Universidade do Estado do Rio de Janeiro

Centro de Tecnologia e Ciências

Instituto de Matemática e Estatística

Ricardo Dutra de Abreu

Polinômios, funções polinomiais, fatoração e algumas aplicações

Rio de Janeiro

2016

Ricardo Dutra de Abreu

Polinômios, Funções Polinomiais, Fatoração e Algumas Aplicações

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-graduação de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade do Estado do Rio de Janeiro.

Orientador: Prof. Dr. Sérgio Luiz Silva

Rio de Janeiro

2016

CATALOGAÇÃO NA FONTE
UERJ / REDE SIRIUS / BIBLIOTECA CTC-A

A162 Abreu, Ricardo Dutra.
Polinômios, funções polinomiais, fatoração e algumas aplicações / Ricardo Dutra de Abreu. – 2015.
69 f.: il.

Orientador: Sérgio Luiz Silva
Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística.

1. Funções (Matemática) - Estudo e ensino (Ensino fundamental) - Teses. 2. Polinômios - Estudo e ensino (Ensino fundamental) - Teses. 3. Matemática - Estudo e ensino - Teses. I. Silva, Luiz Sérgio. II. Universidade do Estado do Rio de Janeiro. Instituto de Matemática e Estatística. III. Título.

CDU 512

_____ _____

Assinatura Data

Ricardo Dutra de Abreu

Polinômios, funções polinomiais, fatoração e algumas aplicações

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-graduação de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), da Universidade do Estado do Rio de Janeiro.

Aprovada em 26 de agosto de 2016

Banca Examinadora:

_____

Prof. Dr. Sérgio Luiz Silva (Orientador)

Instituto de Matemática e Estatística - UERJ

_____

Prof. Dr. Augusto Cesar de Castro Barbosa

Instituto de Matemática e Estatística - UERJ

_____

Prof. Dr. Silas Fantin

Universidade Federal do Estado do Rio de Janeiro - UNIRIO

Rio de Janeiro

2016

DEDICATÓRIA

Às três pessoas mais importantes da minha vida, minha mãe Neuza, minha esposa Claudia e a minha filha Isabella.

AGRADECIMENTOS

Ao Professor Dr. Sérgio Luiz Silva, orientador atento, dedicado, responsável e inspirador. Ao longo do curso de mestrado, escolhê-lo para orientar-me, foi a segunda melhor escolha que fiz. A primeira, foi optar pela UERJ como polo do PROFMAT.

A todos os professores do PROFMAT – polo UERJ, pelas contribuições dadas para a minha formação acadêmica. Cresci muito, em boa medida, graças a eles. Eles dignificaram ainda mais o magistério.

Aos colegas de mestrado, em especial à Geisa Corrêa, os quais mostraram-se sempre solícitos no sentido de ajudar-me a superar algumas dificuldades que se apresentaram no transcorrer do curso.

A verdadeira viagem de descobrimento não consiste em procurar novas paisagens,
mas em ter novos olhos.
Marcel Proust

RESUMO

ABREU, Ricardo Dutra. *Polinômios, funções polinomiais, fatoração e algumas aplicações*. 2016. 69 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística, Rio de Janeiro, 2016.

O conceito de polinômios, suas propriedades e as operações usuais entre eles, é um dos tópicos na disciplina de matemática, previstos para ser ensinado na educação básica brasileira. Todavia, nem sempre este tema é abordado pelo professor, nessa fase do estudante. A justificativa mais frequente para essa lacuna é a "falta de tempo". Quando, no entanto, este assunto é estudado, invariavelmente é realizado com um nível de profundidade inferior ao que poderia e deveria ser desenvolvido. Os aspectos mais débeis nesse caso, residem no conceito de polinômios, na exploração de raízes racionais de polinômios com coeficientes inteiros e na menção ao algoritmo de Briot – Ruffini, o qual pode ser generalizado. Este trabalho oferece uma contribuição importante para suprir, ainda que parcialmente, essa fragilidade do ensino da matemática elementar no Brasil.

Palavras-chave: Fatoração de Polinômios. Polinômios. Funções Polinomiais. Aplicações de Polinômios.

ABSTRACT

ABREU, Ricardo Dutra. Polynomials, polynomial functions, factorization and some applications. 2016. 69 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT), Universidade do Estado do Rio de Janeiro, Instituto de Matemática e Estatística, Rio de Janeiro, 2016.

The concept of polynomials, their properties and basic operations between them, is one of the topics in the mathematics discipline, expected to be taught in Brazilian basic education. However, this subject is not always addressed by the teacher at that student stage. The most frequent reason for this gap is the "lack of time". When, however, this matter is presented, it is invariably carried out with a deep level below what can and should be developed. The weakest aspects in this case lie in the concept of polynomials, on the holding of rational polynomial roots with integer coefficients and mention to Briot - Ruffini algorithm, which can be generalized. This work makes an important contribution to supply, albeit partially, this fragility of elementary mathematics education in Brazil.

Keywords: Factoring polynomials. Polynomials. Polynomial functions. Application Polynomials.

SUMÁRIO

INTRODUÇÃO

Polinômios é um dos tópicos da disciplina de matemática que constam no curriculum dos ensinos fundamental e médio nas escolas brasileiras.

Neste trabalho, resgatamos as definições e os diversos teoremas clássicos e sobejamente conhecidos sobre o tema. Enfatizamos em especial, certos resultados que apesar de não serem inéditos, são pouco explorados em sala de aula. Eles dizem respeito, fundamentalmente, a um dos principais problemas concernentes aos polinômios: sua fatoração.

Os teoremas e proposições que tratam da descoberta de raízes racionais para polinômios com coeficientes inteiros, normalmente não são ministrados em toda a sua extensão na sala de aula. Muito menos ainda a utilização do algoritmo de Briot – Ruffini. Tal algoritmo é ensinado apenas quando o divisor é um polinômio de primeiro grau.

Quando um polinômio $f(x)$ com coeficientes inteiros tem raízes racionais não nulas $\left(\beta = \frac{r}{s}\right)$, sendo r e s primos entre si, podemos afirmar que $(r - ms)$ divide $f(m)$, independentemente do valor inteiro de m. Este resultado auxilia sobremaneira a fatoração da maioria dos polinômios trabalhados no ensino básico. Por outro lado, a generalização do algoritmo de Briot – Ruffini permite que se apresente ao estudante um outro método bastante eficaz de divisão de polinômios.

São duas as principais finalidades desse trabalho, a saber: ressaltar para os professores do ensino básico (fundamental e médio) a importância dos polinômios e contribuir para que eles possam desenvolver um trabalho mais aprofundado quando abordarem a fatoração de polinômios junto aos seus alunos.

Atingidos tais objetivos, a relevância desse trabalho torna-se irrefutável. Primeiro porque, uma vez que os professores tenham bem conhecido a importância do tema central aqui abordado, as chances de se colocá-lo em segundo plano na sala de aula – o que infelizmente ocorre com frequência - ficarão reduzidas. Além disso, uma vez que a fatoração de polinômios - cuja solução é normalmente bastante difícil - seja melhor dominada pelo corpo docente, o tratamento desse assunto se tornará menos árido e, consequentemente, permitirá que as aulas sobre polinômios se tornem mais interessantes.

A metodologia utilizada para elaborar esse trabalho foi a de pesquisa bibliográfica. A partir dessa pesquisa reunimos os diversos resultados e definições que nos interessavam e o

ordenamos de forma adequada aos objetivos que tínhamos estabelecido. Entre os diversos autores pesquisados, aqueles entre os quais mais nos beneficiamos foram Abramo Hefez, Antonio Caminha Muniz Neto e Maria Lúcia Torres Villela.

Este trabalho está estruturado em seis capítulos. O primeiro, apresenta um resumo histórico sobre o desenvolvimento do conceito atual de polinômios e o introduz, a partir de definições conhecidas. O segundo capítulo, é desenvolvido em torno das operações usuais entre polinômios e termina elucidando sobre quando polinômios e funções polinomiais podem ser identificados. O terceiro capítulo esclarece, através de algumas das inúmeras aplicações de polinômios, sobre a grande importância desse tema. O capítulo quatro esmiúça a fatoração de polinômios nos conjuntos numéricos tratados no ensino básico. O penúltimo capítulo propõe algumas atividades a serem desenvolvidas em sala de aula. Finalmente, no último capítulo, é apresentada a conclusão do trabalho.

1 **POLINÔMIOS**

Neste capítulo apresentamos a definição e as estruturas básicas de um polinômio. Iniciamos o capítulo, todavia, historiando brevemente o desenvolvimento do seu conceito atual.

1.1 **Breve desenvolvimento histórico**

A origem do conceito de polinômio, o qual desenvolvemos ao longo deste trabalho, está intimamente ligada à busca pela resolução das equações algébricas. Entre essas, a mais simples é a de primeiro grau, cuja resolução era conhecida desde a antiguidade[1].

Os babilônios, entre 1.800 e 1.600 a.C, já eram capazes de resolver algumas equações do segundo grau[1]. Contudo, foram os árabes que - conhecedores do saber matemático grego mais avançado - desenvolveram-no, produzindo métodos sistemáticos de resolução dessas equações. Não obstante, também se esforçaram no sentido de sua generalização[2]. O matemático muçulmano mais conhecido, que viveu aproximadamente entre 790 e 850, foi al-Khwarizmi[2]. Ele foi um dos principais matemáticos de sua época e nos legou importantes contribuições para a solução definitiva dessas equações algébricas. A fórmula que apresenta a solução de uma equação do segundo grau como a conhecemos hoje é, todavia, devida ao matemático hindu Sridhara, do século X[1]. Ela leva, no entanto, o nome de fórmula de Bháskara, outro matemático indiano que viveu de 1.114 a 1.185[2], em função de ter sido ele quem a publicou em um livro.

Foram necessários quatro séculos para que as equações algébricas de terceiro e quarto graus fossem resolvidas. Este feito foi realizado pelos matemáticos de Bolonha, Itália[1]. Tanto no século XV quanto no XVI, os desenvolvimentos algébricos mais significativos, foram decorrentes dos esforços para se encontrar uma solução para as equações algébricas do terceiro grau[2]. Neste sentido, destacaram-se Scipione Del Ferro, Niccolo Fontana mais conhecido por Tartaglia, Girolamo Cardano, e Ludovico Ferrari. Este último era discípulo de Cardano e foi notabilizado pela resolução da equação de quarto grau[1].

---

1 cf. Hefez, págs. 170 e 177
2 cf. Roque, págs. 194,198 e 207.

As equações algébricas de grau maior ou igual a cinco constituíram-se, desde a segunda metade do século XVI, num dos problemas centrais da matemática naquela época. Este problema só pode ser totalmente elucidado pela Teoria de Grupos de Evariste Galois, na primeira metade do século XIX[1]. A partir de sua teoria, ficou claro a inviabilidade da solução, por radicais, da equação algébrica geral, acima do quarto grau[3]. É verdade que a teoria sobre polinômios já vinha sendo desenvolvida através da contribuição de inúmeros matemáticos, entre os quais D'Alembert. Todavia, a partir da Teoria de Grupos iniciada por Abel e desenvolvida por Galois, a chamada Álgebra Moderna surgiu. Por sua vez, com a Álgebra Moderna, o conceito mais geral de polinômios com o qual lidamos hoje, pode ser desenvolvido.

1.2 **Sequências[4]**

Uma sequência de elementos de um conjunto A é uma função $x: \mathbb{N} \to A$ onde $\mathbb{N} = \{0,1,2,3,4,\dots\}$ é o conjunto dos números naturais. Normalmente uma sequência é indicada por $(a_0, a_1, a_2, a_3, \dots, a_n, \dots)$. Todavia, antes de apresentarmos exemplos de sequência, vamos explicitar sucintamente, outros conjuntos numéricos com os quais, além do conjunto $\mathbb{N}$, lidaremos ao longo de todo esse trabalho. Tais conjuntos são os seguintes:

$\mathbb{Z} = \{\pm n; n \in \mathbb{N}\}$, é o conjunto dos números inteiros;

$\mathbb{Q} = \left\{r = \frac{p}{q}; p, q \in \mathbb{Z}\ e\ q \neq 0\right\}$, é o conjunto dos números racionais;

$\mathbb{R}$ é o conjunto dos números reais;

$\mathbb{C} = \{z = a + bi; a, b \in \mathbb{R}\}$, é o conjunto dos números complexos, sendo $i = \sqrt{-1}$.

Exemplos de sequências:

i.$(0, 2, 4, 6, 8, \dots, 2n, \dots)$.

Neste exemplo, a função $x: \mathbb{N} \to \mathbb{Z}$ é tal que, a cada $n \in \mathbb{N}$ é associado um número inteiro $a_n = 2n$. Além disso, $A = \mathbb{Z}$;

ii.$\left(0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \dots, \frac{n}{n+1}, \dots\right)$.

---

3 cf. Dicionário de biografias científicas, pág. 971.

4 cf. Thomas, pág. 1

Aqui a função $x: \mathbb{N} \to \mathbb{Q}$, é tal que a cada $n \in \mathbb{N}$ é associado um racional $a_n = \frac{n}{n+1}$. Neste exemplo, $A = \mathbb{Q}$;

iii. $\left(i, -\frac{i}{2}, \frac{i}{3}, -\frac{i}{4}, \dots, \frac{i^{2n+1}}{n+1}, \dots\right)$.

Aqui temos a função $x: \mathbb{N} \to \mathbb{C}$, tal que a cada $n \in \mathbb{N}$ é associado um número complexo $a_n = \frac{i^{2n+1}}{n+1}$. Aqui, o conjunto $A = \mathbb{C}$.

1.3 **Corpo e Anel**[5]

Seja K um conjunto qualquer. Representamos por $\mathrm{K} \times \mathrm{K}$ $(ou\ \mathrm{K}^2)$ o produto cartesiano de K com ele próprio, isto é, $\mathrm{K}^2 = \{(a, b); a, b \in \mathrm{K}\}$. Definimos uma operação $(*)$ em K, como uma função $* : \mathrm{K} \times \mathrm{K} \to \mathrm{K}$; $(a, b) \to a * b$.

Seja K um conjunto com duas operações $(+)$ e $(\cdot)$, denominadas, respectivamente, de adição e multiplicação. Chamamos K de corpo, se estas operações possuem as seguintes propriedades para quaisquer $a, b, c \in$ K:

1) Comutativa: $a + b = b + a \ \ e \ \ a \cdot b = b \cdot a$;
2) Associativa: $a + (b + c) = (a + b) + c \ \ e \ \ a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
3) Existem $0\ e\ 1$ em K tais que $a + 0 = a \ \ e \ \ a \cdot 1 = a$;
4) Distributiva: $a \cdot (b + c) = a \cdot b + a \cdot c$;
5) Existência de simétrico: dado qualquer a em K, existe o simétrico $(-a)$ em K tal que $a + (-a) = 0$;
6) Existência de inverso: dado $b \in \mathrm{K}\backslash\{0\}$, existe (b^{-1}) em K tal que $b \cdot (b^{-1}) = 1$.

Exemplos de corpos: $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

Se as operações $(+)$ e $(\cdot)$ de K possuírem todas as propriedades acima enunciadas, exceto, possivelmente, a propriedade 6), então diremos que K é um anel.

Exemplos de anéis: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

---

[5] cf. Hefez, pág. 8

1.4 **Sequência quase toda nula**[6]

Uma sequência $(a_0, a_1, a_2, a_3, \dots)$ de elementos de um anel K é dita quase toda nula se existir $n \in \mathbb{N}$ tal que se $m \geq n$ então $a_m = 0$.

Exemplos de sequências quase todas nulas:

i. $(0, 0, 0, 0, \dots)$. Neste exemplo, podemos tomar $n = 0$;

ii. $(1, 2, 3, 4, 5, \dots, 99, 0, 0, 0, \dots)$. Neste exemplo, podemos tomar $n = 100$;

iii. $\left(1, \sqrt{2}, \sqrt{3}, 2, \sqrt{5}, \sqrt{6}, \dots, 10, 0, 0, 0, \dots\right)$. Neste exemplo, podemos tomar $n = 101$.

1.5 **Polinômio**[7]

Um polinômio sobre um anel K, isto é, com coeficientes em K, é uma expressão do tipo: $f = f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + \cdots = \sum_{i\geq 0} a_i x^i$, onde $(a_0, a_1, a_2, \dots)$ é uma sequência quase toda nula de elementos de K e *x* é chamada de indeterminada.

Na definição acima, convencionamos que:

i. Os elementos $a_i \in$ K são denominados os coeficientes de f;

ii. Quando $a_i = 0$ omitiremos, sempre que for conveniente, o termo $a_i x^i$;

iii. Quando $a_i = \pm 1$, escreveremos $\pm x^i$, ao invés de $(\pm 1)x^i$, para o termo correspondente de f;

iv. O polinômio $0 = 0 + 0x + 0x^2 + \cdots$ é denominado o polinômio identicamente nulo sobre K. Sempre que não houver perigo de confusão com o elemento $0 \in$ K, denotaremos o polinômio identicamente nulo sobre K, simplesmente por 0; mais geralmente, dado $\lambda \in$ K, denotaremos o polinômio $\lambda + 0x + 0x^2 + \cdots$ simplesmente por λ; em cada caso, o contexto deixará claro se estamos nos referindo ao polinômio constante e igual a λ ou ao elemento $\lambda \in$ K;

v. Ao denotarmos por K$[x]$ o conjunto de todos os polinômios sobre K, as inclusões $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ nos levam, automaticamente, às inclusões $\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$.

---

[6] cf. Muniz Neto, pág. 28

[7] cf. Muniz Neto, págs. 28 e 33

vi. No polinômio sobre K, $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + \cdots = \sum_{i\geq 0} a_ix^i$, chamamos cada a_ix^i de monômio.

vii. Neste trabalho, sempre que nos referirmos a K$[x]$ estaremos mencionando $\mathbb{Q}[x], \mathbb{R}[x]$ ou $\mathbb{C}[x]$. Quando desejarmos mencionar $\mathbb{Z}[x]$, o faremos de forma explícita.

viii. Dizemos que os polinômios sobre o corpo K, $f(x) = \sum_{i\geq 0} a_ix^i$ e $g(x) = \sum_{i\geq 0} b_ix^i$ são iguais se $a_i = b_i$ qualquer que seja $i \geq 0$.

1.6 **Grau de um polinômio**[7]

Se $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in$ K$[x]\backslash\{0\}$, com $a_n \neq 0$, dizemos que o inteiro não negativo n é o grau de f e denotamos $\partial f = n$ (lê-se "o grau de f é igual a n"). No caso em que $f(x) = \lambda$, com $\lambda \in$ K$\backslash\{0\}$, então $\partial f = 0$. Portanto, não está definido o grau do polinômio identicamente nulo.

Observação: num polinômio $f(x) \in$ K$[x]\backslash\{0\}$ de grau n, chamamos a_n de coeficiente líder de f. Se, nesse polinômio, $a_n = 1$, dizemos que $f(x)$ é mônico.

Exemplos de polinômios sobre K:

i. $f(x) = 1 + x - x^3 + \sqrt{2}x^7$

K $= \mathbb{R}$; $\partial f = 7$; Sequência dos coeficientes: $(1,\ 1,\ 0, -1,\ 0,\ 0,\ 0, \sqrt{2},\ 0,\ 0,\ 0, \ldots)$.

ii. $f(x) = x + \frac{1}{2}x^2 - x^3 + \frac{3}{5}x^4$

K $= \mathbb{Q}$; $\partial f = 4$; Sequência dos coeficientes: $\left(0,\ 1,\ \frac{1}{2}, -1,\ \frac{3}{5},\ 0,\ 0,\ 0,\ 0,\ 0, \ldots\right)$.

iii. $f(x) = 3 - 2i + (3 + 2i)x + (2 - 3i)x^2$

K $= \mathbb{C}$; $\partial f = 2$; Sequência dos coeficientes: $(3 - 2i, 3 + 2i, 2 - 3i,\ 0,\ 0,\ 0, \ldots)$.

