Universidade Federal da Bahia - UFBA
Sociedade Brasileira de Matematica - SBM
Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Dissertação de Mestrado

Estudo de Anéis de Polinômios aos Elos de Níveis de Ensino

Ângelo Márcio Santana Guimarães

Cruz das Almas - Bahia

Julho de 2016

Estudo de Anéis de Polinômios aos Elos de Níveis de Ensino

Ângelo Márcio Santana Guimarães

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFRB como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Profª. Ms.c Jaqueline Alexsandra de Souza Azevedo

Cruz das Almas - Bahia

Julho de 2016

FICHA CATALOGRÁFICA

G963e Guimarães, Ângelo Márcio Santana.
Estudo de anéis de polinômios aos elos de níveis de ensino / Jaqueline Alexsandra de Souza Azevedo. _ Cruz das Almas, BA, 2016.
76f.; il.

Orientadora: Jaqueline Alexsandra de Souza Azevedo.
Dissertação (mestrado) - Universidade Federal do Recôncavo da Bahia, Centro de Ciências Exatas e Tecnlógicas.

1.Matemática – Anéis (Álgebra). 2.Matemática-Polinômios. 3.Estudo e ensino – Avaliação. I.Universidade Federal do Recôncavo da Bahia, Centro de Ciências Exatas e Tecnológicas. II.Título.

CDD: 512.714

Ficha elaborada pela Biblioteca Universitária de Cruz das Almas - UFRB.

Estudo de Anéis de Polinômios aos Elos de Níveis de Ensino

Ângelo Márcio Santana Guimarães

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFRB como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 28 de Julho de 2016.

Banca Examinadora:

Prof[a] Msc Jaqueline Alexsandra de Souza Azevedo (Orientadora)
UFRB

Prof. Msc Adson Mota Rocha
UFRB

Prof. Dr. Luiz Alberto de Oliveira Silva
UFRB

Dedicatória

À minha família e a todos que contribuíram direta ou indiretamente e que fizeram votos para que esse projeto fosse concluído com sucesso.

Agradecimentos

Agradeço a Deus em primeiro lugar, pela força e coragem durante toda esta longa caminhada.

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

Agradeço também a todos os professores (Juarez, Adson, Erikson, Eleazar, Mariana, Gilberto) que me acompanharam, instruindo e orientando - nos durante esta jornada. E em especial à minha orientadora Profª. Msc. Jaqueline Azevedo, que foi muito importante para a realização deste trabalho.

Aos colegas que iniciaram, acompanharam e também àqueles que por motivos vários tiveram que nos deixar, o meu muito obrigado. Aqui, não posso deixar de lembrar da companhia de deslocamento, semanalmente, dos colegas Ueric e Ronaldo Costa que sem eles as idas e voltas pra casa teria sido entediante.

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

Valeu a pena toda distância, todo sofrimento, todas as renúncias.

"A álgebra é generosa: frequentemente ela
dá mais do que se lhe pediu".
Jean Le Rond d'Alembert

Resumo

Neste trabalho abordaremos o estudo de Anel de Polinômio promovendo uma conexão desta estrutura algébrica entre o estudo da Álgebra no Ensino Superior e na Educação Básica, garantindo uma linguagem acessível, tendo como público alvo, estudantes dos cursos de licenciatura em Matemática e também professores de Matemática que atuam no Ensino Básico. Para tanto, enunciaremos resultados matemáticos, evitando, na medida do possível, o uso exacerbado de demonstrações de teoremas e proposições, pretendemos assim, alcançar essa linguagem simples e acessível a todos os interessados.

Palavras - chave: Álgebra, Anéis de polinômios, Equações Algébricas.

Abstract

In this paper we discuss the study polynomial ring promoting a connection this algebraic structure of the algebra of study in higher education and basic education, ensuring an accessible language, targeting the public, students of bachelor degree in Mathematics and also mathematics teachers operating in basic education. Therefore, will state mathematical results, avoiding as far as possible, the overuse of theorems statements and propositions, we intend to thus achieve this simple language and accessible to all interested parties.

Keywords: Algebra, polynomial Rings, Algebraic Equations.

Sumário

Introdução **1**

1 Anéis e Corpos **3**

1.1 Definições e propriedades de Anéis 3

1.2 Corpos 5

2 Anéis de Polinômios **9**

2.1 Sequências Numéricas 9

2.1.1 Operações com Sequências 10

2.2 Polinômios numa indeterminada x 14

2.2.1 Grau de um Polinômio 15

2.2.2 Adição de Polinômios 16

2.2.3 Multiplicação de polinômios 17

2.2.4 Divisão de Polinômios 25

2.2.5 Métodos para Divisão de Polinômios 29

3 Equações Polinomiais ou Algébricas **37**

3.1 Introdução 37

3.2 Definições 37

3.3 Raízes 38

3.3.1 Teorema Fundamental da Álgebra (TFA) 39

3.3.2 Raízes Complexas 42

3.3.3 Raízes Racionais 44

3.4 Raízes Múltiplas 46

3.5 Transformadas e Equações Recíprocas 51
3.5.1 Equação Recíproca 55
3.5.2 Classificação 59
3.5.3 Propriedades 60
3.5.4 Equações Recíprocas de 1ª espécie e grau par 61

Considerações Finais **64**

Referências Bibliográficas **66**

Introdução

Estudar Matemática tem sido para a grande maioria dos alunos da Educação Básica e também do Ensino Superior um verdadeiro martírio. Até entre a comunidade docente há um consenso no que diz respeito à grande dificuldade encontrada pelos mesmos no momento em que precisam inserir os conteúdos de Matemática relacionados à Álgebra. Quando se trata de Nível Superior ou cursos de graduação que exigem tal disciplina no currículo, essa dificuldade é ainda maior.

Entretanto, esses obstáculos por parte dos alunos teriam explicação na pouca ou má formação no Nível Básico, onde ali se apresentou suas primeiras dificuldades e o professor não conseguiu saná-las, ou no nível superior (graduação) onde aqui o curso tem, normalmente, um perfil voltado ao formalismo excessivo, preenchido por teoremas e proposições de difícil compreensão, sem falar em suas extensas demonstrações de complexidade superior. Haveria alguma conexão de conceitos algébricos entre esses dois níveis ou ciclo de educação (básico e superior)?

Segundo JOSIANE CARLA BAIOCCO, 2010 [1]

> "Deveria ter-se uma conexão entre conteúdo específico e conteúdos pedagógicos. Assim os conteúdos algébricos, que de uma forma ou de outra o professor se depara no seu trabalho na Educação Básica, são vistos de forma isolada e aparecem em muitas das disciplinas no curso de Matemática. É justamente nestes tópicos algébricos que se verifica um distanciamento maior entre a formação específica e a formação pedagógica."

Fundamentando-se nesta necessidade de entender quais relações se estabelecem entre a Álgebra aprendida no Curso de Licenciatura em Matemática e a Álgebra ensinada no Ensino Fundamental e Médio, que este trabalho está sendo realizado. Tendo por objetivo desenvolver um documento que forneça detalhadamente ao leitor interessado informações sobre a construção de conceitos algébricos direcionados ao estudo de polinômios construídos na Educação Básica em conexão aos conceitos algébricos vistos no Ensino Superior.

Nessa perspectiva, é imperioso fazer tal análise com o objetivo de preparar um material que possa ser útil para a comunidade estudantil que tem alguma dificuldade na área Álgebra, acadêmica ou não, expondo assim, os conceitos de forma simples sem perder a beleza e elegância do formalismo e do rigor que tal área do conhecimento exige.

Portanto, na criação desse trabalho, procuramos tratar as informações obedecendo as técnicas apropriadas como a coerência entre os tópicos, buscando mencionar os principais conceitos embasados em exemplos claros, sem perder de vista o rigor da Álgebra.

No primeiro capítulo deste trabalho, recorreremos a conceitos de Anéis e Corpos, priorizando a definição e as principais proposições que sejam importantes para o entendimento dos capítulos seguintes.

No segundo capítulo, abordaremos conceitos de Anéis de Polinômios, estabelecendo a construção de um polinômio através de sequências numéricas para, a partir daí, trabalharmos com polinômios do mesmo modo que visto no segundo grau, só que agora preocupados com a estrutura de Anel. Apresentaremos um dispositivo prático para multiplicações polinomiais e justificaremos os resultados do conteúdo polinômios que foram apenas apresentados aos alunos no Nível Médio.

No terceiro capítulo, consideraremos todas as propriedades vistas sobre Anéis de Polinômios e, a partir daí, faremos uma abordagem de Transformadas e Equações Recíprocas segundo a ótica, principalmente, de Gelson Iezzi, 2005 [5], a fim de construir método de obtenção de raízes neste tipo de equação sem recorrer a dispositivos exaustivos.

Por fim, trazemos nossas considerações finais e apresentaremos as obras consultadas que sustentam o desenvolvimento deste trabalho.

Capítulo 1

Anéis e Corpos

Neste primeiro capítulo, temos como objetivo estabelecer as notações, os conceitos e os resultados básicos necessários que serão utilizados nos demais capítulos desse trabalho. Vamos inicialmente, falar sobre duas estruturas algébricas fundamentas: Anéis e Corpos.

Contudo, não abordaremos o estudo dessas estruturas de forma aprofundada, uma vez que nesse trabalho precisaremos, apenas, de conceitos básicos de Anéis e Corpos.

1.1 Definições e propriedades de Anéis

Enunciaremos aqui, as principais definições e propriedades de Anéis que julgamos importante para um melhor entendimento da proposta do trabalho.

Definição 1.1.1.

Um Anel A é um conjunto não vazio munido de duas operações de adição $(+)$ *e multiplicação* $(\cdot)$, *fechadas no conjunto A, definidas por* $(x, y) \to x + y$ *e* $(x, y) \to x \cdot y$, *respectivamente, satisfazendo as seguintes condições:*

A_1 *(Comutatividade) Para todo x e $y \in A$, temos $x + y = y + x$.*

A_2 *(Associatividade) Para todo x e $y \in A$, temos $(x + y) + z = x + (y + z)$.*

A_3 *(Existência de elemento neutro da adição) Existe* $\mathrm{e} \in A$, *tal que* $x + \mathrm{e} = \mathrm{e} + x = x$ *para todo $x \in A$. Notação:* $\mathrm{e} = 0$. *Este é chamado elemento neutro da adição .*

A_4 *(Existência de elemento simétrico) Para todo elemento $x \in A$, existe um elemento y em A, tal que $x + y = y + x = 0$. Notação: $y = -x$. Este é chamado de simétrico* *de* x.

M_1 *(Associatividade) Para todo* x, y, $z \in A$, *temos* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

M_2 *(Distributividade) Para todo* $x, y, z \in A$, *temos* $x \cdot (y+z) = x \cdot y + x \cdot z$ *e* $(y+z) \cdot x = y \cdot x + z \cdot x$.

Exemplo 1.1.1.

O conjunto dos Números Naturais $\mathbb{N}$ *não representa uma estrutura de Anel por não conferir a propriedade* A_4. *Por outro lado, os conjuntos numéricos* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, *e* $\mathbb{C}$ *(Inteiros, Racionais, Reais e Complexos respectivamente), atendem todas as propriedades de Anéis.*

Exemplo 1.1.2.

O conjunto das matrizes representadas por $M_{n\times n}(\mathbb{R})$ *tem estrutura de Anel, com operação de soma e multiplicação de matrizes.*

Exemplo 1.1.3.

O conjunto dos polinômios com coeficientes em um Anel A, que definiremos no capítulo seguinte, também tem estrutura de Anel com operação de Adição e Multiplicação usual.

Observações.

1. *Utilizaremos a notação* $(A, +, \cdot)$ *para denotar um Anel* A *munido das operações* $(+)$ *e* $(\cdot)$.

2. *Observe que a multiplicação não necessita ser comutativa. Quando a multiplicação for comutativa, diremos que* $(A, +, \cdot)$ *é um Anel Comutativo. A exemplo, o conjunto* $\mathbb{C}$ *é um Anel Comutativo. De fato, dados* $\mathbf{z} = a + bi$ *e* $\mathbf{w} = c + di$, *tem-se:* $\mathbf{z} \cdot \mathbf{w} = (a+bi)\cdot(c+di) = ac+adi+bic+bidi = ca+dia+cbi+dibi = (c+di)\cdot a+(c+di)\cdot bi = (c+di) \cdot (a+bi) = \mathbf{w} \cdot \mathbf{z}$.

3. *Um Anel não necessita ter elemento neutro da multiplicação (isto é, um elemento* y *tal que* $xy = yx = x$ *para todo* $x \in A$*). Quando um Anel* $(A, +, \cdot)$ *possui o elemento neutro da multiplicação dizemos que* $(A, +, \cdot)$ *é um Anel com unidade. Ao elemento* y, *chamado de Unidade do Anel, denotaremos por* 1. *A exemplo, o*

conjunto $\mathbb{C}$ é um Anel com unidade. De fato, tomemos $1 = 1 + 0i \in \mathbb{C}$. Logo, $\mathbf{1} \cdot \mathbf{z} = (1 + 0i) \cdot (a + bi) = 1a - 0b + (1b + 0a)i = 1a + 1bi = a + bi = \mathbf{z}$

4. *Os elementos não nulos de um Anel não necessitam ter inversos multiplicativos (isto é, y é inverso multiplicativo de x se, e somente se, $xy = yx = 1$). Os elementos de um Anel $(A, +, \cdot)$ que possuem inverso multiplicativo são chamados de invertíveis de $(A, +, \cdot)$. Denotaremos x^{-1} ao inverso multiplicativo do elemento x.*

1.2 Corpos

É importante para o prosseguimento desse estudo considerarmos uma estrutura algébrica muito importante chamada de Corpo.

Dentre os conjuntos numéricos, aqui estudados, veremos que nem todos possuem características que os classificam como tal estrutura.

Definição 1.2.1.

Um anel comutativo com unidade é chamado de Corpo se todo elemento não nulo é invertível.

Exemplo 1.2.1.

O Conjunto dos Inteiros $\mathbb{Z}$ não atende a estrutura de Corpo, pois com exceção do -1 e 1, nenhum outro elemento possui inverso multiplicativo.

Exemplo 1.2.2.

É fácil ver que o conjuntos $\mathbb{Q}$ e $\mathbb{R}$ possuem todas as propriedades que os classificam como uma estrutura de Corpos. Um outro conjunto importante, que atende a definição de Corpo é o Conjunto dos Números Complexos $\mathbb{C} = \{a + bi \mid a,\ b \in \mathbb{R}\}$.

De fato, $\forall\ z \in \mathbb{C}$ e $z \neq 0$, $\exists\ z^{-1} \in \mathbb{C}$, tal que $z \cdot z^{-1} = 1$. Assim, z^{-1} é o inverso multiplicativo de z.

Para tanto, definimos o conjugado de z como sendo $\overline{z} = a - bi$. Além disso, $z \cdot \overline{z} = a^2 + b^2$. Vamos mostrar que $z^{-1} \in \mathbb{C}$. Portanto:

$$z^{-1} = \frac{1}{z} = \frac{1}{z} \cdot \frac{\overline{z}}{\overline{z}} = \frac{\overline{z}}{a^2 + b^2} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{bi}{a^2 + b^2}.$$

Notemos que $\dfrac{a}{a^2 + b^2} \in \mathbb{R}$ e $\dfrac{b}{a^2 + b^2} \in \mathbb{R}$. Logo $z^{-1} \in \mathbb{C}$ e $z \cdot z^{-1} = 1$.

Definição 1.2.2.

Um Anel comutativo com unidade é chamado de Domínio de Integridade ou apenas Domínio se vale o seguinte:

$$\forall\ a,\ b \in A,\ se\ a \neq 0\ e\ b \neq 0\ então\ a \cdot b \neq 0.\ Ou,$$
$$\forall\ a,\ b \in A,\ se\ a \cdot b = 0\ então\ a = 0\ ou\ b = 0.$$

Definição 1.2.3. *Um elemento $a \in A$, diferente de zero, diz-se* ***divisor de zero*** *caso exista $b \in A$, diferente de zero, tal que $a \cdot b = 0$.*

Proposição 1.2.1. ***(Lei do cancelamento da multiplicação)***

Sejam $a, b, c \in A$ e A um Domínio de Integridade com $a \neq 0$. Se $ab = ac$, então $b = c$.

Demonstração.

Mostremos através das propriedades de Anéis e da definição de Domínio:

$$\begin{array}{rcll}
ab & = & ac & \\
ab - ac & = & ac - ac & (A_4) \\
ab - ac & = & 0 & (A_3) \\
a(b-c) & = & 0 & (M_2) \\
b - c & = & 0 & (Def.1.2.2) \\
b - c + c & = & 0 + c & (A_4) \\
b + 0 & = & 0 + c & (A_3) \\
b & = & c &
\end{array}$$

□

Sabemos que o Conjunto dos Números Inteiros $\mathbb{Z}$ é comutativo e não possui divisores de zero e atende as propriedades A_1, A_2, A_3, A_4, M_1, M_2 de Anéis. Desse modo, o conjunto dos números inteiros é um Domínio de Integridade.

Além disso, temos que os conjuntos $\mathbb{Q}$ e $\mathbb{R}$ são exemplos claros de Domínios de Integridade, uma vez que estes também possuem estrutura de Anéis e não possuem divisores de zero.

