressão

$$(x - 3) \cdot (x + 3) = 5 \cdot 11 = 55\ cm^2.$$

Proposta pedagógica/intervenção: Para que se chegue à resolução desta atividade é fundamental que o estudante compreenda o que é escrever um polinômio em sua forma fatorada conforme Teorema 2.79 e ainda utilize na resolução propriedades como as do Corolário 2.41 e o Teorema 2.70.

Considerações: Esta atividade, proposta em livro didático do Ensino Fundamental, embora utilize-se das propriedades relacionadas a fatoração de polinômios, também não o aborda de forma explícita, uma vez que, a definição de redutibilidade de polinômio e fatoração de polinômios, são usadas de forma similares. Uma das vantagens de atividades como esta é poder abordar a representação geométrica de um polinômio em sua forma fatorada.

Exemplo 5.2. Atividade proposta em *A Matemática do Ensino Médio* [11]: Ache o maior divisor comum-M.D.C. dos polinômios $p(x) = x^3 - 6x^2 + 5x + 12$ e $q(x) = x^3 - 5x^2 - 2x + 24$.

Habilidade BNCC: (EM13MAT302) Construir modelos empregando as funções polinomiais de 1^o ou 2^o graus, para resolver problemas em contextos diversos, com ou sem apoio de tecnologias digitais. As mesmas habilidades constam na Grade Curricular do EM 5.

Público alvo: Alunos do 3^o ano do Ensino Médio

Objetivo: Aplicar as propriedades dos polinômios relacionadas a divisibilidade, fatoração e M.D.C..

Resposta/Resolução Temos que -1 é raiz de $p(x)$ e daí aplicando o Corolário 2.41, temos que $p(x)$ é divisível por $x+1$. Analogamente verificamos que -2 é raiz de $q(x)$ e portanto o mesmo é divisível por $x+2$. Assim, efetuando estas divisões temos:

$$\begin{array}{rl|l} x^3 - 6x^2 & + 5x + 12 & x+1 \\ \cline{3-3} -x^3 - x^2 & & x^2 - 7x + 12 \\ \cline{1-2} \quad -7x^2 & + 5x & \\ \quad 7x^2 & + 7x & \\ \cline{1-2} & 12x + 12 & \\ & -12x - 12 & \\ \cline{2-2} & 0 & \end{array}.$$

Daí obtemos $x^3 - 6x^2 + 5x + 12 = (x+1)\cdot(x^2 - 7x + 12)$. Podemos facilmente verificar, utilizando a Proposição 4.20 que $x^2 - 7x + 12 = (x-3)\cdot(x-4)$. Daí

$$x^3 - 6x^2 + 5x + 12 = (x+1)\cdot(x-3)\cdot(x-4) \tag{5.1}$$

Agora, dividindo $x^3 - 5x^2 - 2x + 24$ por $x+2$, temos

$$\begin{array}{rl|l} x^3 - 5x^2 & - 2x + 24 & x+2 \\ \cline{3-3} -x^3 - 2x^2 & & x^2 - 7x + 12 \\ \cline{1-2} \quad -7x^2 & - 2x & \\ \quad 7x^2 + 14x & & \\ \cline{1-2} & 12x + 24 & \\ & -12x - 24 & \\ \cline{2-2} & 0 & \end{array}$$

Com isso obtemos $x^3 - 5x^2 - 2x + 24 = (x + 2) \cdot (x^2 - 7x + 12)$. Aplicando a Proposição 4.20 temos:

$$x^3 - 5x^2 - 2x + 24 = (x + 2) \cdot (x - 3) \cdot (x - 4). \tag{5.2}$$

Assim, analisando as formas fatoradas das expressões (5.1) e (5.2) vemos que $(x - 3) \cdot (x - 4) = x^2 - 7x + 12$ é fator comum aos polinômios, logo

$$\text{M.D.C.}\{x^3 - 6x^2 + 5x + 12, x^3 - 5x^2 - 2x + 24\} = x^2 - 7x + 12.$$

Proposta pedagógica/intervenção: Para se efetuar a resolução desta atividade é fundamental que além da abordagem das propriedades de M.D.C entre polinômios, conforme Teorema 2.58 também se tenha abordado as propriedades dos polinômios conforme Corolário 3.3, Corolário 2.41. Um dos pontos a se observar nesta atividade é o fato de se não enfatizar em qual o anel de polinômios a ser considerado (reais ou complexos), embora naturalmente se trabalhe no Ensino Médio com números reais.

Considerações: Embora esta atividade conste em material de aperfeiçoamento destinado aos professores de Ensino Médio, uma vez abordadas corretamente as propriedades dos polinômios referentes a divisibilidade, entre outras, é uma atividade com resolução bem adequada à aplicação aos estudantes.

Exemplo 5.3. Atividade proposta no livro didático *Matemática: Contexto e aplicações* [4]: Dividindo $p(x) = x^3 - 4x^2 + 7x - 3$ por certo polinômio $h(x)$, obtemos quociente $q(x) = x - 1$ e o resto $r(x) = 2x - 1$. Encontre $h(x)$.

Habilidade BNCC: Conforme consta Grade Curricular Ensino Médio 5.

Público alvo: Alunos do 3^{o} ano do Ensino Médio

Objetivo: Divisão euclidiana em polinômios.

Resposta/Resolução O problema nos diz que,

$$x^3 - 4x^2 + 7x - 3 = h(x) \cdot (x - 1) + (2x - 1).$$

Este polinômio deve ser de grau 2, ou seja, $h(x) = ax^2 + bx + c$. Daí temos,

$$\begin{aligned} x^3 - 4x^2 + 7x - 3 &= (ax^2 + bx + c) \cdot (x - 1) + (2x - 1) \\ &= ax^3 + (b - a)x^2 + (c - b + 2)x - c - 1. \end{aligned}$$

Para que tais polinômios sejam iguais, devemos ter:

$$\begin{aligned} ax^3 &= x^3 \quad \Leftrightarrow \quad a = 1 \\ (b - a)x^2 &= -4x^2 \quad \Leftrightarrow \quad b = -3 \\ -c - 1 &= -3 \quad \Leftrightarrow \quad c = 2. \end{aligned}$$

Logo $h(x) = x^2 - 3x + 2$.

Proposta pedagógica/intervenção: Faz-se necessário que o aluno conheça as propriedades relacionadas à divisão entre polinômios conforme Teorema 2.36 e Corolário 2.37, além disso, deve utilizar as propriedades a respeito de grau de um polinômio, Corolário 2.16, para entender como se representa o polinômio a ser encontrado, além das propriedades referentes a igualdade de polinômios, Proposição 2.33.

Considerações: A atividade aborda bastante as propriedades dos polinômios, mas como em quase todas atividades apresentadas no material didático, não se explicita em qual anel de polinômios estão os polinômios, consideramos o conjunto dos números reais.

5.2 Atividades Propostas

Vamos propor algumas atividades relacionadas aos polinômios, funções polinomiais e equações algébricas, passíveis de resolução a alunos do Ensino Médio.

Exemplo 5.4. Consideremos o produto de três números inteiros consecutivos.

1) É possível encontrar três números inteiros e consecutivos cujo produto seja igual a 60?

2) Que expressão algébrica representa o produto de três números consecutivos?

Habilidade BNCC: Conforme consta Grade Curricular Ensino Médio 5.

Público alvo: Alunos do 3º ano do Ensino Médio

Objetivo: Resolver problemas aplicando as propriedades dos polinômios, tendo como particularidade o anel dos coeficientes.

Resolução Considerando o problema dado,

1) Vamos encontrar números inteiros tais que:

$$\begin{aligned}(x-1)\cdot x\cdot(x+1) &= 60\\ x\cdot(x^2-1) &= 60\\ x^3-x-60 &= 0.\end{aligned}$$

Queremos encontrar a raiz inteira (caso exista), desta equação do 3º grau. Para isso, consideremos o polinômio de coeficientes inteiros $p(x) = x^3 - x - 60$. Pela Proposição 3.2 as possíveis raízes deste polinômio são os divisores de 60. Por inspeção, verificamos que 4 é raiz de $p(x)$. Logo, os números procurados são 3, 4 e 5.

2) Pelo item anterior, a expressão algébrica que representa o produto c, de três números inteiros consecutivos é dada por:

$$\begin{aligned}(x-1)\cdot x\cdot(x+1) &= c\\ x\cdot(x^2-1) &= 60\\ x^3-x-c &= 0.\end{aligned}$$

Observemos que de acordo com o Lema 4.3, c é o produto das raízes de $p(x)$. Devemos ressaltar que estamos tratando de um polinômio com coeficientes inteiros, logo nem sempre garantimos a existência de tais raízes.

Considerações: Alguns apontamentos podem ser feitos durante a resolução desta atividade, entre eles, além de se abordar a possível não existência de solução, uma vez que especificamos o conjunto dos números e consequentemente as propriedades inerentes ao polinômio que expressa a situação, também podemos partir de uma situação inversa, ou seja, a partir da expressão de $p(x) = x^3 - x - c$, buscar entender que situação problema a expressão descreve, fazendo uso das propriedades operatórias dos polinômios. Um fator a se observar nesta atividade é que, ao se considerar o produto de três números inteiros consecutivos, tais números podem ser expressos como x, $x + 1$ e $x + 2$, e então a expressão obtida para se encontrar o produto $c = 60$ será representada por:

$$\begin{aligned}(x) \cdot (x+1) \cdot (x+2) &= 60\\ (x^2 + x) \cdot (x+2) &= 60\\ x^3 + 2x^2 + x^2 + 2x &= 0\\ x^3 + 3x^2 + 2x &= 60.\end{aligned}$$

Exemplo 5.5. Consideremos o cubo de bases $ABCD$ e $EFGH$, de aresta x. Sobre as faces deste, efetuamos três cortes transversais de medidas a, b e c, sendo o primeiro corte paralelo à face lateral $BCGF$, no ponto Y da aresta $\overline{DC}$, tal que $\overline{YC} = a$, o segundo corte, paralelo à face da base $EFGH$ no ponto K da aresta $\overline{DH}$, tal que $\overline{KH} = b$, e o terceiro corte, paralelo à face frontal $ABFE$, no ponto U da aresta $\overline{AD}$, tal que $\overline{AU} = c$. Com isso obtemos um paralelepípedo de bases $DULY$ e $KONJ$. Que expressão algébrica relaciona o volume do cubo inicial e o volume do paralelepípedo obtido?

Habilidade BNCC: Conforme consta Grade Curricular Ensino Médio 5.

Público alvo: Alunos do 3º ano do Ensino Médio

Objetivo: Resolver problemas aplicando as propriedades dos polinômios, tendo como particularidade o anel dos coeficientes.

Solução. Vamos representar geometricamente e algebricamente os processos relacionados acima.
O problema nos diz que a partir de um cubo de aresta x e volume $v(x) = x^3$, como na figura abaixo, vamos obter um paralelepípedo de arestas $x - a, x - b$ e $x - c$.

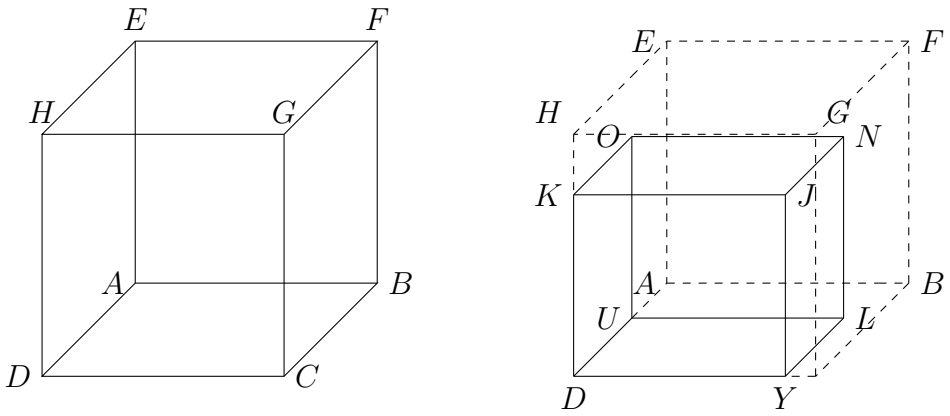

Figura 5.1: Cubo de dimensão x e volume $v(x) = x^3$.

Para isso, efetuamos os três cortes transversais conforme a figura,

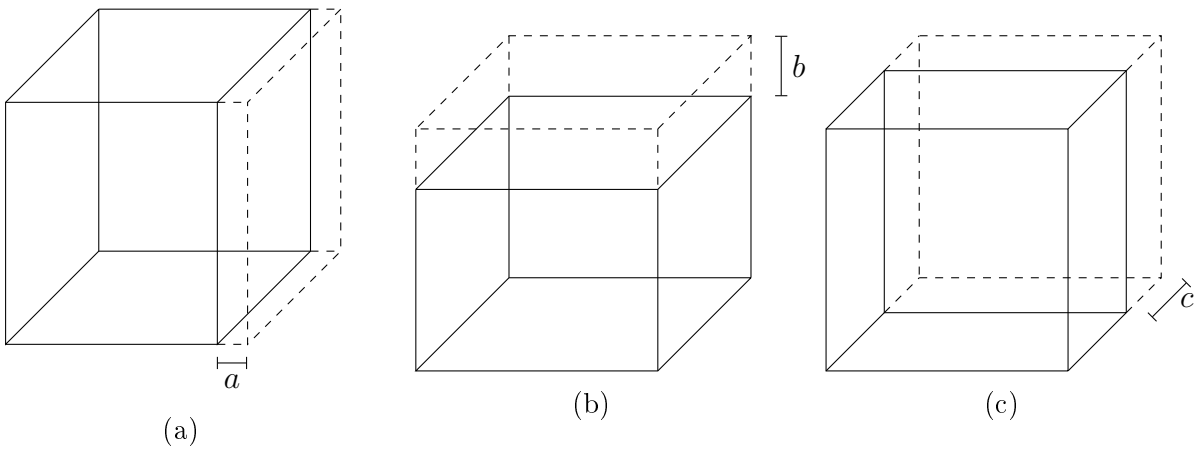

Figura 5.2: Cortes transversais de medidas a, b e c.

Com isso obtemos o paralelepípedo abaixo de arestas $x-a$, $x-b$ e $x-c$, conforme a figura abaixo.

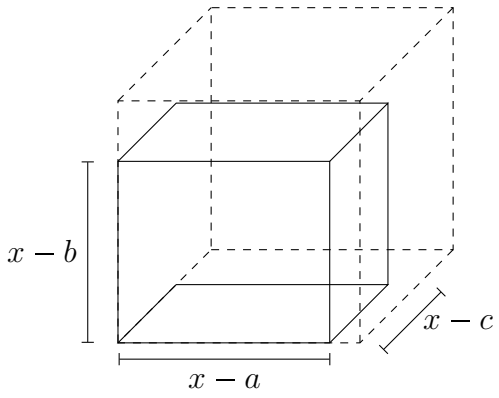

Figura 5.3: Paralelepípedo

Para se chegar ao paralelepípedo da figura 5.3, efetuando os cortes transversais citados, com os seguintes procedimentos:

1. Efetuamos um corte transversal de medida a paralelo a face lateral $BCGF$, como na figura.

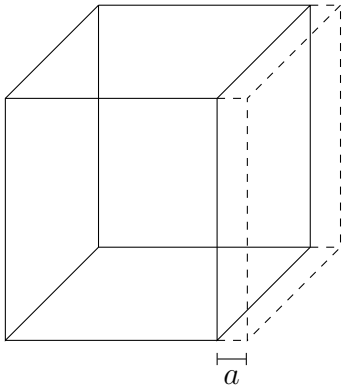

Figura 5.4: Corte transversal 1.

Com isso obtemos um novo paralelepípedo de volume $v(x) = (x - a) \cdot x^2$.

Podemos representar este procedimento através da expressão algébrica,

$$v(x) = x^3 - ax^2.$$

2. Efetuamos um corte transversal de medida b paralelo à face da base $EFGH$, conforme figura abaixo.

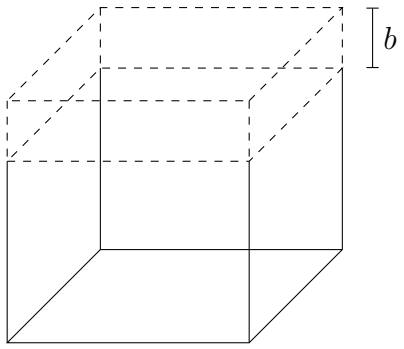

Figura 5.5: Corte transversal 2.

Observemos que para efetuar este corte, estaria 'faltando' o paralelepípedo de $v_1(x) = abx$. Portanto, devemos 'devolvê-lo' e então efetuamos o corte.

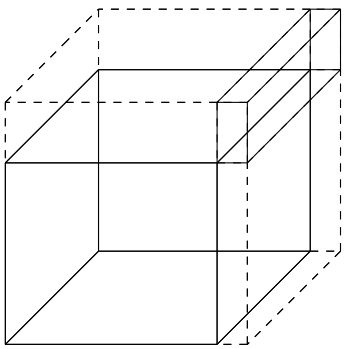

Figura 5.6: Paralelepípedo acrescido e corte.

Estes procedimentos podem ser descritos pela expressão algébrica

$$\begin{aligned} v(x) &= x^3 - ax^2 + abx - bx^2 \\ &= x^3 - ax^2 - bx^2 + abx \\ &= x^3 - (a+b)x^2 + abx. \end{aligned}$$

3. Efetuamos um corte transversal de medida c, paralelo a face frontal $ABFE$, como na figura.

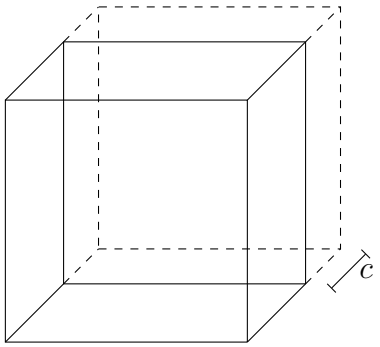

Figura 5.7: Corte transversal 3.

Observemos que novamente, para se efetuar este corte, devemos acrescentar os paralelepípedos $v_2(x) = bcx$ e $v_3 = acx$. No entanto, com isso, estaríamos acrescentado duas vezes o paralelepípedo $v_4(x) = abc$.

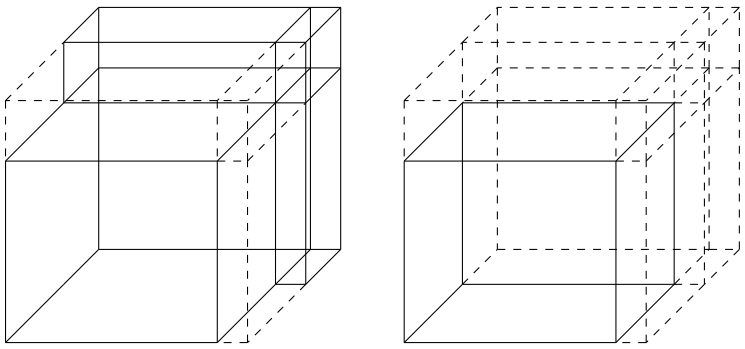

Figura 5.8: Paralelepípedo resultante.

Estes procedimentos podem ser descritos pela expressão algébrica

$$\begin{aligned} v(x) &= x^3 - (a+b)x^2 + abx + acx + bcx + -abc - cx^2 \\ &= x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc. \end{aligned}$$

Considerações: Verificamos nesta abordagem a relação entre o polinômio em sua forma fatorada e a relação com as raízes do mesmo, aprimorando os conhecimentos a respeito de fatoração algébrica e seus significados. Ressaltamos também

que neste exemplo, podem ser aplicadas atividades práticas de 'construção' do paralelepípedo utilizando sólidos geométricos, como os representados durante a resolução da atividade.

Apresentamos aqui algumas sugestões de atividades a serem propostas aos alunos, para que se analise e aplique propriedades referentes aos polinômios e equações algébricas.

Exemplo 5.6. Consideremos o exemplo da página 172 de *A matemática no Ensino Médio*, (ver em [11]).

Cortando-e quadrados de lado 4 cm nos cantos de uma folha de papelão em forma de um quadrado de18 cm de lado, e dobrando-a, formamos uma caixa sem tampa cujo volume é igual a 400 cm^3. Existe algum outro valor do lado do quadrado a ser recortado em cada canto para o qual o volume da caixa resultante também seja igual a 400 cm^3? Que expressão algébrica relaciona a medida x a ser cortada, em relação a medida a do lado, a fim de se obter um volume c?

Exemplo 5.7. Exercício 6, página 193 de [11]: Se um polinômio p é divisível pelos polinômios p_1 e p_2, então p é divisível por p_1p_2. Certo ou errado?

Exemplo 5.8. Analisando o volume dos sólidos abaixo, responda:

1) Para qual valor x temos que o volume do Sólido 1 é igual ao Sólido 2?

2) É sempre possível que dois sólidos de dimensões $(x-a,\ x-b,\ x-c)$ e $(x-d,\ x-e,\ x-f)$, respectivamente, tenham mesmo volume?

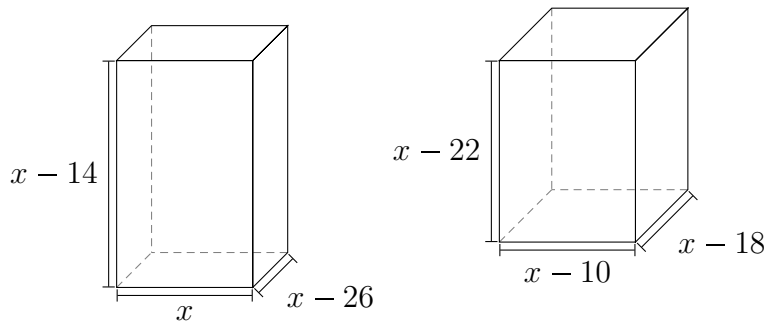

Figura 5.9: Sólido 1 (esquerda), Sólido 2 (direita)

6 Considerações Finais

O objetivo deste trabalho foi apresentar o estudo das propriedades e operações entre polinômios em uma indeterminada. Embora no Capítulo 1 abordarmos o conceito de anéis de modo geral e no Capítulo 2 abordarmos polinômios de maneira geral, a ênfase consiste nos anéis de polinômios sobre os inteiros, racionais, reais e complexos.

Em relação as propriedades aqui abordadas, considerando o ensino de polinômios na Educação Básica, observa-se que não há um tratamento específico, quanto as estruturas algébricas de tais, uma vez que esta abordagem ocorre mais especificamente em relação a funções polinomiais.

Nas atividades de aplicação e sugestão de aplicação buscamos apresentar atividades que buscam a compreensão das propriedades e operações de polinômios relacionados ao anel de seus coeficientes, além de atividades que podem contextualizar as operações algébricas.

Esperamos que este trabalho possa contribuir ao melhor entendimento das operações algébricas relacionadas a polinômios e em especial, a sutil diferença entre o conceito formal de polinômios e as funções polinomiais, que muitas vezes são tratadas como mesmo elemento.

Referências

[1] A.Hefez. *Curso de Álgebra*, volume 1. Instituto de Matemática Pura e Aplicada - IMPA, Rio de Janeiro, 4 edition, 2012.

[2] C.B. Boyer. *A History of Mathematics - História da Matemática*. Editora Edgard Blucher Ltda, São Paulo, 2 edition, 2001.

[3] Ministério da Educação. *BNCC - Base Nacional Comum Curricular*. MEC - Ministério da Educação, Brasília, 2018.

[4] L.R. Dante. *Matemática - Contexto e aplicações*. Ática, São Paulo, 3 edition, 2016.

[5] Secretaria de Estado da Educação. *Caderno do aluno - SP faz escola*. Governo do Estado de São Paulo, São Paulo, 2021.

[6] Y.Lequain e A.Garcia. *Elementos de álgebra*. Instituto de Matemática Pura e Aplicada - IMPA, Rio de Janeiro, 6 edition, 2018.

[7] H.H.Domingues e G. Iezzi. *Álgebra Moderna*. Atual Editora, São Paulo, 3 edition, 1982.

[8] H.H.Domingues e G. Iezzi. *Álgebra Moderna*. Saraiva, São Paulo, 5 edition, 2018.

[9] A. J. Ribeiro e H. N. Cury. *Álgebra para formação do professor: explorando os conceitos de equação e função*. Autêntica Editora, Belo Horizonte, 1 edition, 2015.

[10] S.Lipschutz e M.L.Lipson. *Álgebra Linear*. Bookman, Porto Alegre, 3 edition, 2004.

[11] E.L.Lima et al. *A matemática no Ensino Médio*. Sociedade Brasileira de Matemática - SBM, Rio de Janeiro, 7 edition, 2016.

[12] M.R. G. Gay and W.R. Silva. *Araribа mais - Matemática*. Editora Moderna, São Paulo, 1 edition, 2018.

[13] A. Gonçalves. *Introdução à álgebra*. Instituto de Matemática Pura e Aplicada - IMPA., Rio de Janeiro, 6 edition, 2017.

[14] I.N. Herstein. *Topics in Algebra*. John Wiley and Sons, New York, 1 edition, 1975.

[15] J.R. Giovanni Junior and B. Castrucci. *A conquista da matemática*. FTD, São Paulo, 4 edition, 2018.

[16] L. H. J. Monteiro. *Elementos de Álgebra*. Ao Livro Técnico S.A. - IMPA, Rio de Janeiro, 1 edition, 1969.

[17] L.H. J. Monteiro. *Elementos de álgebra*. LTC - Livros Técnicos e Científicos, Rio de Janeiro, 2 edition, 1978.

[18] S.Lang. *Algebra*, volume 1. Addison-Wesley Publishing Company, New York, 1 edition, 1965.