2 **ALGÉBRA DOS POLINÔMIOS**

Neste capítulo apresentaremos as operações usuais entre polinômios e alguns resultados clássicos, tais como os métodos práticos de divisão entre eles. Ao final deste capítulo, no entanto, desenvolveremos uma das principais contribuições que este trabalho oferece, a saber a generalização do algoritmo de Briot – Ruffini. Trata-se de um assunto pouco conhecido da maioria dos professores de matemática no ensino fundamental e médio brasileiro.

Antes de definirmos adição e produto de polinômios, para posteriormente estudarmos as propriedades dos polinômios baseados nessas operações, enunciaremos um lema.

Lema 2.0.1 Se $(a_k)_{k\geq 0}\ e\ (b_k)_{k\geq 0}$ são sequências quase todas nulas de elementos em K, então também são quase todas nulas as sequências $(a_k \pm b_k)_{k\geq 0}\ e\ (c_k)_{k\geq 0}$, onde o termo c_k, para cada k, é dado por $c_k = \sum_{\substack{i+j=k \\ i,j\geq 0}} (a_i b_j) = \sum_{i=0}^{k} (a_i b_{k-i})$.

Prova:

1º $(a_k \pm b_k)_{k\geq 0}$ é quase toda nula.

Como $(a_k)_{k\geq 0}\ e\ (b_k)_{k\geq 0}$ são sequências quase todas nulas, sabemos que existem $m, n \in \mathbb{N};\ a_i = 0, se\ i > m\ e\ b_j = 0, se\ j > n$. Tomemos $k_0 = máx\{m, n\}$. Sendo assim, as sequências $a_k = b_k = 0, \forall k > k_0$. Portanto, $a_k \pm b_k = 0, \forall k > k_0$. Segue que $(a_k \pm b_k)_{k\geq 0}$ é quase toda nula.

2º $(c_k)_{k\geq 0}$ é quase toda nula

Sejam $m, n \in \mathbb{N}$ tais que $a_i = 0, se\ i > m\ e\ b_j = 0, se\ j > n$. Assim, se $k > m + n$ e $k = i + j$ com $i, j \geq 0$, teremos que, $i > m$ ou $j > n$, pois de outra forma, isto é, se $i \leq m$ e $j \leq n$ então, $m + n < k = i + j \leq m + n$, o que é uma contradição. Analisemos então, para esse $k > m + n,\ 0 \leq i \leq m$. Neste caso, $j > n$ e, portanto, $b_j = 0$. Logo, $a_i b_j = 0$. Se, entretanto, $i > m$, temos $a_i = 0$ e também neste caso $a_i b_j = 0$. Em ambos os casos, temos que o coeficiente definido por $c_k = \sum_{k=i+j} a_i b_j = 0$ para $k > m + n$. Logo, $(c_k)_{k\geq 0}$ é quase toda nula.

2.1 **Adição e multiplicação de polinômios**

Dados em K$[x]$ os polinômios $f(x) = \sum_{k\geq 0} a_k x^k$ *e* $g(x) = \sum_{k\geq 0} b_k x^k$ a soma e o produto de f e g, denotados respectivamente por $f + g$ *e* $f \cdot g$, são os polinômios $(f + g)(x) = \sum_{k\geq 0}(a_k + b_k)x^k$ *e* $(f \cdot g)(x) = \sum_{k\geq 0} c_k x^k$, onde $c_k = \sum_{\substack{i+j=k \\ i,j\geq 0}} a_i b_j$.

Exemplo de adição e multiplicação de polinômios:

Sejam $f(x) = 1 - 2x + 3x^2$ e $g(x) = -4 - 5x + x^2 - 2x^3 + 3x^4$. Então, a adição $(f + g)(x) = -3 - 7x + 4x^2 - 2x^3 + 3x^4$ e, quanto a multiplicação $(f \cdot g)(x)$, obtemos que

$(f \cdot g)(x) = -4 + 3x - x^2 - 19x^3 + 10x^4 - 12x^5 + 9x^6$.

2.2 **Propriedades da adição e da multiplicação de polinômios**

Definidas dessa forma, as operações de adição e multiplicação de polinômios sobre K, gozam das seguintes propriedades para todo $f, g, h \in K[x]$.

1) Comutatividade: $f + g = g + f$ *e* $f \cdot g = g \cdot f$;

2) Associatividade: $(f + g) + h = f + (g + h)$ *e* $(f \cdot g) \cdot h = f \cdot (g \cdot h)$;

3) Distributividade: $f \cdot (g + h) = (f \cdot g) + (f \cdot h)$;

4) Existência do elemento neutro em relação à adição: sendo 0 o polinômio identicamente nulo, temos $f + 0 = f = 0 + f, \forall f \in$ K$[x]$, isto é, o polinômio identicamente nulo é o elemento neutro na operação de adição entre polinômios;

5) Existência de simétrico: dado um polinômio $f \in$ K$[x]$, existe um único polinômio $g \in$ K$[x]$ tal que $f + g = g + f = 0$, a saber $g = -f$. Portanto, se $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, então, $(-f)(x) = -a_0 - a_1 x - \cdots - a_n x^n$;

Observações:

i. A partir da propriedade 5, podemos definir a diferença entre dois polinômios $f, g \in$ K$[x]$, denotada por $f - g$ como sendo $f - g = f + (-g)$;

ii. Para $\alpha \in$ K e $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in$ K$[x]$, temos que

$\alpha . f = \alpha a_0 + \alpha a_1 x + \alpha a_2 x^2 + \cdots + \alpha a_n x^n$;

iii. A observação acima nos leva a $1 . f = f$, $\forall f \in \mathrm{K}[x]$. Portanto, o polinômio constante $1 \in \mathrm{K}$ é o elemento neutro da multiplicação de polinômios;

iv. Por simplicidade, passaremos a escrever o produto de polinômios $(f \cdot g)$, simplesmente por $fg, \forall f, g \in \mathrm{K}[x]$.

v. Embora um polinômio tenha sido apresentado como um objeto abstrato ao ser introduzido como um objeto do tipo $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$ sendo x chamado de indeterminada, pode se dar um sentido concreto ao referido objeto como segue: identificando $\alpha \in K$ com a sequência quase toda nula $\alpha = (\alpha, 0{,}0, \ldots, 0, \ldots)$, colocando x como a sequência quase toda nula $x = (0, 1, 0, \ldots, 0, \ldots)$ e tendo em vista as regras de adição e multiplicação que definem as sequências quase todas nulas que dão a soma e o produto de polinômios, vemos que, para qualquer sequência quase toda nula $(a_0, a_1, a_2, \ldots, a_n, \ldots)$ valem:

$\alpha(a_0, a_1, \ldots, a_n, \ldots) = (\alpha, 0{,}0, \ldots, 0, \ldots)(a_0, a_1, \ldots, a_n, \ldots) = (\alpha a_0, \alpha a_1, \ldots, \alpha a_n, \ldots)$,

$x^2 = x . x = (0{,}0, 1{,}0, \ldots, 0, \ldots)$,

$x^3 = x^2 . x = (0{,}0, 0{,}1, 0, \ldots, 0, \ldots)$,

. . . . . .

. . . . . .

. . . . . .

$x^i = (0{,}0, 0, 0, \ldots, 1{,}0, \ldots, 0, \ldots)$ com 1 na $(i+1) -$ ésima entrada e as demais entradas, zeradas. Consequentemente,

$(a_0, a_1, \ldots, a_n, \ldots) = (a_0, 0, \ldots) + (0, a_1, 0, \ldots) + \cdots + (0, \ldots, 0, a_n, 0, \ldots) \therefore$

$(a_0, a_1, \ldots, a_n, \ldots) = a_0(1, 0, \ldots) + a_1(0{,}1{,}0, \ldots) + \cdots + a_n(0, \ldots, 0{,}1{,}0, \ldots) \therefore$

$(a_0, a_1, a_2, \ldots, a_n, \ldots) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$

2.3 **Divisão de polinômios**[8]

Sejam $f(x), g(x) \in \mathrm{K}[x]$. Se existir $h(x) \in \mathrm{K}[x]$ tal que $f(x) = g(x)h(x)$, então dizemos que $f(x)$ é múltiplo de $g(x)$. Neste caso, se $g(x) \neq 0$, dizemos que $g(x)$ divide $f(x)$. Sempre é possível adicionar, subtrair e multiplicar polinômios. Todavia, o mesmo não

[8] cf. Hefez, pág. 112

ocorre com a divisão entre eles. Em outras palavras, dados polinômios $f(x), g(x) \in$ K$[x]\backslash\{0\}$, nem sempre é possível encontrar um polinômio $h(x) \in$ K$[x]$, tal que $f(x) = g(x)h(x)$. Por exemplo, dados $f(x) = 2x \; e \; g(x) = x^2$, não existe um polinômio $h(x) \in$ K$[x]$ de forma que $f(x) = g(x)h(x)$.

Enunciamos abaixo uma proposição e um teorema que auxiliarão no desenvolvimento deste assunto.

Proposição 2.3.1

Para $f, g \in$ K$[x]\backslash\{0\}$, sendo K um corpo ou o conjunto dos inteiros, temos:

i. $\partial(f+g) \leq max\{\partial f, \partial g\} \; se \; f+g \neq 0$;

ii. $fg \neq 0 \; e \; \partial(fg) = \partial f + \partial g$.

Prova de i.

Sejam $\partial f = n \;\; e \;\; \partial g = m$, com $f(x) = \sum_{k=0}^{n} a_k x^k$ e $g(x) = \sum_{k=0}^{m} b_k x^k$.

Se $m \neq n$ tomemos, sem perda de generalidade, $m < n$. Neste caso, temos que $(f+g)(x) = \sum_{k=0}^{m}(a_k + b_k)\, x^k + \sum_{k=m+1}^{n} a_k x^k \therefore \partial(f+g) = max\{\partial f, \partial g\}$ pois $a_n \neq 0$.

Se $m = n \; e \; f+g \neq 0$, então $a_n + b_n = 0 \; ou \; a_n + b_n \neq 0$.

No primeiro caso $\partial(f+g) < n = max\{\partial f, \partial g\}$.

No segundo, $\partial(f+g) = n = max\{\partial f, \partial g\}$. Em qualquer situação i. é válido.

Prova de ii.

Seja $0 \neq fg = \sum_{k\geq 0} c_k x^k$, onde $c_k = \sum_{\substack{i+j=k \\ i,j\geq 0}} a_i b_j$. No Lema 3.0.1 mostramos que se $k > m+n$, então $c_k = 0$. Por outro lado, $c_{m+n} = \sum_{\substack{i+j=m+n \\ i,j\geq 0}} a_i b_j = a_m b_n \neq 0$. Portanto, temos que $fg \neq 0 \; e \; \partial(fg) = m+n = \partial f + \partial g$.

O Teorema abaixo é válido para um corpo K pois, neste caso, $\beta \in$ K$, \beta \neq 0$ então temos que existe seu inverso $\beta^{-1} \in$ K. Este fato será utilizado na demonstração do teorema que se segue. Não obstante, é importante observar que, da prova de ii da proposição 3.3.1, concluímos que se f e g são polinômios com coeficientes em um corpo K e $fg = 0$ então $f = 0$ ou $g = 0$.

Teorema 2.3.2 (Teorema da Divisão Euclidiana)

Se $f, g \in \mathrm{K}[x]$, com $g \neq 0$, então existem únicos $q, r \in \mathrm{K}[x]$ tais que $f = gq + r$, onde $r = 0 \; ou \; 0 \leq \partial r < \partial g$.

Prova da Unicidade:

Suponhamos, por absurdo, que existam $q_1, q_2, r_1, r_2 \in \mathrm{K}[x]$ satisfazendo as condições do enunciado. Então, $f = gq_1 + r_1 = gq_2 + r_2 (*)$ com $r_i = 0$ ou $0 \leq \partial r_i < \partial g, i = 1,2$.

Analisando o caso em que um dos restos é nulo.

Suponhamos, sem perda de generalidade que $r_1 = 0$, então $r_2 = 0$ ou $r_2 \neq 0$. Em qualquer dos casos, de $(*)$ temos que $g(q_1 - q_2) = r_2 - r_1$. Logo, se $r_1 = 0$ e $r_2 = 0$, concluímos que $q_1 = q_2$, pois $g \neq 0$. Segue que $r_1 = r_2 = 0$ e $q_1 = q_2$. Por outro lado, se $r_2 \neq 0$, então de $(*)$ temos que $g(q_1 - q_2) = r_2$. Como $\partial g \leq \partial g + \partial(q_1 - q_2)$ segue, pela Proposição 3.3.1, que $\partial g \leq \partial g + \partial(q_1 - q_2) = \partial[g(q_1 - q_2)] = \partial r_2 < \partial g$, o que é um absurdo. Portanto, se $r_1 = 0 \Rightarrow r_2 = 0$ e recaímos no caso anterior.

Analisando o caso em que nenhum dos restos é nulo.

Novamente de $(*)$ temos que $g(q_1 - q_2) = r_2 - r_1$. Assim sendo, se $q_1 \neq q_2$, então $r_1 \neq r_2$. Neste caso, temos que:

$\partial g \leq \partial g + \partial(q_1 - q_2) = \partial\big(g(q_1 - q_2)\big) = \partial(r_2 - r_1) \leq max\{\partial r_1, \partial r_2\} < \partial g$ o que é uma contradição. Portanto, $q_1 = q_2 \Rightarrow r_1 = r_2$.

Prova da Existência:

Seja $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ onde b_m tem inverso $b_m^{-1} \in \mathrm{K}[x]$. Então, $\partial g = m$.

Se $f(x) = 0$, então basta tomarmos $q(x) = r(x) = 0$.

Se $f(x) \neq 0$, seja $n = \partial f$. Então, $n < m \; ou \; n \geq m$.

Se $n < m$, então basta tomarmos $q(x) = 0 \; e \; r(x) = f(x)$.

Se $n \geq m$, provamos por indução sobre $n = \partial f$.

Se $n = 0$, então $0 = n \geq m \geq 0 \Rightarrow m = 0$. Portanto, temos $f(x) = a_0$ e também que $g(x) = b_0$. Como $b_0^{-1} \in K[x]$, temos que $f(x) = a_0 b_0^{-1} g(x)$. Dessa forma, estabelecemos que $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.

Suponhamos agora que o resultado seja válido para polinômios com grau menor do que $n = \partial f$. Mostraremos que, neste caso, o resultado também é válido para $f(x)$.

Seja $h(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$. Neste caso, $h(x) = 0$ ou $h(x) \neq 0$. No primeiro caso, temos que $f(x) = a_n b_m^{-1} x^{n-m} g(x)$ e, dessa forma, tomamos $q(x) = a_n b_m^{-1} x^{n-m}$ e $r(x) = 0$. Se, no entanto, $h(x) \neq 0$, observemos que, pelo ítem ii da Proposição 3.3.1, o polinômio $a_n b_m^{-1} x^{n-m} g(x)$ tem grau n. Além disso, seu coeficiente líder é a_n. Consequentemente, $\partial h < n$ pois a_n também é coeficiente líder de $f(x)$. Pela hipótese de indução, existem $q_1(x)\ e\ r_1(x) \in \mathrm{K}(x)$ tais que $h(x) = q_1(x)g(x) + r_1(x)$; $r_1(x) = 0$ ou $0 \leq \partial r < \partial g$. Como, $f(x) = h(x) + a_n b_m^{-1} x^{n-m} g(x)$, então, temos que:
$f(x) = q_1(x)g(x) + r_1(x) + a_n b_m^{-1} x^{n-m} g(x)$.

Logo, segue que $f(x) = [q_1(x) + a_n b_m^{-1} x^{n-m}]g(x) + r_1(x)$. Sendo assim, basta tomarmos $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r(x) = r_1(x)$ para provarmos o resultado.

Observação:

Se $f(x), g(x), q(x)\ e\ r(x) \in \mathrm{K}[x]$ satisfazem as condições do Teorema 3.3.2, então chamamos $f(x)$ de dividendo, $g(x)$ de divisor, $q(x)$ de quociente e $r(x)$ de resto da divisão de $f(x)$ por $g(x)$.

2.4 **Raízes de um polinômio**

Dados $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathrm{K}[x]$ e $\beta \in \mathrm{K}$, definimos $f(\beta)$ como o elemento de K dado por $f(\beta) = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_n\beta^n$, onde as adições e multiplicações são efetuadas no corpo K. Dizemos que $\beta \in \mathrm{K}$ é uma raiz de $f(x) \in \mathrm{K}[x]$ se $f(\beta) = 0$.

Proposição 2.4.1

Seja $f(x) \in \mathrm{K}[x]\backslash\{0\}$. Então, $\beta \in \mathrm{K}$ é uma raiz de $f(x)$ se, e somente se, $(x - \beta)$ divide $f(x)$.

Prova:

Se β é uma raiz de $f(x)$ então, por definição, $f(\beta) = 0$. Por outro lado, pela divisão euclidiana de $f(x)$ por $x - \beta$, existem $q(x), r(x) \in \mathrm{K}[x]$ tais que $f(x) = q(x)(x - \beta) + r(x)$,

com $r(x) = 0$ ou $0 \leq \partial\big(r(x)\big) < \partial(x - \beta) = 1$.

No primeiro caso, isto é, $r(x) = 0$, temos que $(x - \beta) | f(x)$.

No segundo, isto é, $r(x) \neq 0$, então temos que $0 \leq \partial\big(r(x)\big) < 1$. Logo, $\partial\big(r(x)\big) = 0$. Portanto, $r(x) = r \in \mathrm{K}\backslash\{0\} \therefore f(x) = q(x)(x - \beta) + r$. Entretanto, isto é uma contradição, pois nesse caso, $0 = f(\beta) = q(\beta)(\beta - \beta) + r = r$. Logo, $r(x) = 0$ e, consequentemente temos que $x - \beta$ divide $f(x)$.

Reciprocamente, suponhamos que $x - \beta$ divide $f(x)$. Neste caso, pela divisão euclidiana, existe $q(x) \in \mathrm{K}[x]; f(x) = q(x)(x - \beta)$. Segue que $f(\beta) = q(\beta)(\beta - \beta) = 0$. Logo, β é uma raiz de $f(x)$. Isto conclui nossa demonstração.

Dizemos que $\beta \in \mathrm{K}$ é uma raiz de multiplicidade $m \in \mathbb{N}/\{0\}$ quando $(x - \beta)^m$ dividir $f(x)$ e $(x - \beta)^{m+1}$ não dividir $f(x)$ em $\mathrm{K}[x]$. Nesse caso, novamente pela divisão euclidiana, existe $q(x) \in \mathrm{K}[x]; f(x) = (x - \beta)^m q(x), q(\beta) \neq 0$. Denominamos β uma raiz simples de $f(x)$, se $m = 1$, e uma raiz múltipla de multiplicidade m, se $m \geq 2$. Independentemente da multiplicidade da raiz, se $\beta \in K$ é uma raiz de $f(x) \in \mathrm{K}[x]$, então $f(\beta) = 0$.

Observação:

Embora o conceito de raiz de um polinômio pareça estar dissociado do conceito de polinômio mais adiante, sob condições gerais, identificaremos polinômio com função polinomial. Neste caso, a raiz do polinômio será identificada com o zero da função.

Exemplos:

i. Se $f(x) = x - 2$, então 2 é uma raiz simples de f.

ii. Se $f(x) = (x + 3)^2(x^2 - 5x + 4) = (x + 3)^2(x - 1)(x - 4)$. Então -3 é uma raiz de multiplicidade 2 e 1 e 4, são raízes simples de $f(x)$.

iii. Se $f(x) = (x^2 + 1)^3(x^2 + x + 1)^4 = (x - i)^3(x + i)^3 \left(x + \frac{1+\sqrt{3}i}{2}\right)^4 \left(x - \frac{1-\sqrt{3}i}{2}\right)^4$.

Então $\pm i$ são raízes de multiplicidade 3 e $\frac{-1\pm\sqrt{3}i}{2}$ são raízes de multiplicidade 4 de $f(x)$.