Um fato interessante se apresenta quando o professor de nível básico solicita ao aluno que extraia as raízes reais da equação $\alpha : (x-2)(x-3) = 0$. Nesse caso, como estamos trabalhando com o conjunto dos números reais, e este é exemplo de Domínio de Integridade, garantimos uma resolução fácil da equação α acima. Ou seja, se $(x-2)\cdot(x-3) = 0$, então $x - 2 = 0 \Rightarrow x = 2$ ou $x - 3 = 0 \Rightarrow x = 3$.

Podemos mostrar ainda, que essa propriedade não se aplica, por exemplo, ao conjunto das matrizes, que não é um Domínio de Integridade, já que possui divisores de zero. Vejamos,

Sejam as matrizes A e B, com

$$A = \begin{bmatrix} 1 & -1 \\ 2 & -2 \end{bmatrix} e\ B = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

Notemos que $A \cdot B = 0$, sem que $A = 0$ ou $B = 0$.

Nesse contexto, é razoável que o professor munido desse conhecimento, use técnicas e procedimentos adequados ao aluno da educação básico para se fazer compreendido, sem perder tanto o formalismo esperado por tal conteúdo ou conceito de Domínio de Integridade.

Observemos a resolução da equação algébrica no Anel dos inteiros,

$$\begin{aligned}
3(x-2) &= x+4 \\
3x-6 &= x+4 \to \text{(propriedade distributiva)} \\
-x+3x-6 &= -x+x+4 \to \text{(inverso aditivo)} \\
2x-6 &= 0+4 \to \text{(elemento neutro aditivo)} \\
2x-6+6 &= 4+6 \to \text{(inverso aditivo)} \\
2x+0 &= 10 \to \text{(elemento neutro aditivo)} \\
2x &= 2\cdot 5 \to \text{(lei do cancelamento)} \\
x &= 5
\end{aligned}$$

Vemos que as propriedades aqui aplicadas, à luz da teoria de Anéis, nos direciona ao princípio aditivo e multiplicativo usual no Ensino Fundamental e Médio, justificando cada passagem.

Proposição 1.2.2.

Todo Corpo K é um Domínio de Integridade.

Demonstração. Com efeito, seja a um elemento não nulo no corpo K e seja a^{-1} seu inverso.

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

□

Por outro lado, nem todo Domínio de Integridade é um Corpo. Por exemplo, o Anel do Inteiros $\mathbb{Z}$ não possui divisores de zero, sendo assim um Domínio de Integridade mas não é um Corpo, já que seus elementos $z \in \mathbb{Z}$, com exceção do -1 e 1, não possui inverso multiplicativo.

Capítulo 2

Anéis de Polinômios

2.1 Sequências Numéricas

Iniciaremos o estudo de Anéis de Polinômios introduzindo um breve conceito de sequências, uma vez que estaremos usando essa ideia para, a partir daí, definirmos polinômios.

Definição 2.1.1.

Seja $\mathbb{N}$ *o Conjunto dos Números Naturais e* $(A, +, \cdot)$ *um Anel. Uma sequência sobre um Anel* $(A, +, \cdot)$ *é uma função:*

$$f : \mathbb{N} \mapsto A$$

$$n \mapsto f(n) = x_n$$

Nesse sentido, sequências aqui são funções que associam um elemento $n \in \mathbb{N}$ a $x_n \in A$. Assim todas as nossas sequências citadas apresentam ou são constituídas por elementos do Anel $(A, +, \cdot)$. Então sendo a_i a imagem por f do elemento $i \in \mathbb{N}$, a sequência f é definida por:

$$f = (a_0, a_1, a_2, ..., a_i, ...)$$

Dizemos que $a_0, a_1, a_2, ..., a_i, ... \in A$, são os termos da sequência.

Exemplo 2.1.1.

Seja a função definida por

$$f : \mathbb{N} \mapsto \mathbb{Z}$$

$$n \mapsto f(n) = 2n + 1.$$

Então, $(a_n) = (1, 3, 5, 7, ...)$. *(Sequência dos números ímpares positivos)*

Definição 2.1.2.

Dadas duas sequências (a_n), $(b_n) \in A$, *dizemos que a sequência* (a_n) *é igual à sequência* (b_n), *e escrevemos* $(a_n) = (b_n)$, *se, e somente se,* $a_i = b_i$ *para todo* $i \in \mathbb{N}$. *Ou seja, se os termos correspondentes de cada sequência forem iguais.*

2.1.1 Operações com Sequências

Adição

Definição 2.1.3.

Dadas (a_n) *e* (b_n) *sequências sobre o Anel* $(A, +, \cdot)$, *definimos a soma de* (a_n) *com* (b_n), *como sendo a sequência denotada por* $(c_n) = (a_n) + (b_n)$ *e determinada por* $c_i = a_i + b_i$, *para todo* $i \in \mathbb{N}$.

Sejam $(A, +, \cdot)$ um Anel, (a_n) uma sequência com $n \in \mathbb{N}$ e (b_m) outra sequência com $m \in \mathbb{N}$. Considere, sem perdas de generalidade, que $m \leq n$:

$$(a_n) = (a_0, a_1, a_2, ..., a_n) \text{ e } (b_m) = (b_0, b_1, b_2, ..., b_m).$$

Desse modo, a adição dessas sequências é dada por:

$$(a_n) + (b_m) = (a_0 + b_0,\ a_1 + b_1,\ a_2 + b_2, ..., a_m + b_m, ..., a_n + b_n).$$

Devemos perceber que $b_i = 0, \forall\ i > m$.

Multiplicação

Definição 2.1.4.

Dadas (a_n) *e* (b_n) *duas sequências sobre o Anel* $(A, +, \cdot)$*, definimos o produto de* (a_n) *com* (b_n)*, como sendo a sequência denotada por* $(c_n) = (a_n) \cdot (b_n)$ *e determinada por:*

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

para todo $k \in \mathbb{N}$.

Sejam duas sequencias (a_n) e (b_m). O produto de (a_n) por (b_m) gera uma nova sequencia (c_k), com $k = m + n$ e $m \leq n$, definida por:

$$(c_k) = ((c_0),\ (c_1),\ (c_2),\ (c_3), ..., (c_m), ..., (c_n), ..., (c_k)),\ k = m + n,$$

onde,

$$\begin{cases} c_0 = a_0 b_0 \\ c_1 = a_1 b_0 + a_0 b_1 \\ c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 \\ c_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 \\ \vdots \\ c_m = \displaystyle\sum_{i=0}^{m} a_i b_{m-i} \\ \vdots \\ c_n = \displaystyle\sum_{i=0}^{n} a_i b_{n-i},\ b_i = 0,\ se\ i > m \\ \vdots \\ c_k = \displaystyle\sum_{i=0}^{k} a_i b_{k-i}, \begin{cases} a_i = 0,\ se\ i > n \\ b_{k-i} = 0,\ se\ k - i > m \end{cases} \end{cases}$$

Observemos algumas restrições para $a_i,\ i > n$ e $b_{k-i},\ k - i > m$ que devem ser consideradas. Por exemplo, sejam $(A) = (a_0, a_1, a_2)$ e $(B) = (b_0, b_1, b_2, b_3)$ duas sequências. Fazendo as multiplicações conforme a definição anterior, temos que $m = 3$ e $n = 2$, então, $k = 2 + 3 = 5$.

Vamos calcular todos os c_i, com $0 \leq i \leq 5$. Então, $c_i = \sum_{i=0}^{5} a_i b_{5-i}$.

$$\begin{cases} c_0 = a_0b_0 \\ c_1 = a_1b_0 + a_0b_1 \\ c_2 = a_2b_0 + a_1b_1 + a_0b_2 \\ c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3, \ \{a_3b_0 = 0 \\ c_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4, \ \{a_4b_0 = a_3b_1 = a_0b_4 = 0 \\ c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5, \ \{a_5b_0 = a_4b_1 = a_3b_2 = a_1b_4 = a_0b_5 = 0 \end{cases}$$

Desse modo, temos que o produto

$$(C_5) = (A_2 \cdot B_3) = (a_0b_0, \ a_1b_0+a_0b_1, \ a_2b_0+a_1b_1+a_0b_2, \ a_2b_1+a_1b_2+a_0b_3, \ a_2b_2+a_1b_3, \ a_2b_3)$$

Fica assim, definido o produto de duas sequências que também é conhecido como Produto de Cauchy.

Definição 2.1.5.

Sejam $(A, +, \cdot)$ um Anel, (a_n) uma sequência de A e $w \in A$ um elemento fixo. Definimos o produto de w com (a_n), como sendo a sequência denotada por $(c_n) = w \cdot (a_n)$ e determinada por $c_k = w \cdot a_k$, para todo $k \in \mathbb{N}$.

Assim, o produto de (a_n) por w consiste em multiplicar cada termo da sequência de (a_n) por w.

Apresentaremos agora, uma associação entre sequências e uma indeterminada x para finalmente construirmos a estrutura de polinômios sobre um Anel.

Suponhamos, para isso, que um certo Anel $(A, +, \cdot)$ possua unidade 1. Assim, podemos definir as seguintes sequências

$$x^0 = (1, 0, 0, 0, ...)$$

e

$$x = (0, 1, 0, 0, ...)$$

Desta forma, usando multiplicação de sequências

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

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

$\vdots$

$x^n = \underbrace{x \cdot x \cdot x ... x}_{n} = (\underbrace{0, 0, 0, ..., 0}_{n}, 1, 0, 0, 0, ...)$

Desta forma, se desejarmos multiplicar os termos a_i nas sequências, conforme definição acima, e soma-las, conforme definição de soma de sequências, teremos:

$(a_0, 0, 0, ...) + (0, a_1, 0, 0, ...) + (0, 0, a_2, 0, 0, ...) + ... + (\underbrace{0, 0, 0, ..., 0}_{n}, a_n, 0, 0, 0, ...) =$

$(\underbrace{a_0, a_1, ..., a_n}_{n+1}, 0, 0, 0, 0, ...)$. Note que os termos $a_i = 0$, para $i \geq n + 1$. Neste caso, chamaremos esta sequência de quase nula.

Desse modo, temos uma adição de $(n + 1)$ sequências tendo como soma uma estrutura bastante simplificada em termos de potências de x em ordem crescente de 0 a n, e podemos representar a sequência $(f_n) = (a_0,\ a_1,\ a_2, ..., a_n,\ 0,\ 0, ...)$ como sendo $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, facilitando a notação, omitindo o sinal de $(\cdot)$ entre um termo a_i e o termo x^i, com $i \in \mathbb{N}$. Além disso usaremos, doravante, o símbolo $f(x)$ para nos referir à sequência (f_n).

Vamos definir um conjunto para os elementos $f(x)$ que denotaremos por $A[x]$, onde A é um Anel. Aos elementos $f(x)$, $g(x)$, $h(x)$, $p(x)$, dentre outros, convenientemente notados, chamaremos de Polinômios numa indeterminada x. Podemos, assim chamar um Polinômio de uma sequência quase nula, onde os elementos dessa sequência são os coeficientes do referido Polinômio. Logo, se temos uma sequência $f : (a_n) = (a_0, a_1, a_2, ..., a_n, 0, 0, ..)$ com $a_0, a_1, a_2, ..., a_n \in A$, podemos escrever o Polinômio que representa essa sequência como sendo $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$.

Ou seja, $f(x)$ por exemplo, é um polinômio pertencente ao conjunto $A[x]$ e que tem coeficientes no Anel $(A, +, \cdot)$. Formalizamos este conceito, abaixo:

Definição 2.1.6.

Seja $(A, +, \cdot)$ um anel. Então

$$A[x] = \{a_0 + a_1x + ... + a_nx^n;\ n \in \mathbb{N},\ a_i \in A,\ \forall i \in \{1,\ 2, ..., n\}\}$$

Os elementos de $A[x]$ são chamados de polinômios.

Notemos que cada elemento $a_i \in A$ com $i \in \{0, 1, 2, ..., n\}$ poderá ser identificado como um polinômio constante: $p(x) = a_i, i \in \{0, 1, 2, ..., n\}$. Desse modo temos que $A \subseteq A[x]$.

Exemplo 2.1.2.

Seja $\mathbb{Q}$ o Corpo dos Números Racionais, $\mathbb{R}$ o Corpo dos Reais e sejam os polinômios $p(x) = 1 - 4x + \frac{3}{4}x^2 + 2x^3$ e $q(x) = \sqrt{3} + x - \pi x^2 - 3x^3 + \frac{1}{2}x^4 + x^5$. Então, observando os coeficientes de ambos os polinômios podemos afirmar que $p(x) \in \mathbb{Q}[x]$ e consequentemente $p(x) \in \mathbb{R}$, uma vez que todos os coeficientes do polinômio $p(x)$ pertencem a $\mathbb{Q}$ ou $\mathbb{R}$. Por outro lado, o polinômio $q(x) \notin \mathbb{Q}[x]$, pois existem coeficientes de tal polinômio que não pertencem ao corpo dos racionais $\mathbb{Q}$, a saber: $\sqrt{3}$ e π, com $\sqrt{3},\ \pi \in \mathbb{R}$.

2.2 Polinômios numa indeterminada x

Definição 2.2.1.

Seja $(A, +, \cdot)$ um Anel comutativo com unidade 1. Um Polinômio numa indeterminada x sobre um Anel $(A, +, \cdot)$, é uma expressão do tipo

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n = \sum_{j=0}^{n} a_jx^j,$$

onde $n \in \mathbb{N}$ e $a_j \in A$, para $0 \leq j \leq n$.

Temos que todos os $a_{j's} \in A,\ 0 \leq j \leq n$ e são chamados de coeficientes do polinômio $p(x)$. O coeficiente a_0 é chamado termo constante ou independente de x. Além disso, cada parcela a_jx^j, com $0 \leq j \leq n$ será chamada de monômio de $p(x)$ com $a_j \neq 0$.

Para uma melhor construção dessa estrutura convencionaremos o seguinte:

- Para cada Natural n, temos $\theta(x) = 0 + 0x + 0x^2 + ... + 0x^n$ que chamaremos de polinômio identicamente nulo e podemos escrever $\theta(x) = 0$.

- Chamaremos de Polinômio Constante $p(x) = a_0$.

- Os polinômios estarão sempre escrito, convenientemente, segundo suas potências de x em ordem crescente ou decrescente.

- Quando $a_j = 0$ não escreveremos $a_j x^j$, fazendo apenas uso numa eventual necessidade.

Um Anel $(A, +, \cdot)$, por definição, é sempre diferente de vazio, existindo ao menos um elemento que garanta $A[x] \neq \varnothing$. De fato, como $0 \in A$, podemos ter $f(x) = 0 + 0x + 0x^2 + ... + 0x^n$ com $f(x) \in A[x]$.

2.2.1 Grau de um Polinômio

Seja um polinômio não nulo $p(x) \in A[x]$ com $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$. Logo existe $n \geq 0$ tal que $a_n \neq 0$ e $a_i = 0$ para todo $i > n$. Chamamos grau de $p(x)$ a esse número natural n e denotamos por $Gr(p) = n$. Assim:

$$Gr(p) = max\{i : a_i \neq 0\},\ p(x) \neq 0$$

.

De um modo geral podemos dizer que grau de polinômio $p(x)$ é o maior expoente natural entre os monômios que formam $p(x)$. Ou seja, o maior expoente natural da indeterminada x no polinômio.

Exemplo 2.2.1.

Grau de polinômios

$p(x) = a_0 \Rightarrow Gr(p) = 0,\ a_0 \neq 0$ *(polinômio constante).*

$p(x) = a_0 + a_1x^1 \Rightarrow Gr(p) = 1,\ a_1 \neq 0$ *(polinômio linear).*

$p(x) = a_0 + a_1x^1 + a_2x^2 \Rightarrow Gr(p) = 2,\ a_2 \neq 0$ *(polinômio quadrático).*

$p(x) = a_0 + a_1x^1 + a_2x^2 + a_3x^3 \Rightarrow Gr(p) = 3,\ a_3 \neq 0$ *(polinômio cúbico).*

Observações.

1. *No caso de $p(x) = 0$, convenciona-se indicar o grau de* p(x) *por $Gr(p) = -\infty$. Essa definição não gera nenhuma consequência sobre o conceito de grau de polinômio, dada acima.*

2. *O termo ou monômio do polinômio que possuir o maior expoente (que determina o grau de $p(x)$) será chamado de termo dominante e seu coeficiente será chamado de coeficiente líder.*

3. *Se o termo dominante de um polinômio tem coeficiente igual a* 1*, esse polinômio será chamado de mônico.*

4. *Polinômios podem ser ordenados segundo suas potências de x em ordem crescente ou decrescente.*

5. *Se existe um ou mais coeficientes nulos, temos um polinômio incompleto.*

6. *Se um polinômio incompleto tem grau n, então o seu número de termos será menor que $n+1$.*

7. *Um polinômio é dito completo quando possui todas as potências consecutivas a partir do grau mais alto até o termo constante ou vice - versa.*

8. *Quando um polinômio tem grau n e for completo, este terá exatamente $n+1$ termos.*

9. *Se os polinômios $p(x) = a_0+a_1x+a_2x^2+...+a_mx^m$ e $q(x) = b_0+b_1x+b_2x^2+...+b_nx^n$, diremos que $p(x) = q(x)$ se, e somente se, $m = n$ e $a_i = b_i$, $i \in \{0, 1, 2, 3, ..., n\}$.*

2.2.2 Adição de Polinômios

Definição 2.2.2.

Sejam $f(x) = a_0 + a_1x + ... + a_nx^n$ e $g(x) = b_0 + b_1x + ... + b_nx^n$ polinômios de $A[x]$. Se define $f(x) + g(x)$ como sendo

$$(f+g)(x) = f(x) + g(x) = \sum_{i=0}^{n} c_ix^i, \text{ com } \ c_i = a_i + b_i, \ 0 \leq i \leq n.$$

O resultado da adição de dois ou mais polinômios é chamado de soma.

