UNIVERSIDADE FEDERAL DO MATO GROSSO DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO
MATEMÁTICA EM REDE NACIONAL
MESTRADO PROFISSIONAL

FATORAÇÃO DE POLINÔMIOS

Everton Melo de Oliveira

CAMPO GRANDE - MS

28 de agosto de 2015

UNIVERSIDADE FEDERAL DO MATO GROSSO DO SUL
INSTITUTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO
MATEMÁTICA EM REDE NACIONAL
MESTRADO PROFISSIONAL

FATORAÇÃO DE POLINÔMIOS

Everton Melo de Oliveira

Orientadora: Profa. Dra. Elisabete Sousa Freitas

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Instituto de Matemática da Universidade Federal de Mato Grosso do Sul, como parte dos requisitos para obtenção do título de Mestre.

CAMPO GRANDE - MS

28 de agosto de 2015

FATORAÇÃO DE POLINÔMIOS

Everton Melo de Oliveira

Dissertação submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional do Instituto de Matemática da Universidade Federal de Mato Grosso do Sul, como parte dos requisitos para obtenção do título de Mestre.

Banca examinadora:

Prof. Dr. Caudemir Aniz - UFMS
Profa. Dra. Elisabete Sousa Freitas - UFMS (orientadora)
Prof. Dr. Jesus Carlos da Mota - UFG

CAMPO GRANDE - MS

28 de agosto de 2015

Dedico aos meus pais Ademir Paes de Oliveira e Edir Coutinho Melo de Oliveira, assim como meus amigos mais íntimos, pela força que sempre me deram para que eu alcançasse meus objetivos, compreendendo meu afastamento durante essa longa jornada, aceitando minha ausência durante essa busca por novos conhecimentos, dando-me a chance do crescimento intelectual.

Educação não transforma o mundo.

Educação muda as pessoas.

Pessoas transformam o mundo.

Paulo Freire

Agradecimentos

Primeiramente agradeço a Deus e a meus pais, por terem me proporcionado chegar aqui, sempre me dando forças nos momentos mais complicados tanto em minha trajetória acadêmica quanto em minha vida profissional e social. Pais esses que fizeram de tudo para que eu não abandonasse meus objetivos e viesse a desistir de algo já planejado em conjunto anteriormente.

Agradeço também aos diversos professores que tive em minha longa trajetória enquanto estudante, onde cada um deles contribuiu de alguma forma particular desde a pré-escola, representados aqui pela ilustre figura de minha orientadora, Profa. Dra. Elisabete Sousa Freitas, pessoa essa que se destaca por sua imensa e invejável capacidade intelectual, que nunca poupou esforços para me orientar no decorrer de minha trajetória acadêmica.

Agradeço aos meus colegas de turma pela forma agradável que se deu nosso convívio durante esses dois anos de curso, pois tenho certeza que boa parte do meu desempenho, como mestrando, se deu pela grande colaboração de vocês. Assim, destaco principalmente os intermináveis grupos de estudos no apartamento da Mônica, sempre nos finais de semanas ou no período noturno logo após o expediente em nossas respectivas escolas, em que sempre se faziam presentes o Elton, Nivaldo, e esporadicamente a Jucilei, grupo este que podia sempre contar com o ânimo do Sérgio, um carioca "isxxxipeerto", marido da Mônica, sempre nos animando para que ninguém viesse a desanimar no decorrer do estudo. Agora vale uma ressalva, o Sérgio ouviu tanto os nossos debates sobre o conteúdo estudado, que com certeza ele já está apto a cursar o PROFMAT.

Por fim, agradeço imensamente ao programa PROFMAT por me permitir o crescimento intelectual e a CAPES pelo incentivo concedido a mim e a meus colegas para que pudéssemos seguir firme em busca de nossos objetivos.

Finalmente, agradeço a todos, que de alguma forma puderam contribuir para que esse objetivo fosse alcançado.

Resumo

Neste trabalho, estudaremos propriedades do anel de polinômios com coeficientes num corpo K. Tal como é feito no anel dos números inteiros, provaremos o Algoritmo da Divisão e a existência do máximo divisor comum entre polinômios. A partir daí, estabeleceremos o Algoritmo Euclidiano para o cálculo do MDC e o Algoritmo Euclidiano Estendido, desenvolvido por D. E. Knuth. Também demonstraremos alguns teoremas relacionados a fatoração de polinômios e apresentaremos o Método de Kronecker, para determinar os fatores de polinômios. O Teorema Fundamental da Álgebra demonstrado pela primeira vez no ano de 1799 por Gauss, em sua tese de doutorado na Universidade de Helmstadt, possui várias demonstrações em diversas áreas da matemática e no apêndice deste trabalho faremos uma prova, considerada elementar, usando resultados da Análise.

Palavras-chave: Polinômios, Divisão de Polinômios, Método de Kronecker, Teorema Fundamental da Álgebra.

Abstract

In this work, we study properties of the polynomial ring with coefficients in a field K. As it is done in the ring of integers, we prove the Division Algorithm and the existence of the greatest common divisor of polynomials. From there, we will establish the Euclidean Algorithm for the calculation of the MDC and the Extended Euclidean Algorithm, developed by D. E. Knuth. Also we will demonstrate some theorems related to factoring of polynomials and present a Kronecker Method, to determine the factors of polynomials. The Fundamental Theorem of algebra demonstrated for the first time in the year 1799 by Gauss in his doctoral thesis at the University of Helmstadt, has several demonstrations in several areas of mathematics and in the Appendix of this work we will do a demonstration, considered elementary, using results of the analysis.

Keywords: Polynomials, Division of Polynomials, Method Kronecker, Fundamental Theorem of Algebra.

Sumário

INTRODUÇÃO

Com a queda da escola de Alexandria no século VII d.C., os indianos e os árabes passaram a se destacar no desenvolvimento da matemática, mantendo assim em evolução o trabalho já desenvolvido. Nesse desenvolvimento, surge o termo "álgebra", palavra essa de origem não tão nítida quanto a da palavra "aritmética", que descende do grego *arithmos* (número), álgebra é uma variante latina do árabe *al-jabr*, usado no título do livro Hisab AL-ajabr wa'l Muqabalah, escrito em Bagdá em meados de 825, onde literalmente esse título significa "ciência da restauração e redução", e por ser a primeira obra a apresentar uma forma sistemática de se resolver uma equação quadrática, veio a se popularizar dentre os estudiosos da época.

Com o passar dos anos, a denominada álgebra, foi se expandindo muito pela curiosidade de estudiosos, sempre lançando desafios intelectuais, mas também pela necessidade em se resolver diversos problemas numéricos mais abstratos que vinham surgindo a medida que outros mais simples fossem sendo resolvidos anteriormente. Em grande parte, seus objetivos eram a busca de raízes de polinômios. Muito tempo se passou para que a álgebra chegasse a ser o que é hoje.

Muito tempo se passou e diversos intelectuais tiveram suas contribuições somadas no desenvolvimento da álgebra e por consequência, da matemática, estudo esse que foi aprofundado por matemáticos como René Descartes (1596 - 1650), responsável pela aceitação da raiz quadrada de número negativo como resultado de uma equação algébrica, Jean Le Rond d'Alembert (1717 - 1783), que enunciou o Teorema Fundamental da Álgebra, que por sua vez foi demonstrado efetivamente por Carl Friedrich Gauss (1777 - 1855) em sua tese de doutorado.

Nosso objeto de estudo, dentro da álgebra, será o anel dos polinômios, onde de maneira

semelhante ao que ocorre com os anel dos inteiros, provaremos o Teorema Algoritmo da Divisão.

Além do algoritmo da divisão, serão apresentados métodos elementares de divisões de polinômios, o Método dos Coeficientes a Determinar, desenvolvido pelo matemático e filósofo René Descartes, e também o Algoritmo de Briot-Ruffini, que é um método prático para realizar divisões de polinômios por polinômios de grau 1.

Este trabalho também apresentará alguns teoremas relacionados a fatoração de polinômios, e o Método de Kronecker, para determinar fatores de um polinômio.

No apêndice deste trabalho faremos uma prova do Teorema Fundamental da Álgebra, considerada elementar, usando resultados de Análise.

1 NOÇÕES PRELIMINARES

Neste capítulo será feita uma breve exposição de definições e resultados, que serão utilizados no desenvolvimento do trabalho.

1.1 Anel, Domínio de Integridade e Corpo

Seja A um conjunto não vazio onde estejam definidas duas operações, as quais chamaremos de *"Soma"* e *"Produto"* em A, denotadas por $+$ e $\cdot$:

- Soma
  $+ : A \times A \longrightarrow A$
  $(a, b) \mapsto a + b$

- Produto
  $\cdot : A \times A \longrightarrow A$
  $(a, b) \mapsto a \cdot b$

Um conjunto A, com pelo menos dois elementos, munido de duas operações $+$ e $\cdot$ será indicado por $(A, +, \cdot)$.

Definição 1. *Uma terna $(A, +, \cdot)$ será chamada de anel se forem satisfeitas as seguintes condições :*

- *A.1 - Associatividade da Soma*
  $\forall a, b, c \in A,\ (a + b) + c = a + (b + c)$

- *A.2 - Existência do Elemento Neutro com relação a Soma*
  $\exists\ 0 \in A$ *tal que,* $\forall a \in A,\ \ a + 0 = 0 + a = a$

- *A.3 - Existência do Oposto*
  Para cada $a \in A$*, existe um* $x \in A$ *tal que* $x + a = a + x = 0$

- *A.4 - Comutatividade da Soma*
  $\forall a, b,\ \ a + b = b + a$

- *M.1 - Associatividade do Produto*
  $\forall a, b, c \in A,\ \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

- *M.2 - Existência do Elemento Neutro com relação ao Produto*
  $\exists 1 \in A$ *tal que,* $\forall a \in A\ ,\ \ a \cdot 1 = a$ *e* $1 \cdot a = a$

- *M.3 - Comutatividade do Produto*
  $\forall a, b,\ \ a \cdot b = b \cdot a$

- *AM. - Distributividade do Produto em relação à Soma*
  $\forall a, b, c \in A,\ \ a \cdot (b + c) = a \cdot b + a \cdot c$

Observações:

i) A condição $A.2$ garante a existência de um elemento neutro para a soma. É fácil verificar que esse elemento neutro é único. De fato, se 0 e $0'$ são dois elementos neutros para a soma temos que $0 + 0' = 0$ ($0'$ é elemento neutro)
$0 + 0' = 0'$ (0 é elemento neutro)
Portanto, $0 = 0'$. Esse único elemento neutro para a adição é chamado de zero ou elemento nulo e denotado sempre por 0.

De modo análogo, existe um único elemento neutro para o produto. Esse único elemento neutro para a multiplicação é chamado de um e denotado sempre por 1.

ii) Dado $a \in A$, a condição $A.3$ garante a existência de um oposto para a em relação a adição. É fácil verificar que esse oposto é único. De fato, se x e y são dois opostos

de a, temos $x + a = 0$ e $a + y = 0$ e assim,

$$x = x + 0 = x + (a + y) = (x + a) + y = 0 + y = y$$

Esse único inverso de a em relação a soma é denotado por $-a$.

Se $a, b \in A$ então a soma $a + (-b)$ é indicada por $a - b$.

iii) O elemento neutro da soma tem a seguinte propriedade:

$$0 \cdot a = 0, \quad \forall a \in A$$

De fato, basta observar que

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

Definição 2. *Um anel $(D, +, \cdot)$ é chamado Domínio de Integridade ou simplesmente Domínio, se ele satisfaz a seguinte condição*

- *M.4 - O produto de quaisquer dois elementos não nulos de D é um elemento não nulo de D, isto é,*

$$\forall a, b \in D \setminus \{0\}, \quad a \cdot b \neq 0$$

Definição 3. *Um anel $(K, +, \cdot)$ é chamado Corpo, se ele satisfaz a seguinte condição*

- *M.5 - Todo elemento diferente de zero de K possui um inverso em relação ao produto, isto é,*

$$\forall a \in K \setminus \{0\}, \exists b \in K, \text{ tal que } a \cdot b = 1$$

Observações:

i) Se $a \neq 0$ é um elemento de um domínio D e $b, c \in D$, então

$$a \cdot b = a \cdot c \Rightarrow b = c$$

De fato, $a \cdot b = a \cdot c \Rightarrow a \cdot b - a \cdot c = a \cdot (b - c) = 0 \Rightarrow b = c$

ii) Dado $a \in K, a \neq 0$, a condição $M.5$ garante a existência de um inverso em relação ao produto. Esse inverso é único e é denotado por a^{-1} e também por $\frac{1}{a}$.

iii) A condição $M.5$ é mais forte do que a condição $M.4$ e assim segue que todo corpo é um domínio. De fato, suponha que $(K, +, \cdot)$ é um corpo e que $a \cdot b = 0$, com $a \neq 0$. Multiplicando a equação $a \cdot b = 0$ por a^{-1}, obtemos $b = 0$.

iv) Todo domínio $(D, +, \cdot)$ finito é um corpo. De fato, para $a \neq 0$ em D considere o conjunto $\{a^n \mid n \in \mathbb{N}\} \subset D$. Como D é finito, existem naturais $n_1 < n_2$ naturais tais que $a^{n_1} = a^{n_2}$, portanto $a.a^{n_2-n_1-1} = 1$ e assim o elemento a possui inverso.

Exemplo 1 *O primeiro exemplo de anel, com o qual trabalhamos desde o ensino básico, é o anel* $(\mathbb{Z}, +, \cdot)$ *do conjunto dos números inteiros com as operações usuais de adição e multiplicação. O Anel* $(\mathbb{Z}, +, \cdot)$ *é um Domínio que não é corpo. De fato, não cumpre a condição* $M.5$.

Exemplo 2 *Temos que,* $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ *e* $(\mathbb{C}, +, \cdot)$, *respectivamente, conjunto dos números racionais, conjunto dos números reais e conjunto dos números complexos com as operações usuais, são corpos.*

2 POLINÔMIOS

Neste capítulo, daremos destaque a um exemplo particular de anel, denominado anel dos polinômios.

2.1 Anéis de Polinômios

Definição 4. *Seja A um anel qualquer.*
Um polinômio sobre A em uma indeterminada x é uma expressão formal

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + a_nx^n + a_{n+1}x^{n+1} + ...$$

onde $a_i \in A, \forall i \in \mathbb{N}$ e existe $n \in \mathbb{N}$ tal que $a_j = 0 \ \ \forall j > n$.

Exemplo 3 *Os polinômios $h(x) = 0 - x + 3x^2 + 0x^3 - 2x^4 + 0x^5 + 0x^6 + \cdots$, $r(x) = 2 + 4x + x^2 + 0x^3 + 0x^4 + \cdots$ e $s(x) = 2 - x + 0x^2 + 4x^3 + 0x^4 - x^5 + 0x^6 + 0x^7 + \cdots$ pertencem a $\mathbb{Z}[x]$, pois os coeficientes $-1, -2, 0, 3, 4$ pertencem a $\mathbb{Z}$.*

Exemplo 4 *Os polinômios $f(x) = \dfrac{1}{2} + 0x + \sqrt{2}x^2 + 2x^3 + 0x^4 + 0x^5 + \cdots$ e $g(x) = 2 - \sqrt{3}x + 0x^2 + \pi x^3 + 0x^4 - \dfrac{2}{5}x^5 + 0x^6 + 0x^7 + \cdots$ pertencem a $\mathbb{R}[x]$, pois os coeficientes $-\sqrt{3}, -\dfrac{2}{5}, 0, \dfrac{1}{2}, \sqrt{2}, 2, \pi$ pertencem a $\mathbb{R}$.*

Definição 5. *Dois polinômios $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + 0x^{n+1} + 0x^{n+2} + \cdots$ e $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m + 0x^{m+1} + 0x^{m+2} + \cdots$ sobre A serão iguais quando $a_i = b_i \ \ \forall i \in \mathbb{N}$.*

O polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$, com $a_i = 0$, $\forall i \in \mathbb{N}$ será indicado por $f(x) = 0$ e denominado polinômio identicamente nulo sobre A.

Se $a_0 \in A$, o polinômio $f(x) = a_0 + 0x + 0x^2 + \cdots$, onde $a_i = 0 \ \ \forall i > 0 \in \mathbb{N}$, será indicado por $f(x) = a_0$ e donominado polinômio constante.

O polinômio $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + 0x^{n+1} + \cdots$, onde $a_i = 0 \ \ \forall \ i > n \in \mathbb{N}$ será indicado por $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$.

O conjunto de todos os polinômios na variável "x" com coeficientes em A será denotado como $A[x]$.

Exemplo 5 *O polinômio constante $p(x) = 5$ é o polinômio $p(x) = 5 + 0x + 0x^2 + \cdots$*

Para facilitar o entendimento dos próximos passos, utilizaremos uma notação, onde cada polinômio será denotado por uma *upla* $(a_0, a_1, a_2, ...)$, onde $a_i \neq 0$ apenas para um número finito de índices, com a definição canônica de igualdade de *uplas*:

- $p(x) = a_0 + 0x + 0x^2 + 0x^3 + 0x^4 + ... \quad \Leftrightarrow \quad p = (a_0, 0, 0, 0, 0, ...)$
- $p(x) = a_0 + a_1x + 0x^2 + 0x^3 + 0x^4 + ... \quad \Leftrightarrow \quad p = (a_0, a_1, 0, 0, 0, ...)$
- $p(x) = a_0 + a_1x + a_2x^2 + 0x^3 + 0x^4 + ... \quad \Leftrightarrow \quad p = (a_0, a_1, a_2, 0, 0, ...)$
- $p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + 0x^4 + ... \quad \Leftrightarrow \quad p = (a_0, a_1, a_2, a_3, 0, ...)$
- $p(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n + 0x^{n+1} + ... \quad \Leftrightarrow \quad p = (a_0, a_1, a_2, a_3, ..., a_n, 0, 0, ...)$, onde com $a_i \in A$ e $i \in \mathbb{N}$.

Exemplo 6 *Os polinômios $p(x) = 1 + 2x + 3x^2 + 0x^3 + 0x^4 + \cdots$ e $q(x) = -1 + 2x + 4x^2 + x^3 + 5x^4 + 0x^5 + 0x^6 + \cdots$, são indicados por $p = (1, 2, 3, 0, 0, 0, ...)$ e $q = (-1, 2, 4, 1, 5, 0, ...)$.*

Para definirmos as operações ***soma*** e ***produto*** em $A[x]$, denotadas por $+$ e $\cdot$, tomaremos p e q pertencentes a $A[x]$

$$p(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + a_nx^n = (a_0, a_1, a_2, ..., a_n, 0, ...)$$

$$q(x) = b_0 + b_1x + b_2x^2 + ... + b_{m-1}x^{m-1} + b_mx^m = (b_0, b_1, b_2, ..., b_m, 0, ...)$$

- ***Soma***

  $+ : A[x] \times A[x] \longrightarrow A[x]$

  $(p, q) \mapsto p + q$

$$p + q = (c_0, c_1, c_2, c_3, ..., c_n, 0, ..., 0) \text{ , com } c_i = a_i + b_i \text{ e } \forall i \in \mathbb{N}$$

Assim:

$$p + q = (a_0 + b_0, a_1 + b_1, a_2 + b_2, ..., a_n + b_n, ...)$$

Exemplo 7 *Sejam os polinômios* $p(x) = 1+2x+3x^2$ *e* $q(x) = -1+2x+4x^2+x^3+5x^4$, *teremos então que* $p = (1, 2, 3, 0, 0, 0, ...)$ *e* $q = (-1, 2, 4, 1, 5, 0, ...)$. *Assim, somando termo a a termo teremos*

$$p + q = (1 - 1, 2 + 2, 3 + 4, 0 + 1, 0 + 5, 0 + 0, ...) = (0, 4, 7, 1, 5, 0, ...)$$

Logo $p(x) + q(x) = 4x + 7x^2 + x^3 + 5x^4$.

- ***Produto***

  $\cdot : A[x] \times A[x] \longrightarrow A[x]$

  $(p, q) \mapsto p \cdot q$

$$p \cdot q = (c_0, c_1, c_2, c_3, ..., c_n, ...) \text{ , com } c_k = \sum_{i=0}^{k} a_i \cdot b_{k-i} \text{ e } i \in \mathbb{N}$$

Assim:

$$p \cdot q = (a_0 \cdot b_0, a_0 \cdot b_1 + a_1 \cdot b_0, a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, ...), \text{ onde } c_k = 0 \text{ para } k > m + n$$

Explicitamente:

coeficiente de x^0: a_0b_0

coeficiente de x^1: $a_0b_1 + a_1b_0$

coeficiente de x^2: $a_0b_2 + a_1b_1 + a_2b_0$

coeficiente de x^3: $a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$

coeficiente de x^4: $a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0$

coeficiente de x^5: $a_0b_5 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_5b_0$

O conjunto $A[x]$ munido das operações soma e produto será indicado por $(A[x], +, \cdot)$.

Exemplo 8 *Tomando $f(x) = 4+5x+3x^2$ e $g(x) = 2+x^2$ pertencentes a $A[x]$, temos que $f = (4, 5, 3, 0, ...)$ e $g = (2, 0, 1, 0, ...)$.*
Pela definição do produto de polinômios, teremos que:
$f \cdot g = (4 \cdot 2,\ \ 4 \cdot 0 + 5 \cdot 2,\ \ 4 \cdot 1 + 5 \cdot 0 + 3 \cdot 2,\ \ 4 \cdot 0 + 5 \cdot 1 + 3 \cdot 0 + 0 \cdot 2,\ \ 4 \cdot 0 + 5 \cdot 0 + 3 \cdot 1 + 0 \cdot 1 + 0 \cdot 2,\ \ ...)$
$f \cdot g = (8, 10, 10, 5, 3, 0, 0, 0...)$
Logo $f(x) \cdot g(x) = 8 + 10x + 10x^2 + 5x^3 + 3x^4$.

Proposição 1 *$(A[x], +, \cdot)$ é um anel.*

Demonstração: Tomando $f = (a_0, a_1, a_2, ...,)$, $g = (b_0, b_1, b_2, ...,)$ e $h = (c_0, c_1, c_2, ...,)$ em $A[x]$, teremos:

- A.1 - Associatividade da soma
  $(f + g) + h = ((a_0, a_1, a_2, a_3, ...) + (b_0, b_1, b_2, b_3, ...)) + (c_0, c_1, c_2, c_3, ...)$
  $(f + g) + h = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3, ...) + (c_0, c_1, c_2, c_3, ...)$
  $(f + g) + h = ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, (a_2 + b_2) + c_2, (a_3 + b_3) + c_3, ...)$
  Como os termos a_i b_i e c_i com $i \in \mathbb{N}$ pertencem ao anel A, temos que $(a_i + b_i) + c_i = a_i + (b_i + c_i)$, daí
  $(f + g) + h = (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), a_2 + (b_2 + c_2), a_3 + (b_3 + c_3), ...)$
  $(f + g) + h = (a_0 + a_2 + a_3 + ...) + (b_0 + c_0, b_1 + c_1, b_2 + c_2, b_3 + c_3, ...)$
  Logo $(f + g) + h = f + (g + h)$.

- A.2 - Existência do Elemento Neutro com relação a Soma

  O polinômio nulo é o elemento neutro.

  De fato, temos que:

  $f + 0 = (a_0 + 0, a_1 + 0, a_2 + 0, a_3 + 0, ...) = (a_0, a_1, a_2, a_3, ...)$

  e

  $0 + f = (0 + a_0, 0 + a_1, 0 + a_2, 0 + a_3, ...) = (a_0, a_1, a_2, a_3, ...)$

  Logo $f + 0 = f = 0 + f$.

- A.3 - Existência do Oposto

  Indicando por $-f$ o polinômio $-f = (-a_0, -a_1, -a_2, -a_3, ...)$, onde $-a_i$ indica o oposto de a_i no anel A, $\forall i \in \mathbb{N}$, temos que:

  $f + (-f) = (a_0 - a_0, a_1 - a_1, a_2 - a_2, a_3 - a_3, ...) = (0, 0, 0, 0, ...)$

  e

  $-f + f = (-a_0 + a_0, -a_1 + a_1, -a_2 + a_2, -a_3 + a_3, ...) = (0, 0, 0, 0, ...)$

  Logo $f + (-f) = 0 = -f + f$.

- A.4 - Comutatividade da Soma

  $f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3, ...)$

  e

  $g + f = (b_0 + a_0, b_1 + a_1, b_2 + a_2, b_3 + a_3, ...)$

  Como a_i, b_i e c_i com $i \in \mathbb{N}$ pertencem ao anel A, temos que $a_i + b_i = b_i + a_i$.

  Logo $f + g = g + f$.

- M.1 - Associatividade do Produto

  $(f \cdot g) \cdot h = ((a_0, a_1, a_2, ...) \cdot (b_0, b_1, b_2, ...)) \cdot (c_0, c_1, c_2, ...)$

  $(f \cdot g) \cdot h = (a_0 \cdot b_0, a_0 \cdot b_1 + a_1 \cdot b_0, a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, ...) \cdot (c_0, c_1, c_2, ...)$

  $(f \cdot g) \cdot h = ((a_0 \cdot b_0) \cdot c_0, (a_0 \cdot b_0) \cdot c_1 + (a_0 \cdot b_1 + a_1 \cdot b_0) \cdot c_0, (a_0 \cdot b_0) \cdot c_2 + (a_0 \cdot b_1 + a_1 \cdot b_0) \cdot c_1 + (a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0) \cdot c_0, ...)$

  $(f \cdot g) \cdot h = (a_0 \cdot b_0 \cdot c_0, a_0 \cdot b_0 \cdot c_1 + a_0 \cdot b_1 \cdot c_0 + a_1 \cdot b_0 \cdot c_0, a_0 \cdot b_0 \cdot c_2 + a_0 \cdot b_1 \cdot c_1 + a_1 \cdot b_0 \cdot c_1 + a_0 \cdot b_2 \cdot c_0 + a_1 \cdot b_1 \cdot c_0 + a_2 \cdot b_0 \cdot c_0, ...)$

  $(f \cdot g) \cdot h = (a_0 \cdot (b_0 \cdot c_0), a_0 \cdot (b_0 \cdot c_1) + a_0 \cdot (b_1 \cdot c_0) + a_1 \cdot (b_0 \cdot c_0), a_0 \cdot (b_0 \cdot c_2) + a_0 \cdot (b_1 \cdot c_1) + a_1 \cdot (b_0 \cdot c_1) + a_0 \cdot (b_2 \cdot c_0) + a_1 \cdot (b_1 \cdot c_0), a_2 \cdot (b_0 \cdot c_0), ...)$

$(f \cdot g) \cdot h = (a_0 \cdot (b_0 \cdot c_0), a_0 \cdot ((b_0 \cdot c_1) + (b_1 \cdot c_0)) + a_1 \cdot (b_0 \cdot c_0), a_0 \cdot ((b_0 \cdot c_2) + (b_1 \cdot c_1) + (b_2 \cdot c_0)) + a_1 \cdot ((b_0 \cdot c_1) + (b_1 \cdot c_0)) + a_2 \cdot (b_0 \cdot c_0), ...)$

$(f \cdot g) \cdot h = (a_0, a_1, a_2, ...) \cdot (b_0 \cdot c_0, b_0 \cdot c_1 + b_1 \cdot c_0, b_0 \cdot c_2 + b_1 \cdot c_1 + b_2 \cdot c_0, ...)$

$(f \cdot g) \cdot h = (a_0, a_1, a_2, ...) \cdot ((b_0, b_1, b_2, ...) \cdot (c_0, c_1, c_2, ...))$

Logo $(f \cdot g) \cdot h = f \cdot (g \cdot h)$

- M.2 - Existência do Elemento Neutro com relação ao Produto

  O polinômio constante 1 é o elemento Neutro com relação ao Produto.

  De fato, temos que:

  $f \cdot 1 = (a_0, a_1, a_2, ...) \cdot (1, 0, 0, ...) = (a_0 \cdot 1, a_0 \cdot 0 = a_1 \cdot 1, a_0 \cdot 0 + a_1 \cdot 0 + a_2 \cdot 1, ...)$

  $f \cdot 1 = (a_0, 0 + a_1, 0 + 0 + a_2, ...) = (a_0, a_1, a_2, ...)$

  e

  $1 \cdot f = (1, 0, 0, ...) \cdot (a_0, a_1, a_2, ...) = (1 \cdot a_0, 1 \cdot a_1 + 0 \cdot a_0, 1 \cdot a_2 + 0 \cdot a_1 + 0 \cdot a_0, ...)$

  $1 \cdot f = (a_0, a_1 + 0, a_2 + 0 + 0, ...) = (a_0, a_1, a_2, ...)$

  Logo $f \cdot 1 = f = 1 \cdot f$.

- M.3 - Comutatividade do Produto

  $f \cdot g = (a_0, a_1, a_2, ...) \cdot (b_0, b_1, b_2, ...)$

  $f \cdot g = (a_0 \cdot b_0, a_0 \cdot b_1 + a_1 \cdot b_0, a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0, ...)$

  Como os termos a_i e b_i, com $i \in \mathbb{N}$ pertencem ao anel A, temos que $a_i \cdot b_i = b_i \cdot a_i$ e $a_i + b_i = b_i + a_i$, assim:

  $f \cdot g = (b_0 \cdot a_0, b_0 \cdot a_1 + b_1 \cdot a_0, b_0 \cdot a_2 + b_1 \cdot a_1 + b_2 \cdot a_0, ...)$

  $f \cdot g = (b_0, b_1, b_2, ...) \cdot (a_0, a_1, a_2, ...)$

  Logo $f \cdot g = g \cdot f$

- AM. - Distributividade do Produto em relação à Soma

  $f \cdot (g + h) = (a_0, a_1, a_2, ...) \cdot ((b_0, b_1, b_2, ...) + (c_0, c_1, c_2, ...))$

  $f \cdot (g + h) = (a_0, a_1, a_2, ...) \cdot (b_0 + c_0, b_1 + c_1, b_2 + c_2, ...)$

  $f \cdot (g + h) = (a_0 \cdot (b_0 + c_0), a_0 \cdot (b_1 + c_1) + a_1 \cdot (b_0 + c_0), a_0 \cdot (b_2 + c_2) + a_1 \cdot (b_1 + c_1) + a_2 \cdot (b_0 + c_0), ...)$

  $f \cdot (g + h) = (a_0 \cdot b_0 + a_0 \cdot c_0, a_0 \cdot b_1 + a_0 \cdot c_1 + a_1 \cdot b_0 + a_1 \cdot c_0, a_0 \cdot b_2 + a_0 \cdot c_2 + a_1 \cdot b_1 + a_1 \cdot c_1 + a_2 \cdot b_0 + a_2 \cdot c_0, ...)$

$f \cdot (g+h) = (a_0 \cdot b_0, a_0 \cdot b_1 + a_1 \cdot b_0, a_0 \cdot b_1 + a_1 \cdot b_1 + a_2 \cdot b_0, ...) + (a_0 \cdot c_0, a_0 \cdot c_1 + a_1 \cdot c_0, a_0 \cdot c_1 + a_1 \cdot c_1 + a_2 \cdot c_0, ...)$

$f \cdot (g+h) = (a_0, a_1, a_2, ...) \cdot (b_0, b_1, b_2, ...) + (a_0, a_1, a_2, ...) \cdot (c_0, c_1, c_2, ...)$

Logo $f \cdot (g+h) = (f \cdot g) + (f \cdot h)$

Portanto como $(A[x], +, \cdot)$ satisfaz as propriedades listadas, podemos concluir que realmente $A[x]$ é um **anel**. ■

A respeito dos elementos de $(A[x], +, \cdot)$, com a notação introduzida anteriormente, teremos:

$$1 = 1 + 0x + 0x^2 + 0x^3 + 0x^4 + ... = (1, 0, 0, 0, 0, ...) \in A[x]$$
$$x = 0 + 1x + 0x^2 + 0x^3 + 0x^4 + ... = (0, 1, 0, 0, 0, ...) \in A[x]$$
$$x^2 = 0 + 0x + 1x^2 + 0x^3 + 0x^4 + ... = (0, 0, 1, 0, 0, ...) \in A[x]$$

E assim seguem as seguintes observações:

i) Tomando $x \in A[x]$, tem-se que:

$$x \cdot x = (0, 1, 0, 0, ...) \cdot (0, 1, 0, 0, ...)$$
$$x \cdot x = (0 \cdot 0, 0 \cdot 1 + 1 \cdot 0, 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0, 0 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 0, ...)$$
$$x \cdot x = (0, 0, 1, 0, ...) = x^2 \in A[x]$$

ii) Tomando $x,\ x^2 \in A[x]$, tem-se que:

$$x \cdot x^2 = (0, 1, 0, 0, ...) \cdot (0, 0, 1, 0, ...)$$
$$x \cdot x^2 = (0 \cdot 0, 0 \cdot 0 + 0 \cdot 0, 0 \cdot 1 + 1 \cdot 0 + 0 \cdot 0, 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 + 0 \cdot 0 + 0 \cdot 0, ...)$$
$$x \cdot x^2 = (0, 0, 0, 1, 0, ...) = x^3 \in A[x]$$

iii) De modo geral, tomando $x^n,\ x^m \in A[x]$, tem-se:

$$x^n \cdot x^m = x^{n+m} \in A[x]$$

iv) Considerando $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n + 0x^{n+1} \in A[x]$.

Segue que

$f = (a_0, a_1, a_2, ..., a_n, 0, ...)$

Usando as definições da soma e do produto de polinômios:

$f = (a_0, 0, 0, 0, ...) + (0, a_1, 0, 0, ...) + (0, 0, a_2, 0, ...) + ... + (0, ..., 0, a_n, 0, ...)$

$f = (a_0, 0, 0, 0, ...) + (a_1, 0, 0, 0, ...) \cdot (0, 1, 0, 0, ...) + ... + (a_n, 0, 0, 0, ...) \cdot (0, ..., 0, 1, 0, ...)$

Das observações acima decorre que:

$$f(x) = a_0 \cdot 1 + a_1 \cdot x + a_2 \cdot x^2 + ... + a_n \cdot x^n$$

para cada $i \in \mathbb{N}, a_i x^i$ é o produto do polinômio constante a_i pelo polinômio x^i.

Das observações anteriores teremos que para determinar o produto de dois polinômios basta aplicar as propriedades do anel $(A[x], +, \cdot)$, como vemos no exemplo a seguinte.

Exemplo 9 *Considerando* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ *e* $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ *pertencentes a* $(K[x], +, \cdot)$*, temos que:*

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

Usando a propriedade distributiva do produto em relação à soma, temos:

$f(x) \cdot g(x) = a_0 \cdot b_0 + a_0 \cdot b_1x + \cdots + a_0 \cdot b_mx^m + a_1x \cdot b_0 + a_1x \cdot b_1x + \cdots + a_1x \cdot b_mx^m + \cdots + a_nx^n \cdot b_0 + a_nx^n \cdot b_1x + \cdots + a_nx^n \cdot b_mx^m$

$f(x) \cdot g(x) = a_0 \cdot b_0 + a_0 \cdot b_1x + \cdots + a_0 \cdot b_mx^m + a_1 \cdot b_0x + a_1 \cdot b_1x^{1+1} + \cdots + a_1 \cdot b_mx^{m+1} + \cdots + a_n \cdot b_0x^n + a_n \cdot b_1x^{n+1} + \cdots + a_n \cdot b_mx^{n+m}$

Usando a comutatividade da soma e a distributividade do produto, segue que:

$f(x) \cdot g(x) = a_0 \cdot b_0 + (a_0 \cdot b_1 + a_1 \cdot b_0)x + (a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0)x^2 + \cdots + a_n \cdot b_mx^{n+m}$

Exemplo 10 *Sejam* $f(x) = 2 + x + x^2, g(x) = 1 + x^3 + 2x^4$ *polinômios de* $A[x]$*, temos que* $f(x) \cdot g(x) = (2 + x + x^2) \cdot (1 + x^3 + 2x^4)$

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

$f(x) \cdot g(x) = 2 + 2x^3 + 4x^4 + x + x^4 + 2x^5 + x^2 + x^5 + 2x^6$

$f(x) \cdot g(x) = 2 + x + x^2 + 2x^3 + 5x^4 + 3x^5 + 2x^6$

Definição 6. *Seja* $f(x) \in A[x], f(x) \neq 0$*, tal que* $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$*, com* $a_n \neq 0$*. Dizemos que* a_n *é o coeficiente líder e* n *é o grau de* $f(x)$*, indicados por* $ld(f) = a_n$ *e* $grau(f) = n$*.*

Os polinômios de grau n com coeficiente líder $a_n = 1$ são denominados polinômios mônicos.

Observamos que os polinômios constantes não nulos, possuem grau zero e o grau do polinômio nulo não é definido. Assim

$$grau(f) = 0 \text{ se, e somente se, } f(x) = a_0 \neq 0, a_0 \in A$$

Proposição 2 *Para quaisquer polinômios não nulos $f(x)$ e $g(x)$ de $A[x]$, temos:*

i) $f(x) + g(x) = 0$ *ou* $grau(f + g) \leq max\{grau(f), grau(g)\}$;

ii) $f(x) \cdot g(x) = 0$ *ou* $grau(f \cdot g) \leq grau(f) + grau(g)$ *e*
$grau(f \cdot g) = grau(f) + grau(g)$, *se A for domínio de integridade;*

Demonstração: Tomando os polinômios $f(x), g(x) \in A[x] \setminus \{0\}$, segue que:

i) Sejam $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n$ e $g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_mx^m$, polinômios não nulos de grau n e m, respectivamente.
Suponha, sem perda de generalidade, que $n \geq m$ e assim $n = max\{grau(f), grau(g)\}$.
Se $n > m$, então $grau(f + g) = n$.
Se $n = m$, temos que $f(x) + g(x) = 0$ ou $grau(f + g) = n$ quando $a_n + b_n \neq 0$ e $grau(f + g) < n$ quando $a_n + b_n = 0$.
Logo $f(x) + g(x) = 0$ ou $grau(f + g) \leq max\{grau(f), grau(g)\}$.

ii) Sejam $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n$ e $g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_mx^m$, polinômios não nulos de grau n e m, respectivamente.
Temos que $f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + ... + c_{m+n}x^{m+n}$, onde $c_{m+n} = \sum_{i=0}^{k} a_i b_{k-i}$ e $i \in \mathbb{N}$, ou seja $c_{m+n} = a_0b_{n+m} + a_1b_{n+m-1} + ... + a_{n-1}b_{m+1} + a_nb_m + a_{n+1}b_{m-1} + ... + a_{n+m}b_0$
Porém, como $a_i = 0, \forall i > n$ e $b_j = 0, \forall j > m$, segue que $c_{n+m} = a_nb_m$.

Assim, $f(x) \cdot g(x) = 0$ ou $grau(f \cdot g) \leq m + n = grau(f) + grau(g)$.

Se A é um domínio de integridade, como $a_n, b_m \in A$ são ambos não nulos, temos que $a_n b_m \neq 0$.

Assim, $grau(f \cdot g) = m + n = grau(f) + grau(g)$.

Logo $f(x) \cdot g(x) = 0$ ou $grau(f \cdot g) \leq grau(f) + grau(g)$ e $grau(f \cdot g) = grau(f) + grau(g)$ quando A é domínio de integridade.■

Corolário 1 *Se A é um domínio de integridade então $A[x]$ é domínio de integridade.*

Demonstração: Decorre diretamente do item *ii*), da proposição anterior.■

Em particular, temos que se K é um corpo então $K[x]$ é um domínio de integridade.

2.2 Algoritmo da Divisão de Polinômios

Seja K um corpo e $K[x]$ o domínio dos polinômios sobre K na indeterminada x. Introduziremos a divisão entre polinômios, de modo análogo ao que é feito na divisão euclidiana no domínio $\mathbb{Z}$ dos múmeros inteiros.

Teorema 1 *(Algoritmo da Divisão) Sejam $f(x), g(x) \in K[x]$ e $g(x) \neq 0$. Então existem únicos $q(x), r(x) \in K[x]$, tais que $f(x) = q(x).g(x) + r(x)$ onde $r(x) = 0$ ou $grau(r) < grau(g)$.*

Demonstração: Sejam $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ e
$g(x) = b_0 + b_1 x + b_2 x^2 + ... + b_m x^m$ com $grau(g) = m$.

Existência:

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

Suponhamos $f(x) \neq 0$ e $grau f(x) = n$.

Se $n < m$, basta tomar $q(x) = 0$ e $r(x) = f(x)$, e assim $f(x) = 0 \cdot g(x) + f(x)$.

Supondo $n \geq m$, faremos a prova por indução (segunda forma) sobre $grau(f) = n$.

Se $n = 0$, como $n \geq m$, segue que $m = 0$ e assim $f(x) = a_0 \neq 0$, $g(x) = b_0 \neq 0$ e $f(x) = a_0 b_0^{-1} \cdot g(x)$. Neste caso, $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.
Suponhamos a afirmação válida para todo polinômio com grau menor do que n.
Consideramos $f_1(x)$ o polinômio definido por

$$f_1(x) = f(x) - a_n \cdot b_m^{-1} x^{n-m} g(x)$$

Temos que $grau(f_1) < grau(f)$ e segue da hipótese de indução, que existem $q_1(x), r_1(x)$ tais que

$$f_1(x) = q_1(x) \cdot g(x) + r_1(x), \text{ onde } r_1(x) = 0 \text{ ou } grau(r_1) < grau(g)$$

Daí, $f(x) = a_n b_m^{-1} x^{n-m}.g(x) + q_1(x).g(x) + r_1(x) = (q_1(x) + a_n b_m^{-1} x^{n-m}).g(x) + r_1(x)$.
Portanto $q(x) = q_1(x) + a_n b_m^{-1}.x^{n-m}$ e $r_1(x) = r(x)$.
Unicidade:
Tomando $f(x) = q_1(x).g(x) + r_1(x) = q_2(x).g(x) + r_2(x)$, onde $r_i(x) = 0$ ou $grau(r_i) < grau(g)$ com $i = 1, 2$, segue que

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

Se $q_1(x) \neq q_2(x)$ teremos que $grau((q_1 - q_2) \cdot g) \geq grau(g)$ e $grau(r_2(x) - r_1(x)) < grau(g)$, chegando a uma contradição.
Portanto $q_1(x) = q_2(x)$ e daí $r_1(x) = r_2(x)$.■

Sejam $f(x), g(x), q(x)$ e $r(x)$ como no teorema anterior, chamaremos $f(x)$ de dividendo, $g(x)$ de divisor, $q(x)$ de quociente e $r(x)$ de resto.

No caso em que $r(x) = 0$, temos que $f(x) = q(x) \cdot g(x)$ e dizemos que $g(x)$ divide $f(x)$ ou que $g(x)$ é um fator de $f(x)$, denotando por $g(x) \mid f(x)$.
Se $f(x) = q(x) \cdot g(x)$ e $1 \leq grau(g) < grau(f)$, dizemos que $g(x)$ é um fator próprio de $f(x)$.

Dados dois polinômios $f(x)$ e $g(x)$ com $g(x) \neq 0$. A demonstração do teorema acima nos fornece um algoritmo prático para determinarmos o quociente e o resto da divisão de $f(x)$ por $g(x)$ como veremos nos exemplos seguintes.

$$\begin{array}{r|l} f(x) & g(x) \\ \hline -q(x)\cdot g(x) & q(x) \\ \hline r(x) & \end{array}$$

Exemplo 11 *Sejam* $f(x) = x^3 + 2x - 3$ *e* $g(x) = x - 1$ *polinômios pertencentes a* $\mathbb{R}[x]$. *Vamos determinar o quociente e o resto da divisão de* $f(x)$ *por* $g(x)$*:*
No primeiro passo calculamos o polinômio

$$f_1(x) = f(x) - a_n \cdot b_m^{-1} x^{n-m} g(x) = (x^3 + 2x - 3) - x^2 \cdot (x - 1)$$

$$\begin{array}{r|l} x^3 + 2x - 3 & x - 1 \\ \hline -(x^3 - x^2) & x^2 \\ \hline \underbrace{x^2 + 2x - 3}_{f_1} & \end{array}$$

A seguir temos que determinar a divisão $f_1(x)$ *por* $g(x)$*. Usando o mesmo procedimento consideramos*

$$f_2(x) = (x^2 + 2x - 3) - x \cdot (x - 1)$$

$$\begin{array}{r|l} x^2 + 2x - 3 & x - 1 \\ \hline -(x^2 - x) & x \\ \hline \underbrace{3x - 3}_{f_2} & \end{array}$$

Agora a divisão de $f_2(x)$ *por* $g(x)$

$$\begin{array}{r|l} 3x - 3 & x - 1 \\ \hline -(3x - 3) & 3 \\ \hline 0 & \end{array}$$

Resumindo num único diagrama temos

$$\begin{array}{r|l} x^3+2x-3 & x-1 \\ \hline -(x^3-x^2) & x^2+x+3 \\ \hline x^2+2x-3 & \\ \hline -(x^2-x) & \\ \hline 3x-3 & \\ \hline -(3x-3) & \\ \hline 0 & \end{array}$$

$$f(x) = x^2(x-1) + \underbrace{x^2+2x-3}_{f_1} = x^2(x-1) + x(x-1) + \underbrace{3x-3}_{f_2}$$

$$f(x) = x^2(x-1) + x(x-1) + 3(x-1) = (x^2+x+3)(x-1) + 0$$

Portanto, $q(x) = x^2 + x + 3$ *e* $r(x) = 0$.

Exemplo 12 *Sejam* $f(x) = 2x^3 - 4x^2 + x + 2, g(x) = x^2 - x + 1 \in \mathbb{R}[x]$, *temos que:*

$$\begin{array}{r|l} 2x^3-4x^2+x+2 & x^2-x+1 \\ \hline -(2x^3-2x^2+2x) & 2x-2 \\ \hline -2x^2-x+2 & \\ \hline -(-2x^2+2x-2) & \\ \hline -3x+4 & \end{array}$$

Portanto, $q(x) = 2x - 2$ e $r(x) = -3x + 4$.

2.3 Método dos Coeficientes a Determinar de Descartes

O matemático filósofo René Descartes introduziu um método para dividir polinômios, ou para determinar os fatores próprios de um polinômio, baseado na definição da igualdade de polinômios. O método é fundamentado no Algoritmo da Divisão e na Propriedade Multiplicativa do Grau.

Para uma melhor compreensão, começaremos com o seguinte exemplo:

Exemplo 13 *Ao dividir* $f(x) = 2x^4 + x^3 - 3x^2 + 2x - 1$ *por* $g(x) = x^2 + 1$*, devemos encontrar dois polinômios* $q(x)$ *e* $r(x)$ *tais que satisfaçam:*

1. $f(x) = g(x).q(x) + r(x)$
2. $grau(r) < grau(g) = 2$ *ou* $r(x) = 0$

Como $r(x) = 0$ *ou* $grau(r) < 2$*, temos que:*

$$r(x) = mx + n \quad e \quad q(x) = ax^2 + bx + c$$

Para a determinação dos coeficientes $a, b, c, m, n \in A$*, temos que:*

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

$$2x^4 + x^3 - 3x^2 + 2x - 1 = (x^2 + 1).(ax^2 + bx + c) + (mx + n)$$

Segue que:

$$2x^4 + x^3 - 3x^2 + 2x - 1 = ax^4 + bx^3 + (a + c)x^2 + (b + m)x + (c + n)$$

Da igualdade de polinômios, segue que:

$$\begin{cases} a = 2 \\ b = 1 \\ a + c = -3 \Leftrightarrow 2 + c = -3 \Leftrightarrow c = -5 \\ b + m = 2 \Leftrightarrow 1 + m = 2 \Leftrightarrow m = 1 \\ c + n = -1 \Leftrightarrow -5 + n = -1 \Leftrightarrow n = 4 \end{cases}$$

Assim $q(x) = 2x^2 + x - 5$ *e* $r(x) = x + 4$

Ou seja, $2x^4 + x^3 - 3x^2 + 2x - 1 = (x^2 + 1).(2x^2 + x - 5) + (x + 4)$.

Exemplo 14 *seja* $f(x) = x^4+4$*, utilizando o método dos coeficientes a determinar de Descartes, determinaremos dois polinômios de grau 2 com coeficientes inteiros divisores de* $f(x)$.

Como $f(x)$ *é um polinômio mônico, tomaremos* $g(x) = x^2+ax+b, h(x) = x^2+cx+d \in \mathbb{Z}[x]$ *tais que* $f(x) = g(x).h(x)$*, assim:*

$$x^4 + 4 = (x^2 + ax + b).(x^2 + cx + d)$$

Daí:

$$x^4 + 4 = x^4 + (a + c)x^3 + (d + ac + b)x^2 + (ad + bc)x + bd$$

Seque que:

$$\begin{cases} (1) \quad a + c = 0 \\ (2) \quad d + ac + b = 0 \\ (3) \quad ad + bc = 0 \\ (4) \quad bd = 4 \end{cases}$$

Analisando as possibilidades para os valores listados acima, em (4) temos que: $b = 1$ *e* $d = 4$*, ou* $b = 2$ *e* $d = 2$*, ou* $b = 4$ *e* $d = 1$*, ou* $b = -1$ *e* $d = -4$*, ou* $b = -2$ *e* $d = -2$*, ou* $b = -4$ *e* $d = -1$.

De (1), temos que $a = -c$.

Substituindo em (2), obtemos que $d + b = c^2$.

Assim, a única possibilidade é $b = 2$ *e* $d = 2$ *e, nesse caso,* $c = 2$ *ou* $c = -2$.

Logo $a = -2$ *ou* $a = 2$*. A equação (3) é satisfeita.*

Portanto, $f(x) = x^2 - 2x + 2$ *e* $g(x) = x^2 + 2x + 2$.

Ou seja, $x^4 + 4 = (x^2 - 2x + 2).(x^2 + 2x + 2)$.

2.4 Algoritmo de Briot-Ruffini

O algoritmo de Briot-Ruffini simplifica a divisão de um polinômio $f(x) \in K[x]$ por um polinômio da forma $x - \beta$, determinando o quociente $q(x)$ e o resto $r(x)$, que neste caso, devido as propriedades ligadas ao grau do polinômio, será uma constante.

Sejam $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in K[x]$, com $a_n \neq 0$, e $\beta \in K$. Sejam também $q(x) \in K[x]$ e $r \in K$ o quociente e o resto da divisão euclidiana de $f(x)$ por $x - \beta$. Então:

$$f(x) = q(x).(x - \beta) + r \text{ , com } grau(q) = n - 1$$

Segue que $q(x) = q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + ... + q_1 x + q_0$ e assim:

$$f(x) = (q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + ... + q_1 x + q_0).(x - \beta) + r$$

Aplicando a distributiva e o devido agrupamento dos termos semelhantes, temos:

$$f(x) = q_{n-1}x^n + (q_{n-2} - \beta q_{n-1})x^{n-1} + ... + (q_0 - \beta q_1)x + (r - \beta q_0)$$

Ao compararmos com os coeficientes de $f(x)$, temos:

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

Assim, podemos ver que a sequência de igualdades dadas acima à direita são caracterizadas recursivamente, nos permitindo determinar $q(x)$ e o r resultantes da divisão de $f(x)$ por $x - \beta$.

Assim,

$$q(x) = a_n x^{n-1} + (a_{n-1} + \beta q_{n-1})x^{n-2} + (a_{n-2} + \beta q_{n-2})x^{n-3} + ... + (a_2 + \beta q_2)x + (a_1 + \beta q_1)$$

e

$$r = a_0 + \beta q_0$$

O algortimo Briot-Ruffini organiza os dados obtidos anteriormente em uma tabela, obtendo o quociente e o resto recursivamente. A tabela tem duas linhas, na primeira linha iniciamos colocando β, seguido dos coeficientes $a_n, a_{n-1}, ..., a_0$ do dividendo $f(x)$ e na segunda linha, o valor inicial $q_{n-1} = a_n$.

β	a_n	a_{n-1}	$\cdots$	a_2	a_1	a_0
	$q_{n-1} = a_n$					

A seguir, fazendo o cálculo $a_n\beta + a_{n-1} = q_{n-2}$, colocando-o na segunda linha, logo após q_{n-1}, obtemos

β	a_n	a_{n-1}	$\cdots$	a_2	a_1	a_0
	$q_{n-1} = a_n$	$a_n\beta + a_{n-1} = q_{n-2}$				

Continuando recursivamente o processo, teremos

β	a_n	a_{n-1}	$\cdots$	a_2	a_1	a_0
	$q_{n-1} = a_n$	q_{n-2}	$\cdots$	q_1	q_0	r

Assim, $q(x)$ será formado pelo coeficientes restantes na segunda linha em ordem decrescente, com exceção do ultimo, convenientemente separado na ultima coluna, que será r resto da divisão de $f(x)$ por $q(x)$.

Exemplo 15 *Sejam* $f(x) = x^4 - 5x^3 + x^2 - 3x + 6$ *e* $g(x) = x - 2$. *Usando o método Briot-Ruffini, determinaremos* $q(x)$ *e* $r(x)$, *respectivamente o quociente e o resto da divisão de* $f(x)$ *por* $g(x)$.
Para efetuá-la através do método de Briot-Ruffini, devemos dispor os coeficientes do polinômio f(x) precedidos do número 2.

Primeiro repete-se, abaixo do primeiro coeficiente, o próprio número, neste caso o 1.

2	1	−5	1	−3	6
	1				

A seguir multiplicamos o 1*, que foi repetido, pelo* 2 *e somamos com o* −5*, o resultado* $1.2 + (-5) = -3$ *escrevemos abaixo do próprio* −5*.*

2	1	−5	1	−3	6
	1	−3			

Assim será feito recursivamente até que se encerrem os coeficientes listados na tabela.

2	1	−5	1	−3	6
	1	−3	−5	−13	−20

Assim, podemos ver que $q(x) = x^3 - 3x^2 - 5x - 13$ *e* $r(x) = -20$*.*

Pelo método das chaves, temos:

$$
\begin{array}{r|l}
x^4 - 5x^3 + x^2 - 3x + 6 & x - 2 \\
\hline
-(x^4 - 2x^3) & x^3 - 3x^2 - 5x - 13 \\
\hline
-3x^3 + x^2 - 3x + 6 & \\
-(-3x^3 + 6x^2) & \\
\hline
-5x^2 - 3x + 6 & \\
-(-5x^2 + 10x) & \\
\hline
-13x + 6 & \\
-(-13x + 26) & \\
\hline
-20 &
\end{array}
$$

Ou seja,

$$x^4 - 5x^3 + x^2 - 3x + 6 = (x^3 - 3x^2 - 5x - 13).(x - 2) - 20$$

2.5 Máximo Divisor Comum

Neste capítulo vamos provar a existência do máximo divisor comum em $K[x]$, onde K é um corpo, de modo análogo como é feito no anel $\mathbb{Z}$ dos números inteiros.

Definição 7. *Seja $f(x) \in K[x]$ um polinômio qualquer.*
O conjunto indicado por $K[x]f(x)$ é definido do seguinte modo:

$$K[x]f(x) = \{g(x) \cdot f(x) \mid g(x) \in K[x]\}$$

e denominado o conjunto dos múltiplos do polinômio $f(x)$.

Proposição 3 *Considere $f(x)$ um polinômio e $K[x]f(x)$ o conjunto dos múltiplos de $f(x)$. Tem-se que:*

i) Se $p(x), q(x) \in K[x]f(x)$, então $p(x) + q(x) \in K[x]f(x)$.

ii) Se $g(x) \in K[x]f(x)$ e $h(x) \in K[x]$, então $g(x) \cdot h(x) \in K[x]f(x)$.

Demonstração: *i)* De fato, se $p(x)$ e $q(x)$ pertencem a $K[x]f(x)$, existem $r(x), s(x) \in K[x]$ tais que $p(x) = r(x) \cdot f(x)$ e $q(x) = s(x) \cdot f(x)$, assim ao somarmos $p(x)$ e $q(x)$ teremos:

$$p(x) + q(x) = r(x) \cdot f(x) + s(x) \cdot f(x) = (r(x) + s(x)) \cdot f(x)$$

Como $r(x) + s(x) \in K[x]$, temos que $p(x) + q(x) \in K[x]f(x)$.

ii) Tomando $g(x) \in K[x]f(x)$, existe $r(x) \in K[x]$ tal que $g(x) = r(x) \cdot f(x)$, assim ao multiplicar $g(x)$ por $h(x) \in K[x]$, tem-se que

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

Assim,

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

Como $r(x) \cdot h(x) \in K[x]$, temos que $g(x) \cdot h(x) \in K[x]f(x)$.■

Definição 8. *Sejam $f(x)$ e $g(x)$ polinômios.*
O conjunto $K[x]f(x) + K[x]g(x)$ é definido do seguinte modo:

$$K[x]f(x) + K[x]g(x) = \{p(x) + q(x) \mid p(x) \in K[x]f(x), q(x) \in K[x]g(x)\}$$

Exemplo 16 *Tomando $f(x) = 3 + x, g(x) = 2 + x - x^2$, o polinômio $h(x) = 11 + 3x - x^2 - x^3 \in K[x]f(x) + K[x]g(x)$, pois existem $r(x) = 3 - x, s(x) = 1 + x$ polinômios pertencentes a $K[x]$, tais que $11 + 3x - x^2 - x^3 = (3 - x) \cdot (3 + x) + (1 + x) \cdot (2 + x - x^2)$*

Proposição 4 *Sejam $f(x)$ e $g(x)$ polinômios. Tem-se que:*

i) Se $r(x), s(x) \in K[x]f(x) + K[x]g(x)$, então $r(x) + s(x) \in K[x]f(x) + K[x]g(x)$.

ii) Se $r(x) \in K[x]f(x) + K[x]g(x)$ e $h(x) \in K[x]$, então $r(x) \cdot h(x) \in K[x]f(x) + K[x]g(x)$.

Demonstração: *i)* Tomando $r(x), s(x) \in K[x]f(x)+K[x]g(x)$, existem $p(x)$, $q(x)$, $t(x)$ e $u(x)$ polinômios, tais que $r(x) = p(x)\cdot f(x)+q(x)\cdot g(x)$ e $s(x) = t(x)\cdot f(x)+u(x)\cdot g(x)$. Assim,

$$r(x) + s(x) = p(x) \cdot f(x) + q(x) \cdot g(x) + t(x) \cdot f(x) + u(x) \cdot g(x)$$

$$r(x) + s(x) = (p(x) + t(x)) \cdot f(x) + (q(x) + u(x)) \cdot g(x)$$

Portanto $r(x) + s(x) \in K[x]f(x) + K[x]g(x)$.

ii) Tomando $r(x) \in K[x]f(x) + K[x]g(x)$ existem os polinômios $p(x)$, $q(x)$, tais que $r(x) = p(x) \cdot f(x) + q(x) \cdot g(x)$.
Multiplicando $r(x)$ por $h(x) \in K[x]$, tem-se que:

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

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

Portanto $r(x) \cdot h(x) \in K[x]f(x) + K[x]g(x)$.■

Teorema 2 *Sejam $f(x)$ e $g(x)$ polinômios não simultaneamente nulos. Então existe um polinômio $d(x)$ tal que $K[x]f(x) + K[x]g(x) = K[x]d(x)$.*

Demonstração: Inicialmente consideraremos o conjunto indicado por

$$J = \{l(x) \in K[x]f(x) + K[x]g(x) \mid grau(l) \geq 0\} \subset K[x] \setminus \{0\}$$

Como $f(x) = 1 \cdot f(x) + 0 \cdot g(x)$ ou $g(x) = 0 \cdot f(x) + 1 \cdot g(x)$ pertencem a $K[x]f(x) + K[x]g(x)$, tem-se que o conjunto J não é vazio.
Consideraremos $d(x) \in J$ tal que o grau de $d(x)$ seja o menor possível dentre os dos polinômios pertencentes a J. Vamos provar que $K[x]d(x) = K[x]f(x) + K[x]g(x)$.
Como $d(x) \in J$, existem polinômios $r(x), s(x) \in K[x]$ tais que $d(x) = r(x) \cdot f(x) + s(x) \cdot g(x)$.

Tomando um polinômio $p(x) \in K[x]d(x)$, temos que existe $a(x) \in K[x]$ tal que

$$p(x) = a(x) \cdot d(x)$$

E assim

$$p(x) = a(x) \cdot (r(x) \cdot f(x) + s(x) \cdot g(x))$$

$$p(x) = (a(x) \cdot r(x)) \cdot f(x) + (a(x) \cdot s(x)) \cdot g(x)$$

Logo $p(x) \in K[x]f(x) + K[x]g(x)$. Assim $K[x]d(x) \subset K[x]f(x) + K[x]g(x)$.

Por outro lado, tomando $p(x) \in K[x]f(x) + K[x]g(x)$, ao considerar a divisão euclidiana do polinômio $p(x)$ por $d(x)$, existem $q(x), r(x)$ tais que

$$p(x) = d(x) \cdot q(x) + r(x), \text{ onde } r(x) = 0 \text{ ou } grau(r) < grau(d)$$

Supondo $r(x) \neq 0$, segue que $0 \leq grau(r) < grau(d)$.
Como $r(x) = p(x) - d(x) \cdot q(x)$ e $p(x), d(x) \in K[x]f(x) + K[x]g(x)$, tem-se pela proposição demonstrada anteriormente que $r(x) \in K[x]f(x) + K[x]g(x)$ e assim chegamos a uma

contradição, pois $grau(r) < grau(d)$, o que não ocorre pois o $grau(d)$ é o menor grau que ocorre em J.
Temos então que $r(x) = 0$ e assim $p(x) = d(x) \cdot q(x) \in K[x]d(x)$.
Assim $K[x]f(x) + K[x]g(x) \subset K[x]$.
Portanto $K[x]f(x) + K[x]g(x) = K[x]d(x)$.■

Proposição 5 *Sejam $f(x)$ e $g(x) \in K[x] \setminus \{0\}$. Então existe $d(x) \in K[x]$ tal que $K[x]f(x) + K[x]g(x) = K[x]d(x)$ e são válidas as seguintes afirmações:*

i) $\exists r(x), s(x) \in K[x]$ *tais que* $d(x) = r(x) \cdot f(x) + s(x) \cdot g(x)$;

ii) $d(x)$ *é um divisor comum de* $f(x)$ *e* $g(x)$;

iii) se $d'(x)$ *é um divisor comum qualquer de* $f(x)$ *e* $g(x)$, *então* $d'(x)$ *é também divisor de* $d(x)$.

Demonstração:*i*) A existência é garantida pelo teorema anterior.
Como $K[x] \cdot f(x) + K[x] \cdot g(x) = K[x] \cdot d(x)$, vale o item i).

ii) Como $f(x) = 1 \cdot f(x) + 0 \cdot g(x) \in K[x] \cdot f(x) + K[x] \cdot g(x)$, segue que existe $h(x) \in K[x]$ tal que

$$f(x) = h(x) \cdot d(x)$$

Logo $d(x)$ divide $f(x)$.
De modo análogo, $d(x)$ divide $g(x)$.

iii) Seja $d'(x)$ um divisor comum de $f(x)$ e $g(x)$ em $K[x]$, isto é, existe $r'(x), s'(x) \in K[x]$ tais que $f(x) = r'(x) \cdot d'(x)$ e $g(x) = s'(x) \cdot d'(x)$.
Como

$$d(x) = r(x) \cdot f(x) + s(x) \cdot g(x)$$

Temos que

$$d(x) = r(x) \cdot (r'(x) \cdot d'(x)) + s(x) \cdot (s'(x) \cdot d'(x))$$

$$d(x) = (r(x) \cdot r'(x) + s(x) \cdot s'(x)) \cdot d'(x)$$

Logo $d'(x)$ divide $d(x)$.■

Definição 9. *Um polinômio $d(x) \in K[x]$ que satisfaça os itens ii) e iii), é denominado um máximo divisor comum de $f(x)$ e $g(x)$.*

Supondo $d(x)$ e $d'(x)$ dois máximos divisores comuns de $f(x)$ e $g(x)$, temos por $ii)$ que $d(x)$ divide $d'(x)$ e $d'(x)$ divide $d(x)$.
Assim

$$d(x) = h_1(x) \cdot d'(x) \text{ e } d'(x) = h_2(x) \cdot d(x)$$

Donde

$$d(x) = (h_1(x) \cdot h_2(x)) \cdot d(x)$$

Avaliando os graus, conclui-se que $h_1(x) = h_2(x) = a \in K[x] \setminus \{0\}$ é um polinômio constante, e assim $d(x) = a \cdot d'(x)$.

Como dois máximos divisores comuns de dois polinômios diferem apenas por uma constante multiplicativa não nula, existirá um único máximo divisor comum mônico que então será chamado de *mdc* de $f(x)$ e $g(x)$, sendo denotado por $mdc(f(x), g(x))$.

Teorema 3 *(Teorema de Bézout) Considere $K[x]$, onde K é corpo, e $f(x), g(x) \in K[x]$. Se $d(x) = mdc(f(x), g(x))$, então existem polinômios $a(x), b(x) \in K[x]$ tais que $d(x) = a(x)f(x) + b(x)g(x)$.*

Demonstração: Considerando $d'(x)$ tal que $K[x]f(x) + K[x]g(x) = K[x]d'(x)$.
Temos que $d'(x)$ também é um máximo divisor comum entre $f(x)$ e $g(x)$.
Daí $d'(x) = a \cdot d(x),\ a \in K \setminus \{0\}$ e $d(x) = b \cdot d'(x),\ b \in K \setminus \{0\}$.
Portanto $d(x) \in K[x]d'(x)$.■

Proposição 6 *Sejam* $f(x), g(x), q(x), r(x) \in K[x]$ *tais que* $f(x) = g(x) \cdot q(x) + r(x)$, *então* $mdc(f(x), g(x)) = mdc(g(x), r(x))$.

Demonstração: Seja $d(x) = mdc(f(x), g(x))$.
Segue que $d(x)$ é mônico e divide $f(x)$ e $g(x)$ simultaneamente.
Assim $f(x) = d(x) \cdot h_1(x)$ e $g(x) = d(x) \cdot h_2(x)$.
Daí $r(x) = d(x) \cdot h_1(x) - (d(x) \cdot h_2(x)) \cdot q(x) = d(x) \cdot (h_1(x) - (h_2(x) \cdot q(x))$
Portanto $d(x)$ divide $g(x)$ e $r(x)$.

Suponha agora $d'(x)$ tal que $d'(x)$ divide $g(x)$ e $r(x)$, como $f(x) = g(x) \cdot q(x) + r(x)$, concluímos que $d'(x)$ divide $f(x)$ e $g(x)$.
Logo $d'(x)$ divide $d(x)$. Portanto $d(x) = mdc(g(x), r(x))$.■

2.6 Algoritmo Euclidiano - MDC

Sejam $f(x), g(x) \in K[x] \setminus \{0\}$. Pela divisão euclidiana temos que

$$f(x) = g(x)q_1(x) + r_1(x), \text{ com } r_1(x) = 0 \text{ ou } 0 \leq grau\ r_1(x) < grau\ g(x)$$

Se $r_1(x) \neq 0$, podemos dividir $g(x)$ por $r_1(x)$ e assim

$$g(x) = r_1(x)q_2(x) + r_2(x), \text{ com } r_2(x) = 0 \text{ ou } 0 \leq grau\ r_2(x) < grau\ r_1(x)$$

Se continuarmos o processo, dividindo cada $r_i(x)$ por $r_{i+1}(x)$, sem restos nulos, obteremos

$$f(x) = g(x)q_1(x) + r_1(x)$$

$$g(x) = r_1(x)q_2(x) + r_2(x)$$

$$r_1(x) = r_2(x)q_3(x) + r_3(x)$$

$$\vdots \qquad \vdots$$

$$r_{i-1}(x) = r_i(x)q_{i+1}(x) + r_{i+1}(x)$$

$$\vdots \qquad \vdots$$

$$r_{n-2}(x) = r_{n-1}(x)q_n(x) + r_n(x)$$

$$r_{n-1}(x) = r_n(x)q_{n+1}(x)$$

onde $grau\ g(x) > grau\ r_1(x) > grau\ r_2(x) > \cdots > grau\ r_n(x)$ e r_{n+1} é o primeiro resto nulo.

De fato, a sequência de restos tem que conter um resto nulo, caso contrário teríamos uma sequência decrescente infinita de números naturais.

Agora, usando a proposição anterior temos

$mdc(f(x), g(x)) = mdc(g(x), r_1(x)) = mdc(r_1(x), r_2(x)) = \cdots = mdc(r_{n-1}(x), r_n(x)) = mdc(r_n(x), 0)$

Se $r_n(x) = c_0 + c_1x + \cdots + c_mx^m$, com $c_m \neq 0$, observamos que:

- $mdc(r_n(x), 0) = 1$, no caso em que $r_n(x) = c_0 \neq 0$
- $mdc(r_n(x), 0) = \dfrac{1}{c_m} \cdot r_n(x)$, no caso em que $grau(r_n) = m \geq 1$

As divisões sucessivas do Algoritmo Euclidiano costumam ser representadas do seguinte modo:

	$q_1(x)$	$q_2(x)$	$q_3(x)$	$\cdots$	$q_{n-1}(x)$	$q_n(x)$	$q_{n+1}(x)$	
$f(x)$	$g(x)$	$r_1(x)$	$r_2(x)$	$\cdots$	$r_{n-2}(x)$	$r_{n-1}(x)$	$r_n(x)$	0
$r_1(x)$	$r_2(x)$	$r_3(x)$	$r_4(x)$	$\cdots$	$r_{n-1}(x)$	$r_n(x)$	0	

Exemplo 17 *Vamos aplicar o algoritmo de Euclides para calcular o mdc de* $f(x) = x^9 - 1$ *e* $g(x) = x^6 - 1$.

	x^3	x^3	1
$x^9 - 1$	$x^6 - 1$	$x^3 - 1$	$x^3 - 1$
$x^3 - 1$	$x^3 - 1$	0	

Assim $r_3(x) = 0$, $mdc(f(x), g(x)) = mdc(x^3 - 1, 0) = x^3 - 1$.

Exemplo 18 *Vamos aplicar o algoritmo de Euclides para calcular o mdc de* $f(x) = x^3 - 1$ *e* $g(x) = x^2 - 1$.

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

Logo $mdc(x^3 - 1, x^2 - 1) = mdc(x + 1, 0) = x + 1$

Exemplo 19 *Vamos aplicar o algoritmo de Euclides para calcular o mdc de* $f(x) = x^2 - 1$ *e* $g(x) = x^3 - 4x$.

	x	$-\frac{1}{3}x$	$3x$
$x^3 - 4x$	$x^2 - 1$	$-3x$	-1
$-3x$	-1	0	

Logo $mdc(x^3 - 4x, x^2 - 1) = mdc(-1, 0) = 1$

2.7 Algoritmo Euclidiano Estendido - MDC

Sejam $f(x), g(x) \in K[x]$ e as divisões sucessivas com as mesmas notações usadas anteriormente . Queremos determinar polinômios $a(x)$ e $b(x)$ tais que

$$mdc(f(x), g(x)) = a(x) \cdot f(x) + b(x) \cdot g(x)$$

Para calculá-los, utilizaremos o algoritmo Eucliano estendido, formulado por D.E. Knuth (Milwaukee, 10 de janeiro de 1938). A idéia de Knuth consiste em observar que cada resto $r_i(x)$ pode ser expresso em termos de $f(x)$ e $g(x)$, com coeficientes polinomiais obtidos por uma recursão muito simples.

Temos que $r_1(x) = f(x) - g(x)q_1(x)$, logo $r_1(x) = a_1(x) \cdot f(x) + b_1(x) \cdot g(x)$, onde $a_1(x) = 1$ e $b_1(x) = -q_1(x)$.

Continuando, $r_2(x) = g(x) - r_1(x)q_2(x) = g(x) - (f(x) - g(x)q_1(x))q_2(x) = -q_2(x)f(x) + (1 + q_1(x)q_2(x))g(x)$, logo $r_2(x) = a_2(x)f(x) + b_2(x)g(x)$, onde $a_2(x) = -q_2(x)$ e $b_2(x) = 1 + q_1(x)q_2(x)$.

Supondo agora que já calculamos $r_{i-1}(x) = a_{i-1}(x)f(x) + b_{i-1}(x)g(x)$ e $r_i(x) = a_i(x)f(x) + b_i(x)g(x)$, o próximo passo será calcular a expressão de $r_{i+1}(x)$.

Como $r_{i+1}(x) = r_{i-1}(x) - r_i(x)q_{i+1}(x)$, substituindo as expressões de $r_{i-1}(x)$ e $r_i(x)$, temos

$$r_{i+1}(x) = (a_{i-1}(x)f(x) + b_{i-1}(x)g(x)) - (a_i(x)f(x) + b_i(x)g(x))q_{i+1}(x)$$

$$r_{i+1}(x) = (a_{i-1}(x) - a_i(x)q_{i+1}(x))f(x) + (b_{i-1}(x) - b_i(x)q_{i+1}(x))g(x)$$

que nos fornece a recursão desejada.

Embora a recursão possa ser iniciada a partir dos coeficientes $a_1(x), b_1(x), a_2(x)$ e $b_2(x)$, interpretando $f(x)$ e $g(x)$ como se fossem restos, digamos $r_{-1}(x)$ e $r_0(x)$, respectivamente, temos

$$r_{-1}(x) = f(x) = a_{-1}(x)f(x) + b_{-1}(x)g(x) \quad \text{e} \quad r_0(x) = g(x) = a_0(x)f(x) + b_0(x)g(x)$$

e assim podemos começar com $a_{-1}(x) = 1, b_{-1}(x) = 0, a_0(x) = 0$ e $b_0(x) = 1$.

Vamos organizar os dados acima numa tabela, onde os restos e os quocientes aparecem na duas primeiras colunas e as outras duas serão preenchidas com os vários $a_i(x)$ e $b_i(x)$. Começamos a tabela com as duas primeiras colunas preenchidas, as terceiras e quartas

serão preenchidas recursivamente usando as duas primeiras linhas conhecidas, lembrando que $a_1(x) = a_{-1}(x) - a_0(x)q_1(x)$, $a_2(x) = a_0(x) - a_1(x)q_2(x)$, $a_3(x) = a_1(x) - a_2(x)q_3(x)$, $a_4(x) = a_1(x) - a_3(x)q_3(x)$ e assim por diante e a mesmo vale para os $b_i(x)$.

resto	quociente	$a(x)$	$b(x)$
$f(x)$	$*$	$a_{-1}(x)$	$b_{-1}(x)$
$g(x)$	$*$	$a_0(x)$	$b_0(x)$
$r_1(x)$	$q_1(x)$	$a_1(x)$	$b_1(x)$
$r_2(x)$	$q_2(x)$	$a_2(x)$	$b_2(x)$
$r_3(x)$	$q_3(x)$	$a_3(x)$	$b_3(x)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$r_{n-1}(x)$	$q_{n-1}(x)$	$a_{n-1}(x)$	$b_{n-1}(x)$
$r_n(x)$	$q_n(x)$	$a_n(x)$	$b_n(x)$

Exemplo 20 *Vamos aplicar o algoritmo estendido para* $f(x) = x^9 - 1$ *e* $g(x) = x^6 - 1$.

Já calculamos anteriormente que $mdc(f(x), g(x)) = x^3 - 1$ *e abaixo temos os quocientes e restos das divisões sucessivas:*

	x^3	x^3	1
$x^9 - 1$	$x^6 - 1$	$x^3 - 1$	$x^3 - 1$
$x^3 - 1$	$x^3 - 1$	0	

Agora vamos construir a tabela do algoritmo estendido para determinar polinômios $a(x)$ *e* $b(x)$ *tais que* $mdc(f(x), g(x)) = a(x)f(x) + b(x)g(x)$.

resto	*quociente*	a	b
x^9-1	$*$	1	0
x^6-1	$*$	0	1
x^3-1	x^3	1	$-x^3$
x^3-1	x^3	$\underbrace{-x^3}_{a(x)}$	$\underbrace{1+x^6}_{b(x)}$

Portanto, $mdc(f(x),g(x)) = x^3-1 = (-x^3)\cdot(x^9-1)+(1+x^6)\cdot(x^6-1)$.

Exemplo 21 *Vamos aplicar o algoritmo estendido para* $f(x) = x^3+2x^2+x$ *e* $g(x) = -x^4-x^3$.

Calculando o $mdc(f(x),g(x)) = x^2+x$, *abaixo temos os quocientes e restos das divisões sucessivas:*

	$-x$	1	x
$-x^4-x^3$	x^3+2x^2+x	x^3-x^2	x^2+x
x^3-x^2	x^2+x	0	

Agora vamos construir a tabela do algoritmo estendido para determinar polinômios $a(x)$ *e* $b(x)$ *tais que* $mdc(f(x),g(x)) = a(x)f(x)+b(x)g(x)$.

resto	*quociente*	a	b
$-x^4-x^3$	$*$	1	0
x^3+2x^2+x	$*$	0	1
x^3-x^2	$-x$	1	x
x^2+x	1	$\underbrace{-1}_{a(x)}$	$\underbrace{1-x}_{b(x)}$

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

3 FATORAÇÃO DE POLINÔMIOS

3.1 Polinômios e suas Raízes

Seja $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ um polinômio não nulo em $K[x]$, caso exista $\alpha \in K$ tal que $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0 \in K$, diremos que α é uma raiz do polinômio $f(x)$ em K.

Exemplo 22 *Tomando* $f(x) = x^8 - 5x^4 + 4 = (x^2-2)(x^2+2)(x^2-1)(x^2+1)$, *temos que:*

- *Possui duas raízes em* $\mathbb{Q}$, $x = -1,\ 1$;
- *Possui quatro raízes em* $\mathbb{R}$, $x = -1,\ 1, \sqrt{2}, -\sqrt{2}$;
- *Possui oito raízes em em* $\mathbb{C}$, $x = -1,\ 1,\ \sqrt{2},\ -\sqrt{2},\ i,\ -i,\ \sqrt{2}i,\ -\sqrt{2i}$.

Teorema 4 *(Teorema de D'Alembert) Seja* $f(x) \in K[x]$ *um polinômio. Temos que* $\alpha \in K$ *é uma raiz de* $f(x)$ *se, e somente se,* $x - \alpha$ *divide* $f(x)$.

Demonstração: ($\Rightarrow$) Suponha $\alpha \in K$ raiz de $f(x)$.
Pela divisão euclidiana, $f(x) = (x-\alpha).q(x) + r(x)$, onde $r(x) = 0$ ou $grau(r) < 1$, donde em qualquer um dos casos $r(x) = b \in K$ constante.
Substituindo x por α, como α é raiz de $f(x)$, temos que $0 = f(\alpha) = (\alpha - \alpha).q(\alpha) + b$, ou seja $0 = b$.
Portanto, $x - \alpha$ divide $f(x)$.

($\Leftarrow$) Suponha que $g(x) = x - \alpha \in K[x]$ divide $f(x)$.
Segue que existe $q(x) \in K[x]$ tal que $f(x) = (x - \alpha)q(x)$.
Assim, substituindo x por α, temos que $f(\alpha) = (\alpha - \alpha).q(\alpha)$, ou seja, $f(\alpha) = 0.q(\alpha) = 0$.

Portanto α é raiz de $f(x)$.■

Exemplo 23 *Seja* $f(x) = 2x^4 + 3x^3 + 2x^2 - 4x - 5$. *Temos que* $f(-1) = 0$, *logo pelo Teorema de D'Alembert,* $g(x) = x + 1$ *divide* $f(x)$.
De fato,

-1	2	3	2	-4	-5
	2	1	1	-5	0

Logo $2x^4 + 3x^3 + 2x^2 - 4x - 5 = (x + 1) \cdot (2x^3 + x^2 + x - 5)$ *com* $r(x) = 0$.

Teorema 5 *Seja* K *um corpo e* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ *um polinômio não nulo em* $K[x]$ *de grau* n *então o número de raízes de* $f(x)$ *em* K *é no máximo igual ao* $grau(f) = n$.

Demonstração: Usaremos indução sobre o $grau(f) = n$.
Se $n = 0$, $f(x)$ não possui raízes em K e nesse caso não há nada o que demonstrar.
Suponha a afirmação válida para todo polinômio de grau n.

Considere $f(x)$ um polinômio de grau $n + 1$.
Supondo α uma raiz de $f(x)$, então $f(x) = q(x) \cdot (x - \alpha)$, onde $grau(q) = n$.
Daí, como $K[x]$ é domínio de integridade, teremos que $f(\beta) = 0$, se e somente se, $\beta = \alpha$ ou $q(\beta) = 0$, logo as raízes de $f(x)$ serão α e as raízes de $g(x)$.
Usando a hipótese de indução, $q(x)$ tem no máximo n raízes, portanto $f(x)$ terá no máximo $n + 1$ raízes.■

3.2 Polinômios Irredutíveis e Fatoração de Polinômios

Neste tópico falaremos de polinômios irredutíveis que, comparando com o que é feito no dominio $\mathbb{Z}$, dos inteiros, fazem o mesmo papel dos números primos.

Definição 10. *Sejam K um corpo e $f(x) \in K[x]$ com $grau(f) \geq 1$.*
Dizemos que $f(x)$ é um polinômio irredutível em $K[x]$ quando:
Se $f(x) = g(x) \cdot h(x)$ com $g(x), h(x) \in K[x]$, então $f(x)$ ou $g(x)$ é um polinômio constante não nulo. Caso contrário, dizemos que $f(x)$ é redutível. Assim, $f(x)$ é redutível quando $f(x) = g(x) \cdot h(x)$, com $g(x), h(x)$ não constantes.

Com as notações das definições acima, segue que:

i) Se $f(x)$ é redutível, então $grau(g)$ e $grau(h)$ são ambos menores que $grau(f)$, pois $grau(f) = grau(g) + grau(h)$;

ii) Se $f(x)$ é redutível, então os graus de $g(x)$ e $h(x)$ não podem ser ambos maiores que $\frac{grau(f)}{2}$, caso contrário $grau(f) < grau(g) + grau(h)$;

iii) Todo polinômio de grau 1 em $K[x]$ é irredutível;

iv) Só é possível decompor polinômios de grau 2 ou 3 como produtos de polinômios não constantes, se ao menos um desses polinômios tiver grau 1;

v) Em decorrência do Teorema de D'Alembert, um polinômio de grau 2 ou 3 só será irredutível em $K[x]$ se o mesmo não possuir raiz em K.

A definição de irredutível não inclui os polinômios constantes, ou seja, os polinômios constantes estão para a fatoração de polinômios assim como os inteiros 1 e -1 estão para a fatoração de inteiros.

Observamos que no caso onde o polinômio tenha grau maior do que 3, pode acontecer que o polinômio seja redutível mas sem raízes, por exemplo um de grau 4 poderá ser decomposto em dois outros polinômios de grau 2, não sendo necessário que estes possuam raízes em K.

Exemplo 24 *O polinômio $f(x) = x^2 + 1$ é irredutível em $\mathbb{R}[x]$. De fato, supondo $f(x) = g(x) \cdot h(x)$, com $g(x)$ e $h(x)$ polinômios não constantes, necessariamente teríamos*

$f(x) = (ax + b)(cx + d)$, com $a, c \neq 0$. Consequentemente $f(x)$ teria raízes em $\mathbb{R}$, o que não é possível.

Exemplo 25 *Tomando o polinômio $f(x) = x^4 - x^2 - 2$, temos os seguintes casos:*

1. *Sobre o corpo $\mathbb{Q}$*
   $x^4 - x^2 - 2 = (x^2 - 2).(x^2 + 1)$, *onde $g(x) = x^2 - 2$ e $h(x) = x^2 + 1$ são dois polinômios irredutíveis em $\mathbb{Q}$.*

2. *Sobre o corpo $\mathbb{R}$*
   $x^4 - x^2 - 2 = (x - \sqrt{2}).(x + \sqrt{2}).(x^2 + 1)$ *onde $g(x) = x - \sqrt{2}$, $h(x) = x + \sqrt{2}$ e $p(x) = x^2 + 1$ são três polinômios irredutíveis em $\mathbb{R}$.*

3. *Sobre o corpo $\mathbb{C}$*
   $x^4 - x^2 - 2 = (x - \sqrt{2}).(x + \sqrt{2}).(x + i).(x - i)$ *onde $g(x) = x - \sqrt{2}$, $h(x) = x + \sqrt{2}$, $p(x) = x + i$ e $q(x) = x - i$ são quatro polinômios irredutíveis em $\mathbb{C}$.*

Proposição 7 *Sejam $p(x), f(x) \in K[x]$. Se $p(x) \nmid f(x)$ e $p(x)$ é irredutível, então $mdc(f(x), p(x)) = 1$.*

Demonstração: Suponha que $d(x) \mid f(x)$ e $d(x) \mid p(x)$.
Segue que $p(x) = d(x) \cdot g(x)$, com $g(x) \in K[x]$.
Como $p(x)$ é irredutível, concluimos que $d(x)$ ou $g(x)$ é um polinômio constante não nulo.
Se $g(x) = a$, com $a \in K \setminus \{0\}$ então $p(x) = a \cdot d(x)$ e consequentemente $p(x) \mid f(x)$, o que contraria a hipótese.
Portanto, $d(x) = a$, com $a \in K \setminus \{0\}$, consequentemente $\text{mdc}(f(x), p(x)) = 1$.■

Proposição 8 *Sejam $p(x), f(x)$ e $g(x) \in K[x]$. Se $p(x) \mid f(x) \cdot g(x)$ e $p(x)$ é irredutível, então $p(x) \mid f(x)$ ou $p(x) \mid g(x)$.*

Demonstração: Suponhamos $p(x)$ um polinômio irredutível que
divide $f(x) \cdot g(x)$. Suponha que $p(x) \nmid f(x)$.

Como $p(x)$ é irredutível, temos que $mdc(p(x), f(x)) = 1$, assim existem $r(x), s(x) \in K[x]$ tais que $r(x) \cdot p(x) + s(x) \cdot f(x) = 1$.

Daí, multiplicando ambos os lados da equação anterior por $g(x)$, obtemos

$$r(x) \cdot p(x) \cdot g(x) + s(x) \cdot f(x) \cdot g(x) = g(x)$$

Como $p(x) \mid p(x)$ e $p(x) \mid f(x) \cdot g(x)$, concluimos que $p(x) \mid g(x)$.■

Teorema 6 *(Teorema da Fatoração Única) Seja K um corpo e $f(x) \in K[x]$ com grau $f(x) \geq 1$. Então, existem polinômios mônicos irredutíveis $p_1(x), p_2(x), ..., p_m(x)$ e $a \in K \setminus \{0\}$ tais que*

$$f(x) = a \cdot p_1(x) \cdot p_2(x) \cdots p_m(x)$$

Além disto, essa expressão é única, a menos da ordem dos fatores.

Demonstração:

Existência

Vamos provar por indução (segunda forma) sobre $grau(f) = n$.

Se $n = 1$, então $f(x) = ax + b$, com $a \neq 0$, logo $f(x) = a(x + \frac{b}{a}x)$.

Neste caso, temos $m = 1$ e $p_1(x) = x + \frac{b}{a}x$ é mônico irredutível.

Suponhamos que o resultado seja válido para todo polinômio não constante de grau menor do que $n \geq 2$. Vamos provar que também será válido para $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_n \neq 0$, de grau n.

Se $f(x)$ for irredutível, então $f(x) = a_n(x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \cdots + \frac{a_1}{a_n}x + \frac{a_0}{a_n})$, portanto $m = 1$ e $p_1(x) = a_n(x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \cdots + \frac{a_1}{a_n}x + \frac{a_0}{a_n})$ é mônico irredutível.

Podemos assumir que $f(x)$ é redutível. Assim, existem $g(x), h(x) \in K[x]$ polinômios não constantes tais que $f(x) = g(x) \cdot h(x)$.

Temos que $grau(g) < n$ e $grau(h) < n$ e, usando a hipótese de indução, podemos escrever

$$g(x) = b \cdot p_1(x) \cdot p_2(x) \cdots p_r(x)$$

$$h(x) = c \cdot p_{r+1}(x) \cdot p_{r+2}(x) \cdots p_m(x)$$

com $b, c \in K \setminus \{0\}$ e $p_1(x), p_2(x), ..., p_m(x)$ são polinômios mônicos irredutíveis.

Portanto $f(x) = a \cdot p_1(x) \cdot p_2(x) \cdots p_m(x)$, com $a = b \cdot c \neq 0$.

Unicidade

Suponhamos

$$f(x) = a \cdot p_1(x) \cdots p_m(x) = b \cdot q_1(x) \cdots q_r(x)$$

onde $a, b \in K \setminus \{0\}$ e $p_1(x), ..., p_m(x), q_1(x), \cdots, q_r(x)$ polinômios mônicos irredutíveis sobre K.

Como $a =$ *coeficiente lider* de $f(x) = b$, obtemos

$$p_1(x) \cdots p_m(x) = q_1(x) \cdots q_r(x)$$

Assim, temos

$$p_1(x) \mid q_1(x) \cdots q_r(x)$$

e, como $p_1(x)$ é irredutível, $p_1(x)$ divide $q_j(x)$, para algum $j = 1, \ldots r$.

Segue que, $p_1(x) = u \cdot q_j(x)$ com $u \in K \setminus \{0\}$ e comparando os coeficientes líderes concluimos que $u = 1$.

Reenumerando os polinômios $q_1(x), ..., q_r(x)$ podemos assumir $p_1(x) = q_1(x)$, donde

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

Seguiremos a prova usando indução sobre m.

Se $m = 1$ então $r = 1$ e $p_1(x) = q_1(x)$.

Suponhamos a afirmação válida para $m - 1 \geq 1$.

Temos $p_2(x) \cdots p_m(x) = q_2(x) \cdots q_r(x)$, e pela hipótese de indução, $m - 1 = r - 1$, isto é, $m = r$ e $\{p_1(x), p_2(x), ..., p_m(x)\} = \{q_1(x), q_2(x), \ldots, q_m(x)\}$.■

3.3 Fatoração em $\mathbb{C}[x]$

Considerando um polinômio $f(x) \in \mathbb{C}[x]$, este possuirá sempre uma raiz complexa, fato esse conhecido como "Teorema Fundamental da Álgebra"(TFA), demonstrado pela primeira vez no ano de 1799, por Gauss, em sua tese de doutorado na Universidade de Helmstadt.

Este teorema possui várias demonstrações em diversas áreas da matemática e no apêndice

deste trabalho faremos uma prova, considerada elementar, usando resultados da Análise. Usaremos o resultado do TFA na proposição seguinte.

Proposição 9 *Seja $f(x) \in \mathbb{C}[x]$, com $grau(f) = n \geq 1$.*
Então, existem $\beta_1, \beta_2, ..., \beta_n \in \mathbb{C}$, não necessariamente distintos, e $a \in \mathbb{C} \setminus \{0\}$ tais que $f(x) = a(x - \beta_1)(x - \beta_2)...(x - \beta_n)$.

Demonstração: Faremos a prova por indução sobre o $grau(f) = n$.
Se $n = 1$, então $f(x) = ax + b$, com $a, b \in \mathbb{C}$ e $a \neq 0$, teremos que $f(x) = a(x + a^{-1}b)$ e $\beta_1 = -a^{-1}b$.
Suponhamos o resultado válido para polinômios de grau $n \geq 1$.
Considere $f(x) \in \mathbb{C}[x]$ com $grau(f) = n + 1$.
Pelo TFA, $f(x)$ tem uma raiz $\beta \in \mathbb{C}$.
Assim, pelo Teorema de D'Alembert,
$f(x) = q(x)(x - \beta)$, para algum $q(x) \in \mathbb{C}[x]$ e $grau(q) = n$.
Pela hipótese de indução, temos que existem $a, \beta_1, \beta_2, ..., \beta_n \in \mathbb{C}$, com $a \neq 0$, tais que

$$q(x) = a(x - \beta_1)(x - \beta_2)...(x - \beta_n)$$

Assim

$$f(x) = a(x - \beta_1)(x - \beta_2)...(x - \beta_n)(x - \beta)$$

Logo, ao tomarmos $\beta_{n+1} = \beta$, obtemos

$$f(x) = a(x - \beta_1)(x - \beta_2)...(x - \beta_n)(x - \beta_{n+1})\blacksquare$$

Exemplo 26 *Considere $f(x) = x^4 + 1 \in \mathbb{C}[x]$. As raízes de $f(x)$ são $\beta_1 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, $\beta_2 = +\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$, $\beta_3 = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ e $\beta_4 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$. Portanto,*

$$f(x) = \left(x - (\tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i)\right) \cdot \left(x - (\tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}i)\right) \cdot \left(x - (-\tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i)\right) \cdot \left(x - (-\tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}i)\right)$$

Observamos que $f(x) = (x^2 + \sqrt{2}x + 1) \cdot (x^2 - \sqrt{2}x + 1)$ é a fatoração em polinômios mônicos e irredutíveis em $\mathbb{R}[x]$.

4 MÉTODO DE KRONECKER

O método a ser descrito nesta seção, denominado Método de Kronecker, é um algoritmo para encontrar um fator próprio, caso exista, de um polinômio $f(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$, e quando aplicado recursivamente chegará na fatoração completa do polinômio.

- Se $f(x)$ for um polinômio redutível de grau n então $f(x) = g(x) \cdot h(x)$,
  com $1 \leq grau(g) \leq grau(h) < n$. Dizemos que $g(x)$ e $h(x)$ são fatores próprios de $f(x)$, também dizemos que $h(x)$ é um cofator correspondente ao fator $g(x)$.
  Observando que $grau f(x) = grau(g) + grau(h)$, temos que $grau(g) \leq \dfrac{n}{2}$ ou $grau(g) \leq \dfrac{n-1}{2}$, respectivamente, quando n é par ou n é ímpar.
  Procuraremos então um fator $g(x)$ e o método será conclusivo, isto é, determinaremos um fator próprio ou, caso contrário, o polinômio $f(x)$ será irredutível.

- Usaremos o fato que $K[x]$, onde K é um corpo, é um espaço vetorial sobre K, com as operações usuais de adição e multiplicação por um escalar. Considerando os polinômios de $K[x]$, de grau menor do que ou igual a n, teremos um subespaço vetorial de dimensão $n+1$ com a base canônica $\{1, x, x^2, \ldots, x^n\}$.

- Dados inteiros distintos $r_0, r_1, ..., r_n$ consideraremos os polinômios interpoladores de Lagrange, definidos para cada $i = 0, ..., n$ por

$$l_i(x) = \frac{(x - r_0) \cdots (x - r_{i-1}) \cdot (x - r_{i+1}) \cdots (x - r_n)}{(r_i - r_0) \cdots (r_i - r_{i-1}) \cdot (r_i - r_{i+1}) \cdots (r_i - r_n)}$$

  onde

$$l_i(r_j) = \begin{cases} 1 \text{ se } j = i \\ 0 \text{ se } j \neq i \end{cases}$$

  Assim temos $n+1$ polinômios de grau igual a n.

Proposição 10 *Os polinômios interpoladores de Lagrange $l_0, l_1, \ldots, l_n$ formam uma base do espaço vetorial dos polinômios de grau menor ou igual a n em $\mathbb{Q}$.*

Demonstração: Como o conjunto $S = \{l_0, l_1, \ldots, l_n\}$ tem $n+1$ elementos, basta provar que $l_0, l_1, \ldots, l_n$ são linearmente independentes e portanto se trata de uma base. Suponhamos que

$$c_0 l_0(x) + c_1 l_1(x) + \cdots + c_n l_n(x) = 0 \text{ onde } c_0, c_1, \cdots, c_n \in \mathbb{Q}$$

Para cada $0 \leq j \leq n$, substituindo $x = r_j$ nesta expressão, obtemos $c_j = 0$.
Portanto os elementos de S são linearmente independentes.■

No lema seguinte, consideraremos polinômios em $\mathbb{Z}[x]$.
Dizemos que $f(x)$ é irredutível sobre $\mathbb{Z}$ (de modo análogo à definição dada anteriormente, sobre K) quando:
Se $f(x) = g(x) \cdot h(x)$ com $g(x), h(x) \in \mathbb{Z}[x]$, então $f(x)$ ou $g(x)$ é um polinômio constante não nulo.

Lema 7 ***(Lema de Gauss)*** *Seja $f(x) \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$, então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração: Suponhamos que $f(x) \in \mathbb{Z}[x]$ seja redutível sobre $\mathbb{Q}$, isto é, $f(x) = g(x).h(x)$, onde $g(x), h(x) \in \mathbb{Q}[x]$ e $1 \leq grau(g), grau(h) < grau(f)$.
Como $g(x), h(x) \in \mathbb{Q}[x]$, segue que existe um inteiro positivo m, tal que

$$m \cdot f(x) = g_1(x) \cdot h_1(x) \text{ , onde } g_1(x), h_1(x) \in \mathbb{Z}[x]$$

Assim temos, $g_1(x) = a_0 + a_1 x + ... + a_r x^r$ com $a_i \in \mathbb{Z}$ e $h_1(x) = b_0 + b_1 x + ... + b_s x^s$ com $b_i \in \mathbb{Z}$.
Suponha que $p \mid m$, p primo.
Provaremos que $p \mid a_i \forall i \in \{1, ..., r\}$ ou $p \mid b_j, \forall j \in \{1, ..., s\}$.
De fato, se $\exists i \in \{1, ..., r\}$ e $\exists j \in \{1, ..., s\}$ tais que $p \nmid a_i$ e $p \nmid b_j$ consideremos i e j os menores possíveis com esta propriedade.

Como $p \mid m$ temos que p divide o coeficiente de x^{i+j} do polinômio $m.f(x) = g_1(x).h_1(x)$, isto é, $p \mid (b_0a_{i+j} + b_1a_{i+j-1} + b_2a_{i+j-2} + ... + b_ja_i + ... + b_{i+j-1}a_1 + b_{i+j}a_0)$.

Pela nossa escolha de i e j temos que p divide cada parcela, exceto b_ja_i do coeficiente de x^{i+j} de $g_1(x).h_1(x)$.

Como p divide toda a expressão segue também que $p \mid b_ja_i$ e como p é um número primo temos que $p \mid b_j$ ou $p \mid a_i$ o que é uma contradição.

Assim, se p é primo, $p \mid m \Rightarrow p \mid a_i \forall i \in \{1, ..., r\}$ ou $p \mid b_j \forall \in \{1, ..., s\}$.

Sem perda de generalidade, suponhamos que $p \mid a_i \ \ \forall i \in \{1, 2, ..., r\}$.

Assim, $g_1(x) = pg_2(x)$, onde $g_2(x) \in \mathbb{Z}[x]$ e se $m = p.m_1$ temos

$$p.m_1f(x) = pg_2(x).h_1(x)$$

$$m_1.f(x) = g_2(x).h_1(x)$$

Como o número de fatores primos de m é finito, prosseguindo com o argumento acima, chegaremos que:

$$f(x) = g^*(x) \cdot h^*(x) \text{ onde } g^*(x), h^*(x) \in \mathbb{Z}[x]$$

Portanto $f(x)$ é redutível em $\mathbb{Z}$.■

Veremos como funcionará o método nos dois exemplos seguintes.

Exemplo 27 *Seja* $f(x) = x^7 + 4x^6 + 7x^5 + 21x^4 + 21x^3 + 2x^2 + 35x + 7$.

Como $grau(f) = 7 = 2 \cdot 3 + 1$, *procuraremos um fator* $g(x)$ *de grau* ≤ 3 *e assim escolhendo* $r_0 = 0, r_1 = 1, r_2 = 2$ *e* $r_3 = 3$ *teremos 4 polinômios interpoladores de grau* 3*:*

$$l_0(x) = \frac{(x-1)(x-2)(x-3)}{(0-1)(0-2)(0-3)} = -\frac{(x-1)(x-2)(x-3)}{6}$$

$$l_1(x) = \frac{(x-0)(x-2)(x-3)}{(1-0)(1-2)(1-3)} = \frac{x(x-2)(x-3)}{2}$$

$$l_2(x) = \frac{(x-0)(x-1)(x-3)}{(2-0)(2-1)(2-3)} = -\frac{x(x-1)(x-3)}{2}$$

$$l_3(x) = \frac{(x-0)(x-1)(x-2)}{(3-0)(3-1)(3-2)} = \frac{x(x-1)(x-2)}{6}$$

Os polinômios l_0, l_1, l_2, l_3 formam uma base do espaço vetorial dos polinômios de grau menor ou igual a 3 sobre $\mathbb{Q}$.

Suponhamos então que g seja um fator próprio de f, com $grau(g) \leq 3$, com cofator h. Como l_0, l_1, l_2, l_3 é uma base podemos escrever g como uma combinação linear dos polinômios l_i com coeficientes racionais, assim

$$g(x) = c_0 l_0(x) + c_1 l_1(x) + c_2 l_2(x) + c_3 l_3(x)$$

Observamos que, $g(0) = g(r_0) = c_0, g(1) = g(r_1) = c_1, g(2) = g(r_2) = c_2$ e $g(3) = g(r_3) = c_3$.

Neste ponto, como $f(x) \in \mathbb{Z}[x]$, podemos assumir que $g(x) \in \mathbb{Z}[x]$. De fato, se $f(x)$ tem fatores próprios com coeficientes racionais, então tem que ter fatores próprios com coeficientes inteiros (Lema de Gauss).

Para determinarmos o polinômio g, precisamos encontrar os respectivos valores dos coeficientes $c_0, c_1, c_2, c_3 \in \mathbb{Z}$.

Da decomposição $f = g.h$, segue que $f(r_j) = g(r_j)h(r_j)$ e assim $g(r_j) = c_j$ é fator do inteiro $f(r_j)$, para cada $0 \leq j \leq 3$.

Como f é conhecido, podemos fatorar o inteiro $f(r_j)$ e testar todas as possibilidades de fatores como possíveis valores para c_j, para cada $0 \leq j \leq 3$.

Precisamos agora fatorar $f(r_i) = f(i)$, para $0 \leq i \leq 3$. Denotando por D_i o conjunto dos divisores de $f(i)$, devemos agora escolher $c_i \in D_i$ de todas as maneiras possíveis, construir os polinômios

$$c_0 l_0(x) + c_1 l_1(x) + c_2 l_2(x) + c_3 l_3(x)$$

correspondentes e verificar, um a um, se dividem $f(x)$. Paramos ao encontrar o primeiro fator.

Para termos certeza que consideramos todas as combinações possíveis de divisores tomaremos $S = D_0 \times D_1 \times D_2 \times D_3$ e usaremos a ordem lexicográfica na listagem dos elementos de S.

Assim, comparando duas (4)-uplas, na primeira posição onde as entradas são diferentes, a menor será a que tiver a entrada menor. Por exemplo $(1, -2, 5, 7) < (1, -2, 6, 2)$.

Determinaremos então $f(r_i)$*, com* $0 \leq i \leq 3$*, e então verificarmos seus possíveis divisores.*

$$f(0) = 0^7 + 4.0^6 + 7.0^5 + 21.0^4 + 21.0^3 + 2.0^2 + 35.0 + 7 = 7$$

$$f(1) = 1^7 + 4.1^6 + 7.1^5 + 21.1^4 + 21.1^3 + 2.1^2 + 35.1 + 7 = 98$$

$$f(2) = 2^7 + 4.2^6 + 7.2^5 + 21.2^4 + 21.2^3 + 2.2^2 + 35.2 + 7 = 1197$$

$$f(3) = 3^7 + 4.3^6 + 7.3^5 + 21.3^4 + 21.3^3 + 2.3^2 + 35.3 + 7 = 9202$$

Originando assim a seguinte tabela dos divisores de $f(i)$*:*

i	$f(r_i)$	*Divisores de* $f(r_i)$ *"*D_i*"*
0	7	$\pm 1, \pm 7$
1	98	$\pm 1, \pm 2, \pm 7, \pm 14, \pm 49, \pm 98$
2	1197	$\pm 1, \pm 3, \pm 7, \pm 9, \pm 19, \pm 21, \pm 57, \pm 63, \pm 133, \pm 171, \pm 399, \pm 1197$
3	9202	$\pm 1, \pm 2, \pm 43, \pm 86, \pm 107, \pm 214, \pm 4601, \pm 9202$

Aplicando o algoritmo de Kronecker aos elementos de S*, listados na ordem lexicográfica, teremos que verificar* 5877 *elementos antes de encontrarmos a* 4*-upla* $(-1, -7, -19, -43)$ *e daí* $g(x) = c_0 l_0(x) + c_1 l_1(x) + c_2 l_2(x) + c_3 l_3(x) = -1 l_0(x) + -7 l_1(x) - 19 l_2(x) - 43 l_3(x) = x^3 + 5x + 1$ *. Para finalizar, usando o Algoritmo da Divisão, determinamos o cofator* $h(x) = x^4 + 4x^3 + 2x^2 + 7$ *de* $f(x)$ *relacionado a* $g(x)$*.*

Levando em conta o exemplo acima, o método envolve um número excessivo de cálculos e só é viável quando é feito por um computador.

Exemplo 28 *Seja* $f(x) = x^4 + 2x^3 + x^2 - 1$*, usando o Algoritmo de Kronecker, mostraremos que* $f(x) = g(x).h(x)$ *com* $g(x) = x^2 + x + 1$ *e* $h(x) = x^2 + x - 1$*.*

Assim, como $grau(f) = 4 = 2 \cdot 2$, *escolheremos inteiros* r_j *para cada* $0 \leq j \leq 2$. *Tomando* $r_0 = 0, r_1 = 1$ *e* $r_2 = -1$, *teremos os seguintes polinômios interpoladores de Lagrange:*

$$l_0(x) = \frac{(x - r_1).(x - r_2)}{(r_0 - r_1).(r_0 - r_2)} = \frac{(x-1).(x-(-1))}{(0-1).(0-(-1))} = -\frac{(x-1).(x+1)}{1}$$

$$l_1(x) = \frac{(x - r_0).(x - r_2)}{(r_1 - r_0).(r_1 - r_2)} = \frac{(x-0).(x-(-1))}{(1-0).(1-(-1))} = \frac{x.(x+1)}{2}$$

$$l_2(x) = \frac{(x - r_0).(x - r_1)}{(r_2 - r_0).(r_2 - r_1)} = \frac{(x-0).(x-1)}{(-1-0).(-1-1)} = \frac{x.(x-1)}{2}$$

Temos que $l_i(r_i) = 1$ *e* $l_i(r_j) = 1$ *quando* $i \neq j$, *e* $\{l_0, l_1, l_2\}$ *formam uma base do espaço vetorial dos polinômios de grau menor ou igual a* 2 *sobre* $\mathbb{Q}$.

Assim existem coeficientes $c_0, c_1, c_2 \in \mathbb{Q}$ *tais que*

$$g(x) = c_0 l_0(x) + c_1 l_1(x) + c_2 l_2(x)$$

Como $f(x) \in \mathbb{Z}$ *podemos assumir que* $c_0, c_1, c_2 \in \mathbb{Z}$ *(Lema de Gauss).*

Agora determinaremos os possíveis fatores de $f(r_i)$, *para* $0 \leq i \leq 2$.

$$f(r_0) = 0^4 + 2.0^3 + 0^2 - 1 = -1$$

$$f(r_1) = 1^4 + 2.1^3 + 1^2 - 1 = 2$$

$$f(r_2) = (-1)^4 + 2.(-1)^3 + (-1)^2 - 1 = -1$$

Organizando a tabela dos divisores, teremos:

i	$f(r_i)$	*Divisores de* $f(r_i)$ *"*D_i*"*
0	-1	± 1
1	2	$\pm 1, \pm 2$
2	-1	± 1

Organizando as possíveis 3*-uplas de* $S = D_0 \times D_1 \times D_2$ *em ordem lexicográfica, ao todo* 16 *possibilidades distintas listadas na tabela abaixo.*

linha	d_1	d_2	d_3
1	-1	-1	-1
2	-1	-1	1
3	-1	1	-1
4	-1	1	1
5	1	-1	-1
6	1	-1	1
7	1	1	-1
8	1	1	1
9	-1	-3	-1
10	-1	-3	1
11	-1	3	-1
12	-1	3	1
13	1	-3	-1
14	1	-3	1
15	1	3	-1
16	1	3	1

Fazendo os devidos testes, verificamos que a terceira 3*-upla* $(-1, 1, -1)$ *determina um dos fatores de* $f(x)$ *. Assim, substituindo a mesma em* $g = c_0 l_0(x) + c_1 l_1(x) + c_2 l_2(x)$*, resultará o fator* $g(x) = -1l_0(x) + 1l_1(x) - 1l_2(x) = x^2 + x - 1$*.*

Usando o Algoritmo da divisão, determinamos o cofator $h(x) = x^2 + x + 1$*.*

5 CONSIDERAÇÕES FINAIS

Com este trabalho, tivemos a oportunidade de rever conceitos e resultados estudados na graduação, aplicados no estudo de polinômios. No desenvolvimento procuramos usar uma linguagem elementar, por exemplo, ao provar a existência do MDC usamos o conceito de Ideal sem formalizá-lo. Também tivemos a preocupação de explicar com detalhes alguns algoritmos aplicados no ensino médio.

Apesar de não realizarmos um estudo específico, objetivando o Teorema Fundamental da Álgebra (TFA), o mesmo é demonstrado de uma forma elementar, utilizando conhecimentos de análise.

Apesar de grande parte do conteúdo estudado aqui não ser ensinado com tantos detalhes e com demonstrações no ensino básico, este poderá ser destinado a formação complementar dos professores, esperando assim que esta dissertação possa ser usada por professores do ensino médio como referência para o planejamento de aulas e atividades envolvendo polinômios.

6 APÊNDICE A
TEOREMA FUNDAMENTAL DA ÁLGEBRA

Neste apêndice faremos uma prova do Teorema Fundamental da Álgebra (TFA). Considerando um exemplo, temos $p(x) = x^2 + 1$ que não possui raízes reais, possui duas raízes complexas i e $-i$ e assim se decompõe como produto de polinômios de grau um,

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

De fato, qualquer polinômio $p(x)$ em $\mathbb{C}[x]$, possui uma raíz complexa e, consequentemente, qualquer polinômio $p(x) \neq 0$ pode ser decomposto como produto de polinômios de grau um,

$$p(x) = a(x - z_1) \cdot (x - z_2) \cdots (x - z_n)$$

onde $a \in \mathbb{R}$, n é o grau de $p(x)$ e $z_1, z_2, \ldots z_n$ são suas raízes complexas, não necessariamente distintas.

Antes de enunciarmos formalmente o TFA, listaremos alguns fatos sobre funções complexas que serão utilizados na demonstração do teorema. Além disso, provaremos dois resultados que também serão usados.

- Considere $(\mathbb{C}, +, \cdot)$ o corpo dos números complexos, onde se
  $z_1 = a + bi, z_2 = c + di \in \mathbb{C}$, então

  $$z_1 + z_2 = (a + c) + (b + d)i \text{ e } z_1 \cdot z_2 = (ac - bd) + (ad + bc)i$$

- Em $(\mathbb{C}, +, \cdot)$, definimos a norma de um complexo $z = a + bi$ como

  $$|z| = \sqrt{a^2 + b^2}$$

  Se $z_1, z_2 \in \mathbb{C}$, então $|z_1 + z_2| \leq |z_1| + |z_2|$ e $||z_1| - |z_2|| \leq |z_1 + z_2|$.

- Considere $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{C}[x]$. Uma função $f : \mathbb{C} \to \mathbb{C}$, definida por

$$f(z) = a_0 + a_1 \cdot z + \cdots + a_n \cdot z^n$$

  é denominada função polinomial.

- Se $f : \mathbb{C} \to \mathbb{C}$ é uma função polinomial, então f é uma função contínua.

- Seja $f : D \to \mathbb{C}$ uma função contínua, onde $D = \{z \in \mathbb{C} \mid |z| \leq r\}$ é um disco fechado de raio $r \geq 0$. Então existe $z_0 \in D$ tal que $|f(z_0)| \leq |f(z)|$, para todo $z \in D$, isto é , $|f|$ possui um mínimo em D.

- Se $f : D \to \mathbb{C}$, definida num disco fechado de raio $r \geq 0$, é polinomial, então $|f|$ possui um mínimo em D.

Lema 1 *Seja $f : \mathbb{C} \to \mathbb{C}$ uma função polinomial, definida por*

$$f(z) = a_0 + a_1 \cdot z + \cdots + a_n \cdot z^n,\ n \geq 1$$

Então, para cada número real $M > 0$ existe um número real $R > 0$ tal que

$$|z| > R \Longrightarrow |f(z)| \geq M$$

Demonstração: Faremos a prova usando indução finita sobre n.
Suponha $n = 1$. Neste caso $f(z) = a_0 + a_1z$, com $a_1 \neq 0$ e

$$|f(z)| = |a_0 + a_1z| \geq |a_1z| - |a_0| = |a_1|.|z| - |a|$$

Dado $M > 0$ escolha $R = \dfrac{M + |a_0|}{a_1}$, isto é, $M = R|a_1| - |a_0|$ e daí

$$|z| > R \Longrightarrow |f(z)| \geq |a_1|.|z| - |a_0| \geq |a_1|.R - |a_0| = M$$

Suponha agora a afirmação verdadeira para $n - 1 \geq 1$.
Escrevendo $f(z) = a_0 + z \cdot (a_1 + \cdots + a_n \cdot z^{n-1})$ temos que $f(z) = a_0 + z \cdot f_1(z)$.
Dado $M > 0$, escolha $R \geq 1$ (hipótese de indução) tal que

$$|z| > R \Longrightarrow |f_1(z)| \geq M + |a_0|$$

Daí para $M > 0$ temos

$$|f(z)| = |a_0 + zf_1(z)| \geq |z||f_1(z)| - |a_0| \geq R|f_1(z)| - |a_0|$$

$$R|f_1(z)| - |a_0| \geq |f_1(z)| - |a_0| \geq M + |a_0| - |a_0| = M$$

Portanto, $|f(z)| \geq M$ e a afirmação é verdadeira para n.■

Proposição 11 *Seja $f : \mathbb{C} \to \mathbb{C}$ uma função polinomial, definida por*

$$f(z) = a_0 + a_1 \cdot z + \cdots + a_n \cdot z^n,\ n \geq 1$$

Então, existe $z_0 \in \mathbb{C}$ tal que $|f(z_0)| \leq |f(z)|$, para todo $z \in \mathbb{C}$.

Demonstração: Usando o Lema anterior, dado $M = 1 + |a_0|$ existe $R > 0$ tal que

$$|z| > R \Longrightarrow |f(z)| \geq 1 + |a_0|$$

Considerando o disco fechado $D = \{z \in \mathbb{C} \mid |z| \leq R\}$ e usando o resultado enunciado anteriormente temos que, existe $z_0 \in D$ tal que ($|f|$ tem um mínimo em D)

$$|f(z_0)| \leq |f(z)|, \forall z \in D$$

Suponha agora $z \in \mathbb{C} \setminus D$, isto é, $z \in \mathbb{C}$ e $|z| > R$.
Segue que $|f(z)| \geq 1 + |a_0|$ e como $0 \in D$ temos que $|f(z_0)| \leq |f(0)| = a_0$.
Daí $f(z) \geq 1 + |a_0| \geq |a_0| \geq |f(z_0)|$, logo $|f(z_0)| \leq |f(z)|$, para todo $z \in \mathbb{C} \setminus D$.
Portanto, $|f(z_0)| \leq |f(z)|$, para todo $z \in \mathbb{C}$.■

Teorema 8 *(Teorema Fundamental da Álgebra)*
Todo polinômio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{C}[x]$ de grau n, com $n \geqslant 1$, possui uma raiz complexa.

Demonstração: Considere a função polinomial $f : \mathbb{C} \to \mathbb{C}$ definida por $f(z) = a_0 + a_1 \cdot z + \cdots + a_n \cdot z^n$
Temos que, usando a proposição anterior, existe $z_0 \in \mathbb{C}$ tal que $f(z_0) \leq |f(z)|$, para todo

$z \in \mathbb{C}$.

Vamos mostrar que $f(z_0) = a_0 + a_1 \cdot z_0 + \cdots + a_n \cdot z_0^n = 0$, isto é, z_0 é uma raíz do polinômio $f(x)$.

Fazendo a mudança de variáveis $z = w + z_0$, então $f(z) = f(w + z_0) = g_1(w)$ é uma função polinomial e

$$|g_1(0)| = |f(z_0)| \leq |f(z)| = |g_1(w)|, \forall w \in \mathbb{C}$$

Assim, $|f(z_0)| = |g_1(0)|$ e $|g_1|$ tem um mínimo global em $w = 0$.

Suponhamos, por absurdo, que $|f(z_0)| = |g_1(0)| = a \neq 0$

Temos que $f(z) = f(w + z_0) = a_0 + a_1 \cdot (w + z_0) + \cdots + a_n \cdot (w + z_0)^n = g_1(w)$ e assim

$$g_1(w) = a + a_1^{'} w + \cdots + a_n{}' w^n$$

Tomando $g_2(w) = \dfrac{g_1(w)}{a} = 1 + b_1^{'} w + \cdots b_n^{'} w^n$ e escolhendo b o primeiro coeficiente não nulo, a partir do termo constante, de $g_2(w)$ podemos escrever

$$g_2(w) = 1 + bw^m + b_1 w^{m+1} + ... + b_k w^{m+k}, \text{ onde } m + k = n$$

Considere r a m-ésima raiz de $-\dfrac{1}{b}$, isto é, $br^m = -1$.

Agora tome $w = ru$ e $g(u) = g_2(w) = g_2(ru)$.

Temos $|g(u)| = |g_2(w)| = \left|\dfrac{g_1(w)}{a}\right| \geq \left|\dfrac{g_1(0)}{a}\right| = |g_2(0)| = |g(0)| = 1$

Portanto, $|g(u)|$ tem um mínimo em $u = 0$.

Temos que

$$g(u) = 1 + b(ru)^m + b_1(ru)^{m+1} ... + b_k(ru)^{m+k} = 1 - u^m + u^{m+1} G(u)$$

onde

$$G(u) = c_1 + c_2 u + ... + c_k u^{k-1} \text{ com } c_j = b_j r^{m+j}, 1 \leq j \leq k$$

.

Considere $t > 0$ real. Fazendo $u = t$ e calculando $|G(t)|$,

$$|G(t)| = |c_1 + c_2 t + ... + c_k t^{k-1}| \leq |c_1| + |c_2 t + ... + c_k t^{k-1}| = G_0(t)$$

Como $\lim\limits_{t \to 0^+} tG_0(t) = 0$, escolha $0 < t < 1$ tal que $tG_0(t) < 1$ e daí,

$$|g(t)| = |1 - t^m + t^{m+1} G(t)| \leq |1 - t^m| + |t^{m+1} G(t)| = |(1 - t^m)| + t^m t|G(t)| \leq |(1 - t^m)| + t^m (tG_0(t))$$

$$|g(t)| \leq (1 - t^m) + t^m(tG_0(t)) < (1 - t^m) + t^m = 1 = |g(0)|$$

Mas isto contradiz o fato que 0 é um mínimo de $|g|$.

Portanto $f(z_0) = 0$.■

Referências Bibliográficas

[1] BAUMGART, J. K. *Álgebra: Tópicos de História da Matemática.* Atual, São Paulo, 1992.

[2] BIAZZI, R. N. *Polinômios Irredutíveis: Critérios e Aplicações.* Dissertação de Mestrado - PROFMAT/UNESP, Rio Claro, 2014.

[3] Callioli, Carlos A. *Álgebra Linear a Aplicações / Carlos A. Callioli; Hygino H. Domingos; Roberto C. F. Costa.* Atual, São Paulo, 1990.

[4] DELBONI, R. R. *Teorema Fundamental da Ágebra.* Monografia referente a disciplina Elementos de Álgebra - UNICAMP/IMECC, Campinas, 2006.

[5] Esquinca, J. P. C. *Aritmética: Código de Barras e Outras Aplicações de Congruências.* Dissertação de Mestrado - PROFMAT/UFMS, Campo Grande, 2013.

[6] GARCIA Arnaldo *ÁLgebra: Um Curso de Introdução.* Rio de Janeiro, IMPA, 1988.

[7] GONÇALVES, Adilson *Introdução à Álgebra / Adilson Gonçalves.* Projeto Euclides, IMPA, Rio de Janeiro, 2006.

[8] HEFEZ, Abramo *Polinômios e Equações Algébricas / Abramo Hefez; Maria Lucia Torres Villela.* SBM, Rio de Janeiro, 2012.

[9] IEZZI, G. *Matemática: volume único / Gelson Iezzi; Osvaldo Dolce; David Degenszajn; Roberto Périgo.* Atual, São Paulo, 2002.

[10] S. C. Coutinho *Polinômios e Computação Algébrica.* IMPA, Rio de Janeiro, 2012.

[11] S. C. Coutinho *Primalidade em tempo Polinomial: Uma introdução ao Algoritmo AKS.* Coleção Iniciação Científica, SBM, Rio de Janeiro, 2004.