Observação:

Decorre do acima exposto, que a soma das multiplicidades das raízes de um polinômio não nulo é menor ou igual ao grau desse polinômio.

2.5 **Método prático de divisão de polinômios**

Abaixo segue um método prático de divisão de polinômios. Ele é, na verdade, uma exemplificação prática da prova do Teorema 4.3.2 (Divisão Euclidiana entre polinômios), no que concerne à existência do quociente e do resto na divisão de polinômios.
Método da "Divisão Euclidiana"

1º Exemplo $\left(\partial f(x) < \partial g(x)\right)$:
$f(x) = 3x + 4\ e\ g(x) = x^2 - 2x - 5$ em $\mathbb{R}[x]$. Neste caso, não há o que fazer. Logo, temos que $f(x) = g(x) \times 0 + (3x + 4)$. Consequentemente, $q(x) = 0$ e $r(x) = 3x + 4$.

2º Exemplo $\left(\partial f(x) = \partial g(x)\right)$:
$f(x) = 3x^2 + 2x + 1\ e\ g(x) = x^2 - 2x - 5$ em $\mathbb{Q}[x]$.
Passo1:
Como os monômios de maior grau de $f(x)\ e\ g(x)$ são, respectivamente, $3x^2\ e\ x^2$, tomamos o quociente $q(x)$ como sendo o quociente da divisão deles, isto é, $3x^2 \div x^2 = 3$.
Passo 2:
Como $r(x) = f(x) - g(x).q(x)$, calculamos o resto $r(x)$
$r(x) = 3x^2 + 2x + 1 - (x^2 - 2x - 5\ ) \times 3\ \therefore$
$r(x) = 3x^2 + 2x + 1 - 3x^2 + 6x + 15\ \therefore$
$r(x) = 8x + 16$;
Passo 3:
Como $\partial r(x) = 1 < \partial g(x) = 2$, encerramos a divisão. Sendo assim temos que, o quociente é $q(x) = 3$ e o resto é $r(x) = 8x + 16$.
Veja o método prático abaixo:

$$\begin{array}{r|l} 3x^2 + 2x + 1 & x^2 - 2x - 5 \\ \hline -(3x^2 - 6x - 15) & 3 \\ \hline 8x + 16 & \end{array}$$

3º Exemplo $(\partial f(x) > \partial g(x))$:

$f(x) = 4x^4 - x^3 + 3x^2 - 2x + 5$ *e* $g(x) = x^2 - 2x - 5$ em $\mathbb{R}[x]$.

Passo 1:

Como os monômios de maior grau de $f(x)$ *e* $g(x)$ são, respectivamente, $4x^4$ *e* x^2, tomamos o quociente $q_1(x)$ como sendo o quociente da divisão deles, isto é, $4x^4 \div x^2 = 4x^2$.

Passo 2:

Como $r_1(x) = f(x) - g(x) \times q_1(x)$, calculamos o resto $r_1(x)$

$r_1(x) = 4x^4 - x^3 + 3x^2 - 2x + 5 - (x^2 - 2x - 5) \times 4x^2 \therefore$

$r_1(x) = 7x^3 + 23x^2 - 2x + 5;$

Passo 3:

Como $\partial r_1(x) = 3 > \partial g(x) = 2$, continuamos a divisão, dividindo $r_1(x)$ por $g(x)$, pois $r_1(x)$ não é o resto que satisfaz o Teorema da Divisão Euclidiana.

Passo 4:

Como os monômios de maior grau de $r_1(x)$ *e* $g(x)$ são, respectivamente, $7x^3$ *e* x^2, tomamos o quociente $q_2(x)$ como sendo o quociente da divisão deles, isto é, $7x^3 \div x^2 = 7x$.

Passo 5:

Como $r_2(x) = r_1(x) - g(x) \times q_2(x)$, calculamos o resto $r_2(x)$

$r_2(x) = 7x^3 + 23x^2 - 2x + 5 - (x^2 - 2x - 5) \times 7x \therefore$

$r_2(x) = 37x^2 + 33x + 5;$

Passo 6:

Como $\partial r_2(x) = 2 = \partial g(x)$, continuamos a divisão dividindo $r_2(x)$ por $g(x)$, pois $r_2(x)$ ainda não é o resto que procuramos.

Passo 7:

Os monômios de maior grau de $r_2(x)$ *e* $g(x)$ são, respectivamente, $37x^2$ *e* x^2, tomamos o quociente $q_3(x)$ como sendo o quociente da divisão deles, isto é, $37x^2 \div x^2 = 37$.

Passo 8:

Calculamos o resto $r_3(x) = r_2(x) - g(x) \times q_3(x) \therefore$

$r_3(x) = 37x^2 + 33x + 5 - (x^2 - 2x - 5) \times 37 \therefore$

$r_3(x) = 107x + 190.$

Passo 9:

Como $\partial r_3(x) = 1 < \partial g(x) = 2$ encerramos a divisão. Sendo assim, temos que $q(x) = q_1(x) + q_2(x) + q_3(x) = 4x^2 + 7x + 37$ *e* $r(x) = 107x + 190$.

Veja o método prático abaixo:

$$\begin{array}{r|l} 4x^4 - x^3 + 3x^2 - 2x + 5 & x^2 - 2x - 5 \\ \hline -(4x^4 - 8x^3 - 20x^2) & 4x^2 + 7x + 37 \\ \hline 7x^3 + 23x^2 - 2x + 5 & \\ -(7x^3 - 14x^2 - 35x) & \\ \hline 37x^2 + 33x + 5 & \\ -(37x^2 - 74x - 185) & \\ \hline 107x + 190 & \end{array}$$

2.6 **Algoritmo de Briot – Ruffini**

A Proposição 3.4.1 sugere que a divisão de um polinômio qualquer por polinômios da forma $(x - \beta)$ tem uma importância especial. Sendo assim, apresentamos o Algoritmo de Briot – Ruffini, o qual se constitui num outro método prático e bastante eficiente, para a determinação do quociente e do resto da divisão euclidiana de $f(x) \in \mathrm{K}[x]$ por $(x - \beta), \beta \in \mathrm{K}$. Antes de mostrarmos na prática o algoritmo, desenvolveremos sua justificativa.

Sejam $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathrm{K}[x]$; $a_n \neq 0$ *e* $\beta \in \mathrm{K}$. Sejam também $q(x), r(x) \in \mathrm{K}[x]$, respectivamente, o quociente e o resto da divisão euclidiana de $f(x)$ por $(x - \beta)$. Se $\partial r(x) \geq 1$, então podemos promover uma nova divisão euclidiana de $r(x)$ por $(x - \beta)$. Caso o resto dessa nova divisão continue tendo grau maior ou igual a 1, repetimos a mesma operação de divisão euclidiana sobre o novo resto e procedemos assim tantas vezes quantas forem necessárias, a fim de obtermos um resto r tal que $\partial r = 0$, isto é, $r \in \mathrm{K}$. Dessa forma, podemos afirmar que $f(x) = q(x)(x - \beta) + r$ onde temos que $\partial\big(q(x)\big) = n - 1$ *e* $r \in \mathrm{K}$.

Logo, $q(x) = q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + \cdots + q_1 x + q_0$. Portanto, segue que:

$f(x) = (q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + \cdots + q_1x + q_0)(x - \beta) + r \therefore$
$f(x) = q_{n-1}x^n + (q_{n-2} - \beta q_{n-1})x^{n-1} + \cdots + (q_0 - \beta q_1)x + (r - \beta q_0)$. Daí concluímos que:

$$\begin{cases} q_{n-1} = a_n \\ q_{n-2} - \beta q_{n-1} = a_{n-1} \\ q_{n-3} - \beta q_{n-2} = a_{n-2} \\ \vdots \\ q_1 - \beta q_2 = a_2 \\ q_0 - \beta q_1 = a_1 \\ r - \beta q_0 = a_0 \end{cases} \Rightarrow \begin{cases} q_{n-1} = a_n \\ q_{n-2} = a_{n-1} + \beta q_{n-1} \\ q_{n-3} = a_{n-2} + \beta q_{n-2} \\ \vdots \\ q_1 = a_2 + \beta q_2 \\ q_0 = a_1 + \beta q_1 \\ r = a_0 + \beta q_0 \end{cases}$$

A sequência de igualdades à direita acima explicitada é uma fórmula recursiva que permite calcular os coeficientes de $q(x)$, da maior potência para a menor, sucessivamente, a partir do valor inicial conhecido $q_{n-1} = a_n$. Os demais coeficientes $q_j, 0 \leq j \leq n-2$ são determinados, um após o outro, segundo o esquema $q_j = a_{j+1} + \beta q_{j+1}$.

	a_n	a_{n-1}	...	a_2	a_1	a_0
β	$a_n = q_{n-1}$	q_{n-2}	...	q_1	q_0	r
		$\downarrow$		$\downarrow$	$\downarrow$	$\downarrow$
		$a_{n-1} + \beta q_{n-1}$		$a_2 + \beta q_2$	$a_1 + \beta q_1$	$a_0 + \beta q_0$

Exemplo:

Vamos determinar o quociente e o resto da divisão euclidiana em $\mathbb{R}[x]$ do polinômio $f(x) = x^3 - 5x^2 + x + 4$ por $x + 3$ usando o algoritmo de Briot – Ruffini.

	1	-5	1	4
-3	-----	-3	24	-75
	1	-8	25	-71

Portanto, $r = -71\ e\ q(x) = x^2 - 8x + 25$. Logo, -3 não é raiz de $f(x)$ e, além disso, $f(x) = (x^2 - 8x + 25\ )(x + 3\ ) - 71$. Podemos então enunciar o algoritmo de Briot – Ruffini da seguinte forma:

A fim de dividir um polinômio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, com $a_n \neq 0$, pelo polinômio $x - \beta$, realize os seguintes passos abaixo descritos:

1º - Monte uma tabela com $(n + 2)$ colunas e 3 linhas;
2º - Preencha a 1ª linha, a partir da 2ª coluna, colocando um único número em cada coluna, os quais são os coeficientes de $f(x)$, em ordem decrescente dos graus dos monômios $a_i x^i$;
3º - Preencha a 1ª coluna na 2ª linha com o valor β;
4º - Conclua o preenchimento da 2ª coluna deixando - a em branco na 2ª linha e reproduzindo o valor a_n na 3ª linha;
5º - Conclua o preenchimento da tabela através das colunas, a partir da 3ª até a $(n + 2) -$ ésima coluna, da seguinte forma: primeiro, na 2ª linha, coloque o resultado do produto do número que está na 3ª linha da coluna anterior por β e depois, na 3ª linha, coloque o resultado da soma dos dois números que estão nesta mesma coluna nas linhas 1 e 2;
6º - O quociente $q(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ será formado, tomando os coeficientes $b_i, 0 \leq i \leq n - 1$, como sendo os números da 3ª linha obtidos pelas operações no passo anterior, da esquerda para a direita, a partir da 2ª coluna, onde o coeficiente do monômio de maior grau é o número da 2ª coluna e o de menor grau o da $(n + 1)$ - ésima coluna;
7º - O resto r_0 será o elemento que ocupa a última coluna na 3ª linha.

2.7 **A generalização do algoritmo de Briot - Ruffini**

Vamos generalizar o algoritmo de Briot – Ruffini de forma que o divisor $g(x)$ seja um polinômio de grau $m \geq 1$, onde $m \in \mathbb{N}$. Faremos isso começando com um polinômio $g(x)$ cujo coeficiente líder é $b_m = 1$. Caso o polinômio $g(x)$ tenha coeficiente líder $b_m = k \neq 1$, dividimos $f(x)$ por $\frac{1}{k}g(x)$ e tomamos o quociente da divisão de $f(x)$ por $g(x)$ como sendo $\frac{1}{k}q(x)$, onde $q(x)$ é o quociente de $f(x)$ por $\frac{1}{k}g(x)$. Sendo assim, a fim de dividir o polinômio dado por $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_n \neq 0$, pelo polinômio

dado por $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$, onde $\partial f(x) = n \geq \partial g(x) = m$, realize os passos abaixo. A fim de ilustrarmos o algoritmo, concomitante ao enunciado dos passos, realizamos a divisão de $f(x) = 2x^9 + 9x^8 - 10x^7 + 29x^6 - 4x^5 - 36x^4 + 10x^3 + 3x^2 - 7x + 17$ por $g(x) = x^4 + 5x^3 - 4x^2 + 3x - 2$.

1º Passo

Monte uma tabela com $(n + 2)$ colunas e $(m + 2)$ linhas;

No nosso exemplo, 11 colunas e 6 linhas.

2º Passo

Preencha a 1ª linha, a partir da 2ª coluna, colocando um único número em cada coluna. Esses números são os coeficientes de $f(x)$, em ordem decrescente dos graus dos monômios $a_ix^i, 0 \leq i \leq n$;

	2	9	-10	29	-4	-36	10	3	-7	17

3º Passo

Preencha a 1ª coluna, a partir da 2ª linha, com os coeficientes $b_i,\ 0 \leq i \leq m - 1$, com seus sinais trocados, isto é, com $(-b_i)$. Faça isso, colocando na 2ª linha $(-b_{m-1})$, na 3ª $(-b_{m-2})$ e assim sucessivamente até a $(m + 1)$ - ésima linha colocando $(-b_0)$;

	2	9	-10	29	-4	-36	10	3	-7	17
-5										
4										
-3										
2										

4º Passo

Conclua o preenchimento da 2ª coluna reproduzindo o valor $a_n(a_n \times 1)$ na última linha e deixando em branco as demais linhas dessa coluna;

	2	9	-10	29	-4	-36	10	3	-7	17
-5	---									
4	---									
-3	---									
2	---									
	2									

5º Passo

Conclua o preenchimento da 3ª coluna da seguinte forma: coloque na 2ª linha o produto do elemento da última linha da 2ª coluna pelo elemento que está na 2ª linha da primeira coluna $(a_n \times b_{m-1})$; em todas as demais linhas desta coluna, exceto na última, deixe sem preenchimento; na última linha, coloque o resultado da adição dos dois únicos números que se encontram, respectivamente, na 1ª e 2ª linhas desta coluna;

	2	9	-10	29	-4	-36	10	3	-7	17
-5	---	-10								
4	---									
-3	---									
2	---									
	2	-1								

6º Passo

Para $3 \leq j \leq n+2$, proceda da seguinte forma: em cada coluna j, preencha a última linha com o resultado da soma dos demais números dessa mesma coluna. Posteriormente, preencha a diagonal que começa na linha 2 da coluna $j+1$ e termina na linha $m+1$ da coluna $j+m-1$ colocando em cada linha $i, 2 \leq i \leq m+1$ dessa diagonal, o produto do número que se encontra na última linha da coluna j pelo coeficiente que se encontra na 1ª coluna da linha i. Repita esse processo até que seja preenchida a linha $m+1$ da coluna $n+2$.

No nosso exemplo, temos o seguinte:

	2	9	-10	29	-4	-36	10	3	-7	17
-5	---	-10	5	-15	-20	25	30			
4	---		8	-4	12	16	-20	-24		
-3	---			-6	3	-9	-12	15	18	
2	---				4	-2	6	8	-10	-12
	2	-1	3	4	-5	-6				

7º Passo

Na última linha, exceto na primeira coluna, todas as demais colunas que ficaram em branco após o passo anterior, devem ser preenchidas com a soma de todos os números da respectiva coluna. As demais células da tabela devem ficar em branco.

---	2	9	-10	29	-4	-36	10	3	-7	17
-5	---	-10	5	-15	-20	25	30	---	---	---
4	---	---	8	-4	12	16	-20	-24	---	---
-3	---	---	---	-6	3	-9	-12	15	18	---
2	---	---	---	---	4	-2	6	8	-10	-12
---	2	-1	3	4	-5	-6	14	2	1	5

8º Passo

O quociente $q(x) = q_{n-m}x^{n-m} + \cdots + q_1 x + q_0$ será formado, tomando os coeficientes $q_i, 0 \leq i \leq n-m,$ como sendo os números da última linha obtidos pelas operações no passo anterior, da esquerda para a direita, a partir da segunda coluna, onde o

coeficiente do monômio de maior grau é o número da 2ª coluna e o de menor grau, o da $(n-m+2)$- ésima coluna;

No nosso exemplo os coeficientes vão desde a 2ª até a 7ª coluna. Portanto, temos que $q(x) = 2x^5 - x^4 + 3x^3 + 4x^2 - 5x - 6$.

9º Passo

O resto desta divisão $r(x) = r_{m-1}x^{m-1} + r_{m-2}x^{m-2} + \cdots + r_2x^2 + r_1x + r_0$ será formado, tomando os coeficientes $r_i, 0 \leq i \leq m-1$, como sendo os números da última linha obtidos pelas operações no 6º passo, da esquerda para a direita, a partir da coluna número $(n-m+3)$, onde o coeficiente do monômio de maior grau é o número daquela coluna e o de menor grau, o da coluna $(n+2)$.

No nosso exemplo, as colunas vão desde a 8ª até a 11ª. Assim, temos que o resto é dado por: $r(x) = 14x^3 + 2x^2 + x + 5$.

Os passos 8 e 9 podem ser enunciados de forma mais simples, a saber:

Os números que aparecem na última linha da tabela, são os coeficientes das potências de x – em ordem decrescente – da esquerda para a direita, do quociente e do resto, sendo os primeiros $(n-m+1)$ números, os do quociente e os últimos m números, os do resto.

Se tivermos uma divisão por um polinômio não mônico, como por exemplo, o mesmo $f(x)$ do exemplo anterior, dividido por $g(x) = \frac{2}{3}x^4 + \frac{10}{3}x^3 - \frac{8}{3}x^2 + 2x - \frac{4}{3}$, então basta colocarmos em evidência o fator $\frac{2}{3}$ e executamos o algoritmo apresentado, entre $f(x)$ e o polinômio $g_1(x) = x^4 + 5x^3 - 4x^2 + 3x - 2$. Logo, $f(x) = q_1(x)g_1(x) + r(x)$ onde $q_1(x) = 2x^5 - x^4 + 3x^3 + 4x^2 - 5x - 6$ e o resto é $r(x) = 14x^3 + 2x^2 + x + 5$. Sendo assim, $f(x) = \frac{3}{2}q_1(x)\frac{2}{3}g_1(x) + r(x) = q(x)g(x) + r(x)$, sendo $q(x) = \frac{3}{2}q_1(x)$. Portanto, o quociente procurado é $q(x) = 3x^5 - \frac{3}{2}x^4 + \frac{9}{2}x^3 + 6x^2 - \frac{15}{2}x - 9$.

A ideia da demonstração de que esse algoritmo dá certo, é feita do mesmo modo que a demonstração do algoritmo de Briot – Ruffini. Dados os polinômios $f(x), g(x)$ com $\partial g = m$ e $\partial f = n$, $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{m} b_i x^i$ com $n \geq m \geq 1$, o Teorema 3.3.2 - Teorema da Divisão Euclidiana - nos garante a existência e unicidade de $q(x)$ e $r(x)$, onde grau do polinômio $q(x)$ é dado por $\partial q(x) = n - m$ e $r(x) = 0$ ou $\partial r(x) \leq m - 1$, de tal forma que tenhamos $f(x) = q(x)g(x) + r(x)$. Neste caso, tomemos os polinômios $q(x)$ e $r(x)$ como sendo $q(x) = \sum_{i=0}^{n-m} q_i x^i$ e $r(x) = \sum_{i=0}^{m-1} r_i x^i$. **A equação $\boldsymbol{f(x) = q(x)g(x) +}$**

$r(x)$ pode ser reescrita de forma matricial, a saber: $AY = B$. A matriz B é uma matriz de ordem $(n+1) \times 1$, onde sua única coluna é formada pelos coeficientes de $f(x)$ em ordem decrescente das potências de x. Da mesma forma, a matriz Y é uma matriz de mesma ordem que a matriz B, na qual sua única coluna é formada pelos coeficientes de $q(x)$ e $r(x)$, também em ordem decrescente das potências de x, começando pelos coeficientes de $q(x)$ e terminando pelos de $r(x)$. A matriz A, por sua vez, é uma matriz quadrada de ordem $(n+1)$. Trata-se de uma matriz triangular superior cujo determinante é $detA = (b_m)^{n-m+1}$, o qual é não nulo pois $b_m \neq 0$. Sendo assim, podemos afirmar que $\exists A^{-1}; Y = A^{-1}B$. O algoritmo de Briot – Ruffini e sua generalização, no entanto, é desenvolvido para $b_m = 1$. Isto implica que $detA = 1$. A solução Y desse sistema linear possível e determinado, é a prova do algoritmo.

No exemplo a seguir, por meio de um caso particular, justificamos a generalização do algoritmo de Briot – Ruffini. O caso geral é uma simples adaptação ao número de coeficientes dos polinômios envolvidos na divisão.

Sejam os polinômios $\begin{cases} f(x) = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \\ g(x) = x^3 + b_2x^2 + b_1x + b_0 \end{cases}$, com coeficientes em $\mathbb{C}$. Queremos encontrar $q(x)$ e $r(x)$ com coeficientes em $\mathbb{C}$ tais que tenhamos $f(x) = q(x)g(x) + r(x)$ com $r(x) = 0$ ou $\partial r(x) \leq 2$. Considerando que $r(x) = 0$ ou $\partial r(x) \leq 2$, $\partial f(x) = 5$ e $\partial g(x) = 3$ então, necessariamente, $\partial q(x) = 2$. Assim, podemos escrever que $q(x) = q_2x^2 + q_1x + q_0$. Além disso, as condições sobre $r(x)$ nos permitem expressá-lo como $r(x) = r_2x^2 + r_1x + r_0$. Portanto, a fim de encontrarmos a solução $q(x)$ e $r(x)$, basta que determinemos os coeficientes $q_2, q_1, q_0, r_2, r_1 \; e \; r_0$. Igualando os coeficientes dos dois lados da igualdade $f(x) = g(x)q(x) + r(x)$, obtemos:

$$\begin{cases} q_2 = a_5 \\ q_2b_2 + q_1 = a_4 \Rightarrow q_1 = a_4 - q_2b_2 \\ q_2b_1 + q_1b_2 + q_0 = a_3 \Rightarrow q_0 = a_3 - q_2b_1 - q_1b_2 \\ q_2b_0 + q_1b_1 + q_0b_2 + r_2 = a_2 \Rightarrow r_2 = a_2 - q_2b_0 - q_1b_1 - q_0b_2 \\ q_1b_0 + q_0b_1 + r_1 = a_1 \Rightarrow r_1 = a_1 - q_1b_0 - q_0b_1 \\ q_0b_0 + r_0 = a_0 \Rightarrow r_0 = a_0 - q_0b_0 \end{cases}$$

Observamos agora, que as soluções acima podem ser organizadas no seguinte dispositivo prático:

	a_5	a_4	a_3	a_2	a_1	a_0
$-b_2$	*					
$-b_1$	*	*				
$-b_0$	*	*	*			
	a_5					
	q_2					

	a_5	a_4	a_3	a_2	a_1	a_0
$-b_2$	*	$-q_2b_2$				
$-b_1$	*	*	$-q_2b_1$			
$-b_0$	*	*	*	$-q_2b_0$		
	a_5	$a_4 - q_2b_2$				
	q_2	q_1				

	a_5	a_4	a_3	a_2	a_1	a_0
$-b_2$	*	$-q_2b_2$	$-q_1b_2$			
$-b_1$	*	*	$-q_2b_1$	$-q_1b_1$		
$-b_0$	*	*	*	$-q_2b_0$	$-q_1b_0$	
	a_5	$a_4 - q_2b_2$	$a_3 - q_2b_1 - q_1b_2$			
	q_2	q_1	q_0			

	a_5	a_4	a_3	a_2	a_1	a_0
$-b_2$	*	$-q_2b_2$	$-q_1b_2$	$-q_0b_2$	*	*
$-b_1$	*	*	$-q_2b_1$	$-q_0b_2$	$-q_0b_1$	*
$-b_0$	*	*	*	$-q_2b_0$	$-q_1b_0$	$-q_0b_0$
	a_5	$a_4 - q_2b_2$	$a_3 - q_2b_1 - q_1b_2$	$a_2 - q_2b_0 - q_1b_1 - q_0b_2$	$a_1 - q_1b_0 - q_0b_1$	$a_0 - q_0b_0$
	q_2	q_1	q_0	r_2	r_1	r_0

2.8 **Função polinomial**

Dada a $(n+1)$ - upla ordenada de números complexos $(a_0, a_1, a_2, \dots, a_n)$, consideremos a função $f: \mathbb{C} \to \mathbb{C}$ dada por $f(x) = a_0 + a_1x + \cdots + a_nx^n$. A função f assim definida, é denominada **função polinomial associada a $(n+1)$ - upla ordenada dada.**

Na definição acima dizemos que $a_0, a_1, a_2, \dots, a_n$ são os coeficientes de f e $a_0, a_1x, a_2x^2, \dots, a_nx^n$ são chamados os termos de f.

Exemplos de Funções Polinomiais $f: \mathbb{C} \to \mathbb{C}$.

i. $f(x) = 1 - x + 2x^2 - 3x^3$;

ii. $g(x) = \sqrt{3} + \sqrt{5}x^2$;

iii. $h(x) = i + x$.

É claro que, neste caso, podemos estabelecer uma relação bijetora entre os polinômios de grau n em $\mathbb{C}$ e as funções polinomiais $f: \mathbb{C} \to \mathbb{C}$ com $(n+1)$ coeficientes. Para isso, basta associarmos a toda sequência quase toda nula $(a_0, a_1, a_2, \dots, a_n, 0, 0, 0, \dots)$ do polinômio $f(x) = a_0 + a_1x + \cdots + a_nx^n$ em $\mathbb{C}$, à $(n+1)$ - upla ordenada de números complexos $(a_0, a_1, a_2, \dots, a_n)$, a qual está associada à função polinomial $g(x) = a_0 + a_1x + \cdots + a_nx^n$. Esta relação não é apenas bijetora, ela preserva a álgebra e por isso, permite a identificação em $\mathbb{C}$ entre função polinomial e polinômios em $\mathbb{C}$ que é um corpo infinito. De uma forma mais geral, seja $\boldsymbol{\Gamma(p(x))(u)}$ a função, cujo domínio é o conjunto de todos os polinômios com coeficientes em um corpo infinito K e o contra - domínio é o conjunto das funções polinomiais em K, tal que a cada polinômio $p(x) = a_0 + a_1x + \cdots + a_nx^n$ a função Γ associa à função polinomial, de K em K, $\Gamma(p(x))(u) = a_0 + a_1u + \cdots + a_nu^n$. Definida dessa forma, é imediato provar que Γ é uma bijeção. Além disso, verificamos facilmente que tanto $\Gamma(p(x) + q(x)) = \Gamma(p(x)) + \Gamma(q(x))$, como $\Gamma(p(x)q(x)) = \Gamma(p(x))\Gamma(q(x))$. Logo, devido ao fato da bijeção Γ preservar tanto a adição quanto a multiplicação, quaisquer propriedades algébricas dos polinômios podem ser verificadas em funções polinomiais. Evidentemente, a recíproca é verdadeira. Sendo assim, em corpos infinitos, do ponto de vista algébrico, podemos identificar polinômios com funções polinomiais. Há corpos, no entanto, em que tal identidade não é possível ser estabelecida. A fim de demonstrarmos esta afirmação, tomemos o conjunto de todas as classes residuais módulo dois ($\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$), isto é, o conjunto denominado $\overline{k}$ onde $\overline{k} = \{x \in \mathbb{Z}; x \equiv k \bmod 2\}$, sendo $k = 0,1$. É sabido que $\mathbb{Z}_2$, munido das operações usuais $(+)$ e $(\cdot)$, satisfaz a todas as seis propriedades citadas em 2.3, as quais caracterizam um corpo.

Tabela com a operação adição $(+)$ em $\mathbb{Z}_2$

$(+)$	$\overline{0}$	$\overline{1}$

$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

Tabela com a operação multiplicação $(\cdot)$ em $\mathbb{Z}_2$

$(\cdot)$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Os polinômios $f, g\ e\ h$ com coeficientes em $\mathbb{Z}_2, f(x) = x, g(x) = x^2$ e $h(x) = x^3$ são claramente distintos entre si, pois suas respectivas sequências associadas são diferentes, a saber: $(\overline{0}, \overline{1}, \overline{0}, \overline{0}, \overline{0}, \ldots), (\overline{0}, \overline{0}, \overline{1}, \overline{0}, \overline{0}, \overline{0}, \ldots)$ e $(\overline{0}, \overline{0}, \overline{0}, \overline{1}, \overline{0}, \overline{0}, \overline{0}, \ldots)$. *Todavia, com o auxílio das tabelas acima, observamos que as funções polinomiais* $f, g, h: \mathbb{Z}_2 \to \mathbb{Z}_2$ *são idênticas pois têm o mesmo domínio e contra – domínio, além da mesma imagem para cada elemento do domínio*.

Em verdade, se ao invés de $\mathbb{Z}_2$, tomarmos $\mathbb{Z}_m$ – um corpo finito - onde m é qualquer número primo, poderemos apresentar exemplos semelhantes, nos quais a identidade entre polinômios e funções polinomiais, não existe. Não obstante, além da importância teórica para a matemática de se diferenciar polinômios de funções polinomiais, os conjuntos $\mathbb{Z}_m$ com m primo, adquiriram recentemente uma importância ainda maior. Isto se deve ao fato de que o método de criptografia mais usado em aplicações comerciais, é o RSA. Esse método se baseia em cálculo dos resíduos de potências envolvendo números primos.

3 **APLICAÇÕES DE POLINÔMIOS**

Neste capítulo, como indica seu título, **abordamos algumas situações práticas da utilização de polinômios**. Iniciamos pela própria matemática e, posteriormente, exemplificamos a ocorrência deles, tanto numa ciência da natureza – a Física – quanto em uma ciência humana, a Administração e ou Economia.

3.1 **Polinômios de Taylor**[9]

Seja f uma função com derivadas de ordem $k = 1, 2, 3, \dots, N, N \in \mathbb{N}$, em algum intervalo contendo a como um ponto interior. Então, para qualquer $n \in \mathbb{N}$, com $0 \leq n \leq N$, o polinômio de Taylor de ordem n gerado por f em a é o polinômio dado pela seguinte expressão: $P_n(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n$.Caso f seja não nula, tal polinômio tem grau menor ou igual a n, isto é, $0 \leq \partial P_n(x) \leq n$, pois $f^{(n)}(a)$ pode ser nula.

Exemplos:

i. A função $f: \mathbb{R} \to \mathbb{R}$; $f(x) = e^x$ gera o Polinômio de Taylor de ordem n, em torno do ponto $x = 0$, $P_n(x) = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n!}, n \in \mathbb{N}$.

ii. A função $g: \mathbb{R} \to \mathbb{R}$; $g(x) = \cos x$ gera o Polinômio de Taylor de ordem $2n$, em torno de $x = 0$, $P_{2n}(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} \dots + (-1)^n \frac{x^{2n}}{(2n)!}, n \in \mathbb{N}$.

iii. A função $h: \mathbb{R} \to \mathbb{R}$; $h(x) = \ln x$ gera o Polinômio de Taylor de ordem n, em torno de $x = 1, P_n(x) = (x-1) - \frac{(x-1)^2}{2} + \frac{(x-1)^3}{3} - \frac{(x-1)^4}{4} + \cdots + \frac{(-1)^{n-1}(x-1)^n}{n}, n \in \mathbb{N}$.

O teorema abaixo mostra que, sob certas circunstâncias, podemos aproximar funções através do Polinômio de Taylor, por elas gerados.

---

[9] cf. Thomas, págs. 54 e 57

3.2 **Teorema de Taylor**[9]

Se f e suas primeiras n derivadas $f', f'', \dots, f^{(n)}$ forem funções contínuas no intervalo fechado entre a e b e a derivada $f^{(n)}$ for derivável no intervalo aberto entre a e b, então existe um número c entre a e b, tal que:

$$f(b) = f(a) + f'(a)(b-a) + \cdots + \frac{f^{(n)}(a)}{n!}(b-a)^n + \frac{f^{(n+1)}(c)}{(n+1)!}(b-a)^{n+1}.$$

Se, no Teorema de Taylor, fixarmos a e substituirmos b por x, podemos apresentar uma outra versão do teorema, a saber: se f tem derivadas de todas as ordens em um intervalo aberto *I* contendo a, então para cada inteiro positivo n e para cada x em *I*, temos a seguinte expressão para a função $f(x) = f(a) + f'(a)(x-a) + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + R_n(x)$, onde o fator $R_n(x)$, usualmente denominado de resto de ordem n, é dado por $R_n(x) = \frac{f^{(n+1)}(c)}{(n+1)!}(x-a)^{n+1}$, para algum número $c \in (a, x)$.[10]

Dessa forma, temos que $f(x) = P_n(x) + R_n(x)(*)$. A função $R_n(x)$ é determinada pelo valor da $(n+1) -$ ésima derivada $f^{(n+1)}$ no ponto c a qual, por sua vez, depende tanto de a quanto de x. Consequentemente, para qualquer valor de n que desejarmos, a equação $(*)$ nos oferece tanto uma aproximação polinomial de f, de ordem n, quanto uma fórmula para o erro envolvido no uso daquela aproximação sobre o intervalo *I*.

3.3 **Determinando polinômios a partir de pontos do plano**

Seja o conjunto $A = \{(x_i, y_i) \in \mathbb{R}^2; 0 \leq i \leq n, i \in \mathbb{N} \ e \ x_i \neq x_j \ \forall i \neq j\}$. Tomemos um polinômio genérico $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ onde os coeficientes a_i são desconhecidos. Substituindo os elementos de A em $p(x)$ e impondo a condição de $p(x_i) = y_i$, temos o seguinte sistema:

[10] cf. Thomas, pág. 58

$$\begin{cases} a_0 + a_1x_0 + a_2x_0^2 + \cdots + a_nx_0^n = y_0 \\ a_0 + a_1x_1 + a_2x_1^2 + \cdots + a_nx_1^n = y_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. \\ a_0 + a_1x_n + a_2x_n^2 + \cdots + a_nx_n^n = y_n \end{cases}.$$

Tal sistema pode ser escrito sob forma matricial como segue:

$XA = Y, X = \begin{pmatrix} 1\ x_0\ \ x_0^2\ \ \ldots\ldots\ x_0^n \\ 1\ x_1\ \ x_1^2\ \ \ldots\ldots\ x_1^n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 1\ x_n\ \ x_n^2\ \ \ldots\ldots\ x_n^n \end{pmatrix}, A = \begin{pmatrix} a_0 \\ a_1 \\ \ldots. \\ a_n \end{pmatrix} e\ Y = \begin{pmatrix} y_0 \\ y_1 \\ \ldots. \\ y_n \end{pmatrix}$. Por outro lado, o determinante da matriz X é dado por:

$det \begin{pmatrix} 1\ x_0\ \ x_0^2\ \ \ldots\ldots\ x_0^n \\ 1\ \ x_1\ \ x_1^2 \ldots\ \ldots\ x_1^n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 1\ x_n\ \ x_n^2\ \ \ldots\ldots\ x_n^n \end{pmatrix} = \prod_{0\leq i<j<n+1}(x_j - x_i)$. Este, por sua vez, é não nulo pois trata-se do determinante de uma matriz de Vandermonde[11]. Logo, os coeficientes de $p(x)$ são univocamente determinados bastando para isso, resolver a equação matricial $A = X^{-1}Y$. O polinômio $p(x)$ resultante desse processo, é conhecido como Polinômio de Interpolação de Lagrange. Ele pode ser expresso como sendo $p(x) = \sum_{j=0}^{n} p_j(x)$, onde cada parcela do somatório é dada por $p_j(x) = y_j \frac{(x-x_0)(x-x_1)\ldots\overline{(x-x_j)}\ldots(x-x_{n-1})(x-x_n)}{(x_j-x_0)(x_j-x_1)\ldots\overline{(x_j-x_j)}\ldots(x_j-x_{n-1})(x_j-x_n)}$, sendo que os termos sob barras $\overline{(x-x_j)}$ e $\overline{(x_j-x_j)}$, para cada $0 \leq j \leq n$, são omitidos.[12]

3.4 **Exemplos de aplicação de polinômios**

i. Em cinemática, quando estudamos uma partícula em movimento com aceleração constante, utilizamos basicamente duas equações, a saber: $s(t) = s_0 + v_0t + \frac{1}{2}at^2$ e, também, $e\ v(t) = v_0 + at,$[13] onde as funções $s(t)$ e $v(t)$ são, respectivamente, a posição e a velocidade da partícula no instante t e $a \neq 0,$ é a aceleração constante com a qual ela se

[11] cf. Poole, pág. 263
[12] cf. Hefez, pág. 131
[13] cf. Tipler, págs. 29 e 84

move. Portanto, podemos afirmar que tanto $s(t)$ quanto $v(t)$ são polinômios, respectivamente de 2º e 1º graus, na variável t.

ii. Se um corpo é lançado obliquamente (θ^0com o eixo horizontal) com velocidade v_0, sendo a única força atuante nele, o seu próprio peso, então sua posição é dada por $\big(x(t), y(t)\big) = \Big(x_0 + v_0 \cos\theta\, t, y_0 + v_0 \operatorname{sen}\theta\, t - \frac{1}{2} g t^2\Big)$[13] onde (x_0, y_0) é a posição inicial do corpo, t é o tempo e g é a aceleração da gravidade. Portanto, o deslocamento horizontal é dado por um polinômio de primeiro grau em t. O deslocamento vertical é representado por um polinômio de segundo grau em t.

iii. É relativamente comum um administrador de empresas, decidir sobre a quantidade de produtos a ser produzida numa fábrica, baseado (não exclusivamente) no seguinte modelo:

$p\colon [0, \infty[\to \mathbb{R};\ p(x) = a - bx$ é a função demanda, representando o preço de mercado do produto x que o consumidor está disposto a pagar, sendo $a, b \in \mathbb{R}_+, a > b$ e x a quantidade de produtos consumidos;

$R\colon [0, \infty[\to \mathbb{R}; R(x) = p(x)x = (a - bx)x$ é a função receita;

$C\colon [0, \infty[\to \mathbb{R};\ C(x) = m + nx$ é a função custo de produção do produto x, sendo $m, n \in \mathbb{R}_+$onde m representa o custo fixo da empresa ou do produto e n o custo por unidade x produzida;

Dessa forma, se $L\colon [0, \infty[\to \mathbb{R}$ é a função lucro do produto x, então temos que o lucro é dado por: $L(x) = R(x) - C(x) \therefore L(x) = -bx^2 + (a - n)x - m$.

Do ponto de vista comercial, a função lucro acima indica que só é válido atuar nesse mercado se $(a - n)^2 - 4bm > 0$, pois desta forma, há um intervalo para x (produto consumido) em que $L(x) > 0$. Neste caso, o lucro máximo será obtido se $x = \frac{a-n}{2b}$ é a quantidade de produtos produzidos e vendidos.

Também neste exemplo, trabalhamos com um polinômio de segundo grau.

4 FATORAÇÃO DE POLINÔMIOS

Neste capítulo desenvolveremos o Teorema da Fatoração Única nos corpos $\mathbb{C}$, $\mathbb{R}$ e $\mathbb{Q}$ e no anel $\mathbb{Z}$. Abordaremos assim, um dos aspectos centrais do tema polinômios, a saber sua fatoração. Além disso, outra importante contribuição ao ensino deste tema será apresentada. Trata-se das raízes racionais para polinômios com coeficientes inteiros. Apesar de sua importância, esses resultados apresentados particularmente, nas Proposições 4.4.1 e 4.4.2, frequentemente são desprezados nas escolas básicas. Esse fato ocorre, seja em função da pouca importância que se dá ao ensino de polinômios no ensino básico, seja pelo seu desconhecimento por parte dos professores.

Antes de abordarmos a fatoração de polinômios sobre os conjuntos de números Complexos, Reais, Racionais e Inteiros, vamos enunciar o Teorema Fundamental da Álgebra além de introduzir e desenvolver dois conceitos importantes. Esses são passos necessários para nos auxiliar em nosso objetivo final, que é a fatoração de polinômios naqueles conjuntos numéricos. Os conceitos sobre os quais nos referimos, são os de polinômios irredutíveis e polinômios conjugados.

Teorema 4.0.1 (Teorema Fundamental da Álgebra)[14]

Todo polinômio não constante com coeficientes complexos tem uma raiz complexa.

Polinômios Irredutíveis[14]

Sejam K um corpo e $f(x) \in \mathrm{K}[x] \backslash \mathrm{K}$. Dizemos que $f(x)$ é um polinômio irredutível em $\mathrm{K}[x]$ se, sempre que $f(x) = g(x)h(x)$, com $g(x), h(x) \in \mathrm{K}[x]$, então $g(x)$ ou $h(x)$ é um polinômio constante não nulo. Caso contrário, chamamos o polinômio $f(x)$ de não irredutível ou redutível em $\mathrm{K}[x]$.

[14] cf. Hefez, págs. 136 e 192

Proposição 4.0.2

Se $f(x) \in \mathrm{K}[x]$ é um polinômio de grau 1, então $f(x)$ é irredutível.

Prova:

Se $\partial f(x) = 1$, então $f(x) = ax + b$ onde $a, b \in \mathrm{K}$ com $a \neq 0$. Logo, reescrevendo $f(x)$ como sendo $ax + b = g(x)h(x)$, com $g(x), h(x) \in \mathrm{K}[x]$, temos que $g(x)\ e\ h(x)$ são não nulos e que $1 = \partial(ax + b) = \partial g(x) + \partial h(x)$. Segue que uma das duas afirmações seguintes é verdadeira: $\partial g(x) = 1\ e\ \partial h(x) = 0 \Rightarrow h(x) = \gamma \in \mathrm{K}/\{0\}$ ou $\partial g(x) = 0\ e\ \partial h(x) = 1 \Rightarrow g(x) = \delta \in \mathrm{K}/\{0\}$. Em qualquer um dos casos, temos um polinômio constante não nulo. Isto prova a proposição.

Observações:

i. Ao verificarmos se um polinômio é irredutível ou não, é fundamental observarmos sobre qual conjunto $\mathrm{K}[x]$ o polinômio se refere. Como exemplo, o polinômio de segundo grau expresso por $x^2 - 3 = \left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right)$ em $\mathbb{R}[x]$ é redutível. Todavia, $x^2 - 3$ em $\mathbb{Q}[x]$ não é redutível;

ii. Dado um polinômio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathrm{K}[x]$ tal que $\partial f(x) = n \geq 1$, é fácil perceber que $f(x)$ é irredutível se, e somente se, o polinômio mônico $p(x) = x^n + {a_n}^{-1}a_{n-1}x^{n-1} + \cdots + {a_n}^{-1}a_1 x + {a_n}^{-1}a_0$ for irredutível. Portanto, para determinarmos todos os polinômios irredutíveis de $\mathrm{K}[x]$, basta determinarmos os polinômios irredutíveis mônicos.

Conjugados

Seja $z \in \mathbb{C}; z = a + bi$ com $a, b \in \mathbb{R}$ e $i = \sqrt{-1}$. Dizemos que $\overline{z} = a - bi$ é o conjugado de z.

A conjugação de $z \in \mathbb{C}$ tem as seguintes propriedades:

i. $\overline{z} = 0 \Leftrightarrow z = 0$;

ii. $\overline{\overline{z}} = z, \forall\ z \in \mathbb{C}$;

iii. $\overline{z} = z \Leftrightarrow z \in \mathbb{R}$;

iv. $\overline{z \pm w} = \overline{z} \pm \overline{w}$;

v. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$;

vi. se $z \neq 0$, então $\overline{z^{-1}} = (\overline{z})^{-1}$;

vii. Como $\frac{z+\overline{z}}{2} = \frac{(a+bi)+(a-bi)}{2} = a$ e $\frac{z-\overline{z}}{2i} = \frac{(a+bi)-(a-bi)}{2i} = b$, temos que $\mathrm{Re}(z) = \frac{z+\overline{z}}{2}$ e $\mathrm{Im}(z) = \frac{z-\overline{z}}{2i}$. Portanto, $\mathrm{Re}(z)$ e $\mathrm{Im}(z)$ são chamadas, respectivamente, de parte real e parte imaginária de z;

viii. $z\overline{z} = a^2 + b^2 = |z|^2$.

Polinômios Conjugados[15]

Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$. O polinômio conjugado de $f(x)$ é definido por $\bar{f}(x) = \bar{a}_n x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_1 x + \bar{a}_0$, onde $\bar{a}_j$ é o conjugado de $a_j, j = 0, 1, \ldots, n$.

Proposição 4.0.3[15]

Sejam $f(x), g(x), h(x) \in \mathbb{C}[x]$. A conjugação tem as seguintes propriedades:

I. Se $f(x) = g(x) + h(x)$, então $\bar{f}(x) = \bar{g}(x) + \bar{h}(x)$;

II. Se $f(x) = g(x)h(x)$, então $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$;

III. $\bar{f}(x) = f(x) \Leftrightarrow f(x) \in \mathbb{R}[x]$;

IV. Se $\beta \in \mathbb{C}$, então $\bar{f}(\overline{\beta}) = \overline{f(\beta)}$.

Sejam $f(x), g(x)$ *e* $h(x)$ tais que $f(x) = \sum_{j=0}^{r} a_j x^j$, $g(x) = \sum_{j=0}^{m} b_j x^j$ *e* $h(x) = \sum_{j=0}^{n} c_j x^j$.

Prova de I:

a) Suponhamos $m = n$. Assim, como $f(x) = g(x) + h(x)$, segue que $r \leq m$ e $\forall j \in \mathbb{N}$, $0 \leq j \leq m, a_j = b_j + c_j \Rightarrow \bar{a}_j = \overline{b_j + c_j} = \bar{b}_j + \bar{c}_j \Rightarrow \bar{f}(x) = \bar{g}(x) + \bar{h}(x)$.

b) Se $m \neq n$. Neste caso suponhamos, sem perda de generalidade, que $m > n$ e, portanto, $r = m$. Então, como $f(x) = g(x) + h(x)$ temos que:

[15] cf. Hefez, pág. 137 e 138

$\sum_{j=0}^{m} a_j x^j = \sum_{j=0}^{m} b_j x^j + \sum_{j=0}^{n} c_j x^j \Rightarrow$

$\sum_{j=0}^{m} a_j x^j = \sum_{j=0}^{n} b_j x^j + \sum_{n+1}^{m} b_j x^j + \sum_{j=0}^{n} c_j x^j = \sum_{j=0}^{n} (b_j + c_j) x^j + \sum_{n+1}^{m} b_j x^j.$

Logo, $a_j = \begin{cases} b_j + c_j, 0 \leq j \leq n \\ b_j, n+1 \leq j \leq m \end{cases} \Rightarrow \overline{a_j} = \begin{cases} \overline{b_j} + \overline{c_j}, 0 \leq j \leq n \\ \overline{b_j}, n+1 \leq j \leq m \end{cases} \Rightarrow \bar{f}(x) = \bar{g}(x) + \bar{h}(x).$

Prova de II:

Se $f(x) = g(x)h(x)$ então, segue que $a_j = \sum_{\lambda+\mu=j} b_\lambda c_\mu, 0 \leq j \leq r$. Logo, temos que o conjugado $\bar{a}_j = \overline{\sum_{\lambda+\mu=j} b_\lambda c_\mu} = \sum_{\lambda+\mu=j} \overline{b_\lambda c_\mu} = \sum_{\lambda+\mu=j} \bar{b}_\lambda \bar{c}_\mu \Rightarrow \bar{f}(x) = \bar{g}(x)\bar{h}(x)$.

Prova de III:

$\bar{f}(x) = f(x) \Leftrightarrow \bar{a}_j = a_j, \forall j \in \mathbb{N};\ 0 \leq j \leq r \Leftrightarrow a_j \in \mathbb{R}, \forall j \in \mathbb{N};\ 0 \leq j \leq r \Leftrightarrow f(x) \in \mathbb{R}.$

Prova de IV:

Se $\beta \in \mathbb{C}$ então $\bar{f}(\bar{\beta}) = \sum_{j=0}^{r} \bar{a}_j \bar{\beta}^j = \sum_{j=0}^{r} \overline{a_j \beta^j} = \overline{\sum_{j=0}^{r} a_j \beta^j} = \overline{f(\beta)}$.

Corolário 4.0.4[16]: Seja $\beta \in \mathbb{C}$ uma raiz de $f(x) \in \mathbb{C}[x]$ de multiplicidade m. Então $\bar{\beta}$ é uma raiz de $\bar{f}(x)$ com multiplicidade m.

Prova:

Seja $\beta \in \mathbb{C}$ uma raiz de $f(x) \in \mathbb{C}[x]$ de multiplicidade m. Então, tem-se que:

$f(x) = (x-\beta)^m q(x)$ com $q(\beta) \neq 0$.

Do ítem II da Proposição 4.0.3 temos que $\bar{f}(x) = \overline{(x-\beta)^m}\bar{q}(x) = \left(\overline{x-\beta}\right)^m \bar{q}(x)(*)$. Por outro lado, temos que $\left(\overline{x-\beta}\right)^m = \left(x-\overline{\beta}\right)^m$. Portanto, na equação acima $(*)$ temos que $\bar{f}(x) = \left(x-\overline{\beta}\right)^m \bar{q}(x) \Rightarrow \bar{f}(\overline{\beta}) = 0$. Além disso, pelo ítem IV da mesma proposição 4.0.3, $\bar{q}(\bar{\beta}) = \overline{q(\beta)} \neq \bar{0} = 0$. Logo, $\bar{\beta}$ é uma raiz de $\bar{f}(x)$ com multiplicidade m.

Proposição 4.0.5[16]

Seja $f(x) \in \mathbb{R}[x]$. Se $\beta \in \mathbb{C}$ é uma raiz de $f(x)$ com multiplicidade m, então $\bar{\beta}$ também é raiz de $f(x)$ com multiplicidade m.

Prova:

Se $f(x) \in \mathbb{R}[x]$, temos pelo ítem III da Proposição 4.0.3 que $\bar{f}(x) = f(x)$. Logo, pelo corolário anterior, $\bar{\beta}$ também é raiz de $f(x)$ com multiplicidade m.

[16] cf. Hefez, pág. 139

Corolário 4.0.6[16]: Seja o polinômio $f(x) \in \mathbb{R}[x]$. Sendo assim, são válidas as seguintes afirmações:

a) As raízes complexas não reais de $f(x)$ ocorrem aos pares (cada raiz com a sua conjugada).
b) Todo polinômio $f(x)$ de grau ímpar tem, pelo menos, uma raiz real.

Prova de a):

Sejam $f(x) \in \mathbb{R}[x]$ e $\beta \in \mathbb{C}\backslash\mathbb{R}$ uma raiz de $f(x)$ com multiplicidade m. Então $\overline{\beta} \neq \beta$ e, pela proposição anterior, $\overline{\beta} \in \mathbb{C}\backslash\mathbb{R}$ também é raiz de $f(x)$ com multiplicidade m.

Prova de b):

Seja $f(x) \in \mathbb{R}[x]$ um polinômio de grau ímpar. Então $f(x)$ é um polinômio não constante pois $\partial f(x) \geq 1$. O Teorema Fundamental da Álgebra (TFA), garante a existência de ao menos uma raiz de $f(x)$. Portanto, $f(x)$ tem raiz complexa e não real ou tem apenas raízes reais. Se $f(x)$ tiver apenas raízes reais, não há nada mais a provar. Suponhamos, no entanto, que $f(x)$ tenha raízes não reais. Sejam $\beta_i \in \mathbb{C}\backslash\mathbb{R}\, e\, m_i \in \mathbb{N}, 0 \leq i \leq n$ essas raízes e suas respectivas multiplicidades. Então pelo ítem a) deste corolário, tais raízes aparecem em pares, associadas respectivamente a $\overline{\beta_i} \in \mathbb{C}\backslash\mathbb{R}, 0 \leq i \leq n$ com as mesmas multiplicidades. Sendo assim, temos que $f(x) = \sum_{i=1}^{n}(x-\beta_i)^{m_i}\left(x-\overline{\beta_i}\right)^{m_i} q(x)$, onde $q(x) \in \mathbb{R}[x]$ é um polinômio tal que $q(\beta_i)q\left(\overline{\beta_i}\right) \neq 0$ para qualquer $0 \leq i \leq n$. Se $\partial q(x) = 0$ então $\partial f(x) = 2m_i$ o que seria um absurdo, pois $\partial f(x)$ é ímpar. Logo $\partial q(x) \geq 1$ e, consequentemente, $q(x)$ é um polinômio não constante. Novamente pelo TFA, existe ao menos uma raiz β de $q(x)$. Uma vez que sabemos que $q(\beta) \neq 0, \forall \beta \in \mathbb{C}\backslash\mathbb{R}$, concluímos que $\beta \in \mathbb{R}$. Isto conclui a prova do corolário.

4.1 **Fatoração única de polinômios sobre $\mathbb{C}$**

As proposições abaixo mostram que se $f(x) \in \mathbb{C}[x]$, então $f(x)$ sempre pode ser fatorado, isto é, expresso através de produtos. Além disso, elucidam a respeito dos polinômios irredutíveis em $\mathbb{C}[x]$.

Proposição 4.1.1

Seja $f(x) \in \mathbb{C}[x]$; $\partial f(x) = n \geq 1$. Então existem $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{C}$, não necessariamente distintos, e $a \in \mathbb{C}\backslash\{0\}$ tais que $f(x) = a(x-\beta_1)(x-\beta_2)\ldots(x-\beta_n)$.

Prova por indução sobre o grau de $f(x)$:

Se $\partial f(x) = n = 1$, então $f(x) = ax + b$; $a, b \in \mathbb{C}$ e $a \neq 0$. Logo, tem-se que o polinômio $f(x) = a(x-\beta_1), \beta_1 = -a^{-1}b$.

Suponhamos o resultado válido para polinômios de grau n, sendo $n \in \mathbb{N}\backslash\{0\}$. Neste caso, seja $f(x) \in \mathbb{C}[x]$; $\partial f(x) \geq n+1$. Pelo Teorema Fundamental da Álgebra, sabemos que $f(x)$ tem uma raiz $\beta \in \mathbb{C}$. Sendo assim, pela Proposição 2.4.1, temos que $f(x) = q(x)(x-\beta)$, para algum $q(x) \in \mathbb{C}[x]$ e $\partial q(x) = n$. Por hipótese de indução, existem $a, \beta_1, \beta_2, \ldots, \beta_n \in \mathbb{C}, a \neq 0$ tais que: $q(x) = a(x-\beta_1)(x-\beta_2)\ldots(x-\beta_n)$. Logo, o polinômio $f(x)$ pode ser expresso como $f(x) = a(x-\beta_1)(x-\beta_2)\ldots(x-\beta_n)(x-\beta)$.

Tomando $\beta_{n+1} = \beta$, obtemos o resultado da proposição.

Proposição 4.1.2

O polinômio $f(x) \in \mathbb{C}[x]$ é irredutível se, e somente se, ele é de grau 1.

Prova:

A proposição 4.0.2 já garante que se $\partial f(x) = 1$ então ele é irredutível.

Reciprocamente, suponhamos que $\partial f(x) \geq 2$. Pelo Teorema Fundamental da Álgebra, $\exists\, \beta \in \mathbb{C}$ tal que $f(\beta) = 0$ pois como $\partial f(x) \geq 2 \Rightarrow f(x)$ é não constante. Segue, da Proposição 2.4.1, que $\exists\, q(x) \in \mathbb{C}[x]$ tal que $f(x) = q(x)(x-\beta)$. Portanto, $\partial q(x) + 1 \geq 2 \Rightarrow \partial q(x) \geq 1$. Consequentemente, $f(x)$ não é irredutível.

Observações:

i. Obviamente que, na Proposição 4.1.1, a é o coeficiente líder de $f(x)$. Após uma reordenação das raízes de $f(x)$, caso seja necessário, podemos supor que $\beta_1, \beta_2, \ldots, \beta_s$, onde $1 \leq s \leq n$, β_j ocorre com multiplicidade r_j para cada $j = 1, 2, \ldots, s$. Sendo assim, temos que $f(x) = a(x-\beta_1)^{r_1}(x-\beta_2)^{r_2}\ldots(x-\beta_s)^{r_s}$, onde a soma $r_1 + r_2 + \cdots + r_s = n$. Portanto, podemos afirmar que em $\mathbb{C}[x]$ todo polinômio de grau

$n \geq 1$ tem exatamente n raízes, contadas com as suas multiplicidades, isto é, não necessariamente distintas;

ii. Como consequência do resultado expresso na observação acima, poderíamos reenunciar o Teorema Fundamental da Álgebra da seguinte forma: "Todo polinômio $f(x)$ com coeficientes complexos e grau $n \geq 1$, se escreve de maneira única, a menos da ordem dos fatores, como $f(x) = a(x-\beta_1)^{r_1}(x-\beta_2)^{r_2} \ldots (x-\beta_s)^{r_s}$, onde $a \in \mathbb{C}\backslash\{0\}$ é o coeficiente líder de $f(x), \beta_1, \beta_2, \ldots, \beta_s$ são números complexos distintos e $r_1, r_2, \ldots, r_s$ são inteiros positivos tais que $r_1 + r_2 + \ldots + r_s = n$."

4.2 **Fatoração única de polinômios sobre $\mathbb{R}$**

Proposição 4.2.1

Seja o polinômio $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$. Se $\Delta = b^2 - 4ac < 0$, então $f(x)$ é irredutível.

Prova:

Suponhamos, por absurdo, que $f(x)$ seja redutível. Neste caso, $f(x)$ é divisível por polinômios do primeiro grau em $\mathbb{R}[x]$. Portanto, temos que:

$f(x) = (\alpha x + \beta)(\gamma x + \delta)$; $\alpha\gamma \neq 0 \Rightarrow x = -\frac{\beta}{\alpha}$ e $x = -\frac{\delta}{\gamma}$ são raízes de $f(x)$. Todavia, isto é uma contradição com o fato de que $\Delta < 0$.

Proposição 4.2.2

Os polinômios mônicos irredutíveis em $\mathbb{R}[x]$ são da forma $x - a, a \in \mathbb{R}$, ou então da forma $x^2 + bx + c$, com $b^2 - 4c < 0$.

Prova:

A Proposição 4.0.2 já afirma que os polinômios $x - a, a \in \mathbb{R}$, são irredutíveis em $\mathbb{R}$ (são irredutíveis em $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$).

A Proposição 4.2.1, por sua vez, garante que os polinômios $x^2 + bx + c$, com $b^2 - 4c < 0$ são irredutíveis em $\mathbb{R}$.

Suponhamos que $f(x)$ seja um polinômio em $\mathbb{R}[x]$ tal que $\partial f(x) > 2$. Seja $\beta \in \mathbb{C}$ uma raiz de $f(x)$. Temos dois casos a considerar: $\beta \in \mathbb{R}$ ou $\beta \in \mathbb{C}\backslash\mathbb{R}$.

Caso 1:

Se $\beta \in \mathbb{R}$, então $(x-\beta)$ divide $f(x)$ em $\mathbb{R}[x]$. Logo, $f(x)$ é redutível em $\mathbb{R}[x]$, pois $\exists\, q(x) \in \mathbb{R}[x];\ f(x) = q(x)(x-\beta) \Rightarrow \partial q(x) + 1 = \partial f(x) > 2 \therefore \partial q(x) > 1$. Segue, portanto, que $f(x)$ é redutível em $\mathbb{R}[x]$.

Caso 2:

Se $\beta \in \mathbb{C}\backslash\mathbb{R}$, então $\beta \neq \bar{\beta}\ e\ \bar{\beta}$ também é raiz de $f(x)$, pelo Corolário 4.04. Logo, $(x-\beta)\left(x-\bar{\beta}\right)$ divide $f(x)$ em $\mathbb{C}[x]$. Todavia, $(x-\beta)\left(x-\bar{\beta}\right) = x^2 - \left(\beta+\bar{\beta}\right)x + \beta\bar{\beta}$. Logo, $(x-\beta)\left(x-\bar{\beta}\right) = x^2 - 2Re(\beta)x + |\beta|^2 \in \mathbb{R}[x]$. Segue que, $x^2 - 2Re(\beta)x + |\beta|^2$ divide $f(x)$ em $\mathbb{R}[x]$. Logo, $f(x) = q(x)(x^2 - 2Re(\beta)x + |\beta|^2) \therefore \partial q(x) + 2 = \partial f(x) > 2$ $\Rightarrow \partial q(x) \geq 1$. Portanto, novamente, $f(x)$ é redutível em $\mathbb{R}[x]$.

A partir da proposição acima e da segunda observação após a Proposição 4.1.2, podemos reescrever o Teorema Fundamental da Álgebra em $R[x]$ como segue:

"Todo polinômio $f(x)$ com coeficientes reais e grau $n \geq 1$ se escreve de modo essencialmente único, a menos da ordem de seus fatores, como sendo expresso por $f(x) = a(x-\beta_1)^{r_1} \ldots (x-\beta_t)^{r_t} p_1(x)^{n_1} \ldots p_s(x)^{n_s}$, onde $a \in \mathbb{R}\backslash\{0\}$ é o coeficiente líder de $f(x)$; $\beta_1, \ldots, \beta_t$ são as raízes reais de $f(x)$ e para $1 \leq j \leq s$, $p_j(x) = x^2 + b_j x + c_j$ são polinômios distintos com coeficientes reais tais que $b_j^2 - 4c_j < 0, \forall\, j = 1, \ldots, s$; e $r_1, \ldots, r_t, n_1, \ldots, n_s \in \mathbb{N}$ são tais que $r_1, + \cdots + r_t + 2n_1 + \ \ldots + 2n_s = n$."

4.3 **Fatoração única sobre $\mathbb{Q}$**

Antes de enunciarmos a fatoração de um polinômio $f(x) \in \mathbb{Q}[x]$, apresentamos algumas definições, teoremas, proposições e seus corolários, os quais são válidos para os corpos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

Polinômios Associados

Dizemos que dois polinômios $f(x), g(x) \in K[x]\backslash\{0\}$ são associados em $K[x]$ se existir $a \in K\backslash\{0\}$ tal que $f(x) = ag(x)$.

Exemplo:

$f(x) = 3x^2 - 2x + 1$ *e* $g(x) = \sqrt{3}x^2 - \frac{2}{3}\sqrt{3}x + \frac{\sqrt{3}}{3}$ são associados em $\mathbb{R}$, pois verificamos que $f(x) = \sqrt{3}g(x)$ e $\sqrt{3} \in \mathbb{R}\backslash\{0\}$.

Divisor Comum[17]

Sejam $f(x), g(x) \in K[x]\backslash\{0\}$, dizemos que um polinômio $p(x) \in K[x]\backslash\{0\}$ é um divisor comum de $f(x)$ *e* $g(x)$ quando $p(x)$ divide $f(x)$ *e* $g(x)$, isto é, $p(x)|f(x), g(x)$. É claro que sempre existem tais divisores pois basta tomarmos o polinômio $p(x) = a \in K\backslash\{0\}$.

Máximo Divisor Comum[17]

Dados $f(x), g(x) \in K[x]\backslash\{0\}$, dizemos que $d(x) \in K[x]\backslash\{0\}$ é um máximo divisor comum de $f(x)$ *e* $g(x)$ e denotamos por $d(x) = mdc\big(f(x), g(x)\big)$, se as duas condições a seguir forem satisfeitas:

a) $d(x)|f(x), g(x)$ em $K[x]$;

b) Se $d'(x) \in K[x]\backslash\{0\}$ é tal que $d'(x)|f(x), g(x)$ em $K[x]$, então $d'(x)|d(x)$ em $K[x]$.

Denotamos por $fK[x]$ o conjunto dos múltiplos de $f(x)$ em $K[x]$, isto é, em símbolos $fK[x] = \{af(x); a \in K[x]\}$.

O teorema que enunciamos a seguir garante a existência do mdc para dois polinômios não nulos sobre K. Esse mdc, por sua vez, é único a menos de associação.

Teorema 4.3.1 (Teorema de Bézout)[17]

Sejam $f(x), g(x) \in K[x]\backslash\{0\}$. Se $S = \{af(x) + bg(x); a, b \in K[x]\}$, então existe um único polinômio $d(x) \in K[x]\backslash\{0\}$, a menos de associação, satisfazendo as seguintes condições:
a) $S = dK[x]$. Em particular, $d(x)|f(x), g(x)$ em $K[x]$;
b) Se $d'(x) \in K[x]\backslash\{0\}$; $d'(x)|f(x), g(x)$, então $d'(x)|d(x)$.

Prova de a):

Se tomarmos $d(x) \in S\backslash\{0\}$ tal que $\partial d(x) = min\{\partial h(x); h(x) \in S\backslash\{0\}\}$, então neste caso, existem $a_0, b_0 \in K[x]$, sendo que $a_0 \neq 0$ ou $b_0 \neq 0$ tal que $d(x) = a_0 f(x) + b_0 g(x)$.

[17] cf. Muniz Neto, pág. 156

Agora tomemos $c \in K[x]$. Então $cd(x) = (ca_0)f(x) + (cb_0)g(x)$. Isto significa que $cd(x) \in S$. Logo, $dK[x] \subset S$.

Reciprocamente, tomemos $h(x) \in S$, então $h(x) = af(x) + bg(x)$ com $a, b \in K[x]$. Pelo algoritmo da divisão euclidiana, $h(x) = d(x)q(x) + r(x)$, com $q(x), r(x) \in K[x]$ e $r(x) = 0\ ou\ 0 \leq \partial r(x) < \partial d(x)$. Suponhamos então que $r(x) \neq 0$. Então, $\partial r(x) < \partial d(x)$ e portanto, $r(x) = h(x) - d(x)q(x) \therefore r(x) = af(x) + bg(x) - \big(a_0 f(x) + b_0 g(x)\big)q(x) \Rightarrow$ $r(x) = \big(a - a_0 q(x)\big)f(x) + \big(b - b_0 q(x)\big)g(x) \Rightarrow r(x) \in S$. Entretanto, isto é um absurdo, afinal por definição, o grau de $r(x)$ não pode ser menor que o de $d(x)$. Logo, $r(x) = 0$. Isto significa que $h(x) \in dK[x] \Rightarrow S \subset dK[x]$. Dessa forma, concluímos que $S = dK[x]$.

Para provar a segunda afirmação do ítem a), basta observar que se os polinômios $f(x)\ e\ g(x) \in S = dK[x]$, então $f(x)\ e\ g(x)$ são múltiplos de $d(x)$ em $K[x]$. Daí, segue o resultado.

Prova de b):

Seja $d'(x) \in K[x]\backslash\{0\}$ um polinômio que divide tanto $f(x)$ quanto $g(x)$, digamos $f(x) = d'(x)f'(x)$ e $g(x) = d'(x)g'(x)$, com $f'(x), g'(x) \in K[x]$. Se $a, b \in K[x]$, então $af(x) + bg(x) = \big(af'(x) + bg'(x)\big)d'(x)$. Logo, $af(x) + bg(x) \in d'K[x]$. Todavia, como $af(x) + bg(x) \in S$, segue então que $d(x) \in dK[x] = S \subset d'K[x]$. Concluímos que $d(x)$ é múltiplo de $d'(x)$. Consequentemente, $d'(x)|d(x)$.

Quanto a unicidade, a menos de uma associação, basta observar que se tivermos $d'(x)\ e\ d(x) \in K[x]$ ambos $mdc\big(f(x), g(x)\big)$, então $d'(x)|d(x)$ e, portanto, temos que $d(x) = ad'(x), a \in K[x]\backslash\{0\}$. Da mesma forma, como $d(x)|d'(x)$ temos $b \in K[x]\backslash\{0\}$, tal que $d'(x) = bd(x)$. Consequentemente, considerando-se as duas últimas equações, temos que $d(x) = a\big(bd(x)\big) \therefore (1 - ab)d(x) = 0 \Rightarrow ab = 1 \therefore b = a^{-1}$. Logo, $d'(x)\ e\ d(x)$ são polinômios associados.

Em função da unicidade do mdc entre dois polinômios não nulos sobre $K[x]$, convecionaremos que o mdc é um polinômio mônico. Não obstante, quando $mdc\{f(x), g(x)\} = 1$, com $f(x), g(x) \in K[x]\backslash\{0\}$, diremos que $f(x)\ e\ g(x)$ são primos entre si, ou relativamente primos.

Corolário 4.3.2: Se $f(x), g(x) \in K[x]\backslash\{0\}$, então $f(x)\ e\ g(x)$ são primos entre si se, e somente se, existem polinômios $a, b \in K[x]$ tais que $af(x) + bg(x) = 1$.

Prova:

Se $f(x)\ e\ g(x)$ são primos entre si, então $mdc\{f(x), g(x)\} = 1$. Pelo Teorema de Bézout $\exists a, b \in K[x];\ af(x) + bg(x) = 1$.

Reciprocamente, se $d(x) = mdc\big(f(x), g(x)\big)\ e\ af(x) + bg(x) = 1$, então, pelo Teorema de Bézout, $1 \in dK[x] \Rightarrow d(x)|1$. Como $d(x)$ é mônico, então $d(x) = 1$.

Proposição 4.3.3

Seja $p(x) \in \mathbb{Q}[x]\backslash\mathbb{Q}$ um polinômio irredutível. Se $f_1, \dots, f_k \in \mathbb{Q}[x]\backslash\{0\}$ são tais que $p(x)|\ f_1 \dots f_k$, então existe $1 \leq i \leq k; p(x)|f_i(x)$.

Prova:

Seja $p(x)|f(x)g(x)$, então $p(x)|f(x)$ ou $p(x) \nmid f(x)$.

No caso em que $p(x) \nmid f(x)$, seja $d = mdc\big(f(x), p(x)\big)$, então $d|p(x)$. Portanto, $d \in \mathbb{Q}$ ou d é associado a $p(x)$ em $\mathbb{Q}[x]$ pois, por hipótese, $p(x)$ é irredutível. Todavia, se d for associado a $p(x)$ e considerando que $d|f(x)$, segue que $p(x)|f(x)$ o que é uma contradição. Logo, d não é associado a $p(x)$. Então, $d \in \mathbb{Q}$ e, portanto, $d = 1$.

Pelo corolário anterior, existem $a, b \in \mathbb{Q}[x]$ tais que $af(x) + bp(x) = 1$. Isto significa que $a\big(f(x)g(x)\big) + \big(bg(x)\big)p(x) = g(x)$. Como, por hipótese, $p(x)|f(x)g(x)$, então $p(x)|g(x)$, pois ambas as parcelas da soma da equação anterior, são múltiplas de $p(x)$. A conclusão a qual chegamos é a de que se $p(x)$ é irredutível e $p(x)|f(x)g(x)$ mas $p(x) \nmid f(x)$, então $p(x)|g(x)$.

Provaremos agora a proposição por indução sobre k.

Para $k = 2$, acabamos de provar.

Suponhamos válido para $k = m$. Sendo assim, para $k = m + 1$ temos que:

$p(x)|\ f_1(x) \dots f_m(x).f_{m+1}(x) \Rightarrow p(x)|f(x).f_{m+1}(x)$, onde $f(x) = f_1(x) \dots f_m(x)$. Logo, temos que $p(x)|f(x)$ ou $p(x)|f_{m+1}(x)$.

No primeiro caso, por hipótese de indução, existe $1 \leq i \leq m; p(x)|f_i(x)$.

No segundo caso, $i = m + 1$. Portanto, em qualquer dos casos, provamos a proposição.

As próximas duas proposições mostram que em $\mathbb{Q}[x]$, temos a fatoração única de polinômios.

Proposição 4.3.4

Todo polinômio $f(x) \in \mathbb{Q}[x]\backslash\mathbb{Q}$ pode ser escrito como produto de um número finito de polinômios irredutíveis sobre $\mathbb{Q}$.

Prova:

Provaremos por indução sobre $\partial f(x)$.

Para $\partial f(x) = 1$, já foi provado (Proposição 4.0.2).

Suponhamos o resultado válido para $\partial f(x) \leq m$. Assim sendo, um polinômio de $\partial f(x) = m + 1$ ou é irredutível ou não. Se for irredutível, não há o que fazer e o resultado está provado. Se não for irreduível então, por definição, existem $g(x), h(x) \in \mathbb{Q}[x]\backslash\mathbb{Q}$, tais que $f(x) = g(x)h(x)$. Sendo assim, temos que: $m + 1 = \partial f(x) = \partial g(x) + \partial h(x)$. Sabemos que, $\partial g(x) \geq 1$ e que $\partial h(x) \geq 1$. Consequentemente, $\partial g(x), \partial h(x) \leq m$ pois, caso contrário, isto é, se tivéssemos $\partial g(x) > m$ ou $\partial h(x) > m$, então $m + 1 = \partial g(x) + \partial h(x) > m + 1$, o que constituiria um absurdo. Entretanto, por hipótese de indução temos, $g(x) = g_1(x) \dots g_r(x)$ e também, $h(x) = h_1(x) \dots h_s(x); r, s \in \mathbb{N}$, onde $g_i(x)\ e\ h_j(x)$ são polinômios irredutíveis quaisquer que sejam $1 \leq i \leq r$ e $1 \leq j \leq s$. Desta forma, temos que o polinômio $f(x) \in \mathbb{Q}[x]$ pode ser expresso por $f(x) = g_1(x) \dots g_r(x)h_1(x) \dots h_s(x)$ e provamos o resultado.

Observação:

As duas últimas proposições (4.3.3 e 4.3.4) em verdade, são válidas para K$[x]$ onde K é um corpo qualquer.

Proposição 4.3.5

Se $p_1(x) \dots p_k(x), q_1(x), \dots, q_l(x) \in \mathbb{Q}[x]\backslash\mathbb{Q}$ são irredutíveis e tais que $p_1(x) \dots p_k(x) = q_1(x) \dots q_l(x)$, então $k = l$ e, a menos de uma reordenação, $p_i(x)\ e\ q_i(x)$ são associados sobre $\mathbb{Q}$.

Prova:

Suponhamos $k = 1$. Neste caso, temos que $p_1(x) = q_1(x) \dots q_l(x)$. No entanto, como $p_1(x)$ é irredutível e $q_i(x) \notin \mathbb{Q}$, temos que $l = 1 \Rightarrow k = l$. Analogamente, se $l = 1$ concluiremos que $k = 1 \Rightarrow k = l$.

Tomemos $k, l > 1$; como $p_1(x) \dots p_k(x) = q_1(x) \dots q_l(x)$. Ora, então temos que $p(x)p_k(x) = q(x)$, onde $p(x) = p_1(x) \dots p_{k-1}(x)$ *e* $q(x) = q_1(x) \dots q_l(x)$. Logo, concluímos que o polinômio $p_k(x) | q(x) = q_1(x) \dots q_l(x)$. Portanto, pela Proposição 4.3.3, sabemos que $\exists i; p_k(x) | q_i(x), 1 \leq i \leq l$. Suponhamos, sem perda de generalidade, que $i = l$. Como $q_l(x)$ é irredutível, e $p_k(x) \notin \mathbb{Q}$ então $p_k(x) = u_1 q_l(x), u_1 \in \mathbb{Q}\backslash\{0\}$. Consequentemente, temos que $p_1(x) \dots p_{k-1}(x) = q_1(x) \dots u q_{l-1}(x) = q'_1(x) \dots q'_{l-1}(x)$, onde $q'_j(x) = q_j(x), 1 \leq j \leq l-2$ e $q'_{l-1}(x) = u_1^{-1} q_{l-1}(x)$, sendo todos os polinômios irredutíveis sobre $\mathbb{Q}$.

Se supusermos que $k \neq l$, por exemplo, $k > l$, e repetirmos esse processo l −vezes chegaremos a seguinte situação: $p_1(x) \dots p_{k-l}(x) = u_1^{-1} \dots u_l^{-1}$. Todavia, isto é um absurdo, visto que como $p_1(x), \dots, p_k(x) \notin \mathbb{Q}$ e $u_1^{-1} \dots u_l^{-1} \in \mathbb{Q}$. Se, por outro lado, $l > k$, chegaremos também a uma contradição através dos polinômios $q_1(x), \dots, q_l(x) \in \mathbb{Q}[x]\backslash\mathbb{Q}$. Logo, $l = k$.

4.4 **Fatoração única sobre $\mathbb{Z}$**

Antes de desenvolvermos o assunto deste tópico, apresentaremos dois resultados importantes que nos auxiliarão na identificação de raízes racionais em polinômios com coeficientes inteiros.

Proposição 4.4.1[18]

Sejam $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]\backslash\mathbb{Z}$ e $\beta \in \mathbb{Q}$, $\beta \neq 0$, uma raiz de $f(x)$. Escrevendo $\beta = \frac{r}{s}$, com $r, s \in \mathbb{Z}, s \neq 0$ e $mdc(r, s) = 1$, temos que:

a) $s | a_n$;

b) $r | a_0$.

Prova:

Por hipótese temos que $\beta = \frac{r}{s}$ é raiz e, portanto, $f\left(\frac{r}{s}\right) = 0$. Logo, temos o que segue:

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

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

Prova de a):

Escrevemos (1) da forma abaixo:

[18] cf. Hefez, pág. 155

$(a_0 s^{n-1} + a_1 r s^{n-2} + \cdots + a_{n-1} r^{n-1})s + a_n r^n = 0 \Rightarrow$

$bs + a_n r^n = 0$ (2)

Em (2) considerando que $s \mid 0$ e $s \mid bs$ então $s|a_n$, afinal como $mdc(r,s) = 1$, e portanto, $mdc(r^n, s) = 1$.

Prova de b):

Escrevemos (1) da forma abaixo:

$a_0 s^n + (a_1 s^{n-1} + a_2 r + \cdots + a_{n-1} r^{n-2} s + a_n r^{n-1})r = 0 \Rightarrow$

$a_0 s^n + cr = 0$ (3)

Em (3) considerando que $r|0\, e\, r|cr$, então $r|a_0$, afinal como $mdc(r,s) = 1$, e portanto, $mdc(s^n, r) = 1$.

Proposição 4.4.2

Sejam $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]\backslash\mathbb{Z}$ e $\beta \in \mathbb{Q}$, $\beta \neq 0$, uma raiz de $f(x)$. Escrevendo $\beta = \frac{r}{s}$, com $r, s \in \mathbb{Z}\backslash\{0\}$ e $mdc(r,s) = 1$, temos que $(r - ms) \mid f(m), \forall m \in \mathbb{Z}$.

Antes de provarmos essa proposição, vale destacar que o ítem b) da proposição 4.4.1, é um caso particular da proposição que estamos por demonstrar, quando fazemos $m = 0$.

Prova:

Com efeito, dado $m \in \mathbb{Z}$, pelo Teorema 2.3.2 (Divisão Euclidiana), podemos reescrever $f(x)$ como sendo $f(x) = q_{n-1}(x)(x - m) + b_0$, onde $b_0 \in \mathbb{Z}$ e o polinômio $q_{n-1}(x)$ é dado por $q_{n-1}(x) = \sum_{k=1}^{n} b_{n+1-k}(x - m)^{n-k}$. Os coeficientes $b_i \in \mathbb{Z}, 1 \leq i \leq n$ são os restos das sucessivas divisões de $q_{n-i}(x)$ por $(x - m)$ onde $q_{n-i}(x) = \sum_{k=1}^{n+1-i} b_{n+1-k}(x - m)^{n+1-(k+i)}$. Sendo assim, $f(x) = b_n(x - m)^n + b_{n-1}(x - m)^{n-1} + \cdots + b_1(x - m) + b_0$. Portanto, segue o seguinte: $0 = f\left(\frac{r}{s}\right) = b_n\left(\frac{r}{s} - m\right)^n + b_{n-1}\left(\frac{r}{s} - m\right)^{n-1} + \cdots + b_1\left(\frac{r}{s} - m\right) + b_0$. Logo, temos que $b_n(r - ms)^n + b_{n-1}(r - ms)^{n-1}s + \cdots + b_1(r - ms)s^{n-1} + b_0 s^n = 0$. Daí que $[b_n(r - ms)^{n-1} + b_{n-1}(r - ms)^{n-2}s + \cdots + b_1 s^{n-1}](r - ms) = -b_0 s^n$. Portanto, temos que $(r - ms) \mid b_0 s^n$. Por outro lado, como $mdc(r,s) = 1$, da mesma forma temos então que $mdc(r - ms, s^n) = 1$. Consequentemente, $(r - ms) \mid b_0 = f(m)$.

Observação:

O Teorema da Divisão Euclidiana, em geral, não se aplica quando tratamos com polinômios com coeficientes inteiros. Todavia, como dividimos $f(x)$ por $p(x) = x - m$, cujo coeficiente líder é $a_1 = 1$, neste caso, o teorema continua válido. A explanação sobre o Algoritmo de Briot – Ruffini, esclarece essa afirmação.

Corolário 4.4.3[19]**:** Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]\backslash\mathbb{Z}$, com coeficiente líder $a_n = \pm 1$. Se $\beta \in \mathbb{Q}$ é uma raiz de $f(x)$, então $\beta \in \mathbb{Z}$ e, quando $\beta \neq 0$, $\beta | a_0$.

Prova:

Se $\beta = 0$ é uma raiz de $f(x)$, então $\beta \in \mathbb{Z}$.

Se $\beta \in \mathbb{Q}\backslash\{0\}$ é uma raiz de $f(x)$ então, $\exists\, r, s \in \mathbb{Z}\backslash\{0\}$ e $mdc(r,s) = 1$ tais que $\beta = \frac{r}{s}$. Pela Proposição 4.4.1, $s|a_n = \pm 1$. Logo, $s = \pm 1 \Rightarrow \beta = \pm r \in \mathbb{Z}$. Todavia, também pela Proposição 4.4.1, $r|a_0 \Rightarrow \pm r = \beta \mid a_0$.

Exemplo1:

Vamos determinar, tanto em $\mathbb{Q}[x]$ quanto em $\mathbb{Z}[x]$, a fatoração do polinômio dado por $f(x) = 4x^3 + 3x^2 + 3x - 1 \in \mathbb{Z}[x]$.

Solução:

Como $f(0) = -1 \neq 0$, então se existirem raízes racionais de $f(x)$, elas são não nulas.

Seja $\beta = \frac{r}{s}$ e $mdc(r,s) = 1$. Pela Proposição 4.4.1, $s|4$ e $r|(-1)$. Logo, temos que $r \in \{-1, 1\}$ e $s \in \{-4, -2, -1, 1, 2, 4\}$. Além disso, pela Proposição 4.4.2 sabemos que $(r - s) \mid f(1) = 9$ e $(r + s) \mid f(-1) = -5$. Segue $\beta \in \left\{-\frac{1}{2}, \frac{1}{4}\right\}$. Portanto, temos que $f(\beta) = 0, \beta \in \mathbb{Q} \Leftrightarrow \beta = \frac{1}{4}$. Logo, $\left(x - \frac{1}{4}\right) | f(x)$. Finalmente, $f(x) = \left(x - \frac{1}{4}\right)(4x^2 + 4x + 4) \Rightarrow f(x) = 4\left(x - \frac{1}{4}\right)(x^2 + x + 1)$. Esta forma representa a fatoração de $f(x)$ em polinômios mônicos irredutíveis em $\mathbb{Q}[x]$. Consequentemente, $f(x) = (4x - 1)(x^2 + x + 1)$ é uma fatoração em polinômios irredutíveis em $\mathbb{Z}[x]$.

Exemplo2:

Vamos determinar, tanto em $\mathbb{Q}[x]$ quanto em $\mathbb{Z}[x]$, a fatoração do polinômio dado por $f(x) = 6x^5 - 23x^4 - 15x^2 - 6x + 8 \in \mathbb{Z}[x]$.

[19] cf. Hefez, pág. 155

Solução:

Como $f(0) = 8 \neq 0$, se existirem raízes racionais de $f(x)$, elas são não nulas. Seja $\beta = \frac{r}{s}$ e $mdc(r,s) = 1$. Pela Proposição 4.4.1, $s|6$ e $r|8$. Portanto, concluímos sobre os fatores r e s, que $r \in \{-8,-4,-2,-1,1,2,4,8\}$ e $s \in \{-6,-3,-2,-1,1,2,3,6\}$. Além disso, pela Proposição 5.4.2 $(r-s) \mid f(1) = -30$ e $(r+s) \mid f(-1) = -30$. Logo, temos que $\beta \in A = \left\{\pm 4, \pm 2, \pm\frac{2}{3}, \pm\frac{1}{2}\right\}$. Calculando $f(\beta)$, para cada elemento de A verificamos que $f(\beta) = 0 \Leftrightarrow \beta \in \left\{-\frac{2}{3}, \frac{1}{2}, 4\right\}$. Portanto, $f(x) = \left(x+\frac{2}{3}\right)\left(x-\frac{1}{2}\right)(x-4)q_2(x)$, onde $q_2(x)$ é um polinômio do 2º grau. A fim de identificarmos os coeficientes de $q_2(x)$, basta dividir $f(x)$ por $\left(x+\frac{2}{3}\right)\left(x-\frac{1}{2}\right)(x-4)$. Verificamos então, que $q_2(x) = 6(x^2+1)$. Portanto, a fatoração de $f(x)$ é $f(x) = 6\left(x+\frac{2}{3}\right)\left(x-\frac{1}{2}\right)(x-4)(x^2+1)$ em $\mathbb{Q}[x]$. Já em $\mathbb{Z}[x]$, a fatoração de $f(x)$ é $f(x) = (3x+2)(2x-1)(x-4)(x^2+1)$.

Os exemplos acima falam em polinômios irredutíveis em $\mathbb{Z}[x]$. A seguir, vamos definir este conceito em $\mathbb{Z}[x]$, já que até agora ele foi trabalhado em $K[x]$, isto é, em $Q[x], \mathbb{R}[x]$ ou $\mathbb{C}[x]$, os quais tem coeficientes em corpos, diferente de $\mathbb{Z}[x]$ cujos coeficientes estão em um anel. Com este objetivo, introduziremos o conceito de conteúdo do polinômio $f(x)$.

Conteúdo do polinômio $f(x)$[20]

Se $f(x) \in \mathbb{Z}[x]\backslash\{0\}$, o conteúdo $\left(contf(x)\right)$ é o mdc de seus coeficientes não nulos. Se $contf(x) = 1$, dizemos que $f(x)$ é um polinômio primitivo em $\mathbb{Z}[x]$. Em outras palavras, se $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]\backslash\{0\}$, então $cont\left(f(x)\right) = mdc(a_0, \ldots, a_n)$.

Os próximos lemas serão úteis para o desenvolvimento da fatoração em $\mathbb{Z}[x]$.

Lema 4.4.4: Se $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n \in \mathbb{Q}[x]\backslash\{0\}$, no qual seus coeficientes são frações irredutíveis, então o $cont\left(f(x)\right) = mdc(a_r, \ldots, a_{r+s}) - \ a_i, 0 \leq r \leq i \leq r+s \leq n$, são os coeficientes não nulos de $f(x)$ – e o mmc dos denominadores dos coeficientes fracionários, são primos entre si.

Prova:

[20] cf. Muniz Neto, pág. 164

Sejam $a = mdc(a_r, \dots, a_{r+s})$ e $b = mmc(b_0, \dots, b_n)$. Sendo assim, temos que $\forall i,$ $0 \leq i \leq n, a|a_i \; e \; b_i|b \Rightarrow \exists \; \lambda_i \in \mathbb{Z}\backslash\{0\}; \; a_i = \lambda_i a$. Como os coeficientes de $f(x)$ são frações irredutíveis, $mdc(a_i, b_i) = 1, \forall i, 0 \leq i \leq n.$ Logo, concluímos que $\forall i, 0 \leq i \leq n, \exists \alpha_i, \beta_i \in \mathbb{Z}\backslash\{0\}; \; \alpha_i a_i + \beta_i b_i = 1 \Rightarrow \; \alpha_i(\lambda_i a) \; + b = 1 \; \therefore \; (\alpha_i \lambda_i)a + b = 1.$ Logo, $mdc(a, b) = 1$ e, portanto, a e b são primos entre si.

Lema 4.4.5[21]

a) Se $f(x) \in \mathbb{Z}[x]\backslash\{0\}$ e $a \in \mathbb{Z}\backslash\{0\}$, então $cont\big(af(x)\big) = acont\big(f(x)\big)$. Em particular, existe $g(x) \in \mathbb{Z}[x]\backslash\{0\}$ primitivo tal que $f(x) = cont\big(f(x)\big)g(x)$.

b) Se $f(x) \in \mathbb{Q}[x]\backslash\{0\}$, então, a menos de multiplicação por -1, existem únicos $a, b \in \mathbb{Z}\backslash\{0\}$ primos entre si e $g(x) \in \mathbb{Z}[x]$ primitivo, tais que $f(x) = \frac{a}{b} g(x)$.

Prova de a)

Sejam $f(x) \in \mathbb{Z}[x]\backslash\{0\} \; e \; a \in \mathbb{Z}\backslash\{0\}$. Tomemos $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Logo, temos que $af(x) = aa_0 + aa_1 x + \cdots + aa_n x^n \; \therefore \; cont\big(af(x)\big) = mdc\big(aa_{r_1}, \dots, aa_{r_m}\big)$, onde os $a_{r_i}, 1 \leq i \leq m$ são os coeficientes não nulos de $f(x)$. Consequentemente temos que, $cont\big(af(x)\big) = amdc\big(a_{r_1}, \dots, a_{r_m}\big) \; \therefore \; cont\big(af(x)\big) = acont\big(f(x)\big)$.

Em particular, fazendo $g(x) = \frac{1}{cont(f(x))} f(x)$, teremos, para o conteúdo de $g(x)$ o que segue: $cont\big(g(x)\big) = cont\left(\frac{f(x)}{cont(f(x))}\right) = \frac{1}{cont(f(x))} cont\big(f(x)\big) = 1.$ Logo, $g(x)$ é primitivo e $f(x) = cont\big(f(x)\big)g(x)$.

Prova de b)

Se $f(x) \in \mathbb{Q}[x]\backslash\{0\}$, então podemos escrever $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1} x + \cdots + \frac{a_n}{b_n} x^n$, com $mdc(a_i, b_i) = 1.$ Sejam $a = mdc(a_r, \dots, a_{r+s}) \; e \; b = mmc(b_0, \dots, b_n)$, onde os a_i para qualquer $i; \; 0 \leq r \leq i \leq r + s \leq n$ são os coeficientes não nulos de $a_0, \dots, a_n \; de \; f(x)$. Pelo Lema 4.4.4, sabemos que a, b são primos entre si. Por outro lado, se multiplicarmos $f(x)$ por b, temos que $bf(x) = b\frac{a_0}{b_0} + b\frac{a_1}{b_1} x + \cdots + b\frac{a_n}{b_n} x^n = \beta_0 a_0 + \beta_1 a_1 x + \cdots + \beta_n a_n x^n$, onde os coeficientes β_i são tais que $\beta_i = \frac{b}{b_i} \; e \; \beta_i a_i \in \mathbb{Z}, 0 \leq i \leq n$ entre os quais, pelo menos um desses coeficientes, é não nulo, visto que $f(x) \in \mathbb{Q}[x]\backslash\{0\}$. Portanto, $bf(x) \in \mathbb{Z}[x]\backslash\{0\}$.

[21] cf. Muniz Neto, pág. 164

Logo, utilizando o resultado do ítem a), sabemos que existe $g(x) \in \mathbb{Z}[x]\backslash\{0\}$ primitivo tal que $bf(x) = ag(x)$, restando provar apenas que $a, b \in \mathbb{Z}\backslash\{0\}$ podem diferir quanto ao sinal. De fato, a variação do sinal ocorre em função de que se $(a, b) = 1$ então $(-a, -b) = 1$.

Polinômio Irredutível em $\mathbb{Z}[x]$[22]

Um polinômio $f(x) \in \mathbb{Z}[x]\backslash\{0\}; f(x) \neq \pm 1$ é irredutível sobre $\mathbb{Z}[x]$ se, dados $g(x), h(x) \in \mathbb{Z}[x]$ com $f(x) = g(x)h(x)$ então, necessariamente, temos que ou o polinômio $g(x) = \pm 1$ ou o polinômio $h(x) = \pm 1$.

É importante ressaltar que, segundo esta definição de polinômios irredutíveis em $\mathbb{Z}[x]$, é perfeitamente possível $f(x) \in \mathbb{Z}[x]\backslash\mathbb{Z}$ ser redutível sendo $\partial f(x) = 1$. Um exemplo disso é $f(x) = 4x + 2 = 2(2x + 1)$.

Proposição 4.4.6[22]

Sejam $g(x), h(x) \in \mathbb{Z}[x]$ polinômios primitivos, então o polinômio $g(x)h(x)$ é primitivo.

Prova:

Suponhamos, por absurdo, que apesar de $g(x), h(x)$ serem primitivos, $g(x)h(x)$ não é primitivo, isto é, $cont\big(f(x)g(x)\big) \neq 1$. Neste caso, $\exists d \in \mathbb{Z}; d|cont\big(g(x)h(x)\big)$ e $d \neq \pm 1$. Sabemos que d pode ser decomposto em fatores primos, por exemplo, $d = \pm p_1^{\alpha_1} \dots p_n^{\alpha_n}$. Logo, se $d|cont\big(g(x)h(x)\big)$, então $p_i|cont\big(g(x)h(x)\big), 1 \leq i \leq n$. Por outro lado, suponhamos $g(x) = a_0 + a_1x + \cdots + a_rx^r$ e $h(x) = b_0 + b_1x + \cdots + b_sx^s$. Como nenhum número primo divide $cont\big(g(x)\big)$ e nem $cont\big(h(x)\big)$, então existe pelo menos um coeficiente de $g(x)$, digamos a_j, e um de $h(x)$, digamos b_k, tal que $p_i \nmid a_j$ e $p_i \nmid b_k$, $1 \leq j \leq r$ e $, 1 \leq k \leq s$. Tomemos os menores inteiros j e k para os quais isso ocorre. A existência deles é garantida pois $j, k \in A \subset \mathbb{N}$ (Princípio da Boa Ordenação de $\mathbb{N}$). O coeficiente de x^{j+k} de $g(x)h(x)$ é dado pela seguinte expressão $c_{j+k} = a_0b_{j+k} + \cdots + a_{j-1}b_{k+1} + a_jb_k + a_{j+1}b_{k-1} + \cdots + a_{j+k}b_0$. Este coeficiente, por hipótese, é divido por p_i. Entretanto, p_i divide todas as parcelas da soma exceto a a_jb_k. Logo, caímos numa contradição. Portanto, $g(x)h(x)$ é primitivo.

[22] cf. Hefez, págs. 156 à 158

Corolário 4.4.7[22]: Sejam $g(x), h(x) \in \mathbb{Z}[x]\backslash\{0\}$, então o conteúdo do produto dos polinômios é igual ao produto dos conteúdos, isto é, $cont\big(g(x)h(x)\big) = cont\big(g(x)\big)cont\big(h(x)\big)$.

Prova:

Pelo ítem a) do Lema 4.4.5, existem polinômios primitivos $g_1(x), h_1(x) \in \mathbb{Z}[x]\backslash\{0\}$ tal que: $g(x) = ag_1(x), h(x) = bh_1(x)$ sendo $a = cont\big(g(x)\big)$ e $b = cont\big(h(x)\big)$. Logo, temos que $cont\big(g(x)\big)cont\big(h(x)\big) = ab = abcont\big(g_1(x)h_1(x)\big)$ pela Proposição 4.4.6. Segue que

$cont\big(g(x)\big)cont\big(h(x)\big) = cont\big(abg_1(x)h_1(x)\big)$ também pelo ítem a do Lema 4.4.5. Portanto temos, $cont\big(g(x)\big)cont\big(h(x)\big) = cont\big(ag_1(x)bh_1(x)\big) = cont\big(g(x)h(x)\big)$ cqd.

Proposição 4.4.8[23]

Para $f(x), g(x) \in \mathbb{Z}[x]\backslash\mathbb{Z}$, temos que:

a) Se $f(x)$ é primitivo, então $f(x)$ é irredutível em $\mathbb{Z}[x]$ se, e somente se, $f(x)$ for irredutível em $\mathbb{Q}[x]$;

b) Se $f(x)\ e\ g(x)$ forem primitivos e associados em $\mathbb{Q}[x]$, então $f = \pm g$.

Prova de a):

$\big(\Leftarrow\big)$ Suponhamos $f(x) \in \mathbb{Z}[x]\backslash\mathbb{Z}$ é primitivo e irredutível em $\mathbb{Q}[x]$, então pela definição de polinômios irredutíveis no corpo $\mathbb{Q}[x]$, temos que existe $p \in \mathbb{Z}$ assim como $h(x) \in \mathbb{Q}[x]$ tal que $f(x) = ph(x)$. Como $cont\big(f(x)\big) = 1$, visto que $f(x)$ é primitivo, então $1 = cont\big(ph(x)\big) = |p|cont\big(h(x)\big)$ Logo, $|p||1 \therefore p = \pm 1$ e, portanto, $f(x)$ é irredutível em $\mathbb{Z}[x]$.

$\big(\Rightarrow\big)$ Suponhamos $f(x) \in \mathbb{Z}[x]\backslash\mathbb{Z}$ é primitivo e redutível em $\mathbb{Q}[x]$, então temos que $f(x) = p(x)h(x);\ p(x), h(x) \in \mathbb{Q}[x]\backslash\mathbb{Q}$. Pelo ítem b) do Lema 4.4.5, podemos tomar $a, b, c, d \in \mathbb{Z}\backslash\{0\}; p(x) = \frac{a}{b}p_1(x)\ e\ h(x) = \frac{c}{d}h_1(x)$ com $p_1(x)\ e\ h_1(x) \in \mathbb{Z}[x]$, polinômios primitivos e $mdc(a,b) = 1 = mdc(c,d)$. Segue que $bdf(x) = bp(x)dh(x)$, o que implica que $ap_1(x)ch_1(x) = acp_1(x)h_1(x) \Rightarrow cont\big(bdf(x)\big) = cont\big(acp_1(x)h_1(x)\big)$. Logo, temos

[23] cf. Muniz Neto, pág. 165

que $|bd| = |ac| \Rightarrow bd = \pm ac \therefore \frac{ac}{bd} = \pm 1$. Portanto, segue que $f(x) = \pm p_1(x)h_1(x) \Rightarrow$ $f(x)$ é redutível em $\mathbb{Z}[x]$.

Prova de b):

Se $f(x)$ *e* $g(x)$ forem primitivos e associados em $\mathbb{Q}[x]$, então $f(x) = \frac{a}{b}g(x);\ a, b \in \mathbb{Z}\backslash\{0\}$ $\Rightarrow bf(x) = ag(x) \Rightarrow cont\big(bf(x)\big) = cont\big(ag(x)\big)$. Logo, $|b| = |a| \Rightarrow \frac{a}{b} = \pm 1 \therefore f(x) = \pm g(x)$.

Agora estamos em condições de apresentarmos o teorema que aborda a fatoração de polinômios em $\mathbb{Z}[x]$.

Teorema 4.4.10 (Fatoração única em $\mathbb{Z}[x]$)[24]

Seja $f(x) \in \mathbb{Z}[x]\backslash\mathbb{Z}$. Então existem um inteiro não nulo d e $p_1(x), \dots, p_r(x)$, polinômios primitivos irredutíveis em $\mathbb{Z}[x]$, tais que $f(x) = d\big(p_1(x) \dots p_r(x)\big)$. Essa escrita é única, a menos da ordem dos fatores e de sinal.

Prova da existência:

Seja $f(x) \in \mathbb{Z}[x]\backslash\mathbb{Z}$. Pela fatoração única em $\mathbb{Q}[x]$, podemos afirmar que existem polinômios $q_1(x), \dots, q_k(x) \in \mathbb{Q}[x]\backslash\mathbb{Q}$, mônicos e irredutíveis em $\mathbb{Q}[x]$, e inteiros não nulos $b, c > 0$, tais que $f(x) = \frac{b}{c}q_1(x) \dots\ q_r(x)$.

Sejam m_j o mínimo múltiplo comum dos denominadores dos coeficientes não nulos de $q_j(x)$, para cada $j = 1, \dots, r$. Então, $p_j(x) = m_j q_j(x) \in \mathbb{Z}[x]$ é um polinômio primitivo irredutível e $(cm_1 \dots m_r)f(x) = b\big(m_1 q_1(x)\big) \dots \big(m_r q_r(x)\big) = b\big(p_1(x) \dots p_r(x)\big)$. Portanto, $cont\big((cm_1 \dots m_r)f(x)\big) = cont\left(b\big(p_1(x) \dots p_r(x)\big)\right) \therefore (cm_1 \dots m_r)cont\big(f(x)\big) = |b|$.

Como $cont\big(f(x)\big) \in \mathbb{Z}$, então $(cm_1 \dots m_r)|b$. Logo, definindo $d = \frac{b}{(cm_1 \dots m_r)}$, obtemos $f(x) = d\big(p_1(x) \dots p_r(x)\big)$.

[24] cf. Hefez, pág. 160

Prova da unicidade:

A unicidade, segue da fatoração única em $\mathbb{Q}[x]$. A unicidade dos polinômios mônicos $q_j(x)$, a menos da ordem dos fatores, e unicidade da fração $\frac{b}{c}$. Por outro lado, pelo ítem b) do Lema 4.4.5, os polinômios primitivos $p_j(x)$ e os inteiros m_j são únicos, a menos de sinal, para cada $j = 1, \dots, r$. Quando $d \neq \pm 1$, pelo Teorema Fundamental da Aritmética, podemos escrever d como produto de elementos primos e portanto, irredutíveis, obtendo assim a fatoração de $f(x)$ em produto de irredutíveis em $\mathbb{Z}[x]$.

Teorema 4.4.10 (Critério de Eisenstein)[25]

Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio em $\mathbb{Z}[x]$. Suponhamos que exista um número primo p tal que $p \nmid a_n, p|a_0, \dots, p|a_{n-1}\ e\ p^2 \nmid a_0$. Então, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Prova:

Pelo ítem a) do Lema 4.4.5, $f(x) = df_1(x)$, onde $d = cont\big(f(x)\big)\ e\ f_1(x) \in \mathbb{Z}[x]\backslash\{0\}$ é primitivo. Como $p \nmid a_n, p \nmid d$ e, não obstante, as condições do enunciado do teorema continuam válidas para os coeficientes de $f_1(x)$. Suponhamos que $f(x)$ é primitivo. Então pela Proposição 5.4.8 ítem a), basta provar que $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Suponhamos então, por absurdo, que $f(x) = g(x)h(x)$, com $g(x), h(x)$ em $\mathbb{Z}[x]$ e que $1 \leq \partial g(x), \partial h(x) < n = \partial f(x)$. Sejam, $g(x) = b_0 + b_1x + \cdots + b_rx^r$, com $b_j \in \mathbb{Z}, \forall j, 0 \leq j \leq r$ e $h(x) = c_0 + c_1x + \cdots + c_sx^s$, com $c_j \in \mathbb{Z}, \forall j, 0 \leq j \leq s$.Como $a_0 = b_0c_0\ e\ p|a_0$, então $p|b_0$ ou $p|c_0$. Todavia, como $p^2 \nmid a_0$, então $p|b_0\ e\ p \nmid c_0$ ou $p \nmid b_0\ e\ p|c_0$.

Sem perda de generalidade, suponhamos que $p|b_0\ e\ p \nmid c_0$. Como $a_n = b_rc_s\ e\ p \nmid a_n$, então $p \nmid b_r$. Seja l o menor natural, com $l \leq r$, tal que $p \nmid b_l$. Então, temos que $p|b_0, \dots, p|b_{l-1}$ e $a_l = b_0c_l + \cdots + b_{l-1}c_1 + b_lc_0$. Portanto, $p \nmid a_l$ pois p divide todas as parcelas da soma, exceto a última. Contudo, por hipótese, $l = n = \partial f(x) > r$, uma contradição.

Caso $f(x)$ não seja primitivo, basta tomarmos $F(x) = \frac{1}{d}f(x)$ e desenvolvermos a prova para $F(x)$.

[25] cf. Hefez, pág. 162

5. ATIVIDADES PROPOSTAS

Neste capítulo apresentamos algumas sugestões de atividades, com objetivos distintos, que podem ser desenvolvidas em sala de aula.

Atividades 1

Objetivo
Os estudantes deverão fixar os principais resultados (teoremas, proposições e lemas), os quais auxiliam na fatoração de polinômios, através da resolução de exercícios.

Fatore, em polinômios irredutíveis, cada polinômio abaixo em $\mathbb{C}[x]$ e, se possível, em $\mathbb{R}[x], \mathbb{Q}[x]\ e\ \mathbb{Z}[x]$. Quando não for possível a fatoração nesses três últimos conjuntos, justifique sua resposta:

a. $f(x) = x^2 - 3$

Basta achar as raízes de $f(x)$ em $\mathbb{C}[x]$.

$\mathbb{C}[x]\ e\ \mathbb{R}[x] \rightarrow f(x) = \left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right)$

$\mathbb{Q}[x] \rightarrow f(x)$ é irredutível; Critério de Eisenstein, sendo o número primo $p = 3$;

$\mathbb{Z}[x] \rightarrow f(x)$ é irredutível; Proposição 4.4.8.

b. $f(x) = x^4 - 5$

Basta achar as raízes de $f(x)$ em $\mathbb{C}[x]$.

$\mathbb{C}[x] \rightarrow f(x) = \left(x - \sqrt[4]{5}\right)\left(x + \sqrt[4]{5}\right)\left(x - \sqrt[4]{5}i\right)\left(x + \sqrt[4]{5}i\right)$;

$\mathbb{R}[x] \rightarrow f(x) = \left(x - \sqrt[4]{5}\right)\left(x + \sqrt[4]{5}\right)\left(x^2 + \sqrt{5}\right)$;

$\mathbb{Q}[x] \rightarrow f(x)$ é irredutível; Critério de Eisenstein; o número primo é $p = 5$;

$\mathbb{Z}[x] \rightarrow f(x)$ é irredutível; Proposição 4.4.8.

c. $f(x) = x^4 + 4$

Basta achar as raízes de $f(x)$ em $\mathbb{C}[x]$.

$¢[x] \rightarrow f(x) = (x - 1 - i)(x - 1 + i)(x + 1 - i)(x + 1 + i)$;

$\mathbb{R}[x] \rightarrow f(x) = (x^2 - 2x + 2)(x^2 + 2x + 2)$;

$\mathbb{Q}[x] \rightarrow (x^2 - 2x + 2)(x^2 + 2x + 2)$;

$\mathbb{Z}[x] \rightarrow (x^2 - 2x + 2)(x^2 + 2x + 2)$.

d. $f(x) = 3x^3 + 2x^2 + 2x - 1$

Aqui, sabemos que existe pelo menos uma raiz real β para $f(x)$ (Corolário 4.0.6). Por outro lado, $f(0) = -1$, logo $x = 0$ não é raiz. Se $\beta \in \mathbb{Q}\backslash\{0\}$ então sabemos que $\exists\, \beta = \frac{r}{s}; r, s \in \mathbb{Z}\backslash\{0\}\ e\ mdc(r,s) = 1$. Então pelas Proposições 4.4.1 e 4.4.2, $r|1,\ s|3, (r-s) \mid f(1) = 6\ e\ (r+s) \mid f(-1) = -4$. Logo, $r \in \{-1, 1\}$ e, por outro lado, $s \in \{-3, -1, 1, 3\}$. Segue que $\beta = \frac{1}{3}$. Quando dividimos $f(x)$ por $x - \frac{1}{3}$, obtemos que $f(x) = \left(x - \frac{1}{3}\right)(3x^2 + 3x + 3) = 3\left(x - \frac{1}{3}\right)(x^2 + x + 1)$. Segue que:

$\mathbb{C}[x] \rightarrow f(x) = 3\left(x - \frac{1}{3}\right)\left(x + \frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\left(x + \frac{1}{2} - \frac{\sqrt{3}}{2}i\right)$;

$\mathbb{R}[x] \rightarrow f(x) = 3\left(x - \frac{1}{3}\right)(x^2 + x + 1)$;

$\mathbb{Q}[x] \rightarrow 3\left(x - \frac{1}{3}\right)(x^2 + x + 1)$;

$\mathbb{Z}[x] \rightarrow (3x - 1)(x^2 + x + 1)$.

Atividades 2

Objetivo
Os estudantes deverão ser capazes de compreender a importância dos polinômios, através da resolução de problemas práticos e corriqueiros na vida de alguns profissionais.

A seguir, apresentamos dois cenários possíveis de o aluno do ensino médio vivenciar, todos envolvendo polinômios.

Cenário 1

A tabela[26] abaixo apresenta o preço médio nacional para os atacadistas, do quilo do feijão carioca, desde setembro de 2015 até agosto de 2016. Essa tabela sempre é construída de tal forma que, todo mês, ela é apresentada na última semana do mês corrente. Suponha que você trabalha neste mercado, compra de feijão por atacado e que estejamos no mês de agosto do corrente ano. Você quer se planejar para comprar no atacado, o feijão carioca no próximo

26 cf. Agrolink

mês. Estime qual deverá ser o valor do preço médio nacional do feijão carioca para o atacadista em setembro de 2016. Faça isso, utilizando os quatro últimos meses da tabela, para construir um Polinômio de Lagrange e, através desse polinômio, calcule o que se pede.

Mês/Ano	Preço Médio Nacional (R$)
Setembro/2015	2,23
Outubro/2015	2,21
Novembro/2015	2,43
Dezembro/2015	2,68
Janeiro/2016	2,95
Fevereiro/2016	3,36
Março/2016	3,46
Abril/2016	3,51
Maio/2016	3,72
Junho/2016	6,40
Julho/2016	7,30
Agosto/2016	6,60

Solução:

Façamos $x_0 = 1, x_1 = 2, x_2 = 3\ e\ x_3 = 4$ como sendo, respectivamente, os meses de maio, junho, julho e agosto. Sendo assim, $y_0 = 3{,}72, y_1 = 6{,}40, y_2 = 7{,}30\ e\ y_3 = 6{,}60$. Com esses dados e considerando o Polinômio de Lagrange $p(x) = \sum_{j=0}^{3} p_j(x)$, onde os termos em j são $p_j(x) = y_j \frac{(x-x_0)(x-x_1)\ldots\overline{(x-x_j)}\ldots(x-x_{n-1})(x-x_n)}{(x_j-x_0)(x_j-x_1)\ldots\overline{(x_j-x_j)}\ldots(x_j-x_{n-1})(x_j-x_n)}$ (4.3), temos que:

$$p_0(x) = y_0 \frac{(x-x_1)(x-x_2)(x-x_3)}{(x_0-x_1)(x_0-x_2)(x_0-x_3)} \therefore$$

$$p_0(x) = 3{,}72 \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} \therefore$$

$$p_0(x) = -0{,}62(x^3 - 9x^2 + 26x - 24)$$

$$p_1(x) = y_1 \frac{(x-x_0)(x-x_2)(x-x_3)}{(x_1-x_0)(x_1-x_2)(x_1-x_3)} \therefore$$

$p_1(x) = 6{,}40\frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} \therefore$

$p_1(x) = 3{,}2(x^3 - 8x^2 + 19x - 12)$

$p_2(x) = y_2\frac{(x-x_0)(x-x_1)(x-x_3)}{(x_2-x_0)(x_2-x_1)(x_2-x_3)} \therefore$

$p_2(x) = 7{,}30\frac{(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)} \therefore$

$p_2(x) = -3{,}65(x^3 - 7x^2 + 14x - 8)$

$p_3(x) = y_3\frac{(x-x_0)(x-x_1)(x-x_2)}{(x_3-x_0)(x_3-x_1)(x_3-x_2)} \therefore$

$p_3(x) = 6{,}60\frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)} \therefore$

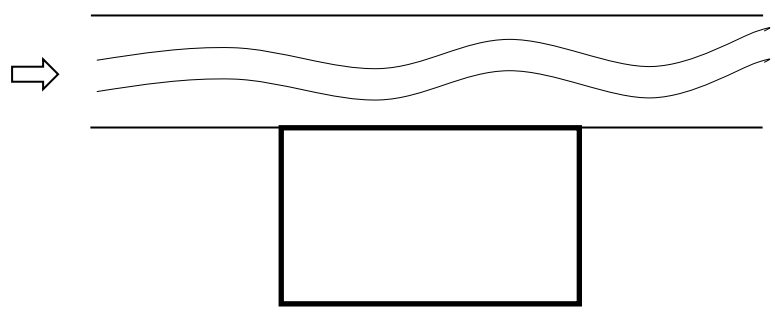
$p_3(x) = 1{,}10(x^3 - 6x^2 + 11x - 6)$

Portanto, como $p(x) = p_0(x) + p_1(x) + p_2(x) + p_3(x)$, temos o seguinte polinômio de grau três: $p(x) = 0{,}03x^3 - 1{,}07x^2 + 5{,}68x - 0{,}92$.

As escolhas que fizemos nos levam ao mês de setembro como sendo $x = 5$. Logo, temos que $p(6) = 0{,}03 \times 5^3 - 1{,}07 \times 5^2 + 5{,}68 \times 5 - 0{,}92 = 4{,}48$. Portanto, uma estimativa para o preço solicitado é de R$ 4,48.

Cenário 2

Você tem uma área retangular em um sítio que será cercada por um rio e, nos outros três lados, será usada uma cerca de arame farpado cujo comprimento é *L* (vide figura abaixo). Qual a maior área que você pode cercar e quais são suas dimensões?



Área retangular ⇨

Solução:

Tomemos como sendo $x\ e\ y$ respectivamente, as medidas horizontal e vertical do retângulo da figura acima. Sendo assim temos que:

$A = xy\ e\ x + 2y = L$, onde A é a área do terreno. Logo, $A(y) = (L - 2y)y$. Portanto, a área cercada é dada por um polinômio de segundo grau com duas raízes reais $\left(0\ e\ \frac{L}{2}\right)$. Como o coeficiente líder é negativo, sabemos que a área terá o maior valor em $y = \frac{L}{4}$. Segue que a área máxima é $A\left(\frac{L}{4}\right) = \frac{L^2}{8}$ e, as medidas do terreno são $y = \frac{L}{4}\ e\ x = \frac{L}{2}$.

Observação:

Qualquer que seja o grau do polinômio $f(x)$, se conhecermos suas raízes, ao menos algumas delas, a fatoração de $f(x)$ em polinômios irredutíveis torna – se bem mais simples. Não obstante, achar as raízes de um polinômio, é resolver a equação $f(x) = 0$. A solução dessa equação para polinômios de primeiro e segundo graus é bastante simples e bem conhecida. Todavia, se $f(x)$ tem grau 3 ou 4, a solução geral da equação $f(x) = 0$ por radicais, é bem menos divulgada. Este assunto é abordado de forma bem didática por Moreira[27] e Milies [28].

[27] cf. Moreira
[28] cf. Milies

CONCLUSÃO

Apesar do papel relevante que os polinômios desempenham na modelação de fenômenos físicos, econômicos e comerciais, na variação de grandezas diversas através do polinômio interpolador de Lagrange e na aproximação de inúmeras funções, por meio do polinômio de Taylor, verificamos empiricamente que este assunto é, quando abordado, tratado de forma bastante superficial na educação básica. Nessa fase do estudante, geralmente não se comenta sobre a diferença entre polinômios e funções polinomiais e tão pouco, são exploradas as formas de se descobrir as raízes racionais de um polinômio. O primeiro fator, além de dificultar o real conceito de polinômios, empobrece o conceito de função reduzindo-o, frequentemente, a uma simples equação matemática. O segundo – sobre as raízes racionais – debilita o estudante quanto a sua capacidade de resolver um dos principais problemas relacionados aos polinômios, a saber: sua fatoração. Em parte, esse cenário se deve a própria formação dos professores da educação fundamental e média no Brasil. Esse trabalho abordou todas essas questões, isto é, ressaltamos a importância dos polinômios, esclarecemos sobre as condições que permitem a identificação entre polinômios e funções polinomiais e evidenciamos os principais resultados que aumentam a capacidade do estudante em fatorar os polinômios. Não obstante, um outro importante objetivo desse trabalho - mostrar que o algoritmo de Briot – Ruffini pode ser usado sob condições mais gerais que aquelas normalmente usadas no ensino básico – também foi atingido. Dessa forma, este trabalho configura-se numa importante contribuição para melhorar o ensino desse tópico na educação básica de matemática no Brasil. Todavia, independentemente de outras contribuições semelhantes a deste trabalho, um estudo mais detalhado sobre didática no ensino de polinômios no nível básico é absolutamente essencial para que a compreensão deste importante tópico seja adequadamente assimilada pelos estudantes.

REFERÊNCIAS

AGROLINK. Disponível em: www.agrolink.com.br/cotacoes/historico. Acesso em: 14/08/2016.

ANDRADE, L. N. Uma generalização de Briot – Ruffini. **Revista do Professor de Matemática**. Rio de Janeiro, n.34, maio/ago. 1997.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Rio de Janeiro: IMPA / SBM, 1997.

DICIONÁRIO de biografias científicas. Rio de Janeiro: Contraponto, 2007.

GARCIA, A. ; LEQUAIN, Y. **Álgebra: um curso de introdução**. Rio de Janeiro: IMPA, 1988.

GONÇALVES, A. **Introdução à Álgebra.** Rio de Janeiro: IMPA, 1979.

HEFEZ, A. ; VILLELA, M. L. T. **Polinômios e equações algébricas**. Rio de Janeiro: SBM, 2012.

HERSTEIN, I. **Tópicos de Álgebra**. São Paulo: Editora da Universidade e Polígono, 1970.

MILIES, C. P. A Solução de Tartaglia para a equação do Terceiro Grau. **Revista do Professor de Matemática**. Rio de Janeiro, n. 25, jan./jun. 1994.

MOREIRA, C. G. T. A. Uma solução das equações do 3º e 4º graus. **Revista do Professor de Matemática**. Rio de Janeiro, n. 25, jan./jun. 1994.

MUNIZ NETO, A. C. **Tópicos de matemática elementar: polinômios**: volume 6. Rio de Janeiro: SBM, 2012.

POOLE, D. **Álgebra linear**. São Paulo: Cengage Learning, 2012.

ROQUE, T. ; CARVALHO, J. B. P. **Tópicos de história da matemática**. Rio de Janeiro: SBM, 2012.

THOMAS, G. B. ; WEIR, M. D. ; HASS, J. **Cálculo**: volume 2. São Paulo: Pearson Education do Brasil, 2012.

TIPLER, A. P. ; MOSCA, G. **Física: para cientistas e engenheiros**: volume 1. Rio de Janeiro: LTC, 2006.