Grau da Soma de Polinômios

Proposição 2.2.1.

Sejam $f(x)$ e $g(x)$ dois polinômios não nulos em $A[x]$, tais que $(f+g)(x) \neq 0$. Então $Gr(f+g) \leq max\{Gr(f), \ Gr(g)\}$.

Demonstração.

Suponhamos $f(x) = a_0+a_1x+...+a_mx^m$ e $g(x) = b_0+b_1x+...+b_nx^n$ com coeficientes líderes $a_m \neq 0$ e $b_n \neq 0$, respectivamente. Assim temos $Gr(f) = m$ e $Gr(g) = n$. Temos 4 casos a considerar:

Caso 1: $(m = n,\ a_m + b_n \neq 0)$

$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n$. Então o coeficiente líder da soma será $(a_n + b_n)$ e o grau dessa soma é $Gr(f + g) = n = m$.

Caso 2: $(m = n,\ a_m + b_n = 0)$

$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_k + b_k)x^k + (a_m + b_n)x^n = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_k + b_k)x^k$ com $k < m = n$.

Então o coeficiente líder da soma será $(a_k + b_k),\ k < m = n$ e $Gr(f + g) = k < m = n$.

Caso 3:$(m \neq n,\ m < n)$

$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_m + b_m)x^m + ... + (0 + b_n)x^n$. (Notemos que $a_i = 0$, para $i > m$).

Então o coeficiente líder será $(0 + b_n) = b_n \neq 0$, sendo que $Gr(f + g) = n$.

Caso 4:$(m \neq n,\ m > n)$

Fazendo análogo ao caso 3, encontramos o coeficiente líder $(a_m + 0) = a_m \neq 0$, sendo que $Gr(f + g) = m$. Portanto, qualquer que seja a situação temos que $Gr(f + g) \leq max\{Gr(f),\ Gr(g)\} = max\{m,\ n\}$. □

2.2.3 Multiplicação de polinômios

Definição 2.2.3.

Sejam $f(x) = a_0 + a_1x + ... + a_nx^m$ *e* $g(x) = b_0 + b_1x + ... + b_nx^n$ *polinômios em* $A[x]$. *Se define* $f(x) \cdot g(x)$ *como sendo*

$$(f \cdot g)(x) = f(x) \cdot g(x) = \sum_{j=o}^{m+n} c_jx^j,$$

com

$$
\begin{aligned}
&c_0 = a_0 b_0 \\
&c_1 = a_1 b_0 + a_0 b_1 \\
&c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 \\
&c_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 \\
&\vdots \\
&c_j = a_0 b_j + a_1 b_{j-1} + ... + a_j b_0 = \sum_{\alpha+\beta=j} a_\alpha b_\beta \\
&\vdots \\
&c_{m+n} = a_m \cdot b_n = \sum_{i=0}^{m+n} a_i b_{m+n-i}, \quad \begin{cases} a_i = 0, \ se \ i > m \\ b_{m+n-i} = 0, \ se \ i < m \end{cases}
\end{aligned}
$$

Consideremos dois polinômios $f(x)$ e $g(x) \in A[x]$ com $f(x) = a_0 + a_1 x + ... + a_m x^m$ e $g(x) = b_0 + b_1 x + ... + b_n x^n$. Para fins de organização vamos considerar $m = n$ sem perda de generalidade. Numa tabela retangular colocamos os coeficientes a_i de $f(x)$ na posição vertical e os coeficientes b_j de $g(x)$ na posição horizontal. Logo após, calculamos $a_i \cdot b_j$ e somamos todos esses produtos em cada diagonal como mostra a figura. Desse modo temos encontrado cada c_k.

f \ g	b_0	b_1	b_2	b_3	...	...	...	b_n
a_0	a_0b_0	a_0b_1	a_0b_2	a_0b_3	...	...	...	a_0b_n
a_1	a_1b_0	a_1b_1	a_1b_2	a_1b_3	...	...	...	a_1b_n
a_2	a_2b_0	a_2b_1	a_2b_2	a_2b_3	...	...	...	a_2b_n
a_3	a_3b_0	a_3b_1	a_3b_2	a_3b_3	...	...	...	a_3b_n
⋮	⋮	⋮	⋮	⋮	.	.	.	⋮
⋮	⋮	⋮	⋮	⋮	.	.	.	⋮
⋮	⋮	⋮	⋮	⋮	.	.	.	⋮
a_m	a_mb_0	a_mb_1	a_mb_2	a_mb_3	...	...	...	a_mb_n

Exemplo 2.2.2.

Sejam $f(x)$ e $g(x) \in A[x]$ com $f(x) = 2 + 3x + 4x^2 - 3x^4$ e $g(x) = 5 + 4x + 3x^2$. Dispomos os coeficientes de ambos os polinômios, conforme o dispositivo anterior:

f \ g	5	4	3
2	10	8	6
3	15	12	9
4	20	16	12
0	0	0	0
-3	-15	-12	-9

Calculando todos os produtos, somando seguindo as setas e agrupando estes resultados encontramos os coeficientes do polinômio $h(x) = f(x) \cdot g(x)$ em ordem crescente das potências de x. Ou seja,

$$h(x) = 10 + 23x + 38x^2 + 25x^3 - 3x^4 - 12x^5 - 9x^6.$$

Atenção para quando o polinômio for incompleto. Devemos preencher com 0 (zero) o monômio que faltar, como foi o caso de $f(x)$ que era incompleto em x^3.

Outro fato importante a considerar é que o produto de dois polinômios é fechado quanto à multiplicação. O que justifica $h(x) = f(x) \cdot g(x)$ e $h(x) \in A[x]$.

Grau do Produto de Polinômios

Proposição 2.2.2.

Sejam $f(x)$ e $g(x)$ dois polinômios não nulos em $A[x]$, tais que $(f \cdot g)(x) \neq 0$. Então

$$Gr(f \cdot g) \leq Gr(f) + Gr(g).$$

No entanto, se A for um Domínio de Integridade, teremos apenas a igualdade.

Demonstração.

Sejam $f(x) = a_0 + a_1x + ... + a_nx^m$ e $g(x) = b_0 + b_1x + ... + b_nx^n$ polinômios de

$A[x]$. Assim, $Gr(f) = m$ e $Gr(g) = n$. Vimos que se define cada elemento c_k do produto $f(x) \cdot g(x)$ como sendo

$$c_k = a_0 b_k + a_1 b_{k-1} + ... + a_k b_0 = \sum_{\alpha+\beta=k} a_\alpha b_\beta$$

Além disso, o coeficiente líder do produto é $c_{m+n} = a_m b_n$ e o termo que possui esse coeficiente vale $a_m b_n x^{m+n}$, com $a_m \neq 0$ e $b_n \neq 0$. Logo, $a_m b_n \neq 0$, quando A for um Domínio de Integridade e $Gr(f \cdot g) = m + n = Gr(f) + Gr(g)$. Caso $(A, +, \cdot)$ não seja um Domínio de Integridade temos a possibilidade de $a_m b_n = 0$. Mas como $a_m b_n$ é o coeficiente líder do produto $f(x) \cdot g(x)$, temos que $Gr(f \cdot g) \leq (m + n) \leq (Gr(f) + Gr(g))$. $\square$

Exemplo 2.2.3.

Se $f(x) = 2 + 4x^3$ e $g(x) = x + 2x^2 + 5x^4$ são dois polinômios em $\mathbb{R}[x]$, temos que $Gr(f) = 3$ e $Gr(g) = 4$, pois os termos que possuem os coeficientes líderes de cada polinômio $f(x)$ e $g(x)$ são respectivamente $4x^3$ e $5x^4$.

Então o coeficiente líder do produto vale: $c_{m+n} = c_{3+4} = 4x^3 5x^4 = 4 \cdot 5 \cdot x^3 \cdot x^4 = 20x^7$. Portanto

$$Gr(f \cdot g) = 3 + 4 = 7.$$

Notemos que vale a igualdade, pois o Corpo dos Reais $\mathbb{R}$ é um Domínio de Integridade.

Teorema 2.2.1.

Seja (A, +, ·) um Anel. Então:

1. *(A[x], +, ·), com a soma e o produto usual de polinômios, é um Anel. Assim $A[x]$ será chamado de Anel de polinômio.*

2. *Se $(A, +, \cdot)$ é comutativo, então $(A[x], +, \cdot)$ é comutativo.*

3. *Se $(A, +, \cdot)$ tem unidade 1, então $(A[x], +, \cdot)$ tem unidade $u(x) = 1$.*

4. *Se $(A, +, \cdot)$ é um Domínio, então $(A[x], +, \cdot)$ também será.*

Demonstração. [1]

Vamos mostrar os seis axiomas de Anel.

Sejam $a(x) = a_0 + a_1x + ... + a_nx^n$, $b(x) = b_0 + b_1x + ... + b_nx^n$ e $c(x) = c_0 + c_1x + ... + c_nx^n$ polinômios arbitrários em $A[x]$. Considere, sem perda de generalidade, que todos tenham o mesmo grau. Todas as propriedades aqui aplicadas tem base no fato de $(A, +, \cdot)$ ser um Anel e assim termos garantido as convenientes passagens.

i) Comutatividade da Adição

$\mathbf{[a + b](x)} = a_0+a_1x+...+a_nx^n+b_0+b_1x+...+b_nx^n = (a_0+b_0)+(a_1+b_1)x+...+(a_n+b_n)x^n = (b_0+a_0)+(b_1+a_1)x+...+(b_n+a_n)x^n = b_0+b_1x+...+b_nx^n+a_0+a_1x+...+a_nx^n = \mathbf{[b + a](x)}$

ii) Associativa da adição

$\mathbf{[a + (b + c)](x)} = a_0+a_1x+...+a_nx^n+(b_0+b_1x+...+b_nx^n+c_0+c_1x+...+c_nx^n) = a_0+a_1x+...+a_nx^n+((b_0+c_0)+(b_1+c_1)x+...+(b_n+c_n)x^n) = a_0+(b_0+c_0)+(a_1+(b_1+c_1))x+...+(a_n+(b_n+c_n))x^n = ((a_0+b_0)+c_0)+((a_1+b_1)+c_1)x+...+((a_n+b_n)+c_n)x^n = \mathbf{[(a + b) + c](x)}$.

iii) Existência de elemento neutro da adição

Seja $e(x) = 0 + 0x + ... + 0x^n = 0 \in A[x]$. Assim temos,

$\mathbf{[a + e](x)} = a_0+a_1x+...+a_nx^n+0+0x+...+0x^n = (a_0+0)+(a_1+0)x+...+(a_n+0)x^n = a_0 + a_1x + ... + a_nx^n = \mathbf{a(x)}$. Além disso,

$\mathbf{[e + a](x)} = (0 + a_0) + (0 + a_1)x + ... + (0 + a_n)x^n = a_0 + a_1x + ... + a_nx^n = \mathbf{a(x)}$.

Portanto, $\mathbf{[a + e](x)} = \mathbf{[e + a](x)} = \mathbf{a(x)}$

iv) Existência de elemento simétrico

Seja $s(x) = -a(x) = -a_0 - a_1x - ... - a_nx^n \in A$.

$\mathbf{[a + s](x)} = a_0 + a_1x + ... + a_nx^n - a_0 - a_1x - ... - a_nx^n = (a_0 - a_0) + (a_1 - a_1)x + ... + (a_n - a_n)x^n = 0 + 0x + ... + 0x^n = 0 = \mathbf{e(x)}$. Além disso,

$\mathbf{[s + a](x)} = -a_0 - a_1x - ... - a_nx^n + a_0 + a_1x + ... + a_nx^n = (-a_0 + a_0) + (-a_1 + a_1)x + ... + (-a_n + a_n)x^n = 0 + 0x + ... + 0x^n = 0 = \mathbf{e(x)}$.

Portanto, $\mathbf{[a + s](x)} = \mathbf{[s + a](x)} = \mathbf{e(x)}$.

v) Associatividade da multiplicação

Temos que $A[x]$ é fechado quanto a operação multiplicação. Assim vamos definir alguns produtos:

$$a(x) \cdot b(x) = d(x),\ com\ d(x) = d_0 + d_1x + ... + d_nx^n,\ d_i = \sum_{j+k=i} a_jb_k$$

$$b(x) \cdot c(x) = f(x),\ com\ f(x) = f_0 + f_1 x + ... + f_n x^n,\ f_i = \sum_{j+k=i} b_j c_k$$

$$[a(x) \cdot b(x)] \cdot c(x) = g(x),\ com\ g(x) = g_0 + g_1 x + ... + g_n x^n,\ g_i = \sum_{j+k=i} d_j c_k$$

$$a(x) \cdot [b(x) \cdot c(x)] = h(x),\ com\ h(x) = h_0 + h_1 x + ... + h_n x^n,\ h_i = \sum_{j+k=i} a_j f_k.$$

Então devemos mostrar que $g_i = h_i,\ \forall i \in \mathbb{N}$.

$$g_i = \sum_{j+k=i} d_j c_k = \sum_{j+k=i} \left(\sum_{\alpha+\beta=j} a_\alpha \cdot b_\beta \right) \cdot c_k = \sum_{\alpha+\beta+k=i} (a_\alpha b_\beta) \cdot c_k =$$

$$\sum_{\alpha+\beta+k=i} a_\alpha \cdot (b_\beta \cdot c_k) = \sum_{\alpha+\gamma=i} a_\alpha \cdot \left(\sum_{\beta+k=\gamma} b_\beta \cdot c_k \right) = \sum_{\alpha+\gamma=i} a_\alpha \cdot f_\gamma = h_i.$$

Daí, $[a(x) \cdot b(x)] \cdot c(x) = a(x) \cdot [b(x) \cdot c(x)]$

vi) Distributividade

Temos que $A[x]$ é fechado quanto à adição e multiplicação. Desse modo,

$$a(x)[b(x) + c(x)] = p(x) \in A[x].$$

Devemos mostrar que

$a(x)[b(x) + c(x)] = a(x)b(x) + a(x)c(x)$ e

$[a(x) + b(x)]c(x) = a(x)c(x) + b(x)c(x)$.

Consideremos,

$$a(x)[b(x) + c(x)] = p(x),\ com\ p(x) = p_0 + p_1 x + ... + p_n x^n,\ p_i = \sum_{j+k=i} a_j (b_k + c_k)$$

$$a(x) \cdot b(x) = d(x),\ com\ d(x) = d_0 + d_1 x + ... + d_n x^n,\ d_i = \sum_{j+k=i} a_j b_k$$

$$a(x)c(x) = q(x), com\ q(x) = q_0 + q_1 x + ... + q_n x^n,\ q_i = \sum_{j+k=i} a_j c_k$$

Assim, é preciso mostrar que $p_i = d_i + q_i,\ \forall i \in \mathbb{N}$. Ou seja,

$$p_i = \sum_{j+k=i} a_j (b_k + c_k) = \sum_{j+k=i} (a_j b_k + a_j c_k) =$$

$$\sum_{j+k=i}(a_jb_k)+\sum_{j+k=i}a_jc_k=d_i+q_i.$$

Portanto, $a(x)[b(x)+c(x)]=a(x)b(x)+a(x)c(x)$. Além disso,

$$[a(x)+b(x)]\cdot c(x)=p(x),\ com\ p(x)=p_0+p_1x+...+p_nx^n,\ p_i=\sum_{j+k=i}(a_j+b_k)\cdot c_k$$

$$a(x)\cdot c(x)=q(x),\ com\ q(x)=q_0+q_1x+...+q_nx^n, q_i=\sum_{j+k=i}a_jc_k$$

$$b(x)\cdot c(x)=f(x),\ com\ f(x)=f_0+f_1x+...+f_nx^n,\ f_i=\sum_{j+k=i}b_jc_k$$

Assim, é preciso mostrar que $p_i=q_i+f_i,\ \forall i\in\mathbb{N}$. Ou seja,

$$p_i=\sum_{j+k=i}(a_j+b_k)\cdot c_k$$

$$p_i=\sum_{j+k=i}(a_jc_k+b_jc_k)$$

$$p_i=\sum_{j+k=i}(a_jc_k)+\sum_{j+k=i}(b_jc_k)$$

$$p_i=q_i+f_i.$$

Portanto, $[a(x)+b(x)]\cdot c(x)]=a(x)\cdot c(x)+b(x)\cdot c(x)$. □

Provamos assim, que $A[x]$ tem estrutura de Anel e será chamado daqui pra frente por **Anel de Polinômio**.

Demonstração. [2]

Sejam $a(x)=a_0+a_1x+...+a_mx^m$ e $b(x)=b_0+b_1x+...+b_nx^n$ com $a(x)$, $b(x)\in A[x]$. Se multiplicarmos $a(x)$ com $b(x)$, ou seja $a(x)\cdot b(x)$, temos,

$$a(x)\cdot b(x)=\sum_{j=0}^{m+n}c_jx^j.$$

Os coeficientes desse produto (c_j) seguem a fórmula

$$c_j=a_0b_j+a_1b_{j-1}+...+a_jb_0=\sum_{\alpha+\beta=j}a_\alpha b_\beta.$$

No entanto, por hipótese $a_j,\ b_j \in A$ e $(A, +, \cdot)$ é um Anel comutativo, ou seja, $a_i \cdot b_k = b_k \cdot a_i$, $0 \leq i < j$, $0 \leq k < j$ e $i,\ j,\ k \in \mathbb{N}$.

Daí,

$$c_j = b_0 a_j + b_1 a_{j-1} + ... + b_j a_0 = \sum_{\beta+\alpha=j} b_\beta a_\alpha,$$

que é, na verdade, os coeficientes do produto $b(x) \cdot a(x)$. Logo,

$$a(x) \cdot b(x) = \sum_{j=0}^{m+n} c_j x^j = b(x) \cdot a(x).$$

□

Demonstração. [3]

Temos que mostrar que existe $u(x) \in A[x]$, tal que $a(x) \cdot u(x) = u(x) \cdot a(x) = a(x)$, $\forall\ a(x) \in A[x]$.

Sejam $a(x) = a_0 + a_1 x + ... + a_n x^n$ e $u(x) = u_0 + u_1 x + ... + u_m x^m$, com $a(x),\ u(x) \in A[x]$.

$$a(x) \cdot u(x) = a(x) \Leftrightarrow \sum_{i=0}^{m+n} c_i x^i = \sum_{i=0}^{n} a_i x^i,$$

com

$$c_i = \sum_{j+k=i} a_j u_k.$$

Temos,

$c_0 = a_0 u_0 = a_0 \Leftrightarrow u_0 = 1$

$c_1 = a_1 u_0 + a_0 u_1 = a_1 \Leftrightarrow u_0 = 1$ e $u_1 = 0$

$c_2 = a_2 u_0 + a_1 u_1 + a_0 u_2 = a_2 \Leftrightarrow u_0 = 1$ e $u_1 = u_2 = 0$

$c_3 = a_3 u_0 + a_2 u_1 + a_1 u_2 + a_0 u_3 = a_3 \Leftrightarrow u_0 = 1$ e $u_1 = u_2 = u_3 = 0$

$\vdots$

$c_n = a_n u_0 + a_{n-1} u_1 + ... + a_1 u_{n-1} + a_0 u_n = a_n \Leftrightarrow u_0 = 1$ e $u_1 = u_2 = u_3 = \ldots = u_n = 0$

Logo, temos que $u(x) = u_0 + u_1 x + ... + u_m x^m = 1 + 0x + ... + 0x^m = 1 + 0 + ... + 0 = 1$. Ou seja $u(x) = 1$ e $a(x) \cdot u(x) = a(x)$. Como é sabido que $A[x]$ é comutativo, temos,

$$a(x) \cdot u(x) = u(x) \cdot a(x) = a(x).$$

Notemos que $c_\alpha = 0$ para $n < \alpha \leq n + m$, pois

$$c_\alpha = a_\alpha u_0 + a_{\alpha-1}u_1 + a_{\alpha-2}u_2 + \ldots + a_1 u_{\alpha-1} + a_0 u_\alpha = 0\cdot 1 + a_{\alpha-1}\cdot 0 + a_{\alpha-2}\cdot 0 + \ldots + a_1\cdot 0 + a_0\cdot 0 = 0.$$

$\square$

Demonstração. [4]

Sejam $a(x) = a_0 + a_1x + ... + a_nx^n$ e $b(x) = b_0 + b_1x + ... + b_mx^m$ dois polinômios quaisquer em $A[x]$ com $a(x) \neq 0$ e $b(x) \neq 0$. Temos que,

$$a(x)\cdot b(x) = \sum_{i=0}^{m+n} c_i x^i \neq 0,$$

pois, sem perda de generalidade,

$$c_{m+n} = \sum_{j+k=m+n} a_j b_k = a_{m+n}b_0 + a_{m+n-1}b_1 + a_{m+n-2}b_2 + ... + a_nb_m + ... + a_0b_{m+n} = a_mb_n \neq 0,$$

uma vez que A não possui divisores de zero. Ou seja, como $a_n \neq 0$ e $b_m \neq 0$ e A é um Domínio, por hipótese, temos $a_n \cdot b_m \neq 0$.

Assim $\forall\ a(x),\ b(x) \in A[x]$ com $a(x) \neq 0$ e $b(x) \neq 0$, temos que $a(x)\cdot b(x) \neq 0$ e $A[x]$ é um Domínio de Integridade. $\square$

2.2.4 Divisão de Polinômios

Definição 2.2.4.

Seja $\mathbb{K}$ uma Corpo. Dados dois polinômios $f(x)$ e $g(x) \neq 0$ em $\mathbb{K}[x]$, dividir $f(x)$ por $g(x)$ é determinar dois outros polinômios $q(x)$ (quociente) e $r(x)$ (resto) de modo que se verifiquem as condições:

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

ii) $Gr(r) < Gr(g)$ *(ou $r(x) = 0$, caso em que a divisão é chamada exata).*

O Teorema seguinte nos garante que, munido de algumas condições, sempre é possível efetuar tal divisão.

Teorema 2.2.2 (Algoritmo da Divisão)**.**

Seja $\mathbb{K}$ *um Corpo. Se* $f(x),\ g(x) \in \mathbb{K}[x]$ *com* $g(x) \neq 0$ *então existem* $q(x),\ r(x) \in \mathbb{K}[x]$ *tais que*

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

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

Demonstração.

Sejam os polinômios

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

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0$$

Existência

Se $f(x) = 0$, então basta tomar $q(x) = r(x) = 0$. Porém se $f(x) \neq 0$ com $Gr(f) < Gr(g)$, tomamos $q(x) = 0$ e $r(x) = f(x)$.

Portanto, partiremos do pressuposto que $n \geq m$, e tomemos o monômio $a_n {b_m}^{-1} x^{n-m} = q_0 x^{n-m}$ para construir o polinômio

$$r_1(x) = f(x) - (q_0 x^{n-m}) \cdot g(x) \tag{2.1}$$

Chamamos (Eq 2.1) de primeiro resto parcial. Notemos que:

$$r_1(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 - (a_n {b_m}^{-1} x^{n-m})(b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0)$$

cancelando o termo $a_n x^n$ proveniente de $f(x)$ e portanto, $Gr(r_1) = p < n$. Para economizar notação, façamos:

$$r_1(x) = c_i x^i + c_{i-1}x^{i-1} + ... + c_1 x + c_0.$$

Fazendo agora, as mesmas operações com base em $r_1(x)$ e não mais em $f(x)$: Tomemos o monômio $c_i {b_m}^{-1} x^{i-m} = q_1 x^{i-m}$ para construir o polinômio

$$r_2(x) = r_1(x) - (q_1 x^{i-m}) \cdot g(x) \tag{2.2}$$

Chamamos (Eq 2.2) de segundo resto parcial. Notemos que:

$$r_2(x) = c_i x^i + c_{i-1}x^{i-1} + ... + c_1 x + c_0 - (c_i {b_m}^{-1} x^{i-m})(b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0)$$

cancelando o termo $c_i x^i$ de $r_1(x)$ e portanto, $Gr(r_2) = j < i = Gr(r_1)$. Podemos escrever $r_2(x)$ como sendo:

$$r_2(x) = d_j x^j + d_{j-1}x^{j-1} + ... + d_1 x + d_0.$$

Do mesmo modo procedemos para obter $r_3(x)$ e para isso formemos o monômio $d_j {b_m}^{-1} x^{j-m} = q_2 x^{j-m}$ e construímos o polinômio

$$r_3(x) = r_2(x) - (q_2 x^{j-m}) \cdot g(x) \tag{2.3}$$

Chamamos (Eq 2.3) de terceiro resto parcial. Além disso, notemos que

$$r_3(x) = d_j x^j + d_{j-1}x^{j-1} + ... + d_1 x + d_0 - (d_j {b_m}^{-1} x^{j-m})(b_m x^m + b_{m-1}x^{m-1} + ... + b_1 x + b_0)$$

o que prova o cancelamento de $d_j x^j$. Daí, $Gr(r_3) = l < j = Gr(r_2)$. Para facilitar a notação:

$$r_3(x) = e_l x^l + e_{l-1}x^{l-1} + ... + e_1 x + e_0.$$

Faremos análogo para construir $r_4(x)$, $r_5(x)$, ... Devemos perceber que a cada operação para se construir um resto parcial, o grau desse resto diminui de, ao menos, uma unidade. Portanto concluímos que, após um certo número p de operações temos um resto parcial $r_p(x)$ de grau inferior ao de $g(x)$ ou $r_p(x) = 0$. Assim, temos o resultado dessa última operação:

$$r_p(x) = r_{p-1}(x) - (q_{p-1} x^{\omega-m}) \cdot g(x) \tag{2.p}$$

Notemos ainda, que $r_p(x)$ surge a partir de uma série telescópica. Desse modo fazendo uma soma das igualdades de (1) a (p), temos:

$$\begin{array}{ll}
(2.1) & r_1(x) = f(x) - (q_0 x^{n-m})g(x) \\
(2.2) & r_2(x) = r_1(x) - (q_1 x^{i-m})g(x) \\
(2.3) & r_3(x) = r_2(x) - (q_2 x^{j-m})g(x) \\
\vdots & \vdots \qquad \vdots \qquad \vdots \qquad \vdots \\
(2.p) & r_p(x) = r_{p-1}(x) - (q_{p-1} x^{\omega-m})g(x)
\end{array}$$

$$\underbrace{r_p(x)}_{r(x)} = f(x) - \underbrace{(q_0x^{n-m} + q_1x^{i-m} + q_2x^{j-m} + ... + q_{p-1}x^{\omega-m})}_{q(x)} g(x)$$

Tomamos $r(x) = r_p(x)$ e $q(x) = q_0x^{n-m} + q_1x^{i-m} + q_2x^{j-m} + ... + q_{p-1}x^{\omega-m}$, obtendo

$$f(x) = q(x) \cdot g(x) + r(x),\ com\ Gr(r) < Gr(g)\ ou\ r(x) = 0.$$

Unicidade:

Suponhamos $r_1(x)$, $q_1(x)$, $r_2(x)$, $q_2(x)$ tal que $f(x) = q_1(x) \cdot g(x) + r_1(x)$ e $f(x) = q_2(x) \cdot g(x) + r_2(x)$. Assim,

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

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

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

Se $q_1(x) \neq q_2(x)$ temos,

$Gr(g \cdot (q_1 - q_2)) = Gr(r_2 - r_1)$. Mas

$Gr(g \cdot (q_1 - q_2)) = Gr(g) + Gr(q_1 - q_2)$. Logo,

$Gr(r_2 - r_1) = Gr(g) + Gr(q_1 - q_2)$

$\boxed{Gr(r_2 - r_1) \geq Gr(g).}$

No entanto, $Gr(r_2 - r_1) = max\{Gr(r_1),\ Gr(r_2)\}$. E como $Gr(r_1) < Gr(g)$ e $Gr(r_2) < Gr(g)$, temos que,

$\boxed{Gr(r_2 - r_1) = max\{Gr(r_1),\ Gr(r_2)\} < Gr(g)}$.

Portanto, temos uma contradição.

Então $q_1(x) = q_2(x)$ e

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

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

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

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

Logo, $f(x) = g(x) \cdot q(x) + r(x)$, com $Gr(r) < Gr(g)$ ou $r(x) = 0$. □

2.2.5 Métodos para Divisão de Polinômios

Método da chave

O Teorema anterior nos ensina como determinar os polinômios $q(x)$ e $r(x)$ a partir de $f(x)$ e $g(x)$ em $\mathbb{K}[x]$ com $\mathbb{K}$ um Corpo.

Veremos um exemplo de como proceder, caso $f(x) = x^4 - 3x^3 + 2x^2 - x + 1$ e $g(x) = x + 1$.

Observação.

Devemos garantir que os polinômios $f(x)$ e $g(x)$ pertençam a um Corpo $\mathbb{K}[x]$ para que as operações executadas sejam sempre possíveis.

Passo 1: Formemos o primeiro termo de $q(x)$ pela operação $q_1(x) = \dfrac{x^4}{x} = x^3$ e construir o primeiro resto parcial $r_1(x)$

$$r_1(x) = f(x) - x^3 \cdot g(x) = x^4 - 3x^3 + 2x^2 - x + 1 - x^4 - x^3 = -4x^3 + 2x^2 - x + 1.$$

Assim, $Gr(r_1) = 3 > 1 = Gr(g)$.

Passo 2: Formemos o segundo termo de $q(x)$ pela operação $q_2(x) = \dfrac{-4x^3}{x} = -4x^2$ e construímos o segundo resto parcial $r_2(x)$

$$r_2(x) = r_1(x) - (-4x^2)g(x) = -4x^3 + 2x^2 - x + 1 - (-4x^3 - 4x^2) = 6x^2 - x + 1.$$

Assim, $Gr(r_2) = 2 > 1 = Gr(g)$.

Passo 3: Formemos o terceiro termo de $q(x)$ pela operação $q_3(x) = \dfrac{6x^2}{x} = 6x$ e construímos o terceiro resto parcial $r_3(x)$

$$r_3(x) = r_2(x) - 6x \cdot g(x) = 6x^2 - x + 1 - 6x^2 - 6x = -7x + 1.$$

Assim, $Gr(r_3) = Gr(g)$.

Passo 4: Formemos o quarto termo de $q(x)$ pela operação $q_4(x) = \dfrac{-7x}{x} = -7$ e construímos o quarto resto parcial $r_4(x)$

$$r_4(x) = r_3(x) - (-7)g(x) = -7x + 1 - (-7x - 7) = 8.$$

Finalmente temos que $Gr(r_4) = 0 < 1 = Gr(g)$ e encerramos o processo de divisão entre $f(x)$ e $g(x)$.

Logo,

$$q(x) = q_1(x) + q_2(x) + q_3(x) + q_4(x) \Rightarrow q(x) = x^3 - 4x^2 + 6x - 7$$

$$e$$

$$r(x) = 8$$

Podemos arrumar as operações acima através do seguinte dispositivo que no Ensino Médio costumamos chamar de **Método da chave**:

$$
\begin{array}{l|l}
\overbrace{x^4 - 3x^3 + 2x^2 - x + 1}^{f(x)} & \overbrace{x+1}^{g(x)} \\ \cline{2-2}
\underline{-x^4 - x^3} & \underbrace{x^3 - 4x^2 + 6x - 7}_{q(x)} \\
\quad -4x^3 + 2x^3 - x + 1 & \\
\quad \underline{+4x^3 + 4x^2} & \\
\qquad\quad +6x^2 - x + 1 & \\
\qquad\quad \underline{-6x^2 - 6x} & \\
\qquad\qquad\quad -7x + 1 & \\
\qquad\qquad\quad \underline{+7x + 7} & \\
\qquad\qquad\qquad\quad \underbrace{+8}_{r(x)} &
\end{array}
$$

Definição 2.2.5. *Dados um Corpo $\mathbb{K}$ e um polinômio $f(x) = a_0 + a_1x + ... + a_nx^n$, $f(x) \in \mathbb{K}[x]$, a substituição de x por $k \in \mathbb{K}$ em $f(x)$ é um elemento de $\mathbb{K}$ dado por $f(k) = a_0 + a_1k + ... + a_nk^n$.*

Exemplo 2.2.4.

Sejam $\mathbb{Q}$ o Corpo dos Números Racionais e $f(x) = x^2 + x^4$ com $f(x) \in \mathbb{Q}[x]$. Assim, temos que $2 \in \mathbb{Q}$ e $f(2) = 2^2 + 2^4 = 4 + 16 = 20 \in \mathbb{Q}$. Podemos ter $f(\alpha) \in \mathbb{Q}$ ainda que $\alpha \notin \mathbb{Q}$. Por exemplo: Seja $\sqrt{2} \in \mathbb{R}$ e $f(\sqrt{2}) = (\sqrt{2})^2 + (\sqrt{2})^4 = 2 + 4 = 6 \in \mathbb{Q}$.

Definição 2.2.6.

Seja $(A, +, \cdot)$ *um Anel comutativo com unidade e* $\alpha \in A$. *Dizemos que* α *é* raiz *de* $f(x) \in A[x]$, *se* $f(\alpha) = 0$.

Exemplo 2.2.5.

Claro que $-2 \in \mathbb{R}$ *é* raiz *do polinômio* $f(x) = -x^3 - 4x^2 + x + 10$ *com* $f(x) \in \mathbb{R}[x]$, *pois* $f(-2) = 0$. *No entanto,* $1 \in \mathbb{R}$ *não é raiz de* $f(x)$, *uma vez que,* $f(1) = -1^3 - 4 \cdot 1^2 + 1 + 10 = -1 - 4 + 1 + 10 = 6 \neq 0$

Definição 2.2.7.

Sejam $(A, +, \cdot)$ *um Anel e* $f(x)$, $g(x) \in A[x]$. *Dizemos que* $g(x)$ *divide* $f(x)$ *em* $A[x]$ *quando existe* $h(x) \in A[x]$ *tal que*

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

Notação: $g(x)|f(x)$.

Teorema 2.2.3. *(Teorema do Resto)*

Sejam $f(x)$ *e* $g(x) = x - \alpha$ *dois polinômios em* $A[x]$. *Então o resto de* $f(x)$ *por* $g(x)$ *é* $f(\alpha)$.

Demonstração.

Pelo teorema da divisão de polinômios temos que $f(x) = q(x) \cdot g(x) + r(x) \quad (1)$, $q(x) \in A[x]$. Note que $r(x) = 0$ ou $r(x) = r$ (constante), já que $Gr(r) = 0 < Gr(g) = 1$. Assim $f(x) = q(x) \cdot g(x) + r$ e substituindo α em (1) temos: $f(\alpha) = q(\alpha) \cdot g(\alpha) + r$, mas $g(\alpha) = 0$ e consequentemente $f(\alpha) = r$. □

Exemplo 2.2.6.

O resto da divisão de $f(x) = x^3 - x^2 + x - 1$ *por* $(x - 2)$ *em* $\mathbb{R}[x]$ *será* $r(x) = f(2) = 2^3 - 2^2 + 2 - 1 = 8 - 4 + 2 - 1 = 5$. *Além disso temos que* $f(1) = 1^3 - 1^2 + 1 - 1 = 1 - 1 + 1 - 1 = 0$. *Desse modo 1 é raiz de* $f(x)$ *e o resto da divisão de* $f(x)$ *por* $(x - 1)$ *é 0, concluindo assim que* $(x - 1)$ *divide* $f(x)$.

Proposição 2.2.3. *(Teorema de D'Alembert)*

Seja $(A, +, \cdot)$ *um domínio de integridade e* $f(x) \in A[x]$. *Então* $\alpha \in A$ *é uma raiz de* $f(x)$ *se, e somente se,* $x - \alpha$ *divide* $f(x)$.

Demonstração.

$\Rightarrow$

Supomos por hipótese α é raiz de $f(x)$. Pela definição 2.2.6 $f(\alpha) = 0$. Além disso, pela divisão euclidiana de $f(x)$ por $x - \alpha$, temos que existem $q(x)$, $r(x) \in A[x]$ tais que: $f(x) = q(x) \cdot (x - \alpha) + r(x)$, onde $r(x) = 0$ ou $Gr(r) < Gr(x - \alpha) = 1$, ou seja, $r(x) = r \in A$. Assim, $f(x) = q(x) \cdot (x - \alpha) + r$.

Substituindo α em $f(x)$, temos: $f(\alpha) = q(\alpha) \cdot (\alpha - \alpha) + r = q(\alpha) \cdot 0 + r = r$. Daí, $f(\alpha) = r$, mas $f(\alpha) = 0$ e $r = 0$, mostrando que $x - \alpha$ divide $f(x)$.

$\Leftarrow$

Se $(x - \alpha)$ divide $f(x)$, então existe $q(x) \in A[x]$ tal que $f(x) = q(x) \cdot (x - \alpha)$. Avaliando f(x) em α, temos: $f(\alpha) = 0$. Desse modo, α é raiz de $f(x)$. $\square$

Dispositivo de Briot-Ruffini

Ao dividir o polinômio $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ por $(x - \alpha)$ obtemos um quociente $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + ... + b_1 x + b_0$ e resto $r(x)$. Se $Gr(f) = n$, $Gr(q) = n - 1$ e $Gr(x - \alpha) = 1$, então $Gr(f) = Gr(q) + Gr(x - \alpha)$ e $Gr(r) = 0$. Neste caso, podemos dizer o resto é uma constante, ou seja, $r(x) = r_0$.

Utilizando o algoritmo da divisão $f(x) = (x - \alpha) \cdot q(x) + r(x)$, temos:

$$\begin{aligned}
a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 &= (x - \alpha) \cdot (b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + ... + b_1 x + b_0) + r(x) \\
&= b_{n-1}x^n + b_{n-2}x^{n-1} + ... + b_1 x^2 + b_0 x - \alpha b_{n-1}x^{n-1} \\
&\quad -\alpha b_{n-2}x^{n-2} - ... - \alpha b_1 x - \alpha b_0 + r(x) \\
&= b_{n-1}x^n + (b_{n-2} - \alpha b_{n-1})x^{n-1} + (b_{n-3} - \alpha b_{n-2})x^{n-2} + ... \\
&\quad +(b_1 - \alpha b_2)x^2 + (b_0 - \alpha b_1)x - \alpha b_0 + r(x)
\end{aligned}$$

Comparando os coeficientes das mesmas potências de x no primeiro e no segundo membro:

$$\begin{aligned}
b_{n-1} &= a_n \\
b_{n-2} &= \alpha b_{n-1} + a_{n-1} \\
b_{n-3} &= \alpha b_{n-2} + a_{n-2} \\
&\vdots \\
b_1 &= \alpha b_2 + a_2 \\
b_0 &= \alpha b_1 + a_1 \\
r(x) &= \alpha b_0 + a_0
\end{aligned}$$

No dispositivo de Briot-Ruffini esses coeficientes $(b_{n-1},\ b_{n-2}, ..., b_1,\ b_0,\ r(x))$ são encontrados conforme os passos:

Tomemos o polinômio $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ e $g(x) = x - \alpha$, $f(x),\ g(x) \in A[x]$. Notemos que $\alpha \in A$ é raiz de $g(x)$.

Passo 1 Dispomos os coeficientes de $f(x)$ ao lado da raiz α de $g(x)$:

$$\begin{array}{c|cccccc|c}
\alpha & a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 \\
\hline
\end{array}$$

Passo 2 Repetimos o primeiro coeficiente (a_n) logo abaixo. Este será o primeiro coeficiente do quociente (coeficiente líder: b_{n-1}).

$$\begin{array}{c|cccccc|c}
\alpha & a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 \\
\hline
 & a_n & & & & & &
\end{array}$$

Passo 3 Para encontrar o segundo coeficiente do quociente (b_{n-2}), multiplicamos a_n por α e somamos com a_{n-1}. Ou seja, $b_{n-2} = \alpha \cdot a_n + a_{n-1} = \alpha \cdot b_{n-1} + a_{n-1}$. Para o terceiro coeficiente (b_{n-3}), multiplicamos b_{n-2} por α e somamos com a_{n-2}, ou seja, $b_{n-3} = \alpha \cdot b_{n-2} + a_{n-2}$. E assim, sucessivamente para encontrar os demais coeficientes. Além disso o último termo encontrado, desse modo, será o resto da divisão.

$$\begin{array}{c|cccccc|c}
\alpha & a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 \\
\hline
 & a_n & \alpha b_{n-1} + a_{n-1} & \alpha b_{n-2} + a_{n-2} & \dots & \alpha b_2 + a_2 & \alpha b_1 + a_1 & r(x) = \alpha b_0 + a_0
\end{array}$$

Assim, os termos $a_n = b_{n-1}$, $b_{n-2} = \alpha \cdot b_{n-1} + a_{n-1}$, $b_{n-3} = \alpha \cdot b_{n-2} + a_{n-2}$, ...,

$b_1 = \alpha b_2 + a_2$, $b_0 = \alpha b_1 + a_1$, $r(x) = \alpha b_0 + a_0$ são os coeficientes da divisão de $f(x)$ por $g(x)$. Desse modo, temos o quociente $q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + ... + b_1 x + b_0$ e resto $r(x) = \alpha b_0 + a_0$.

No uso do dispositivo de Briot-Ruffini é fácil notar que se $Gr(f) = n$, então o grau do quociente $q(x)$ encontrado dividindo $f(x)$ por $g(x) = x - \alpha$ vale $Gr(q) = n - 1$.

Exemplo 2.2.7.

Vamos dividir $f(x) = 2x^3 - 5x^2 + 5x - 3$ por $g(x) = 2x - 3$ com $f(x)$, $g(x) \in \mathbb{Q}[x]$, usando o dispositivo prático de Briot-Ruffini.

Solução:

Temos que a raiz α de $g(x)$ vale

$$2x - 3 = 0 \Rightarrow 2x = 3 \Rightarrow x = \alpha = \frac{3}{2}$$

Dispondo a raiz α e os coeficientes de $f(x)$ no dispositivo

$$\begin{array}{c|ccc|c} \frac{3}{2} & 2 & -5 & 5 & -3 \\ \hline & 2 & 2 \cdot \frac{3}{2} + (-5) & -2 \cdot \frac{3}{2} + 5 & 2 \cdot \frac{3}{2} + (-3) \end{array}$$

Daí, temos que $q(x) = 2x^2 - 2x + 2$ e o resto $r(x) = 0$.

Proposição 2.2.4.

Sejam $(A, +, \cdot)$ um Domínio de Integridade, $f(x) \in A[x]$ e $f(x) \neq 0$. Então o número de raízes de $f(x)$ em $A[x]$ não ultrapassa $Gr(f)$.

Demonstração.

Em se tratando de grau de $f(x)$, temos então que $f(x) \neq 0$, uma vez que se $f(x) = 0$ então $Gr(f)$ não está definido.

Seja $f(x) = a_0 + a_1 x + ... + a_n x^n$ com $Gr(f) = n$. Faremos a demonstração usando o Princípio de Indução Finita sobre n. Além disso, estamos interessados nas raízes em A. Se $f(x)$ não possui raízes em A, nada temos que provar. Pois assim $f(x)$ teria 0(zero) raiz e $0 \leq Gr(f) = n$.

Se $n = 0$, então $f(x) = a_0 \neq 0$ e $f(x)$ não tem raiz.

Se $n = 1$, então $f(x) = a_0 + a_1 x$. Como $(A, +, \cdot)$ é um Corpo, podemos escrever $\alpha_1 = \dfrac{-a_0}{a_1}$ é a única raiz de $f(x)$.

Seja $n > 1$ e vamos admitir que todo polinômio de grau $(n-1)$ tenha no máximo $(n-1)$ raízes em A (hipótese de indução).

Suponhamos que $f(x)$ tenha raiz $\alpha \in A$. Então podemos escrever pela proposição 2.2.3 que $f(x) = (x - \alpha) \cdot q(x)$, $q(x) \in A[x]$.

No caso de $f(x)$ só possuir a raiz $\alpha \in A$, temos que o número de raízes de $f(x)$ é 1 e $1 < Gr(f) = n$. Se $f(x)$ possui mais uma raiz $\beta \in A$, com $\beta \neq \alpha$, então β deve ser raiz de $q(x)$, uma vez que $0 = f(\beta) = (\beta - \alpha) \cdot q(\beta)$. Como $\beta - \alpha \neq 0$, temos $q(\beta) = 0$, já que $A[x]$ é um Domínio pelo teorema 2.2.1 (item 4). Logo β é uma raiz de $q(x)$. Concluímos que $n = Gr(f) = Gr(x - \alpha) + Gr(q) = 1 + Gr(q)$, isto é, $Gr(q) = n - 1$.

Assim, pela hipótese de indução, $q(x)$ tem no máximo $(n-1)$ raízes em A e $f(x)$ tem no máximo n raízes em A (α e as raízes de $q(x)$). □

Exemplo 2.2.8.

Considere $f(x) \in \mathbb{R}[x]$ dado por $f(x) = x^3 - x^2 - x - 2$ com grau igual a 3. Note que 2 é raiz de $f(x)$, então podemos escrever $f(x) = (x-2) \cdot q(x)$, com $q(x) = x^2 + x + 1$. Observemos também, que o polinômio $q(x) = x^2 + x + 1$ não possui raízes em $\mathbb{R}$, e sim em $\mathbb{C}$. Assim, $f(x)$ com grau 3 tem 1 raiz em $\mathbb{R}$.

Definição 2.2.8. *[Multiplicidade da Raiz de um Polinômio]*

Dizemos que $\alpha \in A$ é uma raiz de multiplicidade $m \geq 1$ de um polinômio $f(x) \in A[x]$, se $(x - \alpha)^m$ divide $f(x)$ e $(x - \alpha)^{m+1}$ não divide $f(x)$.

Chamamos raízes simples aquelas que têm multiplicidade 1 e de raízes múltiplas aquelas que têm multiplicidade $m \geq 2$.

Exemplo 2.2.9.

Seja $f(x) = x^3 - 3x^2 + 4$, com $f(x) \in \mathbb{Q}[x]$. Note que 2 é raiz de $f(x)$, então $f(x) = (x-2) \cdot q(x)$, com $q(x) = x^2 - x - 2$ e $q(x) \in \mathbb{Q}[x]$. Além disso, 2 também é raiz de $q(x)$. Logo, $q(x) = (x-2) \cdot (x+1)$ e $f(x) = (x-2) \cdot (x-2) \cdot (x+1) = (x-2)^2 \cdot (x+1)$.

Note que -1 é raiz de $f(x)$. Podemos dizer que 2 é raiz de $f(x)$ com multiplicidade 2 e -1 é raiz simples de $f(x)$.

Este procedimento poderá ser muito delongado caso tenhamos um polinômio com uma raiz de multiplicidade m consideravelmente grande. Pensando nisso, apresentaremos no próximo capítulo alguns resultados que nos ajudará no caso de um polinômio (ou equação polinomial) ter raiz de multiplicidade m relativamente grande.

Capítulo 3

Equações Polinomiais ou Algébricas

3.1 Introdução

Neste capítulo, faremos uma breve abordagem sobre Equações Polinomiais. Essa abordagem sugere principalmente uma forma de aplicações de polinômios levando em consideração todas as propriedades já vistas sobre Anéis de Polinômios.

Observação.

Daqui em diante, para evitar engano entre os conceitos de equação polinomial e polinômio, faremos uso da notação, por exemplo, $f(x)$ ou $p(x)$ para nos referir a polinômios correspondentes às equações $F(x) = 0$ e $P(x) = 0$ respectivamente.

3.2 Definições

Definição 3.2.1.

Seja $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ um polinômio em $A[x]$. Denomina-se Equação Polinomial ou Algébrica toda equação que pode ser escrita na forma:

$a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$, com $a_n \neq 0$ e $n \in \mathbb{N}^*$, em que $a_n, a_{n-1}, ..., a_1, a_0$ são números complexos e n é o grau da equação.

Podemos também, usar a notação $P(x) = 0$ para expressar a mesma equação $P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$.

Exemplos :

1. $2x + 3 = 0$ é uma equação do 1º grau

2. $x^2 - x + 1 = 0$ é uma equação do 2º grau

3. $0x^4 + x^3 + x^2 - 3x + 4 = 0$ é uma equação do 3º grau

4. $3x^4 - 2x + 1 = 0$ é uma equação do 4º grau

Chamamos também, de Equação Polinomial ou Equação Algébrica à sentença aberta $f(x) = g(x)$, com $f(x)$ e $g(x) \in A[x]$. Uma sentença aberta em x pode ser verdadeira ou falsa conforme o valor atribuído a x. Por exemplo, seja $P(x) = x^2 - 3x + 2 = 0$ uma equação polinomial com coeficientes reais, então:

para $x = 0$; $P(0) = 0^2 - 3 \cdot 0 + 2 = 0 - 0 + 2 = 2 \neq 0$ (falsa)
para $x = 1$; $P(1) = 1^2 - 3 \cdot 1 + 2 = 1 - 3 + 2 = 0$ (verdadeira)
para $x = \frac{1}{2}$; $P\left(\frac{1}{2}\right) = \left(\frac{1}{2}\right)^2 - 3\left(\frac{1}{2}\right) + 2 = \frac{1}{4} - \frac{3}{2} + 2 = \frac{3}{4} \neq 0$ (falsa)
para $x = 2$; $P(2) = 2^2 - 3 \cdot 2 + 2 = 4 - 6 + 2 = 0$ (verdadeira)

3.3 Raízes

Definição 3.3.1.

Chama-se raiz de uma equação $F(x) = G(x)$ todo número α que substituindo por x torna a sentença verdadeira. Ou seja, α é raiz de $F(x) = G(x)$ se, e somente se $F(\alpha) = G(\alpha)$ é uma sentença verdadeira.

Desse modo, no exemplo anterior temos que 1 e 2 são as duas raízes da equação $x^2 - 3x + 2 = 0$.

Chamamos de conjunto solução ou conjunto verdade em $\mathbb{R}$ da equação $F(x) = G(x)$ o conjunto S cujos elementos são as raízes reais da equação. O conjunto solução da equação $x^2 - 3x + 2 = 0$ é $S = \{1, 2\}$.

Resolver uma equação polinomial ou algébrica é obter o seu conjunto solução. Obter o conjunto solução de uma equação algébrica não consiste num processo de troca de x por "tentativa e erro". Encontrar as raízes de uma equação nem sempre é tarefa fácil, exigindo para tal, um grau de conhecimento algébrico, às vezes, bastante desenvolvido.

Com base nesse argumento, vamos apresentar algumas propriedades e procedimentos que nos permite encontrar com mais facilidade as raízes de uma equação algébrica.

Para isso retomaremos algumas propriedades de polinômios que também são válidas para equações polinomiais.

3.3.1 Teorema Fundamental da Álgebra (TFA)

Faremos aqui uma referência ao Teorema Fundamental da Álgebra que afirma que qualquer polinômio $p(z)$, com coeficientes no corpo dos complexos de grau ($n \geq 1$) tem todas n raízes complexas.

Teorema 3.3.1.

Toda equação polinomial de grau n $(n \geq 1)$ com coeficientes complexos possui pelo menos uma raiz complexa.

Podemos encontrar a demonstração desse teorema em [8] (Um estudo de polinômios e sua abordagem no ensino).

Como consequência do TFA, temos:

Corolário 3.3.1. *(Teorema da Decomposição)*

Todo polinômio $p(z) = a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0$ com coeficientes no corpo dos complexos, $n \geq 1$ e $a_n \neq 0$ pode ser decomposto num produto de n fatores de 1^o grau, isto é,

$$p(z) = a_n (z - \alpha_1)(z - \alpha_2)(z - \alpha_3) \cdots (z - \alpha_n).$$

onde $\alpha_1,\ \alpha_2,\ \alpha_3, ..., \alpha_n$ são as raízes de $p(z)$. A menos da ordem dos fatores, tal decomposição é única.

Demonstração.

Existência:

Sendo $p(z)$ um polinômio tal que $Gr(p) \geq 1$, aplicando o TFA temos que $p(z)$ tem ao menos uma raiz α_1 em $\mathbb{C}$. Desse modo, $p(\alpha_1) = 0$. Além disso, pelo Teorema de D'Alembert, $(z - \alpha_1)$ divide $p(z)$, e

$$p(z) = (z - \alpha_1) \cdot q_1(z) \quad (I)$$

$q_1(z)$ tem grau $(n - 1)$ e coeficiente dominante a_n.

Se $n = 1$ então $Gr(q_1) = 0$, $q_1(z) = a_n$ (constante) e $p(z) = a_n(z - \alpha_1)$, demonstrando assim, para $n = 1$.

Se $n \geq 2$, então $Gr(q_1) \geq 1$ e vale o TFA para $q_1(z)$, ou seja, $q_1(z)$ tem ao menos uma raiz $\alpha_2 \in \mathbb{C}$. Assim, $(z - \alpha_2)$ divide $q_1(z)$ e

$$q_1(z) = (z - \alpha_2) \cdot q_2(z) \quad (II)$$

Substituindo (II) em (I) temos:

$$p(z) = (z - \alpha_1)(z - \alpha_2) \cdot q_2(z),$$

onde $q_2(z)$ é um polinômio de grau $n - 2$ e coeficiente dominante a_n.

Se $n = 2$, então $Gr(q_2) = 0$, $q_2(z) = a_n$ e

$$p(z) = a_n(z - \alpha_1)(z - \alpha_2)$$

demonstrando assim, para $n = 2$.

Aplicando o TFA sucessivas vezes, chegamos na igualdade:

$$p(z) = (z - \alpha_1)(z - \alpha_2)(z - \alpha_3) \cdots (z - \alpha_n) \cdot q_n(z).$$

onde $q_n(z)$ tem grau zero e coeficiente dominante a_n, ou seja $q_n(z) = a_n$. Logo

$$p(z) = a_n \cdot (z - \alpha_1)(z - \alpha_2)(z - \alpha_3) \cdots (z - \alpha_n)$$

Unicidade:

Suponhamos que $p(z)$ admita duas decomposições:

$p(z) = a_n(z - \alpha_1)(z - \alpha_2)(z - \alpha_3) \cdots (z - \alpha_n)$ e

$p(z) = b_m(z - \beta_1)(z - \beta_2)(z - \beta_3) \cdots (z - \beta_n)$

Desenvolvendo os segundos membros:

$p(z) = a_n z^n - a_n S_1 z^{n-1} + a_n S_2 z^{n-2} - ... \pm a_n S_n$

$p(z) = b_m z^m - b_m S'_1 z^{m-1} + b_m S'_2 z^{m-2} - ... \pm b_m S_m$

Utilizando a definição de igualdade de polinômios, temos:

$$n = m \ e \ a_n = b_m$$

Então, temos a igualdade:

$$(z-\alpha_1)(z-\alpha_2)(z-\alpha_3)\cdots(z-\alpha_n) = (z-\beta_1)(z-\beta_2)(z-\beta_3)\cdots(z-\beta_n) \tag{3.1}$$

Fazendo $z = \beta_1$, temos:

$$(\beta_1-\alpha_1)(\beta_1-\alpha_2)(\beta_1-\alpha_3)\cdots(\beta_1-\alpha_n) = 0$$

Como o produto dos fatores é nulo, e as raízes do polinômio são elementos de um Domínio de Integridade, temos, sem perdas de generalidade,

$$(\beta_1-\alpha_1) = 0 \Rightarrow \beta_1 = \alpha_1.$$

Assim,

$$(z-\alpha_1)(z-\alpha_2)(z-\alpha_3)\cdots(z-\alpha_n) = (z-\alpha_1)(z-\beta_2)(z-\beta_3)\cdots(z-\beta_n) \tag{3.2}$$

Dividindo (Eq 3.2) por $(z-\alpha_1)$ temos:

$$(z-\alpha_2)(z-\alpha_3)\cdots(z-\alpha_n) = (z-\beta_2)(z-\beta_3)\cdots(z-\beta_n)$$

Fazendo $z = \beta_2$

$$(\beta_2-\alpha_2)(\beta_2-\alpha_3)\cdots(\beta_2-\alpha_n) = 0$$

Convenientemente, fazendo $\beta_2 - \alpha_2 = 0 \Rightarrow \beta_2 = \alpha_2$.

Desse modo, concluímos que $\alpha_i = \beta_i \ \forall \ i \in \{1, 2, 3, ..., n\}$.

Portanto, como $n = m$, $a_n = b_m$, $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, $\alpha_3 = \beta_3$, ..., $\alpha_n = \beta_m$, temos que a decomposição é única. $\square$

Notemos que a escolha do Corpo dos Complexos é providencial, uma vez que, por exemplo, o corolário acima poderia não valer para o Corpo dos Reais. Observemos um exemplo:

Exemplo.

Considere o polinômio $p(x) = x^2 + 4$. Observemos que não há raízes do polinômio em $\mathbb{R}[x]$ e não podemos decompô-lo em fatores de 1^o grau. No entanto, no Anel dos Complexos $\mathbb{C}[x]$ temos as raízes $\alpha_1 = -2i$ e $\alpha_2 = 2i$ de $p(x)$. Segue do corolário 3.3.1

$$p(x) = (x - 2i)(x + 2i)$$

é a decomposição de $p(x) = x^2 + 4$ em $\mathbb{C}[x]$.

3.3.2 Raízes Complexas

Numa equação polinomial de coeficientes reais suas raízes poderão ser complexas não reais. Digo raízes, pois se uma equação polinomial possuir esse tipo de raiz ela só deve aparecer em número par. Evidenciaremos esse fato pelo teorema seguinte:

Teorema 3.3.2.

Se uma equação polinomial de coeficientes reais admite como raiz o número complexo $z = a + bi$ $(b \neq 0)$, então admite, também, como raiz o número $\overline{z} = a - bi$, chamado de conjugado de z.

Demonstração.

Seja a equação polinomial $P(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0$ de coeficientes reais que admite a raiz $z = a + bi, (b \neq 0)$, ou seja, $p(z) = 0$. Seja também, $\overline{z} = a - bi$ o conjugado de z. Calculemos $p(\overline{z})$:

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

temos que $(\overline{z})^n = \overline{(z^n)}$. Então:

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

Além disso, temos que se $w = \alpha + 0i = \alpha$ então $\overline{w} = \alpha - 0i = \alpha$. Dai,

$$p(\overline{z}) = \overline{a_n} \overline{(z_n)} + \overline{a_{n-1}} \overline{z^{n-1}} + ... + \overline{a_1 z} + \overline{a_0}$$

como a_i, $i \in \{0, 1, 2, ..., n\}$ é uma constante, então $\overline{a_i}\overline{z^i} = \overline{a_i z^i}$ e

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

Temos ainda que a soma de números conjugados é igual ao conjugado da soma, ou seja, se $w_1 = x+yi$ e $w_2 = x_2+y_2 i$ então $\overline{w_1}+\overline{w_2} = x_1-y_1 i+x_2-y_2 i = x_1+x_2-(y_1+y_2)i = \overline{w_1 + w_2}$. Logo,

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

$$p(\overline{z}) = \overline{0} = 0.$$

Concluímos, assim, que $\overline{z}$ é raiz da equação polinomial

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 = 0$$

$\square$

Observações.

1. *O teorema 3.3.2 só se aplica à equações polinomiais com coeficientes reais. Por exemplo, a equação $P(x) = x^2 + 2ix + 3 = 0$ com coeficientes complexos não reais $(2i)$ tem raízes $r_1 = i$ e $r_2 = -3i$. Porém $\alpha = \overline{r_1}$ e $\beta = \overline{r_2}$ não são raízes de $P(x) = 0$.*

2. *Outra importante consequência do teorema anterior é que se uma equação polinomial com coeficientes reais tem grau ímpar, então ela admite um número ímpar de raízes reais.*

Exemplo 3.3.1.

Resolver a equação $P(x) = x^4 + x^3 + x^2 + 3x - 6 = 0$, sabendo que uma das raízes é $i\sqrt{3}$.

Solução:

Pelo teorema anterior, se $i\sqrt{3}$ é uma das raízes, então $-i\sqrt{3}$ também é raiz da equação $P(x) = 0$. Assim, esta equação polinomial é divisível por $(x - i\sqrt{3})(x + i\sqrt{3}) = (x^2 + 3)$.

Dividindo $p(x)$ *por* x^2+3, *obtemos* x^2+x-2. *Desse modo,*

$$P(x) = (x^2+3)(x^2+x-2) = 0.$$

Resolvendo $x^2+x-2=0$ *temos as duas outras raízes:*

$$r_1 = -2 \text{ e } r_2 = 1$$

Resposta: $S = \{-i\sqrt{3},\ i\sqrt{3},\ -2,\ 1\}$

3.3.3 Raízes Racionais

Teorema 3.3.3.

Se uma equação polinomial $P(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$, $(a_n \neq 0)$, *de coeficientes inteiros, admite uma raiz racional* $\dfrac{p}{q}$ *(onde* $p \in \mathbb{Z}$, $q \in \mathbb{Z}^+$ *com* p *e* q *primos entre si), então* p *é divisor de* a_0 *e* q *é divisor de* a_n.

Demonstração.

Se $\dfrac{p}{q}$ é uma raiz de $p(x)=0$, então temos:

$$a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + ... + a_1\left(\frac{p}{q}\right) + a_0 = 0$$

$$a_n \cdot \frac{p^n}{q^n} + a_{n-1} \cdot \frac{p^{n-1}}{q^{n-1}} + ... + a_1 \cdot \frac{p}{q} + a_0 = 0$$

Multiplicando toda a equação por q^n, temos:

$$a_np^n + a_{n-1}p^{n-1}q + ... + a_1pq^{n-1} + a_0q^n = 0 \tag{3.3}$$

Isolando a_np^n em (3.3),

$$a_np^n = -a_{n-1}p^{n-1}q - a_{n-2}p^{n-2}q^2 - ... - a_1pq^{n-1} - a_0q^n$$

$$a_np^n = -q(a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^1 + ... + a_1pq^{n-2} + a_0q^{n-1}) \tag{3.4}$$

Isolando a_0q^n em (Eq 3.3),

$$a_0q^n = -a_np^n - a_{n-1}p^{n-1}q - ... - a_2p^2q^{n-2} - a_1pq^{n-1}$$

$$a_0q^n = -p(a_np^{n-1} + a_{n-1}p^{n-2}q + ... + a_2pq^{n-2} + a_1q^{n-1}) \tag{3.5}$$

Notemos que a_0, a_1, a_2,...,a_n, p e q são números inteiros. Então:

$$F = a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^1 + ... + a_1pq^{n-2} + a_0q^{n-1},\ F \in \mathbb{Z}$$

$$G = a_np^{n-1} + a_{n-1}p^{n-2}q + ... + a_2pq^{n-2} + a_1q^{n-1},\ G \in \mathbb{Z}$$

Desse modo temos que (Eq 3.4) e (Eq 3.5) valem:

$$a_np^n = -qF$$

$$a_0q^n = -pG$$

E como $q \neq 0$ e $p \neq 0$, temos,

$$\frac{a_np^n}{q} = -F \in \mathbb{Z}$$

e

$$\frac{a_0q^n}{p} = -G \in \mathbb{Z}$$

Concluímos assim que q divide a_np^n e sendo q e p^n primos entre si, temos que a_n é divisível por q, ou seja, q é divisor de a_n.

Além disso, p divide a_0q^n e como p e q^n são primos entre si, temos que a_0 é divisível por p. Ou seja, p é divisor de a_0. □

Exemplo 3.3.2.

Resolver a equação polinomial sabendo que a mesma possui raiz racional $2x^3 - 3x^2 - 2x + 3 = 0$

Solução:

Se a equação tem raízes da forma $\frac{p}{q}$*, então* $p \in \{-3,\ -1,\ 1,\ 3\}$ *e* $q \in \{1,\ 2\}$*. Portanto, temos que* $\frac{p}{q} \in \{-3,\ -\frac{3}{2},\ -1,\ -\frac{1}{2},\ \frac{1}{2},\ 1,\ \frac{3}{2},\ 3\}$.

Dessas supostas raízes vamos começar por conferir os valores inteiros. Lembrando do conceito de raiz para polinômios e fazendo $p(x) = 2x^3 - 3x^2 - 2x + 3$ *temos,* $p(1) = 0$*,* $p(-1) = 0$*,* $p(3) \neq 0$*,* $p(-3) \neq 0$*. Percebemos que* 1 *e* -1 *são raízes do polinômio* $p(x)$ *sendo também raízes da equação polinomial* $P(x) = 0$*. Então podemos reescrevê-la como* $P(x) = (x-1)(x+1) \cdot q(x) = 0$*. Para encontrar* $q(x)$ *vamos usar a divisão de polinômios sabendo que* $p(x)$ *é divisível por* $d(x) = (x-1)(x+1) = x^2 - 1$*. Ou seja,* $q(x) = \frac{p(x)}{x^2 - 1}$*,* $x \neq \pm 1$*:*

$$
\begin{array}{rl|l}
 & 2x^3 - 3x^2 - 2x + 3 & x^2 + 0x - 1 \\ \cline{3-3}
 & \underline{-2x^3 + 0x^2 + 2x} \qquad & 2x - 3 \\
 & -3x^2 + 0x + 3 & \\
 & \underline{+3x^2 + 0x - 3} & \\
 & 0 &
\end{array}
$$

Desse modo, temos $q(x) = 2x - 3$ *e a equação polinomial podendo ser escrita como* $P(x) = (x-1)(x+1)(2x-3) = 0$ *e suas raízes racionais são* $r_1 = -1$*,* $r_2 = 1$ *e* $r_3 = \frac{3}{2}$*.*

3.4 Raízes Múltiplas

Seja a equação $P(x) = x^3 - 4x^2 + 5x - 2 = 0$ com coeficientes inteiros. Utilizando o Teorema 3.3.3 (Raízes Racionais) temos que 2 é uma raiz racional de $P(x) = 0$. Então:

$$
\begin{array}{c|cccc}
2 & 1 & -4 & 5 & -2 \\ \hline
 & 1 & -2 & 1 & 0
\end{array}
$$

Logo, $P(x) = (x-2)(x^2 - 2x + 1) = 0$. Daí,

$$x^2 - 2x + 1 = 0 \Rightarrow (x-1)^2 = 0 \Rightarrow (x-1)(x-1) = 0 \Rightarrow x_1 = 1 \text{ e } x_2 = 1$$

Desse modo, $P(x) = 0$ tem uma raiz igual a 2 e duas raízes iguais a 1.

Definição 3.4.1.

Dizemos que r é raiz de multiplicidade m, com $m \geq 1$, da equação $P(x) = 0$ se, e somente se,

$$p(x) = (x - r)^m \cdot q(x) \text{ e } q(r) \neq 0.$$

Ou seja, dizemos que r é raiz de multiplicidade m de $P(x) = 0$ quando o polinômio $p(x)$ é divisível por $(x - r)^m$ e não é divisível por $(x - r)^{m+1}$.

Se $m = 1$ temos que r é raiz simples; $m = 2$ a raiz é dupla; $m = 3$ a raiz é tripla, etc.

Exemplo 3.4.1.

A equação $x^2 \cdot (x + 2)^3 = 0$ pode ser escrita como: $(x - 0)^2 \cdot (x + 2)^3 = 0$. Assim suas raízes são $r_1 = 0$ com multiplicidade 2 e $r_2 = -2$ com multiplicidade 3.

Notemos que, embora temos uma equação do 5^o grau, seu conjunto verdade terá apenas dois elementos:

$$S = \{0, -2\}$$

Exemplo 3.4.2.

Resolver a equação $P(x) = x^4 - 4x^3 + 5x^2 - 4x + 4 = 0$ sabendo que 2 é raiz de multiplicidade 2, temos:

Fatorando $p(x)$ com o auxílio do dispositivo de Briot-Ruffini:

$$\begin{array}{c|ccccc} 2 & 1 & -4 & 5 & -4 & 4 \\ \hline 2 & 1 & -2 & 1 & -2 & 0 \\ \hline & 1 & 0 & 1 & 0 & \end{array}$$

Então, $P(x) = (x - 2)^2 \cdot (x^2 + 1) = 0$.

Logo, $x^2 + 1 = 0 \Rightarrow x_1 = i$ e $x_2 = -i \Rightarrow S = \{-i,\ i,\ 2\}$

Apresentaremos agora, alguns conceitos a cerca de Derivada Formal, a fim de apresentarmos alguns resultados envolvendo multiplicidade de raiz de um polinômio ou equação polinomial. Vale lembrar que estaremos retomando, para essa abordagem, alguns conceitos de polinômios visto no capítulo anterior.

Definição 3.4.2.

1. *Sejam* $(A, +, \cdot)$ *um anel comutativo com unidade e* $f(x) = a_0 + a_1x + ... + a_nx^n \in A[x]$. *Chamamos de* ***derivada formal*** *de* $f(x)$ *ao polinômio*

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 + ... + na_nx^{n-1} \in A[x].$$

Analogamente, definimos derivada de ordem superior como sendo:

$$f^{(n+1)}(x) = (f^{(n)}(x))', \text{ para todo } f(x) \in A[x].$$

Definimos também que $f^{(0)}(x) = f(x)$, *para todo* $f(x) \in A[x]$.

2. *Se* $f(x) = k$, $\forall x \in A$, k *constante, então a derivada de* $f(x)$ *é igual a* $f'(x) = 0$.

Observação.

A definição de derivada formal de um polinômio que apresentaremos a partir daqui é semelhante à definição de derivada de uma função vista em cursos de cálculo. Vale lembrar que o termo "formal"sugerido segundo IEZZI [5], é empregado pelo fato de estarmos trabalhando com os Anéis de Polinômios $A[x]$ *e neste interessa-nos apenas a relação entre os seus elementos e também sua semelhança com as propriedades de Anel* A, *não nos remetendo aos conceitos de limite de uma função polinomial que leva à ideia de derivada.*

Exemplo 3.4.3.

A derivada formal de $f(x) = x^4+x^3+x^2+3x+7$ *é dado por* $f'(x) = 4x^3+3x^2+2x+3$.

Notemos que se $f(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$, com $f(x) \in A[x]$ temos $f'(x) = k_nx^{n-1} + k_{n-1}x^{n-2} + ... + k_2x + k_1$. Então $f'(x) \in A[x]$, pois $k_{i=1,2,3,...,n}$ de $f'(x)$ foram obtidos por multiplicações de cada expoente de um termo de $f(x)$ por seu respectivo coeficiente. Portanto, como $(A, +, \cdot)$ é fechado para a multiplicação, temos que $f'(x) \in A[x]$.

Proposição 3.4.1.

Sejam A *um anel comutativo com unidade e* $f(x)$, $g(x) \in A[x]$. *Então:*

$$(f(x) + g(x))' = f'(x) + g'(x).$$

Proposição 3.4.2.

Sejam os polinômios $\alpha = ax^r$ *e* $\beta = bx^s$*, com* $\alpha, \beta \in A[x]$*. Se* $\gamma = \alpha \cdot \beta$ *então* $\gamma' = \alpha' \cdot \beta + \alpha \cdot \beta'$

Proposição 3.4.3.

Sejam $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ *e* $\beta = bx^s$*, com* $f(x), \beta \in A[x]$*.*

Proposição 3.4.4.

Sejam $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ *e* $g(x) = b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0$*, com* $f(x),\ g(x) \in A[x]$*. Se* $h(x) = f(x) \cdot g(x)$ *então* $h'(x) = f'(x) \cdot g(x) + f(x) \cdot g'(x)$*.*

As demonstrações das propriedades acima são obtidas através de aplicações diretas da definição de derivadas formais e podemos encontrar em IEZZI [5].

Derivações sucessivas

Já vimos que se $f(x)$ é um polinômio em $A[x]$, então sua derivada é representada por $f'(x)$ e $f'(x) \in A[x]$. Desse modo, podemos determinar a derivada formal de $f'(x)$ que representaremos por $f''(x)$ ou $f^{(2)}(x)$ (segunda derivada formal de $f(x)$). Do mesmo modo, é possível obter a terceira derivada formal de $f(x)$, ou seja, $f'''(x)$ ou $f^{(3)}(x)$ e assim por diante.

Portanto, se temos por exemplo, $f(x) = a_n x^n$ com $a_n, \in A$ e $n \in \mathbb{N}$, então

$$\begin{aligned} f'(x) &= n \cdot a_n \cdot x^{n-1} \\ f^{(2)}(x) &= n \cdot (n-1) \cdot a_n \cdot x^{n-2} \\ f^{(3)}(x) &= n \cdot (n-1) \cdot (n-2) \cdot a_n \cdot x^{n-3} \\ &\vdots \\ f^{(n)}(x) &= n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 \cdot a_n \cdot x^0 = n! \cdot a_n \end{aligned}$$

Observemos que $f^{(k)}(x) = 0$, para $\forall k > n$. Desse modo, dizemos que

$$f^{(r)}(x) = (f^{(r-1)}(x))'$$

Exemplo 3.4.4.

Seja $f(x) = x^5 + x^4 + x^3 + x^2 + x + 7$ *um polinômio em* $\mathbb{R}[x]$*. Encontremos suas sucessivas derivadas:*

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

$f^{(2)}(x) = 4 \cdot 5x^3 + 3 \cdot 4x^2 + 2 \cdot 3x + 2 = 20x^3 + 12x^2 + 6x + 2$

$f^{(3)}(x) = 3 \cdot 20x^2 + 2 \cdot 12x + 6 = 60x^2 + 24x + 6$

$f^{(4)}(x) = 2 \cdot 60x + 24 = 120x + 24$

$f^{(5)}(x) = 120$

Além disso, $f^{(6)}(x) = f^{(7)}(x) = f^{(8)}(x) = ... = 0$

Com base nessa abordagem de derivada formal de polinômio, podemos enunciar o próximo teorema lembrando da definição 3.4.1 de multiplicidade da raiz de uma equação.

Teorema 3.4.1.

Se α *é raiz de multiplicidade* m *da equação polinomial* $F(x) = 0$*, então* α *é raiz de multiplicidade* $(m-1)$ *da equação* $F'(x) = 0$*, onde* $f'(x)$ *é a derivada primeira de* $f(x)$*.*

Demonstração.

Como α é raiz de multiplicidade m de $f(x) = (x-\alpha)^m \cdot q(x)$ então $q(\alpha) \neq 0$, por definição. Calculemos a primeira derivada de $f(x)$ utilizando a proposição 3.4.4.

$$\begin{aligned} f'(x) &= m(x-\alpha)^{m-1} \cdot q(x) + (x-\alpha)^m \cdot q'(x) \\ &= (x-\alpha)^{m-1} \cdot (m \cdot q(x) + (x-\alpha) \cdot q'(x)) \\ &= (x-\alpha)^{m-1} \cdot s(x), \quad \textit{com} \;\; s(x) = m \cdot q(x) + (x-\alpha) \cdot q'(x) \end{aligned}$$

Note que $s(\alpha) = m \cdot q(\alpha) \neq 0$

Assim, α é raiz de multiplicidade $(m-1)$ de $f'(x) = (x-\alpha)^{m-1} \cdot s(x)$ e $s(\alpha) \neq 0$ □

Corolário 3.4.1.

Se α *é raiz de multiplicidade* m *da equação polinomial* $F(x) = 0$*, então* α *é raiz de* $F^{(1)}(x) = F^{(2)}(x) = F^{(3)}(x) = ... = F^{(m-1)}(x) = 0$.

Corolário 3.4.2.

Se α *é raiz das equações polinomiais* $F(x) = F^{(1)}(x) = F^{(2)}(x) = F^{(3)}(x) = ... = F^{(m-1)}(x) = 0$ *e* α ***não*** *é raiz de* $F^{(m)}(x) = 0$*, então a multiplicidade de* α *em* $F(x) = 0$ *é* m*.*

Exemplo 3.4.5.

Vamos verificar se a equação polinomial $F(x) = 2x^3 - 15x^2 + 36x - 23 = 0$ *tem alguma raiz dupla.*

Solução:

Uma eventual raiz dupla da equação $F(x) = 0$ *também é raiz da derivada primeira* $F'(x) = 6x^2 - 30x + 36 = 0$*, portanto:*

$$6x^2 - 30x + 36 = 0 \Rightarrow x^2 - 5x + 6 = 0 \Rightarrow x = 2 \text{ ou } x = 3$$

Assim, se $F(x) = 0$ *possui raiz dupla, esta terá que ser* 2 *ou* 3*. Substituindo em* $F(x) = 0$*, temos*

$$F(2) = 5 \neq 0 \quad e \quad F(3) = 5 \neq 0$$

Concluímos, que $F(x) = 0$ *não possui raiz dupla.*

Observação.

Já vimos que um polinômio em A[x] de grau n possui até n raízes em A. Com isso, percebemos que a multiplicidade de uma raiz não ultrapassa o grau do polinômio. Ou seja, se m *corresponde à multiplicidade de uma raiz de um polinômio* $f(x)$*, então* $m \leq n = Gr(f)$*.*

3.5 Transformadas e Equações Recíprocas

No estudo de equações polinomiais estamos, as vezes, preocupados tão somente com suas raízes que nos passa despercebida um tipo de equação especial chamada de Equações Recíprocas. A identificação desse tipo de equação é importante, pois evita que usemos dispositivo exaustivos para obtenção de raízes em equações comuns quando poderíamos, apenas conhecendo propriedades de tal equação, obter tais raízes de modo facilitado.

Definição 3.5.1.

Transformação de uma equação algébrica $P_1(x) = 0$ *é toda operação com a qual se obtém uma nova equação* $P_2(y) = 0$ *cujas raízes estejam relacionadas com as raízes da equação inicial através de uma lei conhecida* $y = f(x)$*.*

Chamaremos a equação algébrica $P_1(x) = 0$ *de equação primitiva.*

A equação $P_2(y) = 0$ é chamada Equação Transformada e a lei $y = f(x)$ é chamada relação de transformação.

O estudo de Equações Biquadradas vistas na Educação Básica é um bom exemplo de Transformação.

Exemplo 3.5.1.

Seja a equação $P_1(x) = x^4 - 3x^2 - 4 = 0$ uma primitiva e $p_1(x) \in \mathbb{R}[x]$. Qual deverá ser a sua equação transformada pela relação $y = x^2$? E sua solução no Corpo dos Reais?

Solução:

Temos que $P_1(x) = (x^2)^2 - 3x^2 - 4 = 0$ e fazendo a substituição $y = x^2$ encontramos a transformada:

$$P_2(y) = y^2 - 3y - 4 = 0$$

Resolvendo $P_2(y) = 0$ encontramos suas raízes: $y_1 = 4$ e $y_2 = -1$. Daí, retomando à $y = x^2$ temos que:

Para $y_1 = 4$: $x^2 = 4 \Rightarrow x = \pm\sqrt{4} \Rightarrow x = \pm 2$

Para $y_2 = -1$: $x^2 = -1 \Rightarrow x = \pm\sqrt{-1}$. Como $x \in \mathbb{R}$ temos que não há valores de x para $y = -1$. Então a solução de $P_1(x) = 0$ será:

$$S = \{-2, +2\}$$

As três principais transformações que se pode fazer em uma equação polinomial são:

1. **Transformação Multiplicativa**

   Chama-se Transformação Multiplicativa aquela em que a sua lei de transformação é:

   $$y = kx, (k \neq 0)$$

   Seja a equação primitiva $P_1(x) = 0$. Fazendo a substituição de x por $\dfrac{y}{k}$, obtemos a equação transformada $P_2(y) = 0$ com suas raízes mantendo a relação de transformação com as raízes da equação da primitiva. Ou seja, as raízes da transformada equivalem as raízes da primitiva multiplicada po k.

Exemplo 3.5.2.

Dada a equação $P_1(x) = \dfrac{x^2}{4} + \dfrac{x}{2} - 2 = 0$*, obter sua Equação Transformada pela relação* $y = \dfrac{x}{2}$.

Solução:

$P_1(x) = \left(\dfrac{x}{2}\right)^2 + \dfrac{x}{2} - 2 = 0$*, fazendo a substituição sugerida:*

$$P_2(y) = y^2 + y - 2 = 0$$

Note que as raízes dessa transformada $(y_1,\ y_2)$ *mantêm a mesma relação com as raízes da equação primitiva* $(x_1,\ x_2)$*, ou seja*

$$y_1 = \frac{x_1}{2} \text{ e } y_2 = \frac{x_2}{2}$$

2. **Transformação Aditiva**

Chama-se transformação aditiva aquela em que a lei de transformação é:

$$y = x + a$$

Seja a equação primitiva $P_1(x) = 0$. Fazendo a substituição $x = y - a$, obtemos a equação transformada $P_2(y) = 0$ com suas raízes mantendo a lei de transformação em relação as raízes da equação primitiva. Ou seja, as raízes da transformada equivalem as raízes da primitiva acrescida de $a \in \mathbb{C}$.

Exemplo 3.5.3.

Dada a equação $P_1(x) = x^3 + 2x^2 - x - 2 = 0$*, obter sua Equação Transformada pela relação* $y = x + 1$.

Solução:

A relação $y = x + 1$ *é equivalente a* $x = y - 1$*. Fazendo a substituição na primitiva, temos:*

$$P_1(y-1) = (y-1)^3 + 2(y-1)^2 - (y-1) - 2 = 0$$

Desenvolvendo as potências e reduzindo os termos semelhantes, chegamos à equação *transformada*

$$P_2(y) = y^3 - y^2 - 2y = 0$$

É fácil notar que as raízes da transformada $P_2(y) = 0$ $(y_1 = -1,\ y_2 = 0,\ y_3 = 2)$ *são as raízes da primitiva* $P_1(x)$ $(x_1 = -2,\ x_2 = -1,\ x_3 = 1)$ *somada a* 1.

3. **Transformação Recíproca**

Chama-se transformação recíproca aquela em que a lei de transformação é:

$$y = \frac{1}{x},\ x \neq 0$$

Dada a equação primitiva $P_1(x) = 0$, substituindo x por $\frac{1}{y}$ e fazendo as devidas simplificações, obtemos a transformada $P_2(y) = 0$, cujas raízes são os inversos das raízes de $P_1(x) = 0$.

Daremos um enfoque à última transformação por estar mais relacionada com o contexto de nosso trabalho, não sendo as duas primeiras menos importante.

Exemplo 3.5.4.

Obter a transformada que apresenta como raízes os inversos das raízes de $x^2 - 5x + 6 = 0$.

Solução:

A equação primitiva é $P_1(x) = x^2 - 5x + 6 = 0$ *e como desejamos que as raízes da transformada sejam os inversos das raízes da primitiva, então estamos diante de uma Transformação Recíproca. Fazendo* $y = \frac{1}{x}$, *obtemos*

$$P_1(x) = P_1\left(\frac{1}{y}\right) = \left(\frac{1}{y}\right)^2 - 5\left(\frac{1}{y}\right) + 6 = 0 \Rightarrow P_2(y) = 6y^2 - 5y + 1 = 0.$$

Notemos que as raízes de $P_2(y) = 0$ *são:* $\frac{1}{2}$ *e* $\frac{1}{3}$. *Ou seja, os inversos das raízes de* $P_1(x) = 0$ *que são* 2 *e* 3.

Observação.

Para obtermos a Transformada Recíproca, basta invertermos a ordem de todos os coeficientes e trocarmos x *por* y.

Assim, se $P_1(x) = 2x^3 + x^2 - 4x + 5 = 0$ *é uma primitiva, então sua Transformada Recíproca será:*

$$P_2(y) = 5y^3 - 4y^2 + y + 2 = 0$$

3.5.1 Equação Recíproca

Faremos um estudo de um tipo especial de equação com o objetivo de abordar algumas propriedades e técnicas que facilite a sua resolução. Para tanto, precisarmos de mais algumas definições.

Definição 3.5.2.

Equações equivalentes são aquelas que possuem o mesmo conjunto solução.

Exemplo.

As equações $x^2 + x + 1 = 4x - 1$ *e* $x^2 - 3x + 2 = 0$ *são equivalentes pois* $S_1 = \{1, 2\}$ *e* $S_2 = \{1, 2\}$.

Para obter uma equação equivalente a partir de $F(x) = G(x)$, temos duas operações a considerar:

1. Somar aos dois membros da equação um mesmo termo.

2. Multiplicar os dois membros da equação por um mesmo número $k \in \mathbb{C}$.

Exemplo.

Na equação $2x^2 - x - 3 = x + 1$ *podemos aplicar as duas operações descritas anteriormente para concluir que* $2x^2 - x - 3 = x + 1$ *e* $x^2 - x - 2 = 0$ *são equações equivalentes.*

Obter uma equação equivalente deve ter, principalmente, o objetivo de deixá-la mais simples para sua resolução. Assim, se temos a equação $F(x) = G(x)$ com coeficientes em $\mathbb{C}$ (Corpo), então:

$$F(x) = G(x) \Rightarrow F(x) - G(x) = G(x) - G(x) \Rightarrow F(x) - G(x) = 0$$

que é uma equação polinomial redutível à forma:

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0, \ a_i \in \mathbb{C}$$

Transformando uma equação polinomial para a forma $P(x) = F(x) - G(x) = 0$ ou $P(x) = 0$ é possível que aconteçam dois casos que merece um destaque:

1. $P(x) = 0$ é identicamente nula

$$0x^n + 0x^{n-1} + ... + 0x + 0 = 0$$

   Logo, $\forall x \in \mathbb{C}$, x será solução de $P(x) = 0$.

2. $P(x)$ é uma constante não nula. Então

$$0x^n + 0x^{n-1} + ... + 0x + k = 0, \ k \in \mathbb{C}$$

   gerando assim, uma sentença falsa, e neste caso, não há solução para $P(x) = 0$. Ou seja, não há valor de $x \in \mathbb{C}$ tal que $P(x) = 0$.

Definição 3.5.3.

Chamamos uma equação de Recíproca se, e somente se, é equivalente a sua Transformada Recíproca $P\left(\frac{1}{x}\right) = 0$.

Teorema 3.5.1.

Dada a equação recíproca $P(x) = 0$, *se* α *é uma raiz com multiplicidade* m, *então* $\frac{1}{\alpha}$ *também é raiz com a mesma multiplicidade.*

Demonstração.

Pelo conceito de Transformação Recíproca já visto, temos que se $\alpha \neq 0$ é uma raiz de $P(x) = 0$, então $\frac{1}{\alpha}$ também será raiz da equação transformada $P\left(\frac{1}{\alpha}\right) = 0$, com α e $\frac{1}{\alpha}$ de mesma multiplicidade. Por outro lado, se $P(x) = 0$ é equivalente a $P\left(\frac{1}{\alpha}\right) = 0$, dizemos que $P(x) = 0$ é uma equação recíproca e toda raiz da transformada é raiz da primitiva. Daí, $\frac{1}{\alpha}$ é raiz de $P(x) = 0$. $\square$

Exemplo 3.5.5.

A equação $P_1(x) = 2x^3 - 7x^2 + 7x - 2 = 0$ *é uma equação recíproca pois* $P_1(x) = 2x^3 - 7x^2 + 7x - 2 = 0$ *é equivalente à sua transformada recíproca* $P_2(y) = -2y^3 + 7y^2 - 7y + 2 = 0$.

Devemos perceber que a equação $P_1(x) = 0$ pode ser escrita como:

$$P_1(x) = (x-2)(x-1)\left(x - \frac{1}{2}\right) = 0$$

Além disso, a transformada recíproca $P_2(y) = 0$ pode ser escrita como:

$$P_2(y) = -(y-2)(y-1)\left(y - \frac{1}{2}\right) = 0$$

Provando que $P_1(x) = 0$ e $P_2(y) = 0$ são equivalentes por terem as mesmas raízes. Notemos ainda que em relação à raiz 1 seu inverso é $\frac{1}{1} = 1$, ou seja à própria raiz 1.

Teorema 3.5.2.

A condição necessária e suficiente para que uma equação $P(x) = 0$ seja recíproca é que os coeficientes equidistantes dos extremos sejam iguais ou simétricos.

Demonstração.

Seja a equação polinomial de grau n:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x + a_0 = 0$$

Dizemos que a_n e a_0 são os coeficientes extremos, a_{n-1} e a_1 são equidistantes dos extremos, a_{n-2} e a_2 também, etc. De uma maneira geral, a_{n-k} e a_k $(k \leq n)$ são equidistantes dos extremos.

Condição suficiente

Se $a_{n-k} = \pm a_k$, para todo inteiro k $(0 \leq k \leq n)$, temos que $P\left(\frac{1}{x}\right) = 0$. Esse fato é fácil ver pois podemos, depois da substituição de x por $\frac{1}{x}$, multiplicar toda essa nova equação por x^n obtendo

$$a_n + a_{n-1}x + a_{n-2}x^2 + ... + a_2x^{n-2} + a_1x^{n-1} + a_0x^n = 0$$

Como $a_{n-k} = \pm a_k$ então $P\left(\frac{1}{x}\right) = 0$ e $P(x) = 0$ são equivalentes.

Condição necessária

Provemos que se $P(x) = 0$ e $P\left(\frac{1}{x}\right) = 0$ são equivalentes, então $a_{n-k} = \pm a_k$ para todo $k = 0, 1, 2, .., n$.

Como as equações são equivalentes então seus coeficientes correspondentes devem ser proporcionais, ou seja:

$$\begin{array}{rclc} a_n & = & \beta a_0 & (0) \\ a_{n-1} & = & \beta a_1 & (1) \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & = & \beta a_{n-1} & (1') \\ a_0 & = & \beta a_n & (0') \end{array}$$

Tomando as igualdades (k) e (k'), temos:

$$a_{n-k} = \beta a_k \text{ e } a_k = \beta a_{n-k}$$

então:

$$a_{n-k} = \beta(\beta a_{n-k}) \Rightarrow a_{n-k} = \beta^2 a_{n-k}$$

$$\beta^2 = 1 \Rightarrow \beta = \pm 1$$

Portanto temos concluído que: $a_{n-k} = \pm a_k$.

$\square$

Exemplo 3.5.6.

São equações recíprocas:

1. $x^3 - 3x^2 + 3x - 1 = 0$

2. $2x^4 - 4x^3 + 3x^2 - 4x + 2 = 0$

3. $x^5 - 2x^3 - 2x^2 + 1 = 0$ *ou* $x^5 + 0x^4 - 2x^3 - 2x^2 + 0x + 1 = 0$

CUIDADO!

As equações

$$2x^3 - 7x - 2 = 0$$

e

$$4x^4 - 15x^2 - 4 = 0$$

não representam equações recíprocas, uma vez que estas tem raiz 2, porém $\frac{1}{2}$ não é raiz dessas equações. Além disso, baseado no Teorema 3.5.2 ambas as equações nos enganam quanto aos seus coeficientes equidistantes dos extremos. Mas completando-as convenientemente temos: $P_1(x) = 2x^3+0x^2-7x-2 = 0$ e $P_2(x) = 4x^4+0x^3-15x^2-0x-4 = 0$. Desse modo, percebemos imediatamente que $P_1(x) = 0$ não possui os coeficientes equidistantes dos extremos iguais ou simétricos e quanto a $P_2(x) = 0$, podemos dizer que tem os coeficientes equidistantes dos extremos simétricos com a exceção do -15.

3.5.2 Classificação

As equações recíprocas podem ser de dois tipos:

a) Equações Recíprocas de 1ª espécie: são aquelas em que os coeficientes equidistante dos extremos são iguais, ou seja:

$$a_n = a_0,\ a_{n-1} = a_1,\ a_{n-2} = a_2,\ ...$$

Ex. $2x^3 + 3x^2 + 3x + 2 = 0$

b) Equações Recíprocas de 2ª espécie: são aquelas em que os coeficientes equidistantes dos extremos são simétricos, ou seja:

$$a_n = -a_0,\ a_{n-1} = -a_1,\ a_{n-2} = -a_2,\ ...$$

Ex. $x^5 - 2x^4 + x^3 - x^2 + 2x - 1 = 0$

Se $P(x) = 0$ é uma Equação Recíproca de 2ª especie e o $Gr(P)$ é par, então é preciso que o termo central do desenvolvimento de $P(x) = 0$ seja nulo.

Exemplo 3.5.7.

A equação $P(x) = 5x^4 - 13x^3 + ax^2 + 13x - 5 = 0$ *será recíproca de* 2^a *espécie, se* $a = 0$. *Neste caso, a equação fica reduzida a* $P(x) = 5x^4 - 13x^3 + 13x - 5 = 0$, *sendo fácil ver que* 1 *e* -1 *são raízes. Então*

$$P(x) = (x-1)(x+1) \cdot q(x) = 0, \text{ com } q(x) = 5x^2 - 13x + 5.$$

Resolvendo $Q(x) = 0$, temos:

$$5x^2 - 13x + 5 = 0 \Rightarrow x_1 = \frac{13 + \sqrt{69}}{10} \text{ e } x_2 = \frac{13 - \sqrt{69}}{10}$$

Note que $\dfrac{1}{x_1} = x_2$, *o que satisfaz a condição do Teorema 3.5.1*

Assim, temos as equações recíprocas:

- $2x^3 - 7x^2 + 7x - 2 = 0$ (equação recíproca de segunda espécie)
- $3x^2 - 10x + 3 = 0$ (equação recíproca de primeira espécie)
- $x^4 + 2x^3 + 2x^2 + 2x + 1 = 0$ (equação recíproca de primeira espécie)

3.5.3 Propriedades

1. Toda equação $P(x) = 0$, recíproca de 2ª espécie, admite 1 como raiz. Além disso, a divisão por $(x - 1)$ conduz a uma equação recíproca de 1ª espécie.

   Exemplo 3.5.8.

   A equação $P(x) = 3x^4 - 2x^3 + 2x - 3 = 0$ *admite a raiz* 1 *pois* $P(1) = 3 \cdot 1^4 - 2 \cdot 1^3 + 2 \cdot 1 - 3 = 0$. *Além disso, dividindo* $P(x)$ *por* $x - 1$ *usando Briot-Ruffini, temos:*

$$\begin{array}{c|ccccc} 1 & 3 & -2 & 0 & 2 & 3 \\ \hline & 3 & 1 & 1 & 3 & 0 \end{array}$$

   Assim, temos que $P(x) = (x-1)(3x^3+x^2+x+3) = 0$ *e* $Q(x) = 3x^3+x^2+x+3 = 0$ *é uma equação recíproca de* 1^a *espécie.*

2. Toda equação $P(x) = 0$, recíproca de 1ª espécie e grau ímpar, admite -1 como raiz. A divisão de $p(x)$ por $x + 1$ conduz a uma equação recíproca 1ª espécie e grau par.

   Exemplo 3.5.9.

   A equação $P(x) = x^5 - 2x^3 - 2x^2 + 1 = 0$ *(recíproca de* 1^a*) admite* -1 *como raiz, uma vez que* $p(-1) = (-1)^5 - 2(-1)^3 - 2(-1)^2 + 1 = 0$. *Além disso, dividindo* $p(x)$ *por* $(x + 1)$, *temos:*

$$\begin{array}{c|cccccc} -1 & 1 & 0 & -2 & -2 & 0 & 1 \\ \hline & 1 & -1 & -1 & -1 & 1 & 0 \end{array}$$

Assim, temos que $P(x) = (x+1)(x^4 - x^3 - x^2 - x + 1) = 0$ *e* $Q(x) = x^4 - x^3 - x^2 - x + 1 = 0$ *é uma equação recíproca de* 1^a *espécie de grau par.*

3.5.4 Equações Recíprocas de 1ª espécie e grau par

Vamos descrever nesse tópico um procedimento para resolver as equações recíprocas de 1ª espécie e grau par:

Seja a equação $P(x) = 0$ com $a_{n-k} = a_k$ $(0 \leq k \leq n)$ e $n = 2p$ (n é par). Temos que:

Arrumando os coeficientes convenientemente segundo as potências decrescente de x e lembrando que os coeficientes equidistantes dos extremos são iguais, temos

$$a_0 \cdot x^{2p} + a_1 \cdot x^{2p-1} + ... + a_{p-1} \cdot x^{p+1} + a_p \cdot x^p + a_{p-1} \cdot x^{p-1} + ... + a_1 \cdot x + a_0 = 0$$

A estratégia é baixar pela metade o grau de $p(x)$. Fazemos isso dividindo todo o primeiro membro da equação por x^p. Assim temos:

$$a_0 \cdot x^p + a_1 \cdot x^{p-1} + ... + a_{p-1} \cdot x + a_p + a_{p-1} \cdot \frac{1}{x} + ... + a_1 \cdot \frac{1}{x^{p-1}} + a_0 \cdot \frac{1}{x^p} = 0$$

agrupando os termos equidistante dos extremos, temos:

$$a_0 \left(x^p + \frac{1}{x^p} \right) + a_1 \left(x^{p-1} + \frac{1}{x^{p-1}} \right) + ... + a_{p-1} \left(x + \frac{1}{x} \right) + a_p = 0$$

Fazendo $y = x + \frac{1}{x}$, $x^2 + \frac{1}{x^2} = y^2 - 2$, $x^3 + \frac{1}{x^3} = y^3 - 3y$ ... e assim sucessivamente, encontramos a transformada recíproca

$$P_2(y) = a_p + a_{p-1} \cdot y + a_{p-2} \cdot (y^2 - 2) + a_{p-3} \cdot (y^3 - 3y) + ... = 0, \ com \ Gr(P_2) = \frac{n}{2}.$$

Exemplo 3.5.10.

Resolver a Equação $6x^4 + 35x^3 + 62x^2 + 35x + 6 = 0$ *em* $\mathbb{R}$.

Solução:

Dividindo a equação por x^2*, temos:*

$$6x^2 + 35x + 62 + 35 \cdot \frac{1}{x} + 6 \cdot \frac{1}{x^2} = 0$$

Agrupando os termos equidistante das extremidades

$$6\left(x^2+\frac{1}{x^2}\right)+35\left(x+\frac{1}{x}\right)+62=0$$

Fazendo:

$$y=x+\frac{1}{x} \tag{3.6}$$

Obtemos

$$y^2-2=x^2+\frac{1}{x^2}$$

Então,

$$6(y^2-2)+35y+62=0 \Rightarrow 6y^2+35y+50=0$$

que resolvendo em y, temos:

$$y_1=-\frac{5}{2} \text{ e } y_2=-\frac{10}{3}$$

Voltando a (3.6), e substituindo y por $y_1=-\dfrac{5}{2}$ temos:

$$x+\frac{1}{x}=-\frac{5}{2} \Rightarrow 2x^2+5x+2=0$$

cujas raízes são $x_1=-\dfrac{1}{2}$ e $x_2=-2$ (raízes inversas, uma vez que $2x^2+5x+2=0$ é uma equação reciproca.)

Novamente, substituindo y por $y_2=-\dfrac{10}{3}$ em (3.6):

$$x+\frac{1}{x}=-\frac{10}{3} \Rightarrow 3x^2+10x+3=0$$

cujas raízes são $x_3=-\dfrac{1}{3}$ e $x_4=-3$ (raízes inversas, uma vez que $3x^2+10x+3=0$ é uma equação reciproca.)

Então temos a solução no Corpo dos Reais da equação primitiva

$$S=\{-3,-2,-\frac{1}{3},-\frac{1}{2}\}$$

Vejamos os motivos pelos quais, só citamos o processo de resolução das equações de 1ª espécie e grau par:

1. Se temos uma equação recíproca de 1ª espécie e grau ímpar, sabemos que -1 é uma

das raízes e, dividindo por $x + 1$, obtemos uma **equação de 1ª espécie e grau par.**

2. Se temos uma equação recíproca de 2ª espécie e grau ímpar, sabemos que uma das raízes é 1 e, dividindo por $x - 1$, obtemos uma **equação de 1ª espécie e grau par.**

3. Se temos uma equação recíproca de 2ª espécie e grau par, uma das raízes é 1 e, dividindo por $x - 1$, obtemos uma equação de 1ª espécie e grau ímpar. Nesta, já sabemos que tem -1 como uma das raízes e dividindo-a por $x + 1$, obtemos uma **equação de 1ª espécie e grau par.**

Então, de qualquer modo, todas as equações recíprocas acabam recaindo em uma equação recíproca de 1ª espécie e grau par.

Considerações Finais

A presente dissertação de mestrado, constituiu-se na tentativa de abordar conceitos de polinômios em elos com níveis de Ensino Superior e Médio, além de explanar o conteúdo de Estruturas Algébricas de forma bastante simplificada sem fugir muito do formalismo exigido para o entendimento do assunto, nem se prender tanto nos exaustivos processos abstratos que torna o estudo, para alguns alunos da disciplina de Álgebra ou até mesmo professores de Nível Básico, uma tarefa um tanto cansativa ou desmotivante. Para tanto, consultamos ideias de algumas obras, aproveitando o que cada uma tinha de mais explicativo, fazendo convenientes considerações para que a abordagem atingisse o objetivo primordial que é a clareza no entendimento dos conceitos, definições, proposições, teoremas e exemplos. A preocupação dessa abordagem seguindo essa linha de clareza, está centrada, muito precisamente, no fato de tentarmos criar uma proposta de material algébrico que tenha utilidade tanto para os alunos ingressantes em curso de Nível Superior de exatas ou até mesmo alunos e professores de Nível Básico para supostas pesquisas.

No primeiro capítulo, fizemos considerações suaves a respeito de Anéis e Corpos com o objetivo de fundamentar o conteúdo de Anéis de Polinômios no capítulo seguinte, mas existem muitas abordagem aprofundada envolvendo estas estruturas algébricas que merecem investigações, inclusive, para aplicações em outros conteúdos do Ensino Médio. Finalmente no terceiro capítulo, podemos investigar um pouco mais sobre Equações Polinomiais fazendo um enfoque às Equações Recíprocas que por muitas vezes nos passa despercebida. Através do que abordamos, foi possível perceber que, em alguns casos, encontrar o conjunto solução de Equações Algébricas pode ser mais simples que se parece.

Podemos assim, observar que conforme a abordagem feita a cerca de Estruturas Algébricas nesse trabalho é possível estabelecer uma conexão entre tais conteúdos existentes principalmente em cursos de Matemática, apesar de sabermos que apenas relacionar conceitos algébricos não é o suficiente para resolver os problemas relacionados a transmissão do conhecimento matemático, já que esta problemática envolve também questões pedagógicas, dentre elas a reforma curricular em projetos pedagógicos de curso, que não faz parte da nossa proposta, mas que merece devida atenção.

Referências Bibliográficas

[1] BAIOCCO, Josiane Carla. Relação entre a Álgebra aprendida na Licenciatura e a Álgebra ensinada na Educação Básica. URI/Erechim, 2010.

[2] DE CASTRO BUSSMANN, Christian James; DAS DORES SAVIOLI, Ângela Marta Pereira. A Álgebra no Ensino Superior e no Ensino Fundamental e Médio: Existe Conexão?.

[3] DIERINGS, A. R. Ensino de Polinômios no Ensino Médio: Uma Nova Abordagem. 2014. Tese de Doutorado. Tesis doctoral no publicada). Universidade Federal de Santa Maria, Santa Maria: Brasil.

[4] HYGINO, H. D.; GELSON, I. Álgebra moderna. São Paulo: editora atual, 2003.

[5] IEZZI, Gelson. Fundamentos de matemática elementar: complexos, polinômios, equações. Atual, 2005.

[6] JANESCH, Oscar Ricardo. Álgebra II. UFSC/EAD, 2008.

[7] JÚNIOR, Sérgio Brazil. ALGUMAS OBSERVAÇÕES ACERCA DA DEFINIÇÃO DE ANEL A PARTIR DAS BIBLIOGRAFIAS COMUMENTE UTILIZADAS NOS CURSOS DE MATEMÁTICA DA UFAC. ELEMENTOS, p. 24, 2011.

[8] KOERICH, Aline Casagrande et al. Um estudo sobre polinômios e sua abordagem no ensino. 2000.

[9] MARQUES, Cristina Maria. Introdução teoria de anéis. Belo Horizonte, UFMG, 2002.

[10] PONTES, Ronaldo da Silva. Equações polinomiais: Soluções algébricas, geométricas e com o auxílio de derivadas. 2013.