UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Departamento de Ciências Exatas e da Terra

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Dissertação de mestrado

UMA INTRODUÇÃO AOS NÚMEROS ALGÉBRICOS COM APLICAÇÕES PARA O ENSINO MÉDIO

Rodrigo Novaes Dourado

Orientador: Prof. Dr. Maurício de Araújo Ferreira

Feira de Santana

Outubro de 2017

UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Departamento de Ciências Exatas e da Terra

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

UMA INTRODUÇÃO AOS NÚMEROS ALGÉBRICOS COM APLICAÇÕES PARA O ENSINO MÉDIO

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Departamento de Ciências Exatas, UEFS, como requisito parcial para a obtenção do título de **Mestre**.

Orientador: Prof. Dr. Maurício de Araújo Ferreira

Feira de Santana

Outubro de 2017

Ficha Catalográfica - Biblioteca Central Julieta Carteado

D771i Dourado, Rodrigo Novaes
Uma introdução aos números algébricos com aplicações para o Ensino Médio / Rodrigo Novaes Dourado. – 2017.
55 f.: l.

Orientador: Maurício de Araújo Ferreira.
Dissertação (mestrado) – Universidade Estadual de Feira de Santana, Programa de Pós-Graduação em Matemática em Rede Nacional, 2017.

1. Álgebra – Ensino Médio. 2. Matemática – Estudo e ensino. I. Ferreira, Maurício de Araújo, orient. II. Universidade Estadual de Feira de Santana. III. Título.

CDU: 512

UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA
DEPARTAMENTO DE CIÊNCIAS EXATAS
Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

ATA DA SESSÃO PÚBLICA DE DEFESA DE DISSERTAÇÃO DO DISCENTE RODRIGO NOVAES DOURADO DO PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL DA UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Aos dezoito dias do mês de outubro de dois mil e dezessete às 10:00 horas no Auditório da PPGM - Módulo 5, UEFS , ocorreu a Sessão pública de defesa de dissertação apresentada sob o título **"Uma Introdução aos Números Algébricos com Aplicações para o Ensino Médio"**, do discente **Rodrigo Novaes Dourado**, do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Estadual de Feira de Santana, para obtenção do título de MESTRE. A Banca Examinadora foi composta pelos professores: Maurício de Araujo Ferreira (Orientador, UEFS), Manuela da Silva Souza (UFBA) e Kisnney Emiliano de Almeida (UEFS). A sessão de defesa constou da apresentação do trabalho pelo discente e das arguições dos examinadores.
Em seguida, a Banca Examinadora se reuniu em sessão secreta para julgamento final do trabalho e atribuiu o conceito: aprovado.
Sem mais a tratar, foi lavrada a presente ata, que segue assinada pelos membros da Banca Examinadora e pelo Coordenador Acadêmico Institucional do PROFMAT. Feira de Santana, 18 de outubro de 2017.

Prof. Dr. Maurício de Araujo Ferreira (UEFS)
Orientador

Profa. Dra. Manuela da Silva Souza (UFBA)

Prof. Dr. Kisnney Emiliano de Almeida (UEFS)

Visto do Coordenador:

Prof. Dr. Haroldo Gonçalves Benatti
Coordenador do PROFMAT/UEFS

Agradecimentos

A Deus, pelos cuidados divinos e pelas graças derramadas em minha vida;

Aos meus pais, Francisco e Líria, pelo exemplo, incentivo, amor e dedicação. Vocês são os maiores responsáveis por mais esta conquista.

A minha esposa, Naiane Ribeiro, pela paciência, apoio e por todo amor a mim dedicado.

Aos meus irmãos Franco e Francielle por me darem forças e sempre estarem ao meu lado.

Aos meus filhos, Maria Eduarda e Rodrigo Filho, por trazerem felicidade aos meus dias e por serem minha motivação.

Ao meu professor orientador Dr Maurício Ferreira pela dedicação, por estar sempre disponível independente de dia e horário e por não duvidar da minha capacidade em desenvolver este trabalho.

Aos demais professores que com suas aulas enriqueceram nosso saber.

À CAPES pelo apoio financeiro.

Resumo

Este trabalho tem por objetivo apresentar uma pequena introdução sobre os Números Algébricos e Aplicações para o Ensino Médio. Um Número Algébrico é um número complexo que é raiz de um polinômio não nulo de coeficientes racionais. Neste trabalho faremos uma revisão de polinômios, as operações e suas principais propriedades, em seguida definiremos Números Algébricos e Propriedades. Ao final desta dissertação são apresentadas atividades e suas respectivas soluções, que podem ser aplicadas no Ensino Médio.

Palavras-chaves: Polinômios, Números Algébricos, Álgebra.

Abstract

This paper aims to present a short introduction about the Algebraic Numbers.An Algebraic Number is a complex number that is the root of a nonzero polynomial of rational coeficients .In this work we will review polynomials, operations and their main prperties, then we will define Algebraic Numbers and Properties. At the end of this dissertation are presented activities and their respective solutions, which can be applied in High Scholl.

Keywords: Polynomials, Algebraic Numbers, Algebra.

Conteúdo

Introdução

O ensino de polinômios geralmente é trabalhado inicialmente nos 7º e 8º anos do ensino fundamental e posteriormente no 3º ano do ensino médio. Vimos no entanto que o conteúdo de polinômios já nem faz parte do programa de algumas escolas, inclusive algum livros didáticos não apresentam o tema no ensino médio. Os livros didáticos que ainda os apresentam como conteúdo, expressam maior ênfase no processo e método do que no conceito, utilizando exercícios maçantes e repetitivos, priorizando muito a mecanização, a exemplo do uso exacerbado da fórmula de Bhaskara. Metodologia que diverge do PCN de Matemática (Parâmetros Curriculares Nacionais), cuja proposta sugere uma maior ênfase no conceito e em sua importância e não em gravar métodos de resolução.

Neste trabalho apresentamos tópicos do conteúdo de polinômios e números algébricos trazendo as principais definições, demonstrando resultados importantes e sugerindo problemas que possam ser trabalhados no ensino médio. Um número algébrico é qualquer número real ou complexo que é solução de alguma equação polinomial com coeficientes racionais, caso contrário é dito transcendente. A Teoria dos Números é um ramo da matemática que teve seu impulso inicial na busca de soluções inteiras e racionais de equações a coeficientes inteiros (equações diofantinas). Entre outras coisas, isso levou ao estudo das extensões algébricas finitas do corpo dos racionais e ao estudo dos números algébricos e transcendentes.

No capítulo 1 é feito uma breve revisão de estrutura de anéis, polinômios e suas principais propriedades que serão utilizados ao longo do trabalho, enfatizando os polinômios irredutíveis e as possíveis raízes racionais. No capítulo 2, apresentaremos uma pequena introdução aos números algébricos, sua definição e algumas de suas propriedades. No capítulo 3 são propostas algumas atividades envolvendo polinômios e números algébricos que podem ser aplicadas no ensino médio e no capítulo 4 são apresentadas as respectivas soluções dos problemas.

Capítulo 1

Polinômios com coeficientes em um Anel

Iniciaremos este capítulo apresentando as definições de anel, polinômios, as operações e as principais propriedades. As principais referências para este capítulo são [6],[7] e [10] .

Em matemática, um anel é uma estrutura algébrica que consiste num conjunto não vazio munido de duas operações binárias, normalmente chamadas adição e multiplicação, sujeitas as certas regras. Neste capítulo apresentaremos, em especial, os anéis de polinômios, cujos elementos são polinômios na forma usual com coeficientes no anel dado. Apresentaremos também as propriedades e operações de tais elementos, formando assim resultados que serão apresentados ao longo do trabalho.

1.1 Anéis

Seja A um conjunto não vazio. Vamos definir duas operações, as quais chamaremos de *soma* e *produto* em A e denotaremos por $+$ e $\cdot$. Assim,

$$+ : A \times A \to A \qquad \cdot : A \times A \to A$$

$$(a, b) \rightsquigarrow a + b \qquad (a, b) \rightsquigarrow a \cdot b.$$

Definição 1.1. O trio $(A, +, \cdot)$ é um *Anel* se são verificadas as seguintes propriedades, para todos $a, b, c \in A$:

A1) $(a + b) + c = a + (b + c)$ (associatividade da soma);

A2) $a + b = b + a$ (comutatividade da soma);

A3) Existe $0 \in$ A tal que $a + 0 = 0 + a = a$ (existência do elemento neutro da soma);

A4) Para todo $x \in A$ existe um único y pertencente a A, denotado por $y = -x$, tal que $x + y = y + x = 0$ (existência do inverso aditivo);

A5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade do produto);

A6) $a \cdot (b + c) = a \cdot b + a \cdot c$; $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributividade à esquerda e à direita).

Se um anel $(A, +, \cdot)$ satisfaz a propriedade:

A7) Existe $1 \in A, 0 \neq 1$ tal que $x \cdot 1 = 1 \cdot x = x$ para todo $x \in A$,

dizemos que $A, +, \cdot$ é um *anel com unidade.*

Se um anel $(A, +, \cdot)$ satisfaz a propriedade:

A8) Para quaisquer $x, y \in A, x \cdot y = y \cdot x$,

dizemos que $A, +, \cdot$ é um *anel comutativo.*

Se um anel $(A, +, \cdot)$ satisfaz a propriedade:

A9) Para todo $x, y \in A$, se $x \cdot y = 0$ então $x = 0$ ou $y = 0$, dizemos que $(A, +, \cdot)$ é um *anel sem divisores de zero.*

Se $(A, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um *Domínio de Integridade.* Se $(A, +, \cdot)$ é um anel comutativo com unidade e tal que para todo $x \in A, x \neq 0$, existe $y \in A$ tal que $x \cdot y = y \cdot x = 1$, dizemos que A é um corpo.

Por uma questão de praticidade, quando não houver ambiguidade com relação às operações representaremos o anel $(A, +, \cdot)$ apenas por A.

Exemplo 1.1. $A = \mathbb{Z}$ é um anel comutativo com elemento unidade, com as operações usuais de adição e multiplicação dos inteiros, sendo o número 0 o elemento neutro da soma e o número 1, sendo o elemento unidade de $\mathbb{Z}$.

Exemplo 1.2. $n\mathbb{Z}$, o conjunto dos inteiros múltiplos de n, com as operações usuais, é um anel comutativo. Se $n \geq 2$ então $n\mathbb{Z}$ é anel comutativo que não possui unidade.

Exemplo 1.3. As classes de congruência de inteiros módulo n, com $n \geq 2$, com as operações usuais de soma e produto, também formam um anel comutativo com unidade:

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

Se n não é primo, então $\mathbb{Z}_n$ possui divisores de zero. Por exemplo, em $\mathbb{Z}_6$ temos $\overline{2} \cdot \overline{3} = 0$, logo $\overline{2}$ e $\overline{3}$ são divisores de zero. Lembremos que para todo $\overline{a}, \overline{b} \in \mathbb{Z}_n$, temos $\overline{a} = \overline{b} \Leftrightarrow$
$a \equiv b \bmod n \Leftrightarrow a$ e b deixam o mesmo resto quando divididos por n.

Exemplo 1.4. Se $\mathbb{Z}_n$ é um domínio de integridade então n é primo. De fato, suponhamos que n não seja primo, seja $n = ab, 1 < a, b < n$. Agora $n = ab$ implica que $\overline{0} = \overline{n} = \overline{a} \cdot \overline{b}$ onde $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$, ou seja, se $n > 2$ não for primo $\mathbb{Z}$ possui divisores de 0. Absurdo, pois por hipótese $\mathbb{Z}_n$ é um domínio.

Exemplo 1.5. $M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} ; a, b, c, d \in \mathbb{R} \right\}$, o anel de matrizes quadradas de ordem 2, com as operações usuais de matrizes, é um exemplo de anel com unidade não comutativo e com divisores de zero. Sejam

$a = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ e $b = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ elementos de $M_2(\mathbb{R})$ temos que $a, b \neq 0$, mas

$$a.b = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} . \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} .$$

Ou seja, o zero tem fatores não nulos, o que implica que não vale a lei do cancelamento para o produto. Além disso $a.b \neq b.a$, pois

$$b \cdot a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} .$$

Este fato pode ser generalizado para $M_n(\mathbb{R})$.

Definição 1.2. Seja $(A, +, \cdot)$ um anel. Dizemos que um subconjunto $B \subset A$, $B \neq \emptyset$, é um *subanel* de A se B é um anel com as mesmas operações de A. Usaremos a notação $B \leq A$ para representar que B é um subanel de A.

Observação 1.3. $\{0\}$ e A são sempre subanéis de A, chamados os **subanéis triviais**.

A proposição a seguir fornece um critério bastante útil para se determinar se um conjunto B é subanel de um anel A.

Proposição 1.4. *Seja $(A, +, \cdot)$ um anel e seja B um subconjunto de A. Então B é um subanel de A se, e somente se as seguintes condições são verificadas:*

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

(ii) $x, y \in B \Rightarrow x - y \in B$ (B é fechado para a soma e o inverso de todo elemento de B está em B) .

(iii) $x, y \in B \Rightarrow x \cdot y \in B$ (B é fechado para o produto).

Demonstração. ($\Rightarrow$) Se B é um subanel de A então por definição temos claramente as condições (i),(ii) e (iii).

Observe que o elemento neutro $0'$ de B relativamente à adição é o mesmo elemento neutro de A, pois se $b \in B$, então $0' = b + (-b) = 0$.

($\Leftarrow$) Suponhamos que $B \subset A$ e as três propriedades (i), (ii) e (iii) são satisfeitas. Por (i) segue que $B \neq \emptyset$, e por (i) e (ii) temos que: se $x \in B$ então $-x \in B$.

Agora, por (ii) teremos, se $x, y \in B$ então $x + y = x - (-y) \in B$, isto é B é fechado para a soma. Por (iii), B é fechado para o produto.

Como as propriedades associativa, comutativa e distributivas são hereditárias segue imediatamente que B é um subanel de A. □

Exemplo 1.6. (Inteiros de Gauss) O conjunto $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ é um subanel de $\mathbb{C}$. Note que $\mathbb{Z}[i] \neq \varnothing$. Sejam $x = (a + bi)$ e $y = (c + di)$ em $\mathbb{Z}[i]$. Daí $x - y = (a - c) + (b - d)i \in \mathbb{Z}[i]$ e $x \cdot y = (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$. Logo pela Proposição 1.4 $\mathbb{Z}[i]$ é subanel de $\mathbb{C}$.

Exemplo 1.7. Considere o conjunto $A = \mathbb{Q} - \mathbb{Z}$ que é formado pelos números racionais que não são inteiros. O mesmo não é subanel de $\mathbb{Q}$ pois por exemplo, $\frac{3}{2} \in A$ e $\frac{1}{2} \in A$, mas $\frac{3}{2} - \frac{1}{2} = 1 \notin A$. Logo A não é subanel de $\mathbb{Q}$.

Proposição 1.5. *Todo domínio de integridade finito é um corpo.*

Demonstração. Seja D um domínio de integridade com elemento identidade 1 e seja $a \in D \backslash \{0\}$. Vamos mostrar que a é invertível. Se $a = 1$ então a é seu próprio inverso. Seja $a \neq 1$, consideremos a sucessão $a, a^2, a^3, \cdots$ de elementos de D. Como D é finito, existem inteiros positivos i e j, com $i > j$ tais que $a^i = a^j \Leftrightarrow a^i - a^j = 0 \Leftrightarrow a^j(a^{i-j} - 1) = 0$. Como D é domínio $a^j \neq 0$ então $a^{i-j} = 1$. Mas $a \neq 1$ implica que $i - j > 1$, donde a^{i-j-1} é o inverso de a. □

Exemplo 1.8. $\mathbb{Z}_5$ é corpo pois é domínio de integridade finito.

Exemplo 1.9. Temos que $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ são exemplos de domínios de integridade, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ $(\mathbb{C}, +, \cdot)$ são corpos e $(\mathbb{Z}, +, \cdot)$ não é um corpo, porque nem todo elemento de $\mathbb{Z}$ possui inverso multiplicativo, por exemplo $2 \in \mathbb{Z}$ e não existe $y \in \mathbb{Z}$ tal que $2 \cdot y = 1$.

Definição 1.6. Um subconjunto K de um corpo L que, com as operações de adição e de multiplicação de L, é ainda um corpo, será chamado de subcorpo de L.

Exemplo 1.10. Temos $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, sendo $\mathbb{R}$ subcorpo de $\mathbb{C}$ e $\mathbb{Q}$ subcorpo de $\mathbb{R}$, logo $\mathbb{Q}$ também é subcorpo de $\mathbb{C}$.

1.2 Polinômios

Definição 1.7. Um *polinômio com coeficientes em um anel* A em uma indeterminada x é uma expressão do tipo

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

onde n é um numero natural e $a_i \in A$.

O conjunto de todos os polinômios na indeterminada x com coeficientes em A será denotado por $A[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in A \text{ e } n \in \mathbb{N}\}$. Note que $A \subset A[x]$.

Exemplo 1.11. São polinômios em $\mathbb{Z}[x]$:

1) $f(x) = -x^2 + 6x - 7$

2) $g(x) = 5 - 4x + 2x^{10} - x^6$.

Definição 1.8. Dados dois polinômios em $A[x]$,

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \text{ e } g(x) = b_0 + b_1x + \cdots + b_mx^m$$

com $n \geq m$ dizemos que $f(x) = g(x)$ se, e somente se

$$a_k = b_k, \text{ para todo } 0 \leq k \leq m \text{ e } a_k = 0 \text{ se } k > m.$$

Isto é $f(x) = g(x)$ são iguais apenas quando todos os coeficientes das correspondentes potências são iguais.

Exemplo 1.12. Os polinômios

$$f(x) = 1 + 2x + 3x^2 + x^3 \in \mathbb{Z}[x]$$

e

$$g(x) = 1 + 2x - 3x^2 + x^3 \in \mathbb{Z}[x]$$

não são iguais, pois $a_2 = 3 \neq -3 = b_2$. Já os polinômios

$$p(x) = 1 + 3x^2 + x^3 \in \mathbb{Z}[x]$$

e

$$q(x) = 1 + 0x + 3x^2 + x^3 \in \mathbb{Z}[x]$$

são iguais pois todos os seus coeficientes correspondentes são iguais.

Se $p(x) = 0+0x+\cdots+0x^n$ indicaremos $p(x)$ por 0 e o chamaremos de *polinômio identicamente nulo sobre A*. Assim um polinômio $p(x) = a_0 + a_1x + \cdots + a_nx^n$ sobre A é identicamente nulo se e somente se $a_i = 0$ para todo $i \in \mathbb{N}$.

Se $a \in A$ indicaremos por a o polinômio $p(x) = a_0 + a_1x + \cdots + a_nx^n$ onde $a_0 = a$ e $a_i = 0$ para todo $i \geq 1$. O polinômio $p(x) = a$ é o *polinômio constante*.

Em todo polinômio não identicamente nulo, $p(x) \neq 0$, algum coeficiente deve ser diferente de zero, então há um maior número natural n, tal que $a_n \neq 0$, que definimos como o grau de $p(x)$ e denotado por $\text{gr}(f(x)) = n$. Nesse caso, a_n é chamado de *coeficiente líder* de $p(x)$. Os polinômios de grau n com coeficiente líder $a_n = 1$ são chamados de *polinômios mônicos*.

Exemplo 1.13. São polinômios em $\mathbb{R}[x]$:

1) $r(x) = \frac{1}{2}x + \sqrt{3}x^2 + x^3$

2) $s(x) = 2 - \pi x^3 + \sqrt[3]{6}x^5$.

Observe que o $\text{gr}(r(x)) = 3$ e $\text{gr}(s(x)) = 5$ e $r(x)$ é polinômio mônico.

Observação 1.9. Não definimos o grau do polinômio identicamente nulo.

Exemplo 1.14. As expressões $p(x) = x^2 + 3\sqrt{x} + 3$ e $q(x) = x^{\frac{2}{3}} - 4x^2 + 5$ não são polinômios porque nem todos os expoentes da indeterminada x são números naturais.

1.2.1 Operações com Polinômios

Definiremos abaixo operações de *soma* e *produto* no conjunto $A[x]$.
Sejam $f(x)$ e $g(x)$ dois polinômios em $A[x]$, digamos

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

e

$$g(x) = b_0 + b_1x + \cdots + b_nx^m.$$

Podemos supor, sem perda de generalidade, que $m \leq n$.
Soma
$f(x) + g(x) \stackrel{def}{=} (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^n + a_{m+1}a^{m+1} + \cdots + a_nx^n$
Produto
$f(x) \cdot g(x) \stackrel{def}{=} c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$, onde os coeficientes c_k são definidos por

$$c_0 = a_0b_0$$

$$c_1 = a_0b_1 + a_1b_0$$

$$c_2 = a_0b_2 + a_1b_1 + a_2b_0$$

$$\vdots$$

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0 = \sum_{i=0}^{k} a_ib_{k-i}$$

para todo $k = 0, \ldots, m+n$.

Exemplo 1.15. Sejam $f(x) = x^3 + 8x^2 - 5x + 1$ e $g(x) = 2x^3 - 10x^2 + 4x - 9$ em $\mathbb{Z}[x]$. Então, $f(x) + g(x) = c_0 + c_1x + c_2x^2 + c_3x^3$ onde,

$c_0 = a_0 + b_0 = (1 + (-9)) = -8$;

$c_1 = a_1 + b_1 = (-5 + 4) = -1$;

$c_2 = a_2 + b_2 = (8 + (-10)) = -2$;

$c_3 = a_3 + b_3 = (1 + 2) = 3$.

Assim $f(x) + g(x) = -8 - x - 2x^2 + 3x^3$.

Exemplo 1.16. Sejam $f(x) = x^2 + 2x$ e $g(x) = x - 2$ em $\mathbb{Z}[x]$. Então

$f(x) \cdot g(x) = c_0 + c_1x + c_2 + c_3x^3$, onde

$c_0 = a_0 \cdot b_0 = 0 \cdot (-2) = 0$;

$c_1 = a_0b_1 + a_1b_0 = 0 \cdot 1 + 2 \cdot (-2) = -4$;

$c_2 = a_0b_2 + a_1b_1 + a_2b_0 = 0 \cdot 0 + 2 \cdot 1 + 1 \cdot (-2) = 0$;

$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = 0 \cdot 0 + 2 \cdot 0 + 1 \cdot 1 + 0 \cdot (-2) = 1$.

Então $f(x) \cdot g(x) = x^3 - 4x$.

Exemplo 1.17. Sejam $f(x) = 2x + \overline{1}$ e $g(x) = x + \overline{3}$ em $\mathbb{Z}_4[x]$. Então

$f(x) \cdot g(x) = c_0 + c_1x + c_2x^2$ onde,

$c_0 = a_0 \cdot b_0 = \overline{1} \cdot \overline{3} = \overline{3}$

$c_1 = a_0b_1 + a_1b_0 = \overline{1} \cdot \overline{1} + \overline{2} \cdot \overline{3} = \overline{1} + \overline{6} = \overline{1} + \overline{2} = \overline{3}$

$c_2 = a_1b_1 = \overline{2} \cdot \overline{1} = \overline{2}$

Assim $f(x) \cdot g(x) = \overline{3} + \overline{3}x + \overline{2}x^2$.

Proposição 1.10. *Para quaisquer polinômios não nulos $f(x)$ e $g(x)$ de $A[x]$, temos:*

(i) Se $f(x) + g(x) \neq 0$ então $\mathrm{gr}(f(x) + g(x)) \leq max\{\mathrm{gr}(f(x)), \mathrm{gr}(g(x))\}$

(ii) $\mathrm{gr}(f(x) \cdot g(x)) = \mathrm{gr}(f(x)) + \mathrm{gr}(g(x))$*, se A é domínio.*

Demonstração. (i) Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$, polinômios de grau n e m respectivamente. Suponha primeiro que $n > m$, neste caso o termo dominante de $f(x) + g(x)$ será a_n e assim

$$\mathrm{gr}(f(x) + g(x)) = n = \max\{\mathrm{gr}(f(x)), \mathrm{gr}(g(x))\}.$$

Caso $n = m$, temos que o termo dominante será $a_n + b_m$, deste modo $\text{gr}(f(x) + g(x)) = n$ caso $a_n + b_m \neq 0$ ou $\text{gr}(f(x) + g(x)) < n$ caso $a_n + b_m = 0$.

(ii) Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$, polinômios de grau n e m respectivamente. Por definição temos que $f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_kx^k$, onde $c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i$. Temos que $a_i = 0$, para todo $i > n$ e $b_i = 0$, para todo $i > m$. Assim $c_{n+m} = a_n.b_m$ e $c_{n+m} \neq 0$, pois a_n , $b_m \in A$. Portanto

$$\text{gr}(f(x) \cdot g(x)) = m + n = \text{gr}(f(x)) + \text{gr}(g(x)).$$

□

Exemplo 1.18. Sejam $f(x) = 5x^2 + 2x$ e $g(x) = -5x^2 + 6x + 8$, então $f(x) + g(x) = 8x + 8$, ou seja $\text{gr}(f(x) + g(x)) = 1 < \max\{\text{gr}(f(x)), \text{gr}(g(x))\} = 2$.

Exemplo 1.19. Sejam $f(x) = 5x^3 + 2x^2 - 7x$ e $g(x) = -2x^2 + 4x + 1$, então $f(x) + g(x) = 5x^3 - 3x + 1$. Ou seja $\text{gr}(f(x) + g(x)) = 3 = \max\{\text{gr}(f(x)), \text{gr}(g(x))\}$.

Exemplo 1.20. Sejam $f(x) = x^2+1$ e $g(x) = x^2-1$, então $f(x)\cdot g(x) = (x^2+1)(x^2-1) = x^4-1$. Ou seja, $\text{gr}(f(x) \cdot g(x)) = 4 = 2 + 2 = \text{gr}(f(x)) + \text{gr}(g(x))$.

Vale salientar que a propriedade multiplicativa do grau só é válida para polinômios com coeficientes em um domínio de integridade. Por exemplo, tomando os polinômios $f(x) = (\bar{2}x+\bar{1})$ e $g(x) = (\bar{2}x + \bar{3})$ em $\mathbb{Z}_4[x]$, temos

$$f(x) \cdot g(x) = (\bar{2}x + \bar{1}) \cdot (\bar{2}x + \bar{3}) = \bar{3},$$

ou seja, $\text{gr}(f(x) \cdot g(x)) = 0 \neq 1 + 1 = \text{gr}(f(x)) + \text{gr}(g(x))$.

Teorema 1.11. *Dado A um anel, o conjunto dos polinômios $A[x]$, munido das operações de adição e multiplicação, é um anel.*

Demonstração. A demonstração desse teorema consiste em verificarmos um a um os axiomas de anel da definição 1.1. Sejam $f(x), g(x), h(x) \in A[x]$ dados por

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

$$g(x) = b_0 + b_1x + \cdots + b_mx^m,$$

$$h(x) = c_0 + c_1x + \cdots + c_lx^l.$$

Podemos supor sem perda de generalidade, que $l \leq m \leq n$. Sejam $b_k, c_k = 0$ para todo $k > m$ e $a_k = 0$ para todo $k > n$. Assim podemos escrever os polinômios da forma

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

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

$$h(x) = c_0 + c_1x + \cdots + c_nx^n.$$

A1) A adição é associativa. De fato,

$$\begin{aligned}
[f(x) + g(x)] + h(x) &= [(a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n] + c_0 + c_1x + \cdots + c_nx^n \\
&= [(a_0 + b_0) + c_0] + [(a_1 + b_1) + c_1]x + \cdots + [(a_n + b_n) + c_n]x^n \\
&= [a_0 + (b_0 + c_0)] + [a_1 + (b_1 + c_1)]x + \cdots + [a_n + (b_n + c_n)]x^n \\
&= f(x) + [g(x) + h(x)].
\end{aligned}$$

Observe que usamos o fato de que a adição é associativa em A.

A2) A adição de polinômios é comutativa, pois,

$$\begin{aligned}
f(x) + g(x) &= a_0 + a_1x + \cdots + a_nx^n + b_0 + b_1x + \cdots + b_nx^n \\
&= (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n \\
&= (b_0 + b_0) + (b_1 + a_1)x + \cdots + (b_n + a_n)x^n \\
&= g(x) + f(x).
\end{aligned}$$

Novamente, usamos a comutatividade em A.

A3) O elemento neutro em $A[x]$ é o polinômio nulo que pode ser escrito como

$$N(x) = 0_0 + 0_1x + \cdots + 0_nx^n$$

assim temos $f(x) + N(x) = (a_0 + a_1x + \cdots + a_nx^n) + (a_0 + a_1x + \cdots + a_nx^n)$

$$= (a_0 + 0_0) + (a_1 + 0)x + \cdots + (a_n + 0)x^n$$

$$= a_0 + a_1x + \cdots + a_nx^n$$

$$= f(x)$$

Analogamente temos $N(x) + f(x) = f(x)$, pois a adição é comutativa.

A4 O polinômio simétrico de $f(x) = a_0 + a_1x + \cdots + a_nx^n$ é o polinômio $-a_0 - a_1x - \cdots - a_nx^n$, pois,

$$\begin{aligned}
f(x) + (-f(x)) &= (a_0 + a_1x + \cdots + a_nx^n) + (-a_0 - a_1x - \cdots - a_nx^n) \\
&= (a_0 - a_0) + (a_1 - a_1)x + \cdots + (a_n - a_n)x^n \\
&= 0 + 0x + \cdots + 0x^n \\
&= N(x).
\end{aligned}$$

A6) Distributividade.

$$\begin{aligned} f(x)\cdot(g(x)+h(x) &= \left(\sum_{j=0}^{n} a_j x^j\right)\cdot\left(\sum_{j=0}^{m}(b_j+c_j)x^j\right) \\ &= \sum_{j=0}^{n+m}\left(\sum_{j=\lambda+\mu} a_\lambda\cdot(b_\mu+c_\mu)\right)x^j \\ &= \sum_{j=0}^{n+m}\left(\sum_{j=\lambda} +\mu a_\lambda\cdot b_\mu + a_\lambda\cdot c_\mu\right)x^j \\ &= \sum_{j=0}^{n+m}\left(\sum_{j=\lambda} +\mu a_\lambda\cdot b_\mu\right)x^j + \sum_{j=0}^{n+m}\left(\sum_{j=\lambda+\mu} a_\lambda\cdot c_\mu\right)x^j \\ &= f(x)\cdot g(x)+f(x)\cdot h(x). \end{aligned}$$

Os demais itens podem ser encontrados [7] p.100-101. □

Para $f(x), g(x) \in A[x]$, podemos definir a *diferença* $f(x)-g(x)$ entre $f(x)$ e $g(x)$ por $f(x)-g(x)=f(x)+(-g(x))$.

Exemplo 1.21. Sejam $f(x)=2x^2-5x+10$ e $g(x)=x^2-4x+5 \in \mathbb{Z}[x]$. A diferença $f(x)-g(x)=(2x^2-5x+10)-(x^2-4x+5)=2x^2-x^2-5x+4x+10-5=x^2-x+5$.

Exemplo 1.22. O polinômio $f(x)=x$ não possui inverso multiplicativo, de fato suponha que exista $g(x)$ não nulo tal que $f(x)\cdot g(x)=1$. Daí teríamos $\mathrm{gr}(f(x)\cdot g(x))=\mathrm{gr}(1)=0$ e como $\mathrm{gr}(f(x)\cdot g(x))=\mathrm{gr}(f)+\mathrm{gr}(g)$ pela Proposição 1.10 temos $1+\mathrm{gr}(g(x))=0$, o que é impossível ja que $\mathrm{gr}(g(x))\geq 0$. Assim concluímos que não existe polinômio não nulo $g(x)$ tal que $f(x)\cdot g(x)=1$. Ou seja, o polinômio $f(x)=x$ não é invertível.
Usando argumentos análogos podemos mostrar que nenhum polinômio de grau ≥ 1 é inversível. Os únicos polinômios inversíveis em $K[x]$ sendo K corpo são as contantes não nulas, de fato suponhamos que um polinômio $p(x)\neq 0$ possua um inverso multiplicativo em $K[x]$. Assim, existe $q(x)\neq 0 \in K[x]$ tal que $p(x)\cdot q(x)=1$, logo, temos que $p(x)=a\neq 0$ é um polinômio constante. Portanto, os únicos polinômios invertíveis em $K[x]$ são os polinômios constantes não nulos.

Proposição 1.12. *Se A é um domínio, então $A[x]$ é um domínio. Em particular, se K é um corpo, então $K[x]$ é um domínio.*

Demonstração. Suponhamos que A seja um domínio e sejam $f(x)$ e $g(x) \in A[x]$ não nulos, com $\mathrm{gr}(f(x))=m$ e $\mathrm{gr}(g(x))=n$ com coeficientes líderes a_m e b_n respectivamente. Então o coeficiente líder de $f(x)\cdot g(x)$ é $c_{m+n}=a_m\cdot b_n\neq 0$ pois a_m e $b_m \in A$. Logo $\mathrm{gr}(f(x)\cdot g(x))=m+n$, assim $f(x)\cdot g(x)\neq 0$. □

Observação 1.13. Pelo Teorema 1.11, verifica-se que

- $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ são domínios de integridade, pois $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ também o são.
- $\mathbb{Z}_p[x]$ é domínio de integridade, pois $\mathbb{Z}_p$ também o é se p for primo positivo.

1.2.2 Algorítmo da Divisao

Nessa seção apresentamos o algoritmo da divisão e sua relação com raízes de polinômios. Um polinômio dividido por outro resulta em um polinômio quociente e um polinômio resto, o procedimento para isto é chamado *algoritmo da divisão para polinômios*. Veremos ainda na Seção 1.3, que existe uma relação direta entre o conceito de divisibilidade e irredutibilidade polinomial.
Sejam $f(x)$ e $g(x)$ em $A[x]$. Quando existe $h(x) \in A[x]$ tal que $f(x) = g(x) \cdot h(x)$, dizemos que $f(x)$ é múltiplo de $g(x)$. Nesse caso, se $g(x) \neq 0$, dizemos que $g(x)$ divide $f(x)$.

Exemplo 1.23. Dados $f(x) = x^2 - 4$, $g(x) = x + 2$ e $h(x) = x - 2 \in \mathbb{Z}[x]$, temos que $f(x) = g(x) \cdot h(x)$. Portanto $g(x)$ divide $f(x)$.

Proposição 1.14. *Sejam A um anel, $f(x), g(x) \in A[x] \setminus \{0\}$. Se $g(x)$ tem coeficiente líder invertível e divide $f(x)$, então* $\mathrm{gr}(g(x)) \leq \mathrm{gr}(f(x))$.

Demonstração. Como $g(x)$ divide $f(x)$ e ambos são não nulos, então existe $h(x) \in A[x] \setminus \{0\}$ tal que $f(x) = g(x) \cdot h(x)$. Pela Proposição 1.10 (ii) temos

$$\begin{aligned} \mathrm{gr}(f(x)) &= \mathrm{gr}(g(x) \cdot h(x)) \\ &= \mathrm{gr}(g(x)) + \mathrm{gr}(h(x)) \\ &\geq \mathrm{gr}(g(x)). \end{aligned}$$

□

Teorema 1.15. ***(Algoritmo da Divisão)*** *Seja A um anel e sejam $f(x), g(x) \in A[x]$, com $g(x) \neq 0$ e coeficiente líder invertível de $g(x)$ em A. Então existem únicos $q(x), r(x) \in A[x]$ tais que,*

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

onde $r(x) = 0$ ou $\mathrm{gr}(r(x)) < \mathrm{gr}(g(x))$.

Demonstração. Seja $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, onde b_m tem inverso $b_m^{-1} \in A$.
(Prova da existência) Se $f(x) = 0$, então tome $q(x) = r(x) = 0$. Suponhamos que $f(x) \neq 0$. Seja $n = \mathrm{gr}(f(x))$ e escreva $f(x) = a_0 + a_1 x + \ldots + a_m x^n$, com $a_n \neq 0$.

Se $n < m$, então tome $q(x) = 0$ e $r(x) = f(x)$. Podemos supor $n \geq m$. A demonstração é por indução sobre $n = \text{gr}(f(x))$.

Se $n = 0$, então $0 = n \geq m = \text{gr}(g(x))$, logo $m = 0$, $f(x) = a_0 \neq 0$,$g(x) = b_0$, com $b_0^{-1} \in A$. Assim, $f(x) = a_0 b_0^{-1} g(x)$, com $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.

Suponhamos o resultado válido para polinômios com grau menor do que $n = \text{gr}(f(x))$. Vamos mostrar que vale para $f(x)$.

Seja $f_1(x)$ o polinômio definido por $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$. O polinômio $a_n b_m^{-1} x^{n-m} g(x)$ tem grau n e coeficiente líder a_n. Logo, $\text{gr}(f_1(x)) < \text{gr}(f(x))$. Por hipótese de indução, existem $q_1(x)$ e $r_1(x)$ em $A[x]$ tais que

$$f_1(x) = q_1(x)g(x) + r_1(x),$$

Com $r_1(x) = 0$ ou $\text{gr}(r_1(x)) < \text{gr}(g(x))$. Logo,

$$\begin{aligned} f(x) &= f_1(x) + a_n b_m^{-1} x^{n-m} g(x) \\ &\overset{1}{=} (q_1(x)g(x) + r_1(x)) + a_n b_m^{-1} x^{n-m} g(x) \\ &\overset{2}{=} (q_1(x) + a_n b_m^{-1} x^{n-m}) g(x) + r_1(x). \end{aligned}$$

Em (1), substituímos a expressão de $f_1(x)$ e, em (2), usamos a comutatividade da adição e da distributividade em $A[x]$.

Tomamos $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r(x) = r_1(x)$.

(Prova da unicidade) Sejam $q_1(x), r_1(x), q_2(x), r_2(x)$ tais que

$$f(x) = q_1(x)g(x) + r_1(x) \overset{3}{=} q_2 g(x) + r_2(x),$$

onde

$$\begin{aligned} r_1(x) &= 0 \text{ ou } \text{gr}(r_1(x)) < \text{gr}(g(x)) \text{ e} \\ r_2(x) &= 0 \text{ ou } \text{gr}(r_2(x)) < \text{gr}(g(x)). \end{aligned}$$

De (3), segue que $(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)$. Se $q_1(x) \neq q_2(x)$, então $q_1(x) - q_2(x) \neq 0$, assim, $r_2(x) - r_1(x) \neq 0$ e, da Proposição 1.14, obtemos

$$\text{gr}(g(x)) \leq \text{gr}(r_2(x) - r_1(x)) < \text{gr}(g(x)),$$

uma contradição. Portanto, $q_1(x) = q_2(x)$, logo $r_1(x) = r_2(x)$.

□

Exemplo 1.24. Sejam $f(x) = 3x + 7$ e $g(x) = x^2 + 4x + 5$ em $\mathbb{Q}[x]$.

Temos que $\text{gr}(f(x)) = 1 < 2 = \text{gr}(g(x))$, portanto o quociente é $q(x) = 0$ e o resto é $r(x) = f(x) = 3x + 7$. Assim

$$x^2 + 4x + 5 = 0 \cdot (x^2 + 4x + 5) + (3x + 7)$$

Exemplo 1.25. Sejam $f(x) = 2x^2 + 4x + 3$ e $g(x) = x^2 + 3x + 1$ em $\mathbb{Q}[x]$.

(1) O monômio de maior grau de $f(x)$ é $2x^2$ e o monômio de maior grau de $g(x)$ é x^2. O quociente de $2x^2$ por x^2 é $q_1(x) = 2$.

(2) Fazemos o cálculo:
$r_1(x) = f(x) - q_1(x) \cdot g(x) = (2x^2 + 4x + 3) - 2x^2 - 6x - 2 = -2x + 1$

(3) Como $1 = \text{gr}(r_1(x)) < \text{gr}(g(x)) = 2$, concluímos que
$q(x) = q_1(x) = 2$ e $r(x) = r_1(x) = -2x + 1$.

Exemplo 1.26. Faremos a divisão de $f(x) = 3x^4 + 5x^2 + x^2 + 2x - 3$ por $g(x) = x^2 + 3x + 1$

(1) O monômio de maior grau de $f(x)$ é $3x^4$ e o monômio de maior grau de $g(x)$ é x^2. O quociente de $3x^4$ por x^2 é $q_1(x) = 3x^2$

(2) $r_1(x) = f(x)_1(x) \cdot g(x) = (3x^4 + 5x^2 + x^2 + 2x - 3) - 3x^4 - 9x2 - 3x^2 = -4x^3 - 2x^2 + 2x - 3$

(3) Como $3 = \text{gr}(r_1(x)) > \text{gr}(g(x)) = 2$, devemos continuar, dividindo $r_1(x)$ por $g(x)$ pois $r_1(x)$ não é o resto da divisão euclidiana.

(4) O monômio de maior grau de $r_1(x)$ é $-4x^3$ e o monômio de maior grau de $g(x)$ é x^2. O quociente é $-4x$, portanto

$$r_2(x) = r_1(x) - q_2(x) \cdot g(x) = (-4x^3 - 2x^2 + 2x - 3) + 4x^3 + 12x^2 + 4x = 10x^2 + 6x - 3$$

(5) Como $2 = \text{gr}(r_2(x)) = \text{gr}(g(x))$, podemos continuar, calculando a divisão de $r_2(x)$ por $g(x)$ obtemos $q_3(x) = 10$. Então

$$r_3(x) = r_2(x) - q_3(x) \cdot g(x) = (10x^2 + 6x - 3) - 10x^2 - 30x - 10 = -24x - 13.$$

(6) Como $1 = \text{gr}(r_3(x)) < \text{gr}(g(x)) = 2$, terminamos o algorítimo, pois $r_3(x)$ é o resto da divisão euclidiana.

(7) Obtemos

$$q(x) = 3x^2 - 4x + 10 = q_1(x) + q_2(x) + q_3(x) \text{ e } r(x) = r_3(x) = -24x - 12.$$

Nem sempre é possível efetuar a divisão entre polinômios em um anel que não seja um corpo.

Exemplo 1.27. Tomando $f(x) = 3x^5$ e $g(x) = 4x$ em $\mathbb{Z}[x]$, não é possível a divisão de $f(x)$ por $g(x)$ em $\mathbb{Z}[x]$, pois $\frac{3}{4} \notin \mathbb{Z}$.

1.2.3 Raízes de Polinômios

Dados um polinômio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ e um escalar $\alpha \in A$, dizemos que $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$ é o valor de f em α. Como A é anel e, portanto fechado sob as operações de adição e multiplicação, então temos:

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n \in A$$

No caso em que $f(\alpha) = 0$, dizemos que α é uma *raiz* ou um *zero* de f em A.

Exemplo 1.28. Seja $f(x) = x^3 - 2x^2 + 1 \in \mathbb{Z}[x]$. O valor de $f(x)$ em $\alpha = 2$ é

$$f(2) = 2^3 - 2 \cdot 2^2 + 1 = 8 - 8 + 1 = 1.$$

Logo $\alpha = 2$ não é raiz de $f(x)$. Agora para $\alpha = 1$ temos

$$f(1) = 1^3 - 2 \cdot 1^2 + 1 = 1 - 2 + 1 = 0.$$

Portanto $\alpha = 1$ é uma raiz de $f(x)$ em $\mathbb{Z}$.

Exemplo 1.29. Seja $g(x) = \overline{1} + \overline{2}x + \overline{2}x^2 \in \mathbb{Z}_3[x]$, onde $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ é o anel das classes residuais módulo 3. Os valores que $g(x)$ assume em $\mathbb{Z}_3$ são:

$$\begin{aligned} g(\overline{0}) &= \overline{1} + \overline{2} \cdot \overline{0} + \overline{2} \cdot \overline{0}^2 = \overline{1} + \overline{0} + \overline{0} = \overline{1}; \\ g(\overline{1}) &= \overline{1} + \overline{2} \cdot \overline{1} + \overline{2} \cdot \overline{1}^2 = \overline{1} + \overline{2} + \overline{2} = \overline{5} = \overline{2}; \\ g(\overline{2}) &= \overline{1} + \overline{2} \cdot \overline{2} + \overline{2} \cdot \overline{2}^2 = \overline{1} + \overline{4} + \overline{8} = \overline{13} = \overline{1} \in \mathbb{Z}_3. \end{aligned}$$

Como $g(\overline{0}) \neq \overline{0}, g(\overline{1}) \neq \overline{0}$ e $g(\overline{2}) \neq \overline{0}$, então o polinômio $g(x) = \overline{1} + \overline{2}x + \overline{2}x^2 \in \mathbb{Z}_3[x]$ não tem raiz em $\mathbb{Z}_3$. Observe que $\alpha = \overline{0}, \overline{1}, \overline{2}$ são as únicas possibilidades de raiz em $\mathbb{Z}_3$ e, uma vez descartadas estas, podemos concluir que o polinômio não tem raízes em $\mathbb{Z}_3$.

Exemplo 1.30. Seja $f(x) = x^2 + 9 \in \mathbb{R}[x]$. O valor de $f(x)$ no escalar $\beta \in \mathbb{R}$ é dada pela expressão $f(\beta) = \beta^2 + 9 \in \mathbb{R}$. Sabemos que dado $\beta \in \mathbb{R}$, então $\beta^2 \geq 0$. Assim,

$$\beta^2 + 9 > 0.$$

Isto é, a expressão $\beta^2 + 9$ terá sempre um valor positivo e, portanto nunca será igual a zero para qualquer que seja o valor de $\beta \in \mathbb{R}$. Assim concluímos que $f(\beta) \neq 0$ para todo $\beta \in \mathbb{R}$ e isto significa que o polinômio $f(x) = \beta^2 + 9 \in \mathbb{R}[x]$ não possui raiz em $\mathbb{R}$. Por outro lado temos $\mathbb{R} \subset \mathbb{C}$, consequentemente $\mathbb{R}[x] \subset \mathbb{C}[x]$. Agora dado $3i \in \mathbb{C}$ temos que :

$$\begin{aligned} f(3i) &= (3i)^2 + 9 \\ &= -9 + 9 \\ &= 0. \end{aligned}$$

Ou seja $\beta = 3i$ é uma raiz de $f(x) = x^2 + 9$ em $\mathbb{C}$. Dizemos que $\beta = 3i$ é uma raiz complexa de $f(x) = x^2 + 9 \in \mathbb{R}[x]$.

Observe que o exemplo anterior teve o propósito de ressaltar o fato de quando falamos em raiz de um polinômio, devemos especificar o anel com o qual estamos trabalhando.

Exemplo 1.31. 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 $\mathbb{Q}$: -1 ,1.
- Possui quatro raízes em $\mathbb{R}$: $-1, 1, \sqrt{2}, -\sqrt{2}$
- Possui oito raízes em $\mathbb{C}$: $-1, 1, \sqrt{2}, -\sqrt{2}, i, -i, \sqrt{2}i, -\sqrt{2}i$.

Definição 1.16. Dizemos que $\beta \in A$ é uma raiz de $f(x)$ de *multiplicidade* m quando $(x - \beta)^m$ dividir $f(x)$ e $(x - \beta)^{m+1}$ não dividir $f(x)$ em $A[x]$. Nesse caso existe $q(x) \in A[x]$ tal que

$$f(x) = (x - \beta)^m q(x),$$

com $q(\beta) \neq 0$.
Dizemos que β é uma *raiz simples* de $f(x)$, se $m = 1$, e uma *raiz múltipla* se $m \geq 2$.

Exemplo 1.32. Sendo $f(x) = x^3 - 7x^2 + 16x - 12$ um polinômio de coeficientes reais, temos que 2 é raiz dupla e 3 é raiz simples de $f(x)$, uma vez que $f(x) = (x - 2)^2 \cdot (x - 3)$.

Teorema 1.17. *(Teorema do fator) Seja $f(x)$ em $A[x] \setminus \{0\}$. Então, $\beta \in A$ é uma raiz de $f(x)$ se, e somente se, $x - \beta$ divide $f(x)$.*

Demonstração. Suponhamos que $f(\beta) = 0$. Pelo Teorema 1.15 existem $q(x), r(x) \in A[x]$ tais que

$$f(x) = q(x)(x - \beta) + r(x),$$

onde $r(x) = 0$ ou $\text{gr}(r(x)) < \text{gr}(x-\beta) = 1$. Assim, $r(x) = r$ pertence a A e $f(x) = q(x)(x-\beta)+r$. Avaliando $f(x)$ em β temos

$$0 = f(\beta) = q(\beta)(\beta - \beta) + r = r,$$

mostrando que $x - \beta$ divide $f(x)$.

Reciprocamente, suponhamos que $x - \beta$ divida $f(x)$. Então, existe $q(x) \in A[x]$ tal que $f(x) = q(x)(x - \beta)$. Portanto,

$$f(\beta) = q(\beta)(\beta - \beta) = q(\beta) \cdot 0 = 0$$

□

Exemplo 1.33. $x - 2$ divide $f(x) = x^2 - 5x + 6$, pois 2 é raiz de $f(x)$.

Exemplo 1.34. O polinômio $p(x) = x^n - c^n \in A[x]$ é divisível por $d(x) = x - c$. Como $p(c) = c^n - c^n = 0$, temos que c é raiz de $p(x)$ e, portanto pelo Teorema 1.17 $d(x) = x - c$ divide $p(x)$.

Proposição 1.18. *Seja A um domínio de integridade e seja $f(x)$ em $A[x] \setminus \{0\}$. Se $f(x)$ tem grau n, então $f(x)$ tem no máximo n raízes em A.*

Demonstração. Faremos a prova por indução sobre $n = \text{gr}(f(x))$.

Se $n = 0$, então $f(x) = a \neq 0$ não tem raízes em A e o resultado é válido.

Seja $n > 0$. Suponhamos o resultado verdadeiro para polinômios de grau n e seja $f(x)$ um polinômio com $\text{gr}(f(x)) = n + 1$.

Se $f(x)$ não tem raízes em A, então não temos o que demonstrar. Digamos que $f(x)$ tenha uma raiz β em A. Pelo Teorema 1.17, $x - \beta$ divide $f(x)$ em $A[x]$, logo existe $q(x) \in A[x]$ tal que

$$f(x) = q(x)(x - \beta), \text{ com } \text{gr}(q(x)) = n.$$

Por hipótese de indução, $q(x)$ tem no máximo n raízes em A. Observamos que

$$\alpha \in A \text{ é raiz de } f(x) \Leftrightarrow 0 = f(\alpha) = q(\alpha)(\alpha - \beta)$$

Como A é domínio então

$$q(\alpha) = 0 \text{ ou } \alpha - \beta = 0$$

$$\alpha \text{ é raiz de } q(x) \text{ ou } \alpha = \beta.$$

Logo, $f(x)$ tem no máximo $n + 1$ raízes em A. □

Exemplo 1.35. O polinômio $x^2 - 5 \in \mathbb{Q}[x]$ não tem raízes em $\mathbb{Q}$. Entretanto, $x^2 - 5 \in \mathbb{R}[x]$ tem duas raízes reais $\sqrt{5}$ e $\sqrt{-5}$. O polinômio $x^2 + 9 \in \mathbb{Q}[x] \subset \mathbb{R}[x]$ não tem raízes reais, mas em $\mathbb{C}[x]$,
$3i$ e $-3i$ são raízes em $\mathbb{C}$.

Exemplo 1.36. A hipótese de A ser um domínio na Proposição 1.18 é essencial, pois para $A = \mathbb{Z}_6$ que não é domínio, temos que $f(x) = x^2 - x \in \mathbb{Z}_6$ é tal que $f(\overline{0}) = f(\overline{1}) = f(\overline{3}) = f(\overline{4}) = \overline{0}$, ou seja $f(x)$ tem 4 raízes que é maior que $\text{gr}(f(x)) = 2$.

Proposição 1.19. *Seja A um domínio de integridade com uma quantidade infinita de elementos. Se $f(x) \in A[x]$ e $f(\beta) = 0$, para todo $\beta \in A$, então $f(x) = 0$.*

Demonstração. Suponhamos, por absurdo, que $f(x) \in A[x] \setminus \{0\}$ com $f(\beta) = 0$ para todo $\beta \in A$. Seja $n = \text{gr}(f(x))$. É claro que $n \neq 0$. Logo $n \geq 1$. Pela Proposição 1.18, $f(x)$ tem no máximo n raízes em A, contradizendo o fato de A ser infinito. □

Corolário 1.20. *Seja A um domínio de integridade com um número infinito de elementos. Sejam $f(x)$ e $g(x)$ em $A[x]$ tais que $f(\beta) = g(\beta)$, para todo $\beta \in A$. Então, $f(x) = g(x)$.*

Demonstração. Seja $h(x) = f(x) - g(x)$. Então, para todo $\beta \in A, h(\beta) = f(\beta) - g(\beta) = 0$. Pela proposição anterior, $0 = h(x) = f(x) - g(x)$. Logo $f(x) = g(x)$. □

Teorema 1.21. *(Teorema do resto) Sejam A um anel, β um elemento de A e $f(x) = a_0 + a_1x + \ldots + a_nx^n \in A[x]$ um polinômio de grau n. O resto na divisão euclidiana e $f(x)$ por $x - \beta$ é $f(\beta)$;*

Demonstração. Como o coeficiente líder de $x-\beta$ é invertível, temos que existem $q(x), r(x) \in A(x)$ tal que .

$$f(x) = (x - \beta)q(x) + r(x),$$

onde $r(x) = 0$ ou $\text{gr}(r(x)) = 0$ (pois $\text{gr}(x - \beta) = 1$).

Achando o valor numérico de $f(x)$ para $x = \beta$:

$$f(\beta) = (\beta - \beta)q(\beta) + r(\beta) = r(\beta)$$

Sendo $r(x)$ constante, consideremos $r(\beta) = r$. Assim, $r = f(\beta)$, para todo $\beta \in A$.

□

Exemplo 1.37. O resto da divisão de $p(x) = x^3 - 2x^2 + 5$ por $x - 4$ é:
$p(4) = 4^3 - 2 \cdot 4^2 + 5 = 64 - 32 + 5 = 37$

1.3 Polinômios irredutíveis e fatoração

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

Definição 1.22. Seja K um corpo. Dizemos que um polinômio não constante $f(x) \in K[x]$ é *irredutível* em $K[x]$ se $f(x)$ não é produto de dois polinômios em $K[x]$ de graus estritamente menores do que o grau de $f(x)$. Caso contrário $f(x)$ é dito *redutível* em $K[x]$.
Segue diretamente da definição que todo polinômio de grau 1 é irredutível em $K[x]$.

Exemplo 1.38. Por exemplo, $x^2+1 \in \mathbb{R}[x]$ é irredutível em $\mathbb{R}[x]$, pois caso contrário ele poderia ser escrito como um produto polinômios de grau 1 em $\mathbb{R}[x]$, contradizendo o fato de $x^2+1=0$ não possuir raízes reais. Por outro lado x^2+1 é redutível em $\mathbb{C}[x]$ já que $x^2+1=(x+i)(x-i)$.

Isso mostra que irredutibilidade é um conceito que depende do anel de polinômios sobre o qual estamos trabalhando.

Proposição 1.23. *Se K for um corpo e $f(x) \in K[x]$ com $\mathrm{gr}(f(x)) \geq 2$ possuir uma raiz $r \in K$, então $f(x)$ é redutível em $K[x]$.*

Demonstração. De fato, seja r raiz de $f(x) \in K[x]$, então existe $g(x) \in K[x]$ tal que $f(x) = (x-r) \cdot g(x)$ pelo Teorema 1.17, com $\mathrm{gr}(g(x)) \geq 1$. □

Exemplo 1.39. Considere o polinômio $f(x) = x^2 - 2$ em $\mathbb{Q}[x]$. Como f é polinômio de grau 2, se fosse redutível em $\mathbb{Q}[x]$ existiriam $a, b \in \mathbb{Q}$ tais que

$$\begin{aligned} x^2 - 2 &= (x+a) \cdot (x+b) \\ &= x^2 + (a+b)x + ab \\ &\Leftrightarrow \; a+b = 0 \text{ e } a \cdot b = -2 \end{aligned}$$

Resolvendo o sistema acima concluímos que $a = \pm\sqrt{2} \notin \mathbb{Q}$, absurdo. Portanto $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Por outro lado, como $\pm\sqrt{2} \in \mathbb{R}$, então $f(x)$ é redutível em $\mathbb{R}[x]$, pois podemos escrever

$$f(x) = (x + \sqrt{2}) \cdot (x - \sqrt{2}).$$

Proposição 1.24. *Seja K um corpo. Se $f(x) \in K[x]$ e $\mathrm{gr}(f(x)) = 2$ ou 3 então $f(x)$ é redutível sobre K se, e somente se, $f(x)$ possui raiz em K.*

Demonstração. Suponha que $f(x) = g(x)h(x)$ onde $g(x)$ e $h(x)$ possuem grau menores que $f(x)$ e pertençam a $K[x]$. Como $\mathrm{gr}(f(x)) = \mathrm{gr}(g(x)) + \mathrm{gr}(h(x))$ e $\mathrm{gr}(f(x)) = 2$ ou 3, pelo menos um

dos $g(x)$ ou $h(x)$ tem grau 1, digamos $g(x) = ax + b$. Então claramente $\frac{-b}{a}$ é uma raiz de $g(x)$ e então uma raiz de $f(x)$. Reciprocamente, suponha que $f(a) = 0$ onde $a \in K$. Então pelo teorema do fator, $x - a$ é um fator de $f(x)$ e assim $f(x)$ é redutível sobre K. □

A Proposição acima é particularmente útil quando estamos com corpos finitos como $\mathbb{Z}_p$ pois basta verificar os zeros de $f(x)$.

Exemplo 1.40. O polinômio $f(x) = x^3 + x + \overline{1}$ é irredutível em $\mathbb{Z}_2[x]$, pois não possui raiz em $\mathbb{Z}_2[x]$. Com efeito

$$\begin{aligned} f(\overline{0}) &= \overline{0}^3 + \overline{0} + \overline{1} = \overline{1} \\ \text{e} & \\ f(\overline{1}) &= \overline{1}^3 + \overline{1} + \overline{1} = 1. \end{aligned}$$

Exemplo 1.41. O polinômio $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$ em $\mathbb{R}[x]$, então $x^2 - 5$ é redutível em $\mathbb{R}[x]$. Entretanto é irredutível em $\mathbb{Q}[x]$ pois tem grau 2 e não tem raiz em $\mathbb{Q}$.

Proposição 1.25. *Todo polinômio $f(x)$ de grau 1 é irredutível em $K[x]$, onde K é corpo.*

Demonstração. Seja $f(x) = ax + b$, com $a \neq 0$. Escrevendo $f(x) = r(x) \cdot g(x)$, com $r(x)$, $g(x)$ $\in K[x]$ temos que $1 = \text{gr}(ax + b) = \text{gr}(r(x)) + \text{gr}(g(x))$. Logo, $\text{gr}(r(x)) = 0$ e $\text{gr}(g(x)) = 1$ ou $\text{gr}(r(x)) = 1$ e $\text{gr}(g(x)) = 0$. Então $r(x)$ ou $g(x)$ é um polinômio constante não nulo □

Teorema 1.26. *(Fatoração única em $K[x]$) Seja K um corpo. Todo polinômio não constante $f(x) \in K[x]$ é um produto de polinômios irredutíveis em $K[x]$. Essa fatoração é única a menos de uma constante não nula, isto é, se*

$$f(x) = p_1(x) \cdots p_r(x) \quad e \quad f(x) = q_1(x) \cdots q_s(x)$$

são duas fatorações em irredutíveis de $f(x)$ então $r = s$ e, a menos de uma permutação nos índices, $p_i = u_i q_i$ com $u_i \in K$, $u_i \neq 0$ para todo i, $1 \leqslant i \leqslant r$.

Demonstração. (Existência) Seja $f(x) \in K[x]$ um polinômio não constante. Usaremos indução em $gr(f(x)) = n \geqslant 1$. Se $gr(f(x)) = 1$ então $f(x)$ é irredutível. Suponhamos o teorema verdadeiro para todo polinômio de grau $< n$. Se $f(x)$ é irredutível então nada temos a provar, pois $f(x) = 1 \cdot f(x)$. Se $f(x)$ é redutível então$f(x) = g(x) \cdot h(x)$ com $\text{gr}(g(x)) < n$ e $\text{gr}(h(x)) < n$. Por hipótese indutiva $g(x) = u_1 p_1 \cdots p_k$ e $h(x) = u_2 p_{r+1} \cdots p_k$, com $u_1, u_2 \in K$.
Pondo $u = u_1 \cdot u_2$ temos $f(x) = u p_1 \cdots p_k$ como queríamos.
(Unicidade) Suponhamos que

$$f(x) = a \cdot p_1(x) \cdots p_m(x) = b \cdot q_1(x) \cdots q_r(x), \tag{1.1}$$

com $a, b \in F\backslash\{0\}$ e $p_1(x)\cdots p_m(x)$ e $q_1(x)\cdots q_r(x)$ mônicos e irredutíveis. Como a= coeficiente líder de $f(x) = b$, cancelando em 1.1 obtemos

$$p_1(x)\cdots p_m(x) = q_1(x)\cdots qr(x).$$

Como $p_1(x)$ divide o polinômio à esquerda da igualdade acima, temos que $p_1(x)$ divide $q_1(x)\cdots q_r(x)$. Como $p_1(x)$ é primo, então $p_1(x)$ divide q_j para algum $j = 1, \ldots, r$. Portanto, $q_j(x) = up_1(x)$ para algum $u \in F\backslash\{0\}$. Comparando os coeficientes líderes, obtemos $u = 1$ e $q_j(x) = p_1(x)$. Reenumerando os polinômios $q_1(x), \ldots, q_r(x)$, se necessário, podemos supor $p_1(x) = q_1(x)$. Faremos indução sobre m. Se $m = 1$, então $r = 1$. Se $m > 1$, cancelamos $p_1(x)$, obtendo

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

e, por hipótese de indução, $m - 1 = r - 1$, que é equivalente a $m = r$, e cada $p_j(x)$ é igual a $q_j(x)$. □

Observação 1.27. Para que um polinômio (de grau maior que 1) seja irredutível sobre um corpo K é necessário que ele não admita raízes em K. A recíproca não é verdadeira como veremos no exemplo abaixo.

Exemplo 1.42. Considere os polinômios sem raízes em $\mathbb{R}$, onde $f(x) = x^2 + 1$ e $g(x) = x^2 + 2$ em $\mathbb{R}[x]$, então, $h(x) = (x^2 + 1)(x^2 + 2) = x^4 + 3x^2 + 2$, que não admite raízes reais e no entanto é redutível.

Definição 1.28. Dizemos que um corpo K é algebricamente fechado quando todo polinômio não constante com coeficientes em K tem uma raiz em K.

Corolário 1.29. *Seja K um corpo algebricamente fechado e $f(x)$ em $K[x]$, com $\mathrm{gr}(f(x)) = n \geq 1$. Então, existem $\beta_1, \beta_2, \ldots \beta_n \in K\backslash\{0\}$ tais que $f(x) = a(x - \beta_1)\cdots(x - \beta_n)$. A expressão acima é a **forma fatorada** do polinômio.*

Demonstração. A demonstração é, por indução, sobre $n = \mathrm{gr}(f(x))$. Se $\mathrm{gr}(f(x)) = 1$, então $f(x) = ax + b$, com $a, b \in K$ e $a \neq 0$, logo $f(x) = a(x + a^{-1}b)$ e $\beta_1 = -a^{-1}b$. Seja $n \geq 1$ e suponhamos o resultado válido para os polinômios de grau n. Seja $f(x) \in K[x]$ com $\mathrm{gr}(f(x)) = n + 1$. Por hipótese $f(x)$ tem uma raiz $\beta \in K$. Portanto $f(x) = q(x)(x - \beta)$, para algum $q(x) \in K[x]$ e $\mathrm{gr}(q(x)) = n$. Por hipótese de indução, existem $a, \beta_1, \ldots \beta_n \in K$, com $a \neq 0$ tais que $q(x) = a(x-\beta_1)\cdots(x-\beta_n)$. Logo, $f(x) = a(x-\beta_1)\cdots(x-\beta_n)(x-\beta)$. Tomando $\beta_{n+1} = \beta$, obtemos o resultado.

□

Exemplo 1.43. (i) A forma fatorada do polinômio
$f(x) = x^2 + 6x + 8$ em $\mathbb{Q}[x]$ é $f(x) = (x+2)(x+4)$;

(ii) O polinômio $p(x) = 3x^2 - 15x + 12 \in \mathbb{Q}[x]$ tem forma fatorada $p(x) = 3(x-1)(x-4)$;

(iii) Para o polinômio $q(x) = x^3 + 2x^2 - x - 2$ em $\mathbb{C}[x]$ a forma fatorada é
$q(x) = (x+2)(x-i)(x+i)$;

(iv) A forma fatorada de $r(x) = 2x^2 - 3$ em $\mathbb{R}[x]$ é $r(x) = 2\left(x - \sqrt{\frac{3}{2}}\right)\left(x + \sqrt{\frac{3}{2}}\right)$;

Exemplo 1.44. O polinômio $x^3 + 9x$, pode ser escrito como $x(x+3i)(x-3i)$, sendo $\beta_1 = 0$, $\beta_2 = -3i$ e $\beta_3 = 3i$.

Teorema 1.30. *(Teorema Fundamental da Álgebra) Todo polinômio não constante com coeficientes complexos tem uma raiz complexa.*

A demonstração do teorema utiliza resultados da Análise e portanto foge do escopo deste trabalho. A mesma pode ser encontrada em [3] pág 116. Esse teorema é conhecido como "TEOREMA FUNDAMENTAL DA ÁLGEBRA (TFA)". Portanto o TFA nos diz que $\mathbb{C}$ é algebricamente fechado.

Lembre-se que o conjugado do número complexo $z = a + bi$ é $\overline{z} = a - bi$.

Proposição 1.31. *Seja $f(x) = a_0 + a_1x + ... + a_nx^n$ um polinômio em $\mathbb{R}[x]$. Se o número complexo $z = a + bi$ é raiz de $f(x)$ então $\overline{z}$ também é raiz desse polinômio.*

Demonstração. Por hipótese $f(z) = a_0 + a_1z + \cdots + a_nz^n = 0$, pelas propriedades de número complexo temos:

$$\begin{aligned} f(\overline{z}) &= a_0 + a_1\overline{z} + \cdots + a_n\overline{z}^n \\ &= \overline{a_0} + \overline{a_1z} + \cdots + \overline{a_nz^n} \\ &= \overline{a_0 + a_1z + \cdots + a_nz^n} \\ &= \overline{0} = 0. \end{aligned}$$

□

Proposição 1.32. *Em $\mathbb{C}[x]$ um polinômio é irredutível se, e somente se , ele é de grau 1.*

Demonstração. Sabemos, da Proposição 1.25 que todo polinômio de grau 1 é irredutível. Reciprocamente, suponhamos que $f(x) \in \mathbb{C}[x]$ e $\text{gr}(f(x)) \geq 2$. Como $\mathbb{C}$ é algebricamente fechado pelo Teorema 1.30, existe $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$, logo $x - \alpha$ divide $f(x)$. Portanto existe

$q(x) \in \mathbb{C}[x]$ tal que $f(x) = q(x)(x-\alpha)$, com $\text{gr}(q(x)) + 1 = \text{gr}(f(x)) \geq 2$. Portanto, $f(x)$ não é irredutível.

□

Proposição 1.33. *Um polinômio $f(x) \in \mathbb{R}[x]$ é irredutível sobre $\mathbb{R}$ se, e somente se,* $\text{gr}(f(x)) = 1$ *ou* $\text{gr}(f(x)) = 2$ *e $f(x) = ax^2+bx+c$ e seu discriminante, definido como $\triangle = b^2-4ac$ é menor que zero. Todo polinômio $f(x) \in \mathbb{R}[x]$, com* $\text{gr}(f(x))>2$*, é redutível em $\mathbb{R}[x]$.*

Demonstração. Sabemos que qualquer polinômio de grau 1 é irredutível em qualquer corpo K. Um polinômio de grau 2 com coeficientes em qualquer corpo K é irredutível em $K[x]$ se, e somente se, não tem raízes em K. Seja $f(x) = x^2 + bx + c \in \mathbb{R}[x]$. Existe $\beta \in \mathbb{C}$ uma raiz de $f(x)$.

$$\begin{aligned} f(x) \text{ é irredutível em } \mathbb{R}[x] \text{ se, e somente se , } \quad & \beta \in \mathbb{C} \text{ e } \beta \notin \mathbb{R}. \\ \text{Se, e somente se , } \quad & \beta \neq \overline{\beta}. \\ \text{Se, somente se , } \quad & \Delta = b^2 - 4c < 0. \end{aligned}$$

Nesse caso, $x^2 + bx + c = (x-\beta)(x-\overline{\beta}) = x^2 - (\beta + \overline{\beta})x + \beta\overline{\beta}$ e

$$\begin{aligned} \Delta &= (\beta + \overline{\beta})^2 - 4\beta\overline{\beta} \\ &= \beta^2 - 2\beta\overline{\beta} + \overline{\beta}^2 \\ &= \beta^2 - 2\beta\overline{\beta} + \overline{\beta}^2 \\ &= (\beta - \overline{\beta})^2 \\ &= (2 \cdot Im(\beta)i)^2 \\ &= -4(Im(\beta))^2 < 0. \end{aligned}$$

Para demonstrar a última afirmação, seja $f(x)$ um polinômio em $\mathbb{R}[x]$ tal que $\text{gr}(f(x))>2$. Seja $\beta \in \mathbb{C}$ uma raiz de $f(x)$. Temos dois casos

(i) Se $\beta \in \mathbb{R}$, então $x - \beta$ divide $f(x)$ em $\mathbb{R}[x]$. Logo $f(x)$ é redutível em $\mathbb{R}[x]$.

(ii) Se $\beta \in \mathbb{C}\backslash\mathbb{R}$, então $\beta \neq \overline{\beta}$ e $\overline{\beta}$ também é raiz de $f(x)$.

Logo $(x-\beta)\cdot(x-\overline{\beta})$ divide $f(x)$ em $\mathbb{C}[x]$. Entretanto,

$$(x-\beta)\cdot(x-\overline{\beta}) = x^2 - (\beta + \overline{\beta})x + \beta\overline{\beta} = x^2 - 2Re(\beta)x + \mid \beta \mid^2 \in \mathbb{R}[x],$$

logo $x^2 - 2Re(\beta)x + \mid \beta \mid^2$ divide $f(x)$ em $\mathbb{R}[x]$. Então $f(x)$ é redutível em $\mathbb{R}[x]$. □

Irredutibilidade em $\mathbb{Q}[x]$

Neste tópico, restringiremos nosso estudo de polinômios ao anel $\mathbb{Q}[x]$. Focalizaremos sobre os elementos irredutíveis. Sabemos que a existência de fator de grau 1 na fatoração de um polinômio $f(x)$ em $\mathbb{Q}[x]$ equivale à existência em $\mathbb{Q}$ de uma raiz de $f(x)$. O seguinte resultado permitirá determinar as raízes racionais de polinômios com coeficientes em $\mathbb{Z}$.

Proposição 1.34. *Sejam $n > 1$ inteiro, $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio de coeficientes inteiros e p e q inteiros não nulos primos entre si. Se $f\left(\frac{p}{q}\right) = 0$, então $p \mid a_0$ e $q \mid a_n$.*

Demonstração. A partir de $f(\frac{p}{q}) = 0$, obtemos

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

e daí,

$$\begin{cases} a_0q^n = p(-a_np^{n-1} - \ldots - a_1q^{n-1}) \\ a_np^n = q(-a_{n-1}p^{n-1} - \ldots - a_0q^{n-1}) \end{cases}$$

Portanto, $p \mid a_0q^n$ e $q \mid a_np^n$. Mas $MDC(p,q) = 1 \Rightarrow MDC(p^n,q) = MDC(p,q^n) = 1$. Logo $p \mid a_0$ e $q \mid a_n$. □

Corolário 1.35. *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 $\beta \neq 0, \beta$ divide a_0.*

Demonstração. Se $f(x)$ é mônico então $a_n = 1$. Pela Proposição 1.34 , q divide ± 1, logo $\frac{p}{q}$ é um número inteiro. □

Exemplo 1.45. O polinômio x^3+4x^2+2x+2 é irredutível em $\mathbb{Q}[x]$. De fato, qualquer fatoração de um polinômio de grau 3 da origem a um fator de grau 1, que é equivalente a $f(x)$ ter uma raiz racional. As possíveis raízes racionais de $f(x)$ são os inteiros $\alpha \in \{-1, 1, -2, 2\}$. Como $f(-1) = 1$, $f(1) = 8$, $f(-2) = 6$ e $f(2) = 30$, concluímos que $f(x)$ é irredutível em $\mathbb{Q}[x]$

Exemplo 1.46. Vamos determinar a fatoração em irredutíveis de $\mathbb{Q}[x]$ do polinômio
$f(x) = 2x^4 - 5x^3 - 2x^2 - 4x + 3$
Vamos inicialmente pesquisar as raízes racionais da equação $f(x) = 0$. Se $\frac{p}{q}$ é raiz então
$p \in \{1, -1, 3, -3\}$ e $q \in \{1, 2\}$ portanto $\frac{p}{q} \in \{1, -1, 3, -3, \frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2}\}$.
Calculando$f(\frac{p}{q})$ para cada $\frac{p}{q}$ obtemos $f(3) = 0$ e $f(\frac{1}{2}) = 0$, portanto f é divisível por
$(x-3)(x-\frac{1}{2})$, dividindo obtemos $2x^2 + 2x + 2$. Portanto $f(x) = (x-3)(x-\frac{1}{2})(2x^2+2x+2)$ é a fatoração de $f(x)$ em polinômios irredutíveis em $\mathbb{Q}[x]$, uma vez que $2x^2 + 2x + 2$ não tem raízes.

Lema 1.36. *(Gauss) Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$ então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

Teorema 1.37. *(Critério de Eisentein) Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n$ um polinômio em $\mathbb{Z}[x]$. Suponhamos que exista um inteiro primo p tal que $p \nmid a_n, p \mid a_0, \ldots, p \mid a_{n-1}$ e $p^2 \nmid a_0$. Então $f(x)$ é irredutível em $\mathbb{Q}[x]$.*

Demonstração. É suficiente provar que $f(x)$ é irredutível sobre $\mathbb{Z}$. Suponhamos por contradição que,

$$f(x) = g(x) \cdot h(x) \quad \text{com} \quad g(x), h(x) \in \mathbb{Z}[x],$$

$$1 \leq \text{gr}(g), \text{gr}(h) < \text{gr}(f) = n.$$

Seja,

$$g(x) = b_0 + b_1x + ... + b_rx^r \in \mathbb{Z}[x], \text{gr}(g) = r;$$

$$h(x) = c_0 + c_1x + \cdots + c_sx^s \in \mathbb{Z}[x], \text{gr}(h) = s.$$

Assim $n = r + s$.
Agora $b_0 \cdot c_0 = a_0$ e assim $p \mid b_0$ ou $p \mid c_0$ e como $p^2 \nmid a_0$ segue que p divide apenas um dos inteiros b_0, c_0. Vamos admitir, sem perda de generalidade, que $p \mid b_0$ e $p \nmid c_0$. Agora $a_n = b_r \cdot c_s$ é o coeficiente de $x^n = x^{r+s}$ e portanto $p \nmid a_r$ e $p \mid b_0$. Seja b_i o primeiro coeficiente de $g(x)$ tal que $p \nmid b_i$. Agora $a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + \ldots + b_i \cdot c_0$ e portanto como $p \mid b_0, \ldots, b_{i-1}, p \nmid b_i$ e $p \nmid c_0 \Rightarrow p \nmid a_i \Rightarrow i = n$ o que é um absurdo pois $1 \leq i \leq r < n$. □

Exemplo 1.47. O polinômio $x^{17} + 6x^{13} - 15x^4 + 3x^2 - 9x + 12$ é irredutível em $\mathbb{Q}[x]$. Pois pelo Teorema 1.37 basta tomarmos $p = 3$, observe que 3 divide $6, -15, 3, -9, 12$, 3 não divide $a_{17} = 1$ e $3^2 = 9$ não divide $a_0 = 12$.

Exemplo 1.48. Seja $f(x) = x^3 + 2x + 10$ é irredutível em $\mathbb{Q}$. Temos que $a_3 = 1, a_2 = 0, a_1 = 2$ e $a_0 = 10$. Valem as hipótese do Teorema 1.34 para o primo $p = 2$.

Exemplo 1.49. $f(x) = x^5 + 4x + 2 \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Q}[x]$. Temos $a_5 = 1, a_1 = 4$, $a_4 = a_3 = a_2 = 0$ e $a_0 = 2$. Valem as hipóteses do critério de Eisenstein para o primo $p = 2$.

Exemplo 1.50. Há polinômios irredutíveis em $\mathbb{Q}[x]$ de grau n, para todo $n \geq 1$. A saber, $f(x) = x^n - p$, onde p é um natural primo, é irredutível em $\mathbb{Q}[x]$, para todo $n \geq 1$.
De fato, o caso $n = 1$ é trivial. Para $n \geq 2$, aplicamos o Proposição 1.34 com o p primo. Nesse caso, $a_0 = p, a_1 = \ldots = a_{n-1} = 0$ e $a_n = 1$.

Capítulo 2

Números Algébricos

Neste capítulo falaremos sobre núm eros algébricos e suas principais propriedades. As principais referências para este capítulo são [7],[8],[10].

Definição 2.1. Um corpo K é dito uma **extensão** de F se K contém F como um subcorpo. Notação: $K|F$. O corpo F é chamado de corpo base da extensão $K|F$.

Exemplo 2.1. São exemplos de extensão de corpos:

$$\mathbb{R}|\mathbb{Q}, \quad \mathbb{C}|\mathbb{Q}, \quad \mathbb{C}|\mathbb{R}$$

Se K é uma extensão do corpo F podemos ver K como um espaço vetorial sobre F onde os vetores sao os elementos de K e os escalares são os elementos de F. A dimensão do espaço vetorial K sobre o corpo F sera chamada de **grau da extensão** e será denotado por $[K : F]$.

Uma extensão $K|F$ será dita finita, se K como espaço vetorial sobre F for finito, ou seja, se $[K : F] < \infty$.

Exemplo 2.2. $\mathbb{C}$ é uma extensão de grau 2 sobre $\mathbb{R}$ pois $\{1, i\}$ forma uma base para o espaço vetorial $\mathbb{C}$ sobre $\mathbb{R}$. Significa que cada vetor $w \in \mathbb{C}$ pode ser escrito de maneira única como uma combinação linear de 1 e i. Ou seja existem escalares α e β únicos em $\mathbb{R}$ tal que $w = \alpha \cdot 1 + \beta \cdot i$.

Exemplo 2.3. Seja $K = \{a + b\sqrt{5}; a, b \in \mathbb{Q}\}$. A extensão $K|\mathbb{Q}$ é finita, pois K é um espaço vetorial sobre $\mathbb{Q}$ gerado por 1 e $\sqrt{5}$.

Lembremos que a base de um espaço vetorial K sobre F é um subconjunto de K que gera K e é linearmente independente.

Definição 2.2. Seja $F \subset K$ uma extensão de corpos. Um elemento $\alpha \in K$ é dito **algébrico sobre** F se existe um polinômio não nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Um número real que é algébrico sobre $\mathbb{Q}$ é chamado de **número algébrico.**

É claro que todo racional s, sendo raiz do polinômio $x - s \in \mathbb{Q}[x]\backslash\{0\}$, é número algébrico.

Exemplo 2.4. O número $\sqrt[3]{5}$ é algébrico pois é raiz do polinômio não nulo $x^3 - 5 \in \mathbb{Q}[x]$.

Exemplo 2.5. O número $2 + \sqrt{3}$ é algébrico . De fato, seja

$$\begin{aligned} a &= 2 + \sqrt{3} \\ a - 2 &= \sqrt{3} \\ (a-2)^2 &= (\sqrt{3})^2 \\ a^2 - 4a + 1 &= 0. \end{aligned}$$

Portanto a é raiz do polinômio $x^2 - 4x + 1$, não nulo de coeficientes racionais.

Exemplo 2.6. Sejam $r \in \mathbb{Q}_+^*$ e $n \in \mathbb{N}$. Se w é uma raiz enésima da unidade, ou seja,$w \in \mathbb{C}$ tal que $w^n = 1$, então $\sqrt[n]{r}w$ é algébrico. De fato seja

$$\begin{aligned} \alpha &= \sqrt[n]{r}w \\ \alpha^n &= (\sqrt[n]{r}w)^n \\ \alpha^n &= (\sqrt[n]{r})^n \cdot w^n \\ \alpha^n &= r \cdot 1 \\ \alpha^n - r &= 0. \end{aligned}$$

Portanto α é raiz do polinômio $x^n - r$ não nulo de coeficientes racionais.

Definição 2.3. Se $\alpha \in L$ é algébrico, então um polinômio mônico $f(x) \in K[x]$ de grau mínimo que admite α como raiz é chamado de **polinômio minimal** de α sobre K e será denotado por p_a.

Exemplo 2.7. i e $\sqrt{5}$ são números algébricos com polinômios minimais sobre $\mathbb{Q}$ dados por x^2+1 e $x^2 - 5$, respectivamente.

Proposição 2.4. *Se a é algébrico sobre $\mathbb{Q}$ e p_a é um polinômio minimal de a, então:*

(i) p_a é irredutível sobre $\mathbb{Q}$;

(ii) Se $f \in \mathbb{Q}[x]$ é tal que $f(a) = 0$ então p_a divide f em $\mathbb{Q}[x]$.

Demonstração. (i) Se fosse $p_a = f(x)g(x)$, com f e g não constantes e de coeficientes racionais, então $f(x)$ e $g(x)$ teriam graus menores que p_a e ao menos um deles teria a por raiz, uma contradição à minimalidade do grau de p_a. Logo p_a é irredutível sobre $\mathbb{Q}$.

(ii) Pelo Teorema 1.15, existem polinômios q , $r \in \mathbb{Q}[x]$ tais que

$$f(x) = p_a(x) \cdot q(x) + r(x),$$

como $r = 0$ ou $0 \leq \text{gr}(r(x)) < \text{gr}(p_a)$. Se $r \neq 0$, então

$$r(\alpha) = f(\alpha) - p_\alpha.q(\alpha) = 0,$$

com $\text{gr}(r(x)) < \text{gr}(p_\alpha)$ novamente contradizendo a minimalidade do grau de p_α.

□

Corolário 2.5. *Se $\alpha \in \mathbb{C}$ é algébrico e $f \in \mathbb{Q}[x] \setminus \{0\}$ é um polinômio mônico, irredutível e tal que $f(\alpha) = 0$ então $f = p_\alpha$.*

Demonstração. Temos que p_α divide f em $\mathbb{Q}[x]$. Mas como f é irredutível deve existir um racional não nulo c tal que $f = c \cdot p_\alpha$. Por fim , como f e p_α são mônicos devemos ter $c = 1$. □

Exemplo 2.8. O polinômio minimal de $\sqrt[5]{3}$ sobre $\mathbb{Q}$ é $x^5 - 3$, haja visto que o mesmo é mônico e irredutível sobre $\mathbb{Q}$. De fato, tomando $p = 3$, o mesmo é irredutível de acordo com o Teorema 1.37.

Exemplo 2.9. Vamos determinar qual é o polinômio mônico em $\mathbb{Z}[x]$ de grau mínimo que tem $1 + \sqrt[3]{2}$ como raiz. Ou seja determinar quem é o polinômio mínimo.
Seja $\alpha = 1 + \sqrt[3]{2}$, temos que

$$\alpha = 1 + \sqrt[3]{2}$$

$$\alpha - 1 = \sqrt[3]{2}$$

$$(\alpha - 1)^3 = (\sqrt[3]{2})^3$$

$$\alpha^3 - 3\alpha^2 + 3\alpha - 1 = 2$$

$$\alpha^3 - 3\alpha^2 + 3\alpha - 3 = 0.$$

Ou seja, α é raiz do polinômio $p(x) = x^3 - 3x^2 + 3x - 3 \in \mathbb{Z}[x]$. Utilizando Teorema 1.37 , com $p = 3$ determinamos que o mesmo é irredutível e, portanto é polinômio minimal de acordo com o Corolário 2.5.

Definição 2.6. (**Polinômios Ciclotômicos**) Pra cada $n \in \mathbb{N}$, o polinômio minimal Φ_n da raiz primitiva n-ésima da unidade $w_n = \cos\frac{2\pi}{n} + i\,\text{sen}\,\frac{2\pi}{n}$ é denominado o n-ésima polinômio ciclotômico.

Exemplo 2.10. $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. De fato sabemos que o polinômio $x^{p-1} + x^{p-2} + \cdots + x + 1$ é irredutível. Como

$$(x-1) \cdot (x^{p-1} + x^{p-2} + \cdots + x + 1) = x^p - 1$$

e w_p é raiz de $x^p - 1$ mas não de $x - 1$, segue que w_p é raiz de $x^{p-1} + x^{p-2} + \cdots + x + 1$. Portanto segue do Corolário 2.5 que $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Proposição 2.7. *Todo número complexo é algébrico sobre* $\mathbb{R}$.

Demonstração. De fato, dado número complexo $\alpha = a + bi$, encontraremos um polinômio em $\mathbb{R}[x]$ tal que $p(\alpha) = 0$. Ora, sabemos que se $p(\alpha) = 0$ então $p(\bar{\alpha}) = 0$. Portanto

$$p(x) = (x - (a + bi) \cdot (x - (a - bi)) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x] \backslash \{0\}$$

Ou seja $\alpha = a + bi$ é raiz de um polinômio não nulo de coeficientes em $\mathbb{R}$.

□

Seja $K|F$ uma extensão de corpos e seja $\alpha \in K$. Definimos a **adjunção** de α a F como sendo o menor subcorpo de K contendo $F \cup \{\alpha\}$ e o denotamos por $F(\alpha)$. Assim , $F \subset F(\alpha) \subset K$ e $\alpha \in F(\alpha)$.

Exemplo 2.11. O menor subcorpo de $\mathbb{R}$ contendo $\mathbb{Q} \cup \{\sqrt{3}\}$ é $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3}; a, b \in \mathbb{Q}\}$.

Lema 2.8. *Sejam K uma extensão de F e $\alpha \in K$ algébrico sobre F com polinômio minimal $p_\alpha \in F(X)$ de grau n. Então $[F(\alpha) : F] = n$.*

Demonstração. A demostração deste Lema aplica o conceito e resultado sobre ideal, que não foi contemplado no trabalho, a prova pode ser encontrada em $cf.$[7](pág 217) □

Lema 2.9. *Sejam $F \subset K$ corpos. Suponhamos que $[K : F] < \infty$. Então todo elemento $\alpha \in K$ é algébrico sobre F.*

Demonstração. Seja K uma extensão finita de grau n. Por definição de grau, a dimensão de K como um espaço vetorial sobre F é n. O conjunto $X = \{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ tem $n + 1$ elementos e, portanto, tem cardinalidade maior que a dimensão de K sobre F. Então X é linearmente dependente, ou seja existem $a_0, a_1, \ldots, a_n \in F$ não todos nulos , tais que

$$a_0 \cdot 1 + a_1 \cdot \alpha + \ldots + a_n \alpha^n = 0.$$

Logo , $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in F$ é não nulo e tem α como raiz. Assim, todo elemento $\alpha \in K$ é algébrico sobre F. □

Lema 2.10. *Se $F \subset K$ e $K \subset L$ são extensões finitas então $F \subset L$ é finita e* $[L : F] = [L : K] \cdot [K : F]$.

Demonstração. Suponha que $[L : K] = n$ e $[K : F] = m$. Por definição de grau, seja

$$\alpha = \{\alpha_1, \ldots, \alpha_n\}$$

uma base de L sobre K e seja

$$\beta = \{\beta_1, \ldots, \beta_m\}$$

uma base de K sobre F. Considere o conjunto $\gamma = \{\alpha_i b_j : 1 \leq i \leq n, 1 \leq j \leq m\} \subset L$ com mn elementos. Basra mostrar que γ é uma base de L sobre F.

(i) γ é um conjunto de geradores de L sobre F: Seja $u \in L$. Por definição de base, existem escalares $a_1, \ldots, a_n \in K$ tais que

$$u = a_1\alpha_1 + \ldots + a_n \tag{2.1}$$

Desde que β é base de K sobre F e $a_1, \ldots, a_n$ são elementos de K então, para cada $i = 1, \ldots, n$ existem escalares $b_{1i}, \ldots, b_{mi} \in F$ tais que

$$\begin{aligned} a_1 &= b_{11}\beta_1 + \ldots + b_{1m}\beta_m \\ a_2 &= b_{21}\beta_1 + \ldots + b_{2m}\beta_m \\ &\vdots \\ a_n &= b_{n1}\beta_1 + \ldots + b_{nm}\beta_m \end{aligned}$$

Substituindo as igualdades acima na igualdade 2.1 obtemos

$$\begin{aligned} u &= (b_{11}\beta_1 + \ldots + b_{1m}\beta_m)\alpha_1 + \ldots (b_{n1}\beta_1 + \ldots + b_{nm}\beta_m)\alpha_n \\ &= \sum_{1 \leq i \leq n, 1 \leq j \leq m} b_{ij}\alpha_i\beta_j. \end{aligned}$$

(ii) γ é um conjunto linearmente independente: Seja dada uma combinação linear nula

$$\sum_{1 \leq i \leq n, 1 \leq j \leq m} b_{ij}\alpha_i\beta_j = 0$$

com $b_{ij} \in F$. Podemos escrever a igualdade acima na forma :

$$(b_{11}\beta_1 + \ldots + b_{n1}\beta_m)\alpha_1 + \ldots + (b_{n1}\beta_1 + \ldots + b_{nm}\beta_m)\alpha_n = 0$$

em que $b_{i1}\beta_1 + \ldots b_{im}\beta_m \in K$ para todo $i =, \ldots, n$. Mas $\alpha_1, \ldots, \alpha_n$ são linearmente independentes sobre K donde

$$\begin{aligned} b_{11}\beta_1 + \ldots b_{1m}\beta_m &= 0 \\ b_{21}\beta_1 + \ldots b_{2m}\beta_m &= 0 \\ &\vdots \\ b_{n1}\beta_1 + \ldots b_{nm}\beta_m &= 0 \end{aligned}$$

com $b_{ij} \in F$. Como $\beta_1, \ldots, \beta_m$ são linearmente independentes sobre F segue que $b_{ij} = 0$ para todo $i = 0, \ldots, n$ e para todo $j = 0, \ldots, m$.

□

Teorema 2.11. *Sejam a, b algébricos sobre F. Então $a \pm b, a \cdot b$ e $\frac{a}{b}$ (se $b \neq 0$) são algébricos sobre F.*

Demonstração. Por hipótese, a é algébrico sobre F, logo $[F(a) : F] < \infty$ pelo Lema 2.8. Seja $K = F(a)$. Como b é algébrico sobre F então b também é algébrico sobre K,pois todo polinômio em $F[x]$ também está em K. Seja $L = K(b)$. Pelo Lema 2.8, $[K : F] < \infty$. Pelo Lema 2.10, $[L : F] = [L : K] \cdot [L : K] < \infty$. Segue do Lema 2.9 que todo elemento de L é algébrico sobre F. Como $a, b \in F \subset L$ e L é corpo,$a \pm b, a \cdot b$ e $\frac{a}{b} \in L$. Portanto, $a \pm b, a \cdot b$ e $\frac{a}{b}$ são algébricos sobre F. □

O conjunto dos números algébricos de F sobre K formam um corpo, pois é fechado para adição e multiplicação bem como sob inversos aditivo e multiplicativo, segundo Teorema 2.11. Esse corpo é chamado de **Fecho Algébrico de F em K e denotado por** $\overline{F}$.

Definição 2.12. Um número complexo diz-se **inteiro algébrico** se for raiz de algum polinômio mônico não identicamente nulo e com coeficientes inteiros.

Exemplo 2.12. Seja $a \in \mathbb{Z}$, então a é inteiro algébrico, pois é raiz da equação $x - a = 0$.

Exemplo 2.13. $\sqrt{5}$ é inteiro algébrico, pois é raiz da equação $x^2 - 5 = 0$.

Exemplo 2.14. Todo número da forma $\sqrt{b}$, com $b \in \mathbb{N}$ é um inteiro algébrico. De fato,

$$x = \sqrt{b} \Rightarrow x^2 = (\sqrt{b})^2 \Rightarrow x^2 - b = 0.$$

Teorema 2.13. *Todo inteiro algébrico real é um número inteiro ou irracional*

Demonstração. Suponha por absurdo que $\frac{p}{q}$ com $p \in \mathbb{Z}$ e $q > 1$ seja raiz do polinômio $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Ora o critério das raízes racionais acarreta que se $\frac{p}{q}$ é raiz de $p(x)$ então p divide a_0 e q divide a_n como $a_n = 1 \Rightarrow q$ divide 1, o que é um absurdo, pois $q > 1$ □

Definição 2.14. Um número $a \in \mathbb{C}$ que não é raiz de nenhuma equação polinomial com coeficientes racionais é dito número **transcendente** ou equivalentemente, número transcendente é número que não é algébrico.

Com esta definição, não fica claro que existam números transcendentes, isto é, números não algébricos. Em 1981 o matemático francês Liouville estabeleceu a existência de números transcendentes. Ele fez exibindo certos números que provou sendo não algébricos. Mais tarde ainda provou-se que π é um número transcendente. Um outro avanço no século XIX foi feito por Cantor, em contraste com o de Liouville, ao não exibir um numero transcendente de forma explícita, tem a vantagem de demonstrar que, em certo sentido,há muito mais números transcendentes do que algébricos. A existência de números transcendentes pode ser demonstrada como fez Cantor.

Mostraremos abaixo a existência de números complexos que são transcendentes. Mas antes vejamos a definição de conjunto enumerável .

Definição 2.15. Um conjunto A é enumerável se seus elementos puderem ser postos em correspondência biunívoca com os números naturais ou se A for finito.

Admitiremos os seguintes resultados, que podem ser encontrados em [3] pág 197.

Proposição 2.16.

(a) O conjunto $\mathbb{Q}$ dos números racionais é enumerável.

(b) O conjunto $\mathbb{R}$ dos números reais não é enumerável.

(c) O conjunto $\mathbb{C}$ dos números complexos não é enumerável.

(d) A união de uma quantidade enumerável de conjuntos enumeráveis é enumerável.

Teorema 2.17. *(Cantor) O conjunto do números algébricos é enumerável.*

Demonstração. Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$, onde $a_n \neq 0$ e todos os a_i são inteiros. Consideremos a *altura* h do polinômio, definida por

$$h = \mid a_0 \mid + \mid a_1 \mid + \cdots + \mid a_n \mid + n$$

obviamente h é um número inteiro ≥ 1. Além disso, $f(x)$ deve possuir no máximo n raízes complexas de acordo com o Teorema 1.30, das quais todas, algumas, ou nenhuma delas podem

ser reais. Agora, o número de polinômios com coeficientes inteiros com uma dada altura é apenas um número finito. Isso significa que a cardinalidade do conjunto de todas as raízes de todos os polinômios com uma dada altura é apenas um número finito. Portanto o conjunto de todas as raízes de todos os polinômios de todas as alturas formam um conjunto enumerável.

□

Corolário 2.18. *Existem números transcendentes.*

Demonstração. Suponha por absurdo que nenhum complexo fosse transcendente. Então todos os complexos seriam algébricos. Pelo Teorema 2.17, isso nos daria que $\mathbb{C}$ é enumerável. Mas isto é absurdo. □

Corolário 2.19. *O conjunto dos transcendentes é não enumerável.*

Demonstração. O conjunto $\mathbb{C}$ é dado pela união disjunta entre o conjunto dos números algébricos e o conjunto dos números transcendentes. Se este fosse enumerável, então $\mathbb{C}$ também o seria, uma vez que a união de dois conjuntos enumeráveis também é enumerável. Novamente chegaríamos em um absurdo. □

Exemplo 2.15. Admitindo-se a transcendência dos números π e e, o Teorema 2.11, permite justificar a transcendência de vários tipos de números complexos. Por exemplo, o número $e+\sqrt{3}$ é transcendente, visto que, se fosse algébrico, teríamos

$$e = (e + \sqrt{3}) - \sqrt{3},$$

uma diferença entre dois números algébricos, logo algébrico.

Capítulo 3

Atividades

Neste capítulo mostraremos algumas atividades apresentadas na forma de problemas. As atividades aqui propostas podem ser aplicadas a alunos a partir do 3º ano do Ensino Médio e podem ser trabalhadas de forma individual ou em grupos.

Atividade 01 O **Número de ouro ou proporção áurea** (Φ) é um número irracional, sendo um dos mais misteriosos enigmáticos que surge numa infinidade de elementos da natureza sob a forma de uma razão. Nos *Elementos de Euclides*, a obra mais influente de toda a História da Matemática, aparece um segmento de reta dividido em duas partes.

$$\Phi = \frac{a+b}{a} = \frac{a}{b}$$

(A razão entre o segmento inteiro $a+b$ e a parte maior a é igual a razão entre as partes maior e menor.)

a) Mostre que Φ é um inteiro algébrico ou seja que ele seja raiz de uma equação do tipo

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

com coeficientes inteiros.

b) Encontre o valor de ϕ.

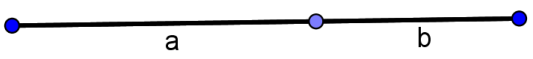

Figura 3.1:

Atividade 02 Sejam a, b e c números reais com $a \neq 0$.

a) Mostre que a mudança $x + \frac{1}{x} = z$ transforma a equação $ax^4 + bx^3 + cx^2 + bx + a = 0$ numa equação de segundo grau.

b) Determine todas as raízes da equação $x^4 + 3x^3 - 2x^2 + 3x + 1 = 0$.

Atividade 03 Um número é algébrico se o mesmo é raiz de um polinômio com coeficientes racionais, caso contrário será transcendente. Seja $\overline{\mathbb{Q}}$ o conjunto dos números algébricos e T o conjunto dos transcendentes. Admitindo-se que o conjunto dos algébricos $\overline{\mathbb{Q}}$ forma um corpo ou seja valem as propriedades de fechamento, comutatividade, associatividade, para soma e produto. Mostre que se $\alpha, \beta \in T$ então $(\alpha + \beta)$ ou $(\alpha - \beta) \in T$.

Atividade 04 Sempre que um número algébrico for raiz de uma equação de grau n, com coeficientes inteiros, mas não for raiz de nenhuma equação de grau menor, com coeficientes inteiros, dizemos tratar-se de um *número algébrico de grau n*. Por exemplo $\sqrt{2}$ é de grau 2, pois é raiz do polinômio $x^2 - 2$ e não é raiz de um polinômio de grau um com coeficientes inteiros. Um **Teorema Sobre Construções Geométricas** afirma que :*Começando com um segmento de comprimento unitário, qualquer comprimento que possa ser construído com régua e compasso é um número algébrico de grau 1, ou 2, ou 4, ou 8,..., isto, é um número algébrico de grau igual a uma potência de 2.* Responda:

a) O número $\sqrt{1 + \sqrt{2}}$ é algébrico?

b) Qual o grau do número $\sqrt{1 + \sqrt{2}}$?

c) O número $\sqrt{1 + \sqrt{2}}$ é construtível com régua e compasso? Justifique.

Atividade 05 Sendo Z_1 e Z_2 as raízes não reais da equação $x^3 - x^2 - x - 15 = 0$. O que podemos afirmar a respeito do produto $Z_1 \cdot Z_2$? Podemos afirmar que esse produto é um numero real positivo? Por que?

Atividade 06 Seja x um número real positivo. O volume de um paralelepípedo reto-retângulo, é dado em função de x, pelo polinômio $x^3 + 10x^2 + 33x + 36$. Se uma aresta do paralelepípedo mede $x + 4$, determine a área da face perpendicular a essa aresta.

Atividade 07 Qualquer solução de uma equação polinomial da forma

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

onde os coeficientes $a_0, \ldots, a_{n-1}$ são números inteiros, é chamada um *inteiro algébrico.*

a) Mostre que $x = \sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}$ é um inteiro algébrico.

b) Mostre que $x = 1$.

Atividade 08 Um número algébrico é qualquer número real ou complexo que é solução de alguma equação polinomial com coeficientes racionais , caso contrário é dito transcendente. Dado o polinômio $x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$, responda:

a) O número $\alpha = \sqrt{2} + \sqrt{3}$ é raiz de $p(x)$?

b) α é algébrico ou transcendente?

c) α é racional ou irracional? Justifique.

Atividade 09 Seja o polinômio $p(x) = x^2 + mx + n \in \mathbb{R}$, sejam x_1 e x_2 as raízes de $p(x)$. a) Mostre que $x_1 + x_2 = -m$ e $x_1 \cdot x_2 = n$

b) Sabendo-se que a equação $x^2 + mx + n = 0$ com $m, n \in \mathbb{R}$, admite $x_1 = 5 - 2i$ como uma raiz. Determine os valores de m e n.

Atividade 10 (UFCE- Adaptada) Um engenheiro projetou duas caixas d'agua de mesma altura. Uma em formato de um cubo e outra em formato de paralelepípedo reto retângulo com $6m^2$ de área da base. O volume da caixa cúbica deve ser $4m^3$ menor que o da outra caixa. Nessas condições, qual deve ser a medida da aresta da caixa cúbica?

Atividade 11 (Olimpíada de Matemática da Academia de Ciências do Estado de São Paulo - 1977) Dada a equação $x^2 - (a + c)x + ac - b^2 = 0$. a) Demonstre que ela tem solução real quaisquer que sejam os números a, b e c.

b)Supondo que $b = 0$ e que a equação tem uma só solução, que relação existe entre a e c?

c)Decida se a seguinte sentença é verdadeira ou falsa: "se $b \neq 0$, a equação tem sempre duas soluções distintas". Justifique sua resposta.

Atividade 12 (OBMEP-2008-Adaptada) José quer cercar completamente um terreno retangular de $400m^2$. Ao calcular o comprimento da cerca, ele se enganou, fez os cálculos como se o terreno fosse quadrado e comprou 2 metros de cerca a menos que o necessário. Qual a diferença entre o comprimento e a largura do terreno?

Atividade 13 Os alunos de uma turma fizeram uma coleta para juntar R$405,00, custo de uma excursão. Todos contribuíram igualmente. Na última hora, porem, dois alunos desistiram. Com isso, a parte de cada aluno sofreu um aumento de R$1,20. Quantos alunos tem a turma?

Atividade 14 A teoria dos números algébricos e transcendentes possibilitou aos matemáticos resolver três problemas geométricos, bem conhecidos que proviam da antiguidade. Esses três problemas

conhecidos sob o nome de , *Duplicação do cubo*, *Trissecção do ângulo* e *Quadratura do círculo*, consiste em efetuar as seguintes construções usando apenas régua (sem marcas) e compasso.

a) **Duplicação do cubo**

Dada a aresta de um cubo, o problema consiste em construir, com régua e compasso, a aresta de um cubo que tenha o dobro do volume do cubo cuja aresta é dada.

b) **Trissecção de um ângulo**

Dado um ângulo β, queremos trissectá-lo com régua e compasso.

c) **Quadratura do círculo**

Significa construir um quadrado cuja a área seja igual à de um círculo dado ou de modo equivalente, construir um círculo de área igual à de um quadrado dado.

Sabe-se agora que tais construções são impossíveis; isto é, elas não podem ser efetuadas pelos métodos de construção da Geometria Euclidiana. O Engenheiro francês Pierre Laurent Wantzel demonstrou os seguintes fatos algébricos sobre a construção usando régua e compasso.

(i) *Um elemento geomérico é construtível com régua e compasso quando e apenas quando os números que o definem derivam dos dados do problema através de uma quantidade finita de operações de soma, subtração, multiplicação, divisão e extração de raízes quadradas.*

(ii) *A condição necessária e suficiente para que as três raízes de uma equação do terceiro grau, de coeficientes racionais, sejam construtíveis por régua e compasso é que uma delas seja racional.*

Mostre que as três construções são impossíveis usando-se apenas régua e compasso.

Atividade 15 Usando as fórmulas trigonométricas :

$$\cos(a+b) = \cos a \cos b - \operatorname{sen} a \operatorname{sen} b,$$

$$\operatorname{sen}(a+b) = \operatorname{sen} a \cos b + \cos a \operatorname{sen} b$$

Mostre que:

a) $\operatorname{sen}(3\beta) = 3\operatorname{sen}\beta - 4\operatorname{sen}^3(\beta)$

b) $\operatorname{sen} 10^0$ é um número algébrico ou seja que ele é raiz de um polinômio não nulo com coeficientes inteiros.

c) $\operatorname{sen} 10^0$ é um número irracional.

Capítulo 4

Respostas

Atividade 01

a) De fato, seja

$$\begin{aligned} \phi &= \frac{a+b}{a} = \frac{a}{b} \\ \phi &= 1 + \frac{1}{\phi} \\ \phi^2 &= \phi + 1 \\ \phi^2 - \phi - 1 &= 0. \end{aligned}$$

Ou seja ϕ é raiz do polinômio $x^2 - x - 1$ mônico de coeficientes inteiros. Portanto ϕ é inteiro algébrico.

a) Resolvendo a equação $\phi^2 - \phi - 1 = 0$ obtemos

$$\begin{aligned} \phi &= \frac{-(-1) \pm \sqrt{(-1)^2 - 4 \cdot 1 \cdot 4}}{2 \cdot 1} \\ \phi &= \frac{1+\sqrt{5}}{2}. \end{aligned}$$

Observe que tomamos apenas a raiz positiva pois ϕ é razão de segmentos.

Atividade 02

a) Se $x + \frac{1}{x} = z$ então $(x + \frac{1}{x})^2 = z^2$. Desenvolvendo temos $x^2 + \frac{1}{x^2} = z^2 - 2$. Sendo $x \neq 0$ e dividindo a equação $ax^4 + bx^3 + cx^2 + bx + a = 0$ por x^2 obtemos $ax^2 + bx + c + + \frac{b}{x} + \frac{a}{x^2} = 0$ ou seja $a(x^2 + \frac{1}{x^2}) + b(1 + \frac{1}{x}) + c = 0 \Rightarrow$ $a(z^2 - 2) + bz + c = 0 \Rightarrow az^2 + bz + c - 2a = 0$.

b) Fazendo a mudança de variável $x + \frac{1}{x} = z$ temos: $z^2 + 3z - 2 - 2 = 0 \Rightarrow z^2 + 3z - 4 = 0$ resolvendo a equação em z encontramos $z = 1$ ou $z = -4$. Para $z = 1 \Rightarrow x + \frac{1}{x} = 1 \Rightarrow$

$x^2-x+1=0 \Rightarrow x=\frac{1+\sqrt{3}i}{2}$ ou $x=\frac{1-\sqrt{3}i}{2}$. Par $z=-4 \Rightarrow x+\frac{1}{x}=-4 \Rightarrow x^2+4x+1=0$ resolvendo encontramos $x=-2+\sqrt{3}$ ou $x=-2-\sqrt{3}$. Assim as raízes da equação $x^4+3x^3-2x^2+3x+1=0$ são: $\frac{1+\sqrt{3}i}{2}, \frac{1-\sqrt{3}i}{2}, -2+\sqrt{3}$ e $-2-\sqrt{3}$.

Atividade 03 Suponha por absurdo que $(\alpha+\beta)$ e $(\alpha-\beta) \in \overline{\mathbb{Q}}$. Como $\overline{\mathbb{Q}}$ é corpo então a soma pertence a $\overline{\mathbb{Q}}$. mas
$(\alpha+\beta)+(\alpha-\beta)=2\alpha=\alpha+\alpha$ que é transcendente, absurdo.

Atividade 04

a) Seja $\alpha=\sqrt{1+\sqrt{2}}$. Elevando ao quadrado e arrumando temos:

$$\alpha^2-1=\sqrt{2}$$

Elevando novamente ao quadrado temos:

$$\alpha^4-2\alpha^2-1=0$$

Portanto $\alpha=\sqrt{1+\sqrt{2}}$ é raiz do polinômio x^4-2x^2-1. Logo α é algébrico.

b) O número $\sqrt{1+\sqrt{2}}$ tem grau 4 pois o mesmo satisfaz a equação $x^4-2x^2-1=0$ de grau 4, mas não satisfaz nenhuma equação de grau 3, 2 ou 1, com coeficientes inteiros.

c) Sim, pois $\sqrt{1+\sqrt{2}}$ é um número algébrico de grau 4 e, portanto uma potência de 2.

Atividade 05 Como os coeficientes da equação $x^3-x^2-x-15=0$ são números reais, as possíveis raízes complexas aparecem aos pares. Como a equação tem grau 3 concluímos que as raízes não reais Z_1 e Z_2 são conjugadas. Sejam $Z_1=a+bi$ com $a,b \in \mathbb{R}$ então $Z_2=a-bi$ portanto $Z_1 \cdot Z_2=(a+bi)\cdot(a-bi)=a^2+b^2$. Ou seja o produto é número real positivo, pois $a^2 \geq 0$ e $b^2>0$ implica $a^2+b^2>0$.

Atividade 06 O volume do paralelepípedo reto-retângulo é dado pelo produto entre uma aresta e a área da face perpendicular a essa aresta, então para encontrarmos a área dessa aresta basta dividirmos o volume pela aresta. Dividindo $(x^3+10x^2+33x+36)$ por $x+4$ obtemos x^2+6x+9. Portanto a área dessa face é dada por x^2+6x+9.

Atividade 07

a) Seja

$$\begin{aligned} x &= \sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}, \text{ (elevando ambos os membros ao cubo temos)} \\ x^3 &= (\sqrt[3]{2+\sqrt{5}})^3 + 3\cdot(\sqrt[3]{2+\sqrt{5}})^2 \cdot \sqrt[3]{2-\sqrt{5}} + 3\cdot \sqrt[3]{2+\sqrt{5}} \cdot \sqrt[3]{(2-\sqrt{5})^2} + (\sqrt[3]{2-\sqrt{5}})^3 \\ &= 4 + 3\cdot \sqrt[3]{-2-\sqrt{5}} + 3\cdot \sqrt[3]{-2+\sqrt{5}} \\ &= 4 - 3\left(\cdot \sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}\right) \\ &= 4 - 3x. \end{aligned}$$

Ou seja $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$ é raiz do polinômio mônico de coeficientes inteiros $x^3 + 3x - 4$, portanto é inteiro algébrico.

b) Como $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$ é real e é raiz do polinômio $p(x) = x^3 + 3x - 4$ e as possíveis raízes racionais de $p(x)$ são os divisores de 4, verifica-se facilmente que 1 é raiz de $p(x)$. Dividindo $p(x)$ por $x-1$ obtemos x^2+x+4 cujas raízes são complexas, pois $\Delta = -15$. Assim $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$ é a única raiz real de $p(x) = x^3 - 3x + 4$ logo $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}} = 1$.

Atividade 08

a) Sim, pois $p(\sqrt{2}+\sqrt{3}) = (\sqrt{2}+\sqrt{3})^4 - 10\cdot(\sqrt{2}+\sqrt{3})^2 + 1 = 0$.

b) $\alpha = \sqrt{2}+\sqrt{3}$ é algébrico pois é raiz de uma equação com coeficientes inteiros.

c) $\alpha = \sqrt{2}+\sqrt{3}$ é irracional, pois α é raiz de $p(x)$ conforme item (a) e as possíveis raízes racionais de $p(x)$ são -1, +1, mas $p(-1) = p(+1) = -8 \neq 0$.

Atividade 09

a) Sejam x_1 e x_2 as raízes de $p(x) = x^2 + mx + n$. Então podemos escrever:

$$\begin{aligned} x^2 + mx + n &= (x - x_1)\cdot(x - x_2) \\ &= x^2 - (x_1 + x_2)\cdot x + x_1 \cdot x_2. \end{aligned}$$

Ou seja $x_1 + x_2 = -m$ e $x_1 \cdot x_2 = n$

b) Como os coeficientes de $p(x)$ são reais e $x_1 = 5 - 2i$ então $x_2 = 5 + 2i$. Ora $x_1 + x_2 = (5-2i) + (5+2i) = 10$, acarreta que $m = -10$, e como $x_1 \cdot x_2 = (5-2i)\cdot(5+2i) = 25 + 4 = 29$, acarreta que $n = 29$.

Atividade 10 A área da base do paralelepípedo é igual a $ab = 6$ e o volume é $V = abx$ logo $V = 6x$, sendo x a altura. O volume do cubo é igual a $V = x^3$. Assim o valor de x é a raiz da

equação $x^3 + 4 = 6x$, ou seja $x^3 - 6x + 4 = 0$. Testando as possíveis raízes inteiras, que são os divisores de 4, percebemos que 2 é raiz da equação $x^3 - 6x + 4 = 0$. Dividindo $x^3 - 6x + 4 = 0$ por $x - 2$, para obtermos as outras duas raízes, obtemos $x^2 + 2x - 2$ (que é um polinômio de grau 2), logo as duas raízes restantes são a da equação $x^2 + 2x - 2 = 0$, isto é,

$$\begin{aligned} x = & \frac{-2 \pm \sqrt{4+8}}{2} \\ = & \frac{-2 \pm \sqrt{12}}{2} \\ = & -1 \pm \sqrt{3}. \end{aligned}$$

Logo, a medida x da aresta deve ser 2m ou $(-1 + \sqrt{3})$m.

Atividade 11

a) A equação $x^2 - (a + c)x + ac - b^2$ tem solução real desde quando $\Delta \geq 0$ mas:

$$\begin{aligned} \Delta &= [-(a+c)]^2 - 4 \cdot 1 \cdot (ac - b^2) \\ &= a^2 + 2ac + c^2 - 4ac + 4b^2 \\ &= a^2 - 2ac + c^2 + 4b^2 \\ &= (a-c)^2 + (2b)^2 \\ &\geq 0, \end{aligned}$$

Pois é soma de dois quadrados. Assim a equação $x^2-(a+c)x+ac-b^2$ tem solução real.

b) A equação $x^2 - (a + c)x + ac - b^2$ tem única solução somente quando $\Delta = 0$. Como $b = 0$ então $\Delta = (a - c)^2 = 0$ se, somente se $a = c$.

c) Verdadeira, pois sendo $b \neq 0$ acarreta que $\Delta = (a - c)^2 + (2b)^2 > 0$

Atividade 12 Como José pensou que era um quadrado, a medida do lado seria $L = \sqrt{400} = 20m$ ou seja o perímetro seria $80m$. Mas no anunciado ele na verdade comprou $2m$ a menos, então o perímetro na verdade seria de $82m$. Temos assim o sistema

$$\begin{cases} a + b = 41 (I) \\ a \cdot b = 400 (II) \end{cases}$$

substituindo I em II temos:

$(41 - b) \cdot b = 400 \Rightarrow b^2 - 41b + 400 = 0$. Resolvendo a equação obtemos:

$b = 16$ ou $b = 25$. Se $b = 16$ então $a = 25$, se $b = 25$ então $a = 16$.

Então a diferença entre o comprimento e a largura é $9m$.

Atividade 13 Denotemos por x o número de alunos da turma. O que era estipulado que cada um pagasse era $\frac{405}{x}$. Com a desistência de dois alunos passou a ser $\frac{405}{x-2}$. Se há menos alunos dividindo a conta, é obvio que o valor que cada um tem que pagar aumenta. A diferença entre esses dois valores é de R$1,20. Logo:

$$\frac{405}{x-2} - \frac{405}{x} = 1,2$$

multiplicando por $x \cdot (x-2)$ obtemos:

$$405x - 405 \cdot (x-2) = 1,2 \cdot x \cdot (x-2) \Rightarrow x^2 - 2x - 675 = 0$$

Resolvendo temos :

$$\begin{aligned} x &= \frac{-(-2) \pm \sqrt{(-2)^2 - 4 \cdot 1 \cdot (-675)}}{2 \cdot 1} \\ &= \frac{2 \pm \sqrt{2704}}{2} \\ &= \frac{2 \pm 52}{2} \end{aligned}$$

$x = 27$ ou $x = -25$. Ora A quantidade não pode ser negativa, portanto o número de alunos é 27.

Atividade 14 O item (i) equivale a dizer que um número que expressa o comprimento de um segmento construtível é necessariamente *algébrico.* Este resultado elimina o problema da **quadratura**. De fato tomando-se como unidade de comprimento o raio de um círculo dado, o lado do quadrado equivalente procurado é $\sqrt{\pi}$. Logo se o problema fosse resolúvel com os instrumentos euclidianos, seria possível construir um segmento de comprimento $\sqrt{\pi}$ a partir do segmento unitário . Mas isso é impossível pois π, e consequentemente $\sqrt{\pi}$ não são algébricos.

O item(ii) elimina os outros dois problemas.

Para o problema da **duplicação do cubo** tome como unidade de comprimento a aresta do cubo dado e denote por x a aresta do cubo procurado. Devemos ter então $x^3 = 2$ que é equivalente a $x^3 - 2 = 0$. Mas a equação $x^3 - 2 = 0$ não tem nenhuma raiz racional, pois as possíveis raízes racionais de $x^3 - 2 = 0$ seriam $\pm 1, \pm 2$ que por simples inspeção verificamos que nenhuma delas é raiz, portanto é impossível a quadratura do cubo com régua e compasso.

Para a **trissecção do ângulo**, o raciocínio é o seguinte: se um ângulo é construtível

por régua e compasso, então o seu cosseno também o é e reciprocamente. Consideremos a identidade trigonométrica $\cos\theta = 4\cos^3(\frac{\theta}{3}) - 3\cos(\frac{\theta}{3})$. Quando $\theta = 60^o$, fazendo $x = \cos(\frac{\theta}{3})$, obtém-se

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

que é equivalente a

$$8x^3 - 6x - 1 = 0$$

Mas essa equação cúbica de coeficientes racionais não tem raiz racional, portanto não é possível trissecar o ângulo de 60^o.

Atividade 15

a) Tomando $a = b = \beta$ e substituindo nas fórmulas trigonométricas temos:

$$\begin{aligned} \cos(2\beta) &= \cos^2\beta - \operatorname{sen}^2\beta, \\ \operatorname{sen}(2\beta) &= 2\operatorname{sen}\beta\cos\beta. \end{aligned}$$

Agora

$$\begin{aligned} \operatorname{sen}(3\beta) &= \operatorname{sen}(\beta + 2\beta) \\ &= \operatorname{sen}\beta\cos 2\beta + \cos\beta\operatorname{sen}2\beta \\ &= \operatorname{sen}\beta(\cos^2\beta - \operatorname{sen}^2\beta) + \cos\beta(2\operatorname{sen}\beta\cos\beta) \\ &= \operatorname{sen}\beta(1 - 2\operatorname{sen}^2\beta) + 2\operatorname{sen}\beta - 2\operatorname{sen}^3\beta \\ &= 3\operatorname{sen}\beta - 4\operatorname{sen}^3\beta. \end{aligned}$$

Como queríamos mostrar.

b) Tome $\beta = 10^o$, usando a relação do item a, obtemos:

$$\operatorname{sen}30^o = 3\operatorname{sen}10^o - 4\operatorname{sen}^3 10^o$$

Mas $\operatorname{sen}30^o = \frac{1}{2}$ ou seja

$$\frac{1}{2} = 3\operatorname{sen}10^o - 4\operatorname{sen}^3 10^o$$

fazendo $x = \operatorname{sen}10^o$ temos

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

multiplicando por 2 e rearrumando temos:

$$8x^3 - 6x + 1 = 0$$

Portanto $\operatorname{sen}10^o$ é algébrico pois é raiz de uma equação polinomial de coeficientes inteiros.

c) Do item b) $\operatorname{sen} 10$ é raiz da equação $8x^3 - 6x + 1 = 0$. Mas as possíveis raízes racionais da equação $8x^3 - 6x + 1 = 0$ são $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$. Mas nenhum desses oito números são raízes da equação, como pode ser verificado por substituição. Assim a equação $8x^3 - 6x + 1 = 0$ não tem raízes racionais e portanto $\operatorname{sen} 10^{\circ}$ é um número irracional.

4.1 Considerações Finais

Esta dissertação teve como principal objetivo apresentar os Números Algébricos e Aplicaçôes no Ensino Médio. É sabido que muitos alunos e professores de matemática sequer ja tinha ouvido falar em números algébricos ou transcendentes, crêem que o conjuntos dos números reais só podiam ser visto como uma união disjunta entre racionais e irracionais. Os livros didáticos nem fazem referência. Espero que este trabalho sirva como material pelo menos introdutório, ao conceito de números algébricos e transcendentes e suas principais propriedades. Foi um desafio a busca ou elaboração das atividades propostas no final do trabalho, mas enriquecedora, pois sempre devemos apresentar situações problemas e não apenas os exercícios repetitivos, que acabam por desmotivar ainda mais os alunos, que ja carregam dentro de si uma grande aversão à Matemática.

Bibliografia

[1] BOYER, Carl Benjamin. **História da Matemática**. 2ª ed. Trad. ELZA F. OMIDE. São Paulo: Edgard Blücher, 1996

[2] EVES, Howard Whitley. **Introdução à história da Matemática**. 5ª ed.Campinas: Unicamp, 1997.

[3] GARBI, Gilberto G. **O Romance das Equações Algébricas**. São Paulo: Makron Books, 1997.

[4] GARCIA, Arnaldo e LEQUIAN, Yves. **Elementos de álgebra**. 4ª ed. Rio de Janeiro: Impa, Projeto Euclides, 2008.

[5] GIOVANNI, José Ruy e BONJORNO, José Roberto. **Matemática: uma nova abordagem**: vol3. São Paulo: FTD, 2001.

[6] GONÇALVES, Adilson. **Introdução à Álgebra**. 5ª ed. Rio de Janeiro: Impa, Projeto Euclides, 2008.

[7] HEFEZ, Abramo e VILLELA, Maria Lúcia Torres. **Polinômios e Equações Algebricas**. 1ª ed. Rio de Janeiro: SBM, 2012. (Coleção Profmat)

[8] MARTINEZ, FABIO Brochero; et al. **Teoria dos Números**: um passeio com primos e outros números familiares pelo mundo inteiro. 3ª ed. Rio de Janeiro: IMPA, 2013.

[9] MONTEIRO, Luiz Henrique Jacy. **Elementos de Álgebra**. Rio de Janeiro: Ao Livro Técnico S.A., 1969.

[10] NETO, Antonio Caminha Muniz. **Tópicos de Matemática Elementar**: Volume 6 - Polinômios. 1ª ed. Rio de Janeiro: SBM, 2012. (Coleção Professor de Matemática)

[11] NIVEN, Ivan.**Números: racionais e irracionais**.traduçao de Renato Watanabe. Rio de Janeiro: SBM,1990.(Coleção Iniciação Científica)

[12] MARQUES, Maria Cristina. **Introdução à Teoria de Anéis**. UFMG. Disponível em ⟨ http//www.mat.ufmg.br/ marques/Apostila-Aneis.pdf⟩. Acesso em 01 nov. 2015.

[13] SANTOS, José Plinio de Oliveira. **Introdução à Teoria dos Números**. Rio de Janeiro: Impa, 1998. (Coleção Matemática Universitária)