UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

FRANCISCO DANILO ALBUQUERQUE BARRETO

A IRREDUTIBILIDADE DE POLINÔMIOS E O TEOREMA DE DUMAS

FORTALEZA

2021

FRANCISCO DANILO ALBUQUERQUE BARRETO

A IRREDUTIBILIDADE DE POLINÔMIOS E O TEOREMA DE DUMAS

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional, da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de concentração: Álgebra.

Orientador: Prof. Dr. José Alberto Duarte Maia

Coorientador: Prof. Ms. José Afonso de Oliveira

FORTALEZA
2021

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

B262i Barreto, Francisco Danilo Albuquerque.
A irredutibilidade de polinômios e o teorema de Dumas / Francisco Danilo Albuquerque Barreto. – 2021.
92 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2020.
Orientação: Prof. Dr. José Alberto Duarte Maia.
Coorientação: Prof. Me. José Afonso de Oliveira.

1. Irredutibilidade (matemática). 2. Raiz racional. 3. Teorema de Dumas. 4. Polinômios. 5. Números irracionais. I. Título.

CDD 510

FRANCISCO DANILO ALBUQUERQUE BARRETO

A IRREDUTIBILIDADE DE POLINÔMIOS E O TEOREMA DE DUMAS

Dissertação apresentada ao Mestrado Profissional em Matemática em Rede Nacional, da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de concentração: Álgebra.

Aprovada em: 21/01/2021

BANCA EXAMINADORA

_____

Prof. Dr. José Alberto Duarte Maia (Orientador)
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. José Valter Lopes Nunes
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Francisco Régis Vieira Alves
Instituto Federal de Educação e Ciência do Ceará (IFCE)

Ao meu Deus.

À minha esposa, Lidiane.

Aos meus pais, Sr. Dionízio e D. Graça

Aos meus filhos, Daniel Levi e Débora Lívia.

AGRADECIMENTOS

Não podia deixar de iniciar agradecendo primeiramente a Deus – em quem confio e é socorro bem presente na minha vida, essencialmente nas horas de angústia e de sentimentos de incapacidade. Agradeço a Ele por me subsidiar dentro de minhas impossibilidades e não permitir que eu desfalecesse durante todo o percurso que trilhei nesse curso.

À minha esposa, pela paciência, amorosidade, compreensão e companheirismo, dentre outras qualificações, que são aspectos vitais para quem passa por todo esse processo e ainda tem que lidar com a rotina de trabalho escolar de três turnos, as constantes viagens aos sábados para as aulas presencias e disponibilizar-se de tempo para estudar em casa.

Aos meus amados e maravilhosos filhos, Daniel e Débora, que embora com meu cuidado de longe, a pouca idade não foi determinante na maturidade e percepção de que seria por pouco tempo e logo colheríamos o bônus. Seus entendimentos e respostas às minhas necessidades quanto pai e estudante assíduo diariamente foi um divisor de águas na minha persistência em concluir o curso – sempre atenciosos e amorosos incondicionalmente.

Ao meus pais, que até o momento nunca mediram esforços em aspectos diversos, inclusive recursos, para dar amparo de modo que minha preocupação estivesse apenas ligada ao meu bom desempenho.

Aos meus irmãos, em destaque ao Dênis, em que saliento as vezes que me assistiu na cidade de Fortaleza quando o solicitei – seja para pernoitar em sua casa ou resolver problemas mecânicos com meu carro.

Ao meu orientador, Prof. Dr. José Alberto Duarte Maia, pelas respostas às minhas dúvidas e por seu cuidado em sempre me atender de modo responsável e dentro de suas possibilidades, driblando uma pandemia e a distância geográfica.

Ao meu coorientador, Prof. Ms. José Afonso de Oliveira, pelas contribuições pertinentes de grande valia para a escrita desse trabalho.

Aos colegas da minha turma, pelo fortalecimento mútuo, onde tivemos momentos ímpares de aprendizado acadêmico.

E, agradeço aos admiráveis professores do curso os quais me tiraram da inércia onde estava e me fizeram deslumbrar e trilhar um caminho que outrora era utópico para mim quanto professor da rede pública, o de voltar a estudar e estudar uma matemática belíssima e

empolgante. Ficará em minha memória a maestria com a qual transmitiram os conhecimentos da mais bela das ciências.

“Uma boa notação possui uma engenhosidade e uma sugestividade que, às vezes, a faz parecer um professor de verdade.” (RUSSELL, 1956)

RESUMO

O Critério de Dumas é um método que possibilita a verificação da irredutibilidade de polinômios com coeficientes inteiros por meio das análises de suas representações em diagramas. Este estudo se inicia com a visão geral de números, abordando desde a classificação de racionais e irracionais, a categorias mais especiais como os números algébricos e os transcendentes (apenas conceitual). Temos como direcionamento de nosso estudo a obtenção – de modo prático, abrangente e eficiente – de mecanismos que nos poupem tempo quando for necessário classificarmos certo número no conjunto dos reais. É nesse âmbito que focamos nosso estudo, associando determinado número real à raiz de um polinômio – de onde temos a ideia de irredutibilidade vinculada a irracionalidade de um número – e daí podemos decompô-lo como produto de polinômios. Assim, apresentamos os métodos – Teorema das Raízes Racionais, Critério de Eisenstein e Critério de Dumas – comumente utilizados para a avaliação se dado polinômio possui ou não raízes racionais.

Palavras-chave: raiz racional; polinômios; números irracionais; irredutibilidade (matemática).

ABSTRACT

The Dumas Criterion is a method that makes it possible to verify the irreducibility of polynomials with integer coefficients through the analysis of their representations in diagrams. This study begins with an overview of numbers, covering from the classification of rational and irrational, to more special categories such as algebraic and transcendent numbers (only conceptual). Our aim of our study is to obtain - in a practical, comprehensive and efficient way - mechanisms that save us time when it is necessary to classify a certain number in the set of reais. It is in this context that we focus our study, associating a given real number to the root of a polynomial - from where we have the idea of irreducibility linked to the irrationality of a number - and from there we can break it down as a product of polynomials. Thus, we present the methods - Theorem of Rational Roots, Eisenstein's Criterion and Dumas's Criterion - commonly used to evaluate whether a given polynomial has rational roots or not.

Keywords: rational root; polynomials; irrational numbers; irreducibility (mathematics).

SUMÁRIO

1 INTRODUÇÃO 10

2 POLINÔMIOS: CONCEITOS BÁSICOS, DEFINIÇÕES E PROPRIEDADES 12

2.1 Algumas Definições e Teoria Básica em Polinômio 13

2.2 Propriedades dos Polinômios 17

2.2.1 *Polinômios Primitivos e Conteúdo de um Polinômio* 18

2.2.2 *Lema de Gauss* 18

2.3 Números reais: Algébricos e Transcendentes 19

2.4 Irredutibilidade de um Polinômio sobre $\mathbb{Q}[X]$ 20

***2.4.1 Irredutibilidade e o Teorema do Resto* 20**

***2.4.2 As Raízes de um Polinômio como critério de irredutibilidade* 24**

***2.4.3 Critério de Eisenstein para Irredutibilidade* 27**

***2.4.4 Os Polinômios Ciclotômicos* 33**

3 NÚMEROS REAIS: RACIONAIS E IRRACIONAIS; ALGÉBRICOS E TRANSCENDENTES 35

3.1 Os Números Racionais 36

3.2 Números Irracionais: identificação mediante raízes de polinômios 43

4 DIAGRAMA DE NEWTON E O CRITÉRIO DE DUMAS 55

4.1 Diagrama de Newton para Representação de Polinômio em $\mathbb{Z}[X]$ 55

4.2 Critério de Dumas para verificação de irredutibilidade de Polinômios 67

5 CONCLUSÃO 78

REFERÊNCIAS 80

APÊNCICE A - ANÉIS, DOMÍNIO DE INTEGRIDADE E CORPO 82

APÊNCICE B - EXTENSÕES DE CORPOS 89

1 INTRODUÇÃO

A ideia de números paira sobre as civilizações desde suas primeiras concepções de contagem e, quanto mais evoluímos, as necessidades, em consonância com os números, o fazem também. É daí que surgem conceitos e classificações numéricas, especificações que proporcionarão estudos posteriores mais detalhados e soluções de problemas mais específicos.

Inteirar-se das ideias da álgebra quanto às estruturas algébricas – anéis, corpos, extensões, grupos e outras – trará para outro patamar os números. Porém ainda nos deparamos com situações intrigantes simples de afirmarmos se tal número é racional ou irracional, se dado polinômio tem raízes racionais ou até mesmo se podemos escrever certo polinômio como produto de polinômios com coeficientes inteiros.

É em meio a esses questionamentos que apresentamos nosso trabalho, um estudo focado em mostrar que as raízes racionais de um polinômio e sua redutibilidade nos racionais estão intrinsicamente ligadas aos números irracionais. Para isso apresentaremos meios facilitadores de sondagem da existência de tais números raízes.

No Capítulo 2 mostraremos uma teoria básica dos polinômios – as operações e propriedades –, abordando alguns conceitos como polinômios primitivos e conteúdo de um polinômio, apresentando um resultado importante nesse sentido, o ***Lema de Gauss***, aproximando, assim, o leitor, por meio de uma abordagem específica e clara, de uma classificação diferente dos números reais em algébricos e transcendentes.

Em seção ainda nesse capítulo, traremos uma abordagem sobre critérios de divisibilidade de um polinômio, associando-os ao ***Teorema do Resto*** e a um estudo de estratégias que nos servem de suporte para uma sondagem rápida se um tal polinômio com coeficientes inteiros teria ou não raízes racionais e, por conseguinte, se o mesmo é ou não irredutível sobre os racionais.

Com essa finalidade, ainda nesse capítulo, trataremos do teorema das raízes racionais, um método indicador que consiste em, existindo uma raiz racional, obedecer determinada condição. Mas a morosidade desse método, embora direcionado e certeiro caso exista tal raiz, possibilitou-nos apresentar alguns outros critérios, que nos aliviará do sofrimento de avaliação se não encontrarmos uma raiz racional.

Assim, chegamos a um dispositivo prático que nos ajuda a remir tempo e esforço desnecessário na busca das raízes racionais de um polinômio. Nesse sentido, apresentaremos no Capítulo 2 o ***Critério de Eisenstein***, um método que exime a procura de raízes racionais de um polinômio por testagem, que, na prática, consiste em tomarmos um número primo *p* que satisfaz a hipótese (as condições de aplicabilidade do critério) e rapidamente veremos se dado polinômio com coeficientes inteiros possui ou não raízes racionais, e eventualmente podemos concluir se o mesmo é redutível ou não nos racionais. É preciso ressaltar, porém, que há limitações em tal critério, dentre as quais podemos citar os casos dos polinômios ciclotômicos.

Após esse estudo dos polinômios, adentraremos no capítulo seguinte abordando a classificação dos números reais em racionais e irracionais, trazendo exemplos curiosos de números sobre e formados por radicais e suas demonstrações de irracionalidades. Acompanhados de fatos históricos contundentes do surgimento dessa ideia, como: o primeiro número irracional a ser descoberto e como os gregos representavam tais números geometricamente.

Nesse âmbito, para evitarmos estudar caso a caso de irracionalidade, nos apropriaremos do nosso estudo dos polinômios obtidos por manipulações algébricas do problema gerador, onde assimilaremos a irracionalidade com a inexistência de raízes racionais do polinômio em questão, em outras palavras, a irredutibilidade do polinômio nos racionais. Contudo, observamos que ainda havia a necessidade, para pouparmos esforços, de um mecanismo mais prático e abrangente que o ***Critério de Eisenstein*** para avaliarmos as raízes racionais de tais polinômios obtidos durante esse processo, que não fosse a verificação, uma a uma, das supostas raízes racionais ou até mesmo a inexistência da mesma.

Para sanar o imbróglio, recorremos, no Capítulo 4 à ideia de Newton em representar um polinômio geometricamente e apresentamos o ***Critério de Dumas*** para a checagem rápida e abrangente da irredutibilidade nos racionais de polinômios com coeficientes racionais, o objetivo central de nosso estudo. Tais estudos, finalmente, mostraram-se suficientemente abrangentes para avaliar quaisquer polinômios com coeficientes racionais, quanto às suas raízes racionais, oportunizando uma estratégia que podemos aplicar na gama de polinômios que podem surgir nas manipulações algébricas ou que nos sejam apresentados.

2 POLINÔMIOS: CONCEITOS BÁSICOS, DEFINIÇÕES E PROPRIEDADES

O surgimento dos *polinômios* e a obtenção de suas raízes, está intrinsicamente atrelado à história da matemática. Apesar de sem tempo e local pré-definidos, notadamente percebemos isso quando lemos sobre a busca incansável dos primeiros métodos de resoluções de equações algébricas – quadráticas, cúbicas e quárticas, entre outras, ou podemos dizer, na busca das raízes de tais polinômios.

Neste capítulo apresentaremos uma teoria básica – propriedades e operações – e daremos algumas definições sobre em *polinômios*, que serão bastante úteis na compreensão dos assuntos abordados no capítulo quatro, tema central desse estudo.

Veremos aqui as definições de números reais algébricos e transcendentes, em que os números algébricos – especificamente para nós os números irracionais – estão intimamente conectados com polinômios irredutíveis em $\mathbb{Q}[X]$, a saber que, qualquer número algébrico é a raiz de um polinômio irredutível único (até um fator constante).

Contudo, a noção de um número algébrico vai bem mais além do que foi apresentado, uma vez que, no início do século passado, P. Ruffini (1765-1822) e NH Abel (1802-1829) provaram que existem equações de grau superiores a quatro que são não solucionáveis por meio de radicais. Podemos estender essa discussão também para os ***Polinômios Ciclotômicos*** (em seção mais adiante no capítulo), cujas raízes são simples e da unidade, o que estudaremos ainda nesse capítulo condições de irredutibilidade nesse modelo de polinômios. E ratificamos, nesse momento, que os números racionais e radicais irracionais não esgotam todos os números algébricos.

Será também pauta de nosso estudo nesse capítulo, a ideia de divisibilidade de polinômios, onde traremos o ***Algoritmo de divisão de Euclides*** para polinômios, em que focaremos no ***Teorema do Resto*** e no dispositivo prático de ***Briot-Ruffini***. Em seguida, faremos uma conexão entre raízes de um polinômio e irredutibilidade do mesmo, apresentando um dos resultados mais significativos sobre o tema, o ***Lema de Gauss***. Por conseguinte, abordaremos os radicais irracionais (onde todos são algébricos) e polinômios irredutíveis; e discutiremos o ***Critério de Eisenstein*** para a irredutibilidade de polinômios e o fato da existência de números irracionais como raízes.

2.1 Algumas Definições e Teoria Básica em Polinômio

Definição 2.1 – Definiremos *polinômio* sobre K na variável X, à expressão formal $p(X) = a_0 + a_1X + \cdots + a_nX^n + \cdots$, em que $a_i \in K$, $\forall i \in \mathrm{N} \cup \{0\}$ e, existe um número natural m, tal que, $a_j = 0$ para todo $j \geq m$.

Neste caso, K será um ***Anel*** ou um ***Corpo***[1].

Denominaremos os elementos $a_i \in K$ de *coeficientes* de $p(X)$. E podemos denotar $p(X)$, quando $a_j = 0$ para todo $j > n$, simplificadamente por

$$p(X) = \sum_{k=0}^{n} a_k X^k \qquad (1)$$

Exemplo 2.1 *– A expressão $p(X) = X^4 + 3X^3 - 4X + 15$ é um polinômio. Mas a expressão $q(X) = 10 + X + X^2 + 3X^3 + \cdots$ não é um polinômio, uma vez que seus coeficientes não são quase todos nulos.*

Se tivermos $a_i = 0$, $\forall i \in \mathrm{N} \cup \{0\}$, isto é, $p(X) = 0 + 0X + \cdots + 0X^n + \cdots$, então denotaremos $p(X)$ por 0, ou seja, $p(X) = 0$, e será denominado *polinômio nulo*. Agora se $p(X) = a_0 + 0X + \cdots + 0X^n + \cdots$, isto é, $a_j = 0$ para todo $j > 0$, teremos apenas $p(X) = a_0$ e o chamaremos por *polinômio constante.*

Denotamos por $K[X]$ o conjunto de todos os polinômios sobre K, isto é, todos os polinômios cujos os coeficientes pertencem a K, *em que K é qualquer um dos conjuntos* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$. Além disso, as inclusões $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, garantem as inclusões $\mathbb{Z}[X] \subset \mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X]$. Analisemos os dois próximos exemplos:

Exemplo 2.2 *– Dado o polinômio $p(X) = 3X^3 + \sqrt{5}\,X^2 - 4X + 1$, note que $p(X) \notin \mathbb{Q}[X]$, pois $\sqrt{5} \notin \mathbb{Q}$ e, consequentemente, $p(X) \notin \mathbb{Z}[X]$. Mas por outro lado, $p(X) \in \mathbb{R}[X]$, pois todos os seus coeficientes são números reais e, consequentemente, $p(X) \in \mathbb{C}[X]$.*

[1] As definições de **Anel** e de **Corpo** você encontra no **Apêndice A**

Exemplo 2.3 *– São polinômios em* $\mathbb{Z}[X]$: $p(X) = 5 - 2X + 5X^2 - X^3$ *e* $q(X) = X^2 + 2$. *São polinômios em* $\mathbb{R}[X]$: $p(X) = 5 - \frac{\sqrt{10}}{3}X + X^3$ *e* $q(X) = \sqrt{2}X^2 + 2$.

Definição 2.2 *– Para* $p(X) = \sum_{k=0}^{n} a_k X^k \in K[X] \setminus \{0\}$, com $a_n \neq 0$, *dizemos que* a_n *é o coeficiente líder de* $p(X)$ *e,* quando $a_n = 1$, *dizemos que o polinômio é mônico. E definimos o inteiro positivo n como o grau de* $p(X)$, *onde denotamos por* $gr(p(X)) = n$.

Exemplo 2.4 *– Assim, dado o polinômio* $q(X) = 10 + X + X^2 + 3X^3$, *temos que seu coeficiente líder é 3 e o* $gr(q(X)) = 3$.

Definição 2.3 *– Sejam os polinômios* $p(X) = \sum_{k\geq 0} a_k X^k$ *e* $q(X) = \sum_{j\geq 0} b_j X^j$ *com coeficientes num corpo K. Definimos a soma como* $p(X) + q(X) = \sum_{l\geq 0} c_l X^l$, *tal que* $c_l = a_l + b_l$. *E definimos o produto como* $p(X) \cdot q(X) = \sum_{l\geq 0} c_l X^l$, *onde* $c_l = \sum_{\substack{k+j=l \\ k,j\geq 0}} a_k b_j$.

Proposição 2.1 *– Seja um corpo K e dados os polinômios* $p(X), q(X) \in K[X] \setminus \{0\}$, *tais que* $gr(p(X)) = n$ *e* $gr(q(X)) = m$, *segue que:*

(a) $gr(p(X) + q(X)) \leq max\{ gr(p(X)), gr(q(X))\}$ *se* $p(X) + q(X) \neq 0$.

(b) $gr((pq)(X)) = gr(gr(p(X)) + gr(q(X)))$ *se* $p(X) \cdot q(X) \neq 0$.

Demonstração:

Sejam os polinômios $p(X) = \sum_{k=0}^{n} a_k X^k$ *e* $q(X) = \sum_{j=0}^{m} a_j X^j$, *tais que* $a_n\, b_m \neq 0$.

(a) Temos dois casos a analisar.

Primeiro para $m = n$, *temos que,* $p(X) + q(X) = (p+q)(X) = \sum_{i=0}^{n} (a_i + b_i) X^i$, *e daí temos duas situações a considerar. Se* $a_n + b_n \neq 0$, *então* $gr(p(X) + q(X)) = n = max\{gr(p(X)), gr(q(X))\}$. *Agora, se* $a_n + b_n = 0$, *segue que* $gr(p(X) + q(X)) < n = max\{ gr(p(X)), gr(q(X))\}$.

Por outro lado, se tivermos $m \neq n$, *onde podemos supor, sem perda de generalidade, que* $m > n$, *teremos que*

$$(p+q)(X)=\sum_{i=0}^{n}(a_i+b_i)X^i$$
$$=(a_0+b_0)+(a_1+b_1)X+\cdots+(a_n+b_n)X^n+(a_{n+1}+b_{n+1})X^{n+1}+\cdots+b_mX^m$$

e, assim gr(p(X) + q(X)) = m = max{ gr(p(X)), gr(q(X))}.

Com isso, mostramos que em qualquer um dos casos tem-se que

$$gr(p(X)+q(X))\leq max\{\ gr(p(X)),\ gr(q(X))\}.$$

(b) Sendo $p(X)\cdot q(X)=(pq)(X)=\sum_{l\geq 0}c_lX^l$, *onde* $c_l=\sum_{\substack{k+j=l\\k,j\geq 0}}a_kb_j$. *Como* $a_n\, b_m\neq 0$, *é imediato que* $c_{m+n}\neq 0$ *e, portanto,* $(pq)(X)\neq 0$ *e* $gr((pq)(X)) = gr(gr(p(X)) + gr(q(X)))$.

■

Teorema 2.1 (*Algoritmo da Divisão Euclidiana de polinômios*) – *Dado o corpo K e sejam os polinômios* $p(X),d(X)\in K[X]$, *com* $d(X)\neq 0$. *Então existem únicos* $q(X),r(X)\in K[X]$, *tais que:*

$$p(X)=q(X)d(X)+r(X)$$

em que $r(X)=0$ *ou* $gr(r(X))<gr(d(X))$.

Demonstração:

Vide [HEFEZ, Abramo e VILELA, Maria L. T., *pp. 92-93*].

Exemplo 2.5 – *Faremos a divisão euclidiana em* $\mathbb{Z}[X]$ *de*

$$p(X) = 4X^5+3X^4 - 8X^2 +10X - 6 \text{ por } d(X) = X^2 - 2X + 1.$$

Solução: *A solução apresentada é apenas a aplicação da demonstração do* ***Teorema 2.1***.

Inicialmente, temos que o monômio de maior grau de p(X) é $4X^5$ *e de d(X) é* X^2.

Daí, determinando q(X) tal que $p(X)=q(X)d(X)+r(X)$, *obtemos:*

$$p(X)=d(X)q(X)+r(X)=d(X)\times 4X^3+(11X^4-4X^3-8X^2+10X-6).$$

Efetuando agora a divisão de r(X) por d(X), onde também tomamos os respectivos monômios de maior grau, $11X^4$ *e* X^2, *onde teremos:*

$$r(X)=d(X)q_1(X)+r_1(X)=d(X)\times 11X^2+(18X^3-19X^2+10X-6).$$

Dando continuidade, pois o gr($r_1(X)$) ainda é maior que o gr(d(X)), e procedendo de maneira análoga aos processos anteriores, para divisão de $r_1(X)$ por d(X), obtemos:

$$r_1(X) = d(X)q_2(X) + r_2(X) = d(X) \times 18X + (17X^2 - 8X - 6).$$

Assim, efetuando agora a divisão de $r_2(X)$ por d(X), pois ainda temos gr($r_2(X)$) igual ao gr(d(X)), obteremos

$$r_2(X) = d(X)q_3(X) + r_3(X) = d(X) \times 17 + (26X - 23).$$

Note-se que, finalmente gr($r_3(X)$) < gr(d(X)), portanto, pela divisão euclidiana, segue que:

$$p(X) = (X^2 - 2X + 1) \times (4X^3 + 11X^2 + 18X + 17) + (26X - 23).$$

O processo acima explicitado pode ser apresentado pelo seguinte dispositivo prático, que também é uma reinterpretação ou uma releitura da demonstração do mesmo **Teorema 2.1**. Assim, segue:

$$\begin{array}{r|l}
4X^5 + 3X^4 - 8X^2 + 10X - 6X^2 - 2X + 1 & X^2 - 2X + 1 \\
\cline{2-2}
-4X^5 + 8X^4 - 4X^3 4X^3 + 11X^2 + 18X + 17 & 4X^3 + 11X^2 + 18X + 17 \\
\cline{1-1}
11X^4 - 4X^3 - 8X^2 + 10X - 6 & \\
-11X^4 + 22X^3 - 11X^2 & \\
\cline{1-1}
18X^3 - 19X^2 + 10X - 6 & \\
-18X^3 + 36X^2 - 18X & \\
\cline{1-1}
17X^2 - 8X - 6 & \\
-17X^2 + 34X - 17 & \\
\cline{1-1}
26X - 23 &
\end{array}$$

Portanto, temos que $p(X) = (X^2 - 2X + 1) \times (4X^3 + 11X^2 + 18X + 17) + (26X - 23)$.

Um ponto importante no estudo dos polinômios é o valor de um polinômio $p(X) = \sum_{k=0}^{n} a_k X^k \in K[X]$ para um número $c \in K$ (um ***Domínio de Integridade*** [2] ou um ***Corpo***), que é obtido quando substituímos *X* por *c* em *p(X)*, isto é, $p(c) = \sum_{k=0}^{n} a_k c^k$.

Agora, podemos fazer a seguinte afirmação: se para algum $c \in K$, $p(c) = 0$, diremos que $c \in K$ é raiz de $p(X)$. E mais, se para $c \notin K$, existir um polinômio $p(X) \in K[X]$, tal que o anule, isto é, $p(c) = 0$, então *c* é algébrico sobre *K*. Daí, concluímos que para dado um certo $c \notin \mathbb{Q}$, existir $p(X) \in \mathbb{Q}[X]$ tal que $p(c) = 0$, teremos que *c* é algébrico sobre $\mathbb{Q}$; e mais, que todo irracional é algébrico sobre $\mathbb{Q}$. (A definição de algébrico e transcendente apresentaremos na **Definição 2.5**.)

2.2 Propriedades dos Polinômios

De agora em diante, quando conveniente, a notação de *p(X)* será denotada algumas vezes como simplesmente *p*, isto é, na expressão $p(X) \in K[X]$ escreveremos apenas $p \in K[X]$, quando conveniente.

Apropriados das definições e teoria básica dos polinômios, dentre elas a soma e produto, é fácil ver que, dados os polinômios $f, g, h \in K[X]$, as operações de soma e produto satisfazem as seguintes propriedades:

a) Comutatividade:

Soma: $f + g = g + f$ Produto: $f \times g = g \times f$

b) Associatividade:

Soma: $(f + g) + h = f + (g + h)$ Produto: $(f \times g) \times h = f \times (g \times h)$

c) Distributividade:

$$f \times (g + h) = (f \times g) + (f \times h)$$

[2] A definição de ***Domínio de Integridade*** você encontra no **Apêndice A**

2.2.1 Polinômios Primitivos e Conteúdo de um Polinômio

Introduziremos uma definição importante para polinômios em $\mathbb{Z}[X]$, haja vista a necessidade para o desenvolvimento e entendimento daqui em diante do que iremos abordar.

Definição 2.4 – *Seja* $p(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}(X)$ *um polinômio não nulo. Definimos por conteúdo de p(X) como o máximo divisor comum (mdc) de seus coeficientes e denotaremos por cont(p(X)). E, quando mdc(*a_0*,* $a_{1, \ldots,}$ a_n*) = 1, denominaremos tal polinômio por polinômio primitivo.*

Diante disso, sendo $p(X) \in \mathbb{Z}[X]$ e *cont(p(X)) = k*, segue que $p(X) = kp_1(X)$, em que $p_1(X)$ é um polinômio primitivo. Vejamos uma importante proposição dos polinômios primitivos.

2.2.2 Lema de Gauss

Proposição 2.2 (Lema de Gauss) *– Sejam p(X), q(X)* $\in \mathbb{Z}[X]$*, polinômios primitivos, então o produto p(X)q(X) também será um polinômio primitivo.*

Demonstração:

Vide [HEFEZ, Abramo e VILELA, Maria L. T., *p. 129*].

Exemplo 2.6 *– Dados os polinômios* $p(X) = 2X^2 - 3X + 4$ *e* $q(X) = 5X^3 + 2X^2 + 3X - 6$*. Temos que mdc(2,-3,4) = 1, logo cont(p(X)) = 1 e p(X) é um polinômio primitivo e, mdc (5,2,3,-6) = 1 e q(X) também é um polinômio primitivo. Então,*

$$\begin{aligned} p(X)q(X) &= (2X^2 - 3X + 4)(5X^3 + 2X^2 + 3X - 6) \\ &= 10X^5 - 11X^4 + 20X^3 - 13X^2 + 30X - 24 \end{aligned}$$

Note-se que mdc (10,-11,20,-13,30,-24) = 1, e daí cont(p(X)q(X)) = 1 e, portanto, p(X)q(X) é um polinômio primitivo.

2.3 Números Algébricos e Transcendentes

Para avaliarmos a classificação dos números reais em Algébricos e Transcendentes, é necessário fazermos algumas considerações. A primeira delas é sobre *extensões de corpos*[3] e, por conseguinte, faremos a seguinte definição:

Definição 2.5 – *Dada uma extensão de corpos* $\mathbb{L} \mid \mathbb{K}$*. Então, se para algum* $\alpha \in \mathbb{L}$*, existir um polinômio não nulo* $p(x) \in K[x]$*, tal que* $p(\alpha) = 0$*, então definimos* α *como algébrico sobre* $\mathbb{K}$*. Do contrário,* α *será definido como transcendente.*

Assim, dado um polinômio não-nulo, $p(X) = a_n X^n + \cdots + a_1 X + a_0$, com coeficientes racionais, por exemplo, se houver um número real irracional que o anule, isto é, é raiz do polinômio, dizemos que tal número real é um *número algébrico*. E se, um número real irracional não satisfizer nenhum polinômio com essas características, dizemos que ele é um *número transcendente*.

Exemplo 2.7 – *O número* $\sqrt{7} \in \mathrm{Q}[\sqrt{7}]$[4] *é algébrico sobre* $\mathbb{Q}$*, visto que é raiz do polinômio* $p(X) = X^2 - 7 \in \mathbb{Q}[X]$*. E que,* $\sqrt[3]{1+\sqrt{5}} \in \mathbb{Q}\left[\sqrt[3]{1+\sqrt{5}}\right]$*, é algébrico sobre* $\mathbb{Q}$*, visto que é raiz do polinômio* $q(X) = X^6 - 2X^3 - 4 \in \mathbb{Q}[X]$*. Já os números* $5^{\sqrt{3}}$*,* $\log 5$ *e* $\frac{\pi}{3}$ *são números transcendentes, pois não são soluções de nenhuma equação com coeficientes racionais.*

Exemplo 2.8 – *Uma das raízes do polinômio* $p(X) = X^3 + 9X - 4$ *é o número irracional* $\sqrt[3]{3} - \sqrt[3]{9}$*, logo ele é um número algébrico sobre* $\mathbb{Q}$*, pois trata-se de um número irracional.*

Vale ressaltar nessa discussão que um número que é *algébrico* sobre determinado corpo nem sempre o será em relação a outro corpo. Vejamos mais um caso:

---

[3] Consultar **Apêndice B**

[4] $\mathbb{Q}[\sqrt{7}]$ é uma extensão do corpo dos racionais, isto é, uma adjunção dos racionais com a $\sqrt{7}$. Consultar **Apêndice B.**

Exemplo 2.9 *– Temos que as das raízes do polinômio* $f(x) = x^2 + x + 1$ *são* $\frac{-1+\sqrt{3}i}{2}$ *e* $\frac{-1-\sqrt{3}i}{2}$*, isto é, não são algébricos sobre* $\mathbb{Q}(\sqrt{3})$*, mas são sobre* $\mathbb{Q}(\sqrt{3})(i)$.

São números *transcendentes* $5^{\sqrt{7}}$, π, $e^{i\pi}$, log23, dentre outros. Mas nosso objetivo é avaliar as raízes as raízes de polinômios, ou seja, os números *algébricos*, mais precisamente sobre a irracionalidade dos números e a irredutibilidade dos polinômios.

2.4 Irredutibilidade de um Polinômio sobre $\mathbb{Q}[X]$

Fazendo um *feedback* do que abordamos até aqui, falamos de uma correlação entre os polinômios (semelhantemente a solucionar equações polinomiais) – suas raízes, os números algébricos e a irredutibilidade sobre os racionais. Apropriamo-nos de uma teoria elementar sobre os polinômios, fornecendo-nos meios necessários para desenvolvermos essa seção, em que trataremos teoremas mais específicos sobre a possibilidade de decomposição de um polinômio, que nos ajudarão a compreender melhor a ideia de irredutibilidade dos polinômios com coeficientes racionais e suas conexões com os números irracionais (*a posteriori*), que é o objetivo principal de nossa pesquisa. Apresentaremos os mecanismos – técnicas de verificações rápidas – para previamente detectarmos se um polinômio é redutível ou não sobre os racionais.

2.4.1 Irredutibilidade e o Teorema do Resto

Pelo **Teorema 2.1**, se dados dois polinômios não nulos $p(X)$ e $d(X)$ em $K[X]$, dizemos que $p(X)$ é divisível por $d(X)$ quando o resto $r(X)$ da divisão euclidiana do polinômio $p(X)$ por outro polinômio $d(X)$ for zero. Significando que podemos expressar $p(X)$ como sendo o resultado do produto dos polinômios $d(X)$ por $q(X)$, em que $q(X)$ também é um polinômio em $K[X]$. Ou seja, se tal decomposição é possível, afirmamos que o *polinômio é redutível*.

Por outro lado, se dado um polinômio

$$p(X) = a_0 + a_1X + \cdots + a_nX^n,$$

com $gr(p(X)) = n$ e $p(X) \in K[X]$, se não pudermos representa-lo como um produto de dois polinômios não constantes com coeficientes em $K[X]$, o denominamos de *polinômio irredutível*. Agora, salientamos que nosso estudo será direcionado de agora em diante à polinômios $p(X) \in \mathbb{Q}[X]$.

Exemplo 2.10 *- O polinômio* $p(X) = 1 + X + X^2 + X^3 + X^4 + X^5$ *é redutível em* $\mathbb{Q}[X]$*, pois podemos escrevê-lo como*

$$p(X) = 1 + X + X^2 + X^3 + X^4 + X^5 = (1 + X)(1 + X^2 + X^4).$$

Enquanto o polinômio $q(X) = (1 + X^2 + X^4)$ *é um polinômio irredutível em* $\mathbb{R}[X]$*, isto pelo fato de não podermos representá-lo como produto de polinômios com coeficientes reais. Segue também, que o mesmo é redutível em* $\mathbb{C}[X]$*, pois podemos expressá-lo como* $(1 + X^2 + X^4) = \left(X - \sqrt{\frac{-1+i\sqrt{3}}{2}}\right)\left(X + \sqrt{\frac{-1-i\sqrt{3}}{2}}\right)$*, que é um produto de polinômios com coeficientes complexos.*

Os casos mais simples de irredutibilidade de polinômio em $\mathbb{R}[X]$ são o polinômio expresso como um binômio "$a_0 + a_1X$" – esse caso inclui também até o domínio de integridade $\mathbb{Z}[X]$ – e o polinômio expresso como um trinômio "$a_0 + a_1X + a_2X^2$", quando o discriminante é negativo, o que pode ser visto claramente no ***Exemplo 2.10*** para o polinômio $(1 + X^2 + X^4)$, que chamamos de polinômio biquadrado.

Veremos a seguir alguns teoremas importantes que tratam sobre resto da divisão entre polinômios, tais que nos auxiliará na associação direta na investigação da redutibilidade para certos polinômios.

Teorema 2.2 (*Teorema do Resto*) – *Sejam* $a \in \mathbb{R}$ *e p(X) um polinômio em* $\mathbb{R}[X]$*. O resto da divisão de p(X) por (X – a) é p(a).*

Demonstração:

Vide [NETO, Aref A.; SAMPAIO, José L. P.; LAPA, Nilton; CAVALLANTTE, Sidney L., *p. 129*]

Pelo ***Teorema 2.2***, no caso em que *a* é uma raiz de *p*(*X*), ou seja, *p(a) = r(X) = 0,* portanto, *(X – a)* divide o polinômio *p*(*X*), logo temos:

$$p(X) = (X - a)q(X),$$

em que q(*X*) é o quociente dessa divisão, mostrando que *p*(*X*) é redutível.

Para dar praticidade na determinação do resto, no ***Teorema do Resto***, há um dispositivo, conhecido como ***Dispositivo de Briot-Ruffini***[5], que nos permite trabalhar apenas com os coeficientes de $p(X)$ e com $a \in \mathbb{R}$, em que ao final do processo obtemos o resto da divisão de $p(X)$ *por* $(X - a)$, podendo ser um número real não nulo ou zero, isto é, uma raiz de $p(X)$. No nosso caso específico, para exemplificar, vamos considerar como uma raiz.

Vejamos como funciona: sejam $p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ e c uma de suas raízes, daí dispomos os coeficientes de $p(X)$ e sua raiz c, da seguinte forma

ca_n	a_{n-1}	a_{n-2}	$\cdots$	a_1	a_0
a_n	$ca_n + a_{n-1}$	$ct_{n-2} + a_{n-2}$	$\cdots$	$ct_1 + a_1$	$ct_0 + a_0$
	$\uparrow$	$\uparrow$	$\cdots$	$\uparrow$	$\uparrow$
	t_{n-2}	t_{n-3}	$\cdots$	t_0	r

Onde: para o valor de t_{n-2}tomamos o produto do coeficiente líder pela raiz e somamos com o coeficiente de X^{n-1}; para o valor de t_{n-3}tomamos o produto de t_{n-2} pela raiz, somamos com o coeficiente de X^{n-2}; e assim por diante, até obtermos o resultado $ct_0 + a_0$, que representa o resta da divisão de $p(X)$ por $(X - c)$. Como c é raiz de $p(X)$, segue que $ct_0 + a_0 = 0$ e, consequentemente, temos que $p(X)$ é redutível e podemos escrevê-lo como

$$p(X) = (X - c)\, q(X).$$

Na divisão de polinômios, no que diz respeito à determinação do quociente e do resto dessa divisão, faz-se necessária uma prévia da forma (grau) dos polinômios, que poderão ser o quociente e o resto. Essa sondagem nos permitirá deduzir em meio a um problema quais os graus dos polinômios que estamos à procura.

Um método de grande importância é o de coeficientes a determinar, também conhecido nos livros didáticos por ***"Método de Descartes"***, que nos permite deduzir os graus dos polinômios em uma certa operação, como na divisão, por exemplo.

O ***Método de Descartes***[6] afirma que, na divisão do polinômio $p(X)$ por $d(X)$ (suponhamos que $gr(p(X)) \geq gr(d(X))$), o quociente $q(X)$ e o resto $r(X)$, na identidade

[5] Também conhecido na literatura como ***Algoritmo de Horner-Rufinni***. *Vide* [CAMINHA, A. **Tópicos de Matemática Elementar**, Volume 6: Polinômios, *pp*. 45-47]

[6] É um dispositivo prática que permite a dedução dos graus dos polinômios.

$$p(X) = p(X)\, q(X) + r(X)$$

nos fornece que: $gr(p(X)) = gr(d(X)q(X) + r(X))$. E como $gr(r(X)) \leq gr(d(X))$, ou ainda *r(X) = 0*, podemos escrever que

$$gr(p(X)) = gr(d(X)) + gr(q(X)).$$

Seria extremamente enfadonho o processo de divisão habitual para alguns polinômios, sendo de suma importância a observação dado por ***Descartes*** em relação ao grau de polinômios numa divisão euclidiana.

Exemplo 2.11 – *Qual o resto da divisão do polinômio* $p(X) = X^{50} + X - 1$ *por* $s(X) = X^2 - 1$*?*

Solução**:** *Inicialmente, note que* $s(X) = X^2 - 1 = (X + 1)(X - 1)$.

Os valores de p(X) para X = - 1 e X = 1 são:

$$p(-1) = (-1)^{50} + (-1) - 1 = -1 \text{ e } p(1) = 1^{50} + 1 - 1 = 1$$

Segue do ***Teorema 2.1****, que*

$$p(X) = s(X)q(X) + r(X) = (X^2 - 1)q(X) + r(X) = (X + 1)(X - 1)q(X) + r(X)$$

Agora, como gr(s(X)) = 2, logo gr(r(X)) ≤ 1, ou seja, r(X) = aX + b ou r(X) = c. E pelo ***Teorema do Resto****, temos:*

(i) $p(-1) = ((-1)^2 - 1)q(-1) + r(-1) = -a + b \quad \Rightarrow \quad -a + b = -1$

(ii) $p(1) = (1^2 - 1)q(1) + r(1) = a + b \quad \Rightarrow \quad a + b = 1$

Daí, por (i) e (ii) formamos o sistema: $\begin{cases} -a + b = -1 \\ a + b = 1 \end{cases}$*, onde teremos b = 0 e a = 1.*

Portanto, o resto da divisão de p(X) por s(X) é r(X) = X.

Pelo exemplo logo acima, dentro do contexto em estudo, percebemos que o polinômio $p(X) = X^{50} + X - 1$ é irredutível sobre $\mathbb{R}$ – cuja uma justificativa mais imediata será apresentada mais adiante – e sua decomposição é dada por:

$$p(X) = X^{50} + X - 1 = (X^2 - 1)q(X) + X.$$

2.4.2 As raízes de um polinômio como um critério de irredutibilidade em Q[X]

Até o momento expomos ideias sobre a irredutibilidade de polinômios em determinadas situações-problemas. Nessa seção, apresentaremos alguns teoremas que tratam sobre a irredutibilidade pelo fato do polinômio $p(X) \in K[X]$, com $gr(p(X)) \geq 2$ não possuir raízes em K, fato esse já mencionamos em alguns momentos nesse capítulo.

A *priori*, salientamos que o fato de um polinômio não possuir raízes racionais, não implica necessariamente que o mesmo seja irredutível sobre os racionais. Como podemos observar no exemplo a seguir:

Exemplo 2.12 *– O polinômio* $p(X) = X^4 + 64$*, pode ser escrito como*

$$p(X) = X^4 + 64$$
$$= X^4 + 64 + 16X^2 - 16X^2$$
$$= [X^4 + 16X^2 + 64] - 16X^2$$
$$= (X^2 + 8)^2 - (4X)^2$$
$$= (X^2 + 4X + 8)(X^2 - 4X + 8).$$

Portanto, $p(X) = X^4 + 64$ *é um polinômio redutível, embora nenhuma de suas quatro raízes não sejam nem reais (racionais).*

O teorema a seguir está relacionado ao famoso matemático alemão Carl Friedrich Gauss (1777-1855).

Teorema 2.3 *– Se um número* α *é simultaneamente a raiz de dois polinômios* $p(X)$ *e* $q(X)$*, um dos quais, digamos* $q(X)$*, é irredutível, então, para um inteiro apropriado* $d \neq 0$*, o polinômio* $dp(X)$ *é divisível por* $q(X)$*:*

$$dp(X) = l(X)\, q(X).$$

Demonstração:

Sejam $p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ *e* $q(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0$ *e, suponhamos sem perda de generalidade* $n > m$

Pelo ***Teorema 2.1****, efetuando a divisão de* $p(X)$ *por* $q(X)$*, obtemos*

$$p(X) = l_1(X)q(X) + r_1(X)$$

onde, $l_1(X) = \frac{a_n}{b_m}X^{n-m} + \cdots$ *e* $r_1(X) = r_{m-1}X^{m-1} + \cdots$ *são polinômios em X e com coeficientes racionais.*

Se $r_1(X) = 0$*, teremos que p(X) é divisível por q(X), e não precisamos provar mais nada, pois*

$$p(X) = l_1(X)q(X) = \frac{1}{d}l(X)q(X)$$

em que d é o denominador comum dos coeficientes de l(X).

Agora, suponha que $r_1(X) \neq 0$*. Como gr(r(X)) < gr(q(X)) e o número α está entre suas raízes, porque*

$$r_1(\alpha) = p(\alpha) - l_1(\alpha)q(\alpha) = 0.$$

E dividindo q(X) por $r_1(X)$*, no resto obteremos um novo polinômio* $r_2(X)$ *com propriedades semelhantes. Com gr(*$r_2(X)$*) < gr(*$r_1(X)$*) e, portanto, também menor que o grau de q(X).*

Iterando, até um número k limite de procedimentos, chegaremos a uma contradição,

$$r_k(X) = c \neq 0,$$

ou seja, α não será uma raiz de $r_k(X)$ *ou não teremos que q(X) é divisível por* $r_k(X)$*, isto é,* $q(X) = l_k(X)\ r_k(X)$*. Daí, podemos extrair os múltiplos comuns de numeradores e denominadores de todos os coeficientes racionais e reescrever a última equação como*

$$q(X) = \frac{a}{b}l(X)\ r(X),$$

em que $\frac{a}{b}$ *é uma fração irredutível e* $l(X)$ *e* $r(X)$ *são polinômios primitivos (ver* ***Definição 2.3****).*

Assim, resta-nos mostrar que o coeficiente $\frac{a}{b}$ *é um número inteiro, ou seja, que b = ±1. Suponha-se, por contradição, que b tenha um divisor p primo, logo na equação*

$$b\ q(X) = a\ l(X)\ r(X)$$

implica que todos os coeficientes do lado direito são divisíveis por p, pois o número a não pode ser divisível por p, pois, caso contrário, a fração $\frac{a}{b}$ *não seria irredutível.*

Portanto, todos os coeficientes do polinômio $l(X)r(X)$ *são divisíveis por p, o que é impossível pela* ***Proposição 2.2 (Lema de Gauss)****. Com isso, concluímos que o polinômio*

$$q(X) = [\pm a\ l(X)]\ r(X),$$

é redutível, o que contradiz as suposições do Teorema e, portanto, completa a prova.

■

Tomemos os exemplos a seguir, uma aplicação do teorema ora visto.

Exemplo 2.13 *– Dados os polinômios* $p(X) = X^4 + X^3 - 3X^2 - 5X - 2$ *e* $q(X) = \frac{1}{2}X - 1$ *em* $\mathbb{R}[X]$*. Notemos que* $p(2) = q(2) = 0$*, logo X = 2 é raiz de ambos os polinômios e, além disso, q(X) é irredutível pois trata-se de um binômio da forma* $a_0 + a_1X$*.*

Pela Divisão Euclidiana de p(X) por q(X), segue que

$$p(X) = (2X^3 - 2X^2 + 10X + 10)\ q(X) + 8,$$

isto é, q(*X*) *não divide p*(*X*).

No entanto, tomando 2p(X), obteremos

$$2p(X) = (4X^3 + 12X^2 + 12X + 4)\ q(X).$$

Portanto, segue que, $2p(X)$ *é divisível por q*(*X*).

O teorema logo acima demonstrado está relacionado ao nome do famoso matemático alemão Carl Friedrich Gauss (1777-1855).

Como um polinômio de grau n ≥ 2 não pode dividir um binômio linear, a propriedade de que um polinômio irredutível de grau n ≥ 2 não pode ter um número racional entre suas raízes é uma consequência desse teorema.

Assim, obtemos uma ferramenta conveniente para encontrar novos números irracionais. Tudo o que precisamos fazer é procurar as raízes dos polinômios irredutíveis.

Há um teorema importante que trata das raízes de um polinômio, se esse possui ou não raízes racionais e apresentaremos ele a seguir.

Teorema 2.4 (Teorema das Raízes Racionais) – *Considere* $p(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in Z[X] \backslash Z$. *E considere* $\frac{p}{q} \in \mathbb{Q}$,*tal que p,q* $\in \mathbb{Z} \backslash \{0\}$ *e mdc(p,q) = 1, uma raiz de p(X). Então,* $p \mid a_0$ *e* $q \mid a_n$.

Demonstração:

Vide [NETO, Aref A.; SAMPAIO, José L. P.; LAPA, Nilton; CAVALLANTTE, Sidney L., *pp. 243-244*].

Vale ressaltar que o ***Teorema 2.4*** não garante a existência de uma raiz racional, mas apenas afirma que na existência de uma raiz racional $\frac{p}{q}$, teremos que $p \mid a_0$ *e* $q \mid a_n$, em que *p,q* $\in \mathbb{Z} \backslash \{0\}$ e *mdc(p,q) = 1.*

2.4.3 Critério de Eisenstein para Irredutibilidade de Polinômio em Q[*X*]

Diante do que foi visto, uma porta para o mundo enigmático de polinômios irredutíveis foi aberta. E a seguinte proposição do matemático alemão F.G.M. Eisenstein (1823 – 1852), nos coloca em posição confortável para investigação da existência de raízes racionais de um polinômio. Relatamos ainda sobre a produtividade de Eisenstein, que diante da indiferença de seus contemporâneos, suas ideias não foram apreendidas até muitos anos depois.

Proposição 2.3 (**Critério De Eisenstein)** – *Suponha-se que, para um dado polinômio p(X) em* $\mathbb{Z}[X]$*, seja possível encontrar um número primo p, de modo que o coeficiente líder* a_n *não seja divisível por p, todos os coeficientes restantes* a_k*, k = 0, 1, ..., n-1, são divisíveis por p, enquanto o termo constante* a_0*, sendo divisível por p, não é divisível por* p^2*. Então o polinômio p*(*X*) *é irredutível em* $\mathbb{Q}[X]$.

Demonstração:

Suponhamos que, contrariamente à afirmação do critério de Eisenstein, os coeficientes do polinômio p(*X*) *satisfaçam todas as condições estabelecidas e, no entanto, o polinômio seja redutível, ou seja, podemos escrevê-lo como*

$$p(X) = d(X)\, q(X),$$

onde, $d(X) = b_l X^l + b_{l-1} X^{l-1} + \cdots + b_0$ *e* $p(X) = c_m X^m + c_{m-1} X^{m-1} + \cdots + c_0$, *também são polinômios com coeficientes inteiros com os respectivos coeficientes líderes* b_l *e* c_m *são não nulos. Além disso, pela* ***Proposição 2.1***

$$gr(p(X)) = gr(d(X)) + gr(q(X)).$$

Daí, assumindo sem perda de generalidade, por definição, $m \geq l \geq 1$. *E, coletando os coeficientes de potências iguais de X no produto* $d(X)q(X)$ *e equiparando-os aos coeficientes correspondentes de p(X), obtemos*

$$\begin{aligned}
a_0 &= b_0 c_0 \\
a_1 &= b_0 c_1 + b_1 c_0 \\
a_2 &= b_0 c_2 + b_1 c_1 + b_2 c_0 \\
&\vdots \\
a_l &= b_0 c_l + b_1 c_{l-1} + \cdots + b_l c_0 \\
&\vdots \\
a_m &= b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0 \\
&\vdots \\
a_n &= b_l c_m
\end{aligned}$$

Na primeira dessas equações, o termo constante a_0 *é divisível por p, de onde* b_0 *ou* c_0 *é divisível por p. No entanto, p não pode dividir esses dois números, pois seu produto* $b_0 c_0$ *não é divisível por* p^2, *o que contraria a hipótese.*

Suponha agora que p divide b_0 *e não divide* c_0. *Passando para a segunda equação, observamos que* a_1 *é divisível por p e* $b_0 c_1$ *é divisível por p. Portanto,* $b_1 c_0$ *é divisível por p e, portanto,* b_1 *é divisível por p.*

Desta forma, prosseguimos até a $(l + 1)^o$ *equação (coeficientes de* X^l*), o que implica que* a_l *é divisível por p e todos os coeficientes* $b_0, b_1, \ldots, b_{l-1}$ *são divisíveis por p. Portanto,* $b_l c_0$ *é divisível por p e, portanto,* b_l *é divisível por p.*

Agora pulem-se as linhas e seja vista a última equação. Implica que $a_n = b_l c_m$ *é divisível por p, o que contradiz a suposição.*

Se na primeira equação c_0 é divisível por p, enquanto b_0 não é, podemos repetir toda a linha de raciocínio até a equação m+1 (coeficientes de x^m) e pular para a última equação, obtendo o mesmo resultado.

Portanto, a decomposição p(X) = d(X)q(X) é impossível e, concluímos com isso que o polinômio p(X) é irredutível.

■

Exemplo 2.14 *– Para o polinômio* $p(X) = X^4 + 10X^3 + 20X^2 + 30X + 22$*, pelo* ***Critério de Eisenstein****, temos que para o primo p = 2, segue que 2 divide todos os coeficientes de p(X), exceto o coeficiente líder, além disso $p^2 = 4$ não divide termo independente, portanto p(X) é irredutível sobre* $\mathbb{Q}[X]$.

Tal ferramenta disponibilizada por *Eisenstein* nos permite catalogar inúmeros polinômios irredutíveis sobre $\mathbb{Q}[X]$. A partir daí, podemos afirmar, por exemplo, que o polinômio dado por $X^2 - 2$ é irredutível pelo critério de Eisenstein (considere o primo $p = 2$). Daí podemos obter novos números irracionais $\sqrt[n]{p}$, onde *p* é um número primo e *n = 2, 3, 4, ...* Isto é, para todo número *p*, $\sqrt[n]{p}$ é raiz do polinômio

$$X^n - p = 0,$$

que é irredutível sobre $\mathbb{Q}[X]$ de acordo com o ***Critério de Eisenstein***.

De modo mais abrangente, temos que o número

$$\sqrt[n]{p_1 p_2 \cdots p_k}$$

é irracional sempre que $p_1, p_2, ..., p_k$ são números primos distintos. Esse número é a raiz do polinômio irredutível

$$x^n - p_1 p_2 \cdots p_k = 0,$$

também de acordo com o mesmo critério.

Exemplo 2.15 *– Temos que* $\sqrt{4 + \sqrt[3]{6}}$ *é raiz do polinômio* $p(X) = X^6 - 12X^4 + 48X^2 - 70$*, que pelo* ***Critério de Eisenstein*** *é irredutível sobre Q[X], onde para verificar isso, basta tomarmos o primo p = 2.*

Exemplo 2.16 *– Verifique se o número* $\sqrt{1 + \sqrt[3]{2 - \sqrt{10}}}$ *é irracional.*

Solução: *Temos duas formas de verificarmos se tal número é irracional. Uma delas seria mostrarmos que o mesmo não é racional, usando a definição de número racionai, assunto apresentado apenas no capítulo seguinte. Então vamos à outra maneira, seria aplicando o* ***Critério de Eisenstein****. Nesse segundo caso, fazemos*

$$\sqrt{1+\sqrt[3]{2-\sqrt{6}}} = X.$$

Elevando ao quadrado ambos os lados da igualdade, isto é,

$$\left(\sqrt{1+\sqrt[3]{2-\sqrt{6}}}\right)^2 = X^2$$

e, realizando algumas operações, obtemos

$$\sqrt[3]{2-\sqrt{6}} = X^2 - 1$$

Agora, vamos elevar ao cubo, ou seja,

$$\left(\sqrt[3]{2-\sqrt{6}}\right)^3 = (X^2-1)^3$$

onde chegamos a

$$-\sqrt{6} = X^6 - 3X^4 + 3X^2 - 3$$

E, novamente elevando ao quadrado

$$\left(-\sqrt{6}\right)^2 = (X^6 - 3X^4 + 3X^2 - 3)^2$$

e teremos

$$X^{12} - 6X^{10} + 15X^8 - 24X^6 + 27X^4 - 18X^2 + 3 = 0$$

Portanto, teríamos que $X = \sqrt{1+\sqrt[3]{2-\sqrt{6}}}$ *seria uma raiz do polinômio dado por* $p(X) = X^{12} - 6X^{10} + 15X^8 - 24X^6 + 27X^4 - 18X^2 + 3$, *e utilizando o* ***critério de Eisenstein*** *tomamos o primo 3 e verificamos a irredutibilidade de tal polinômio em* $\mathbb{Q}[X]$, *ou seja, tal polinômio não tem raiz em* $\mathbb{Q}[X]$, *o que implica em* $\sqrt{1+\sqrt[3]{2-\sqrt{6}}}$ *ser irracional.*

Outras irracionalidades das formas citadas acima incluem também

$$\sqrt[l]{a+\sqrt[m]{b+\cdots+\sqrt[n]{p_1p_2\cdots p_k}}}, \qquad (1)$$

em que p_i são números primos distintos para todo i = 1, 2, ..., k. Originando, por meio de manipulações algébricas adequadas, polinômios irredutíveis sobre os racionais.

Embora os exemplos consignados até agora deem uma ideia de como o ***critério de Eisenstein*** funciona, temos na verdade, que o mesmo não vai muito além das realizações dos antigos gregos. Assim, a irracionalidade da última expressão em (1) pode ser facilmente comprovada aumentando-a sucessivamente às potências *l*, *m*,... e *n*, e aplicando o mesmo raciocínio usado para provar a irracionalidade de 2 ou construindo polinômios e mostrando que eles satisfazem ao ***Critério de Eisenstein***.

Um resultado mais substancial pode ser obtido considerando a soma

$$\frac{a_1}{b_1}\sqrt[n_1]{p^{m_1}}+\frac{a_2}{b_2}\sqrt[n_2]{p^{m2}}+\cdots+\frac{a_k}{b_k}\sqrt[n_k]{p^{m_k}}. (2)$$

Se os números $\frac{m_1}{n_1}, \frac{m_2}{n_2}, \cdots, \frac{m_k}{n_k}$são frações apropriadas distintas, então a soma (2) representa um número irracional. De fato, suponha o contrário, que a soma (2) seja um número racional $\frac{x}{y}$, isto é,

$$\frac{a_1}{b_1}\sqrt[n_1]{p^{m_1}}+\frac{a_2}{b_2}\sqrt[n_2]{p^{m2}}+\cdots+\frac{a_k}{b_k}\sqrt[n_k]{p^{m_k}}=\frac{x}{y}.$$

E considere $n = n_1n_2\cdots n_k$e $b = b_1b_2\cdots b_k$. Então, o número $\sqrt[n]{p}$ é raiz do seguinte polinômio:

$$P(X)=\frac{a_1}{b_1}bX^{\frac{m_1}{n_1}n}+\frac{a_2}{b_2}bX^{\frac{m_2}{n_2}n}+\cdots+\frac{a_k}{b_k}bX^{\frac{m_k}{n_k}n}-\frac{x}{y}b$$

O grau desse polinômio é menor ou igual a *n*. No entanto, devido ao **Teorema 2.3**, ele deve ser divisível pelo polinômio irredutível $X^n - p$ que tem grau *n*, o que é, obviamente, impossível.

Poderíamos continuar assim, inventando novas irracionalidades, combinando os exemplos e casos aqui expostos. Mas o excesso de confiança no sucesso até aqui obtido nos dá inspiração e cria ilusões, pois podemos imaginar que acumular radicais e aplicar as quatro operações aritméticas aos números inteiros *a*, *b*, ... em (1) sempre resultará em números

irracionais novos e facilmente obtidos. No entanto, um bom remédio contra a ilusão na matemática é estudar "casos particulares". Um caso especial do problema em estudo é o problema da irracionalidade do radical $\sqrt[n]{a^n + b^n}$ para arbitrários *a, b, n*, onde $n \geq 3$, que é equivalente ao último teorema de Fermat.

Não temos dúvidas da grande serventia do ***Critério de Eisenstein*** sobre irredutibilidade de polinômios no corpo dos racionais e a identificação de números irracionais, mas tal critério não nos permite catalogar uma gama de polinômios irredutíveis com coeficientes inteiros, pois existem infinitos polinômios irredutíveis, como:

$$X^2 + 1, \quad X^4 + 1, \quad X^6 + X^3 + 1, \quad (3)$$

cujos coeficientes não possuem um tal número primo divisor comum, conforme enuncia o critério.

Nesses casos (3), usamos um artifício o qual denominamos de ***mudança de variável aditiva***, que é um procedimento de encontrar um polinômio cujas raízes sejam as do polinômio original somadas (ou subtraídas) de uma quantidade inteira *h*.

Ou seja, dado o polinômio $p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, e seja $\alpha \in \mathbb{R}$ uma raiz de $p(X)$, isto é,

$$p(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0.$$

E, a partir deste, encontramos o polinômio $q(X) = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0$, com $\beta \in \mathbb{R}$ uma raiz de $q(X)$, isto é,

$$q(\beta) = b_n \beta^n + b_{n-1} \beta^{n-1} + \cdots + b_1 \beta + b_0 = 0,$$

de tal forma que $\beta = \alpha + h$ ou $\beta = \alpha - h$. Assim, segue que,

$$q(\beta) = b_n (\alpha + h)^n + b_{n-1} (\alpha + h)^{n-1} + \cdots + b_1 (\alpha + h) + b_0 = 0.$$

Assim, se o polinômio $q(X)$ é irredutível, segue que o polinômio $p(X)$ também é. Vejamos como essa ideia de mudança de variável funciona.

Exemplo 2.17 *– O polinômio* $p(X) = X^4 + 1$ *é irredutível e sua comprovação pode ser reduzida ao que foi argumentado logo acima. Para isso façamos p(X+1), onde obteremos:*

$$p(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2,$$

que é irredutível pelo ***critério de Eisenstein*** *(basta tomarmos o primo p = 2).*

Assim, podemos provar que os polinômios, $t(X) = X^2 + 1$ e $k(X) = X^6 + X^3 + 1$, são irredutíveis usando a mesma estratégia e argumentando pelo mesmo motivo.

2.4.4 Os Polinômios Ciclotômicos

Uma transformação semelhante ao exposto no ***Exemplo 2.16*** resolve o problema da redutibilidade para o polinômio

$$p(X) = \frac{X^n - 1}{X - 1} = X^{n-1} + X^{n-2} + \cdots + X + 1,$$

o qual denominamos como um polinômio "ciclotômico".

O entendimento dessa classe de polinômios dá-se das raízes gregas, e que significa cortar o círculo. Tais raízes são números complexos, que juntamente com o número 1, formam as enésimas raízes da unidade - "cortam o círculo" de raio 1 em *n* arcos iguais.

Mas vale se perguntar: será que todos polinômios dessa forma são irredutíveis sobre os racionais? Vejamos a seguinte proposição que trata sobre esse assunto.

Proposição 2.4 *– O polinômio* $p(X) = X^{n-1} + X^{n-2} + \cdots + X + 1 \in \mathbb{Q}[X]$, *em que n é composto, é redutível sobre* $\mathbb{Q}[X]$.

Demonstração:

De fato, seja n um número composto, logo podemos escrevê-lo como n = pk, com p e k inteiros não nulos. Daí,

$$\begin{aligned} p(X) &= X^{n-1} + X^{n-2} + \cdots + X + 1 \\ &= \frac{X^n - 1}{X - 1} \\ &= \frac{X^{pk} - 1}{X - 1} \\ &= \frac{X^p - 1}{X - 1}\left(X^{p(k-1)} + X^{p(k-2)} + \cdots + X + 1\right) \end{aligned}$$

ou seja, $p(X) = (X^p + X^{p-1} + \cdots + X + 1)\left(X^{p(k-1)} + X^{p(k-2)} + \cdots + X + 1\right)$. *Portanto,* $p(X)$ *é redutível.*

■

Assim, podemos concluir que ao menos uma das raízes do polinômio ciclotômico

$$p(X) = X^{n-1} + X^{n-2} + \cdots + X + 1 \in \mathbb{Q}[X],$$

em que *p* é um número composto, é um número racional. Os demais polinômios em que isso não ocorre são polinômios irredutíveis sobre os racionais.

De fato, podemos provar que um *polinômio ciclotômico, em que p é um número primo*[7], não tem raízes reais – todas são complexas – nos garantindo sua irredutibilidade sobre os racionais.

Uma questão mais difícil é determinar quando tais raízes "são irracionais", ou seja, quando elas podem ser representadas por radicais quadráticos e quando as raízes podem ser obtidas a partir de números inteiros aplicando as quatro operações aritméticas e as operações de extração de raízes quadradas.

[7] Vide [GONÇALVES, Adilson., *p.85*]

3 NÚMEROS REAIS: RACIONAIS E IRRACIONAIS

Neste capítulo abordaremos os números reais, no que se refere à classificação em racionais e irracionais. Para tanto, apresentaremos um pouco da história de seu surgimento.

Foi com um dentre os discípulos de Pitágoras, ao observar que a diagonal de um quadrado é incomensurável com seu lado, que as discussões sobre "número que não é racional" se iniciaram, pois os gregos acreditavam que dados dois segmentos sempre haveria a comensurabilidade, ou seja, que os números naturais mais as frações (os racionais) sempre seriam suficientes para solucionar esse problema.

Assim, os números reais – racionais e irracionais – já evidenciados de forma um tanto intuitiva e sem os devidos cuidados, serviram de alicerce para o desenvolvimento da matemática. Porém, foi com o trabalho do matemático francês Augustin-Louis Cauchy, em 1821, quando desenvolveu uma teoria relacionada ao Cálculo – definições de continuidade, diferenciabilidade e integral definida a partir do conceito de limite – que notou-se a necessidade de mais rigor nas definições dos números irracionais, haja vista serem estritamente necessárias para o desenvolvimento da Análise.

Foi nesse contexto que os matemáticos, no sentido de tornar o sistema dos números reais mais rigoroso e, com isso, transmitir mais segurança o que viesse da Análise, que o sistema dos números reais passou a ser deduzido a partir de um conjunto de postulados que o caracterizem. Foi o que defendeu o matemático alemão Karl Weierstrass.

Assim como o matemático francês Charles Méray, Weierstrass observou que, ao separar o Cálculo da Geometria e referenciá-lo conceitualmente apenas em número, haveria a necessidade de conceituar números irracionais que não dependessem do conceito de limites.

Weierstrass não publicou suas ideias sobre a aritmetização dessa análise, porém tais resultados vieram ser conhecidos através de um livro de seu aluno, Ernst Kossak. Todavia, desde 1858, o matemático alemão Richard Dedekind, a partir das suas aulas de Cálculo, já observara e se debruçara em resolver esse problema dos "números irracionais".

Foi com as teorias apresentadas por Eduard Heine e George Cantor que Dedekind despertou-se, pouco antes de seu artigo sobre *continuidade e números irracionais*, para uma

aritmética dos números reais mais robusta em que buscou desmistificar as dúvidas e a funcionalidade dos irracionais em sua teoria.

Assim, no final do século XIX, inspirado no trabalho do discípulo de Platão, Eudóxio de Cnido – que resolvera o problema de segmentos incomensuráveis – foi que Dedekind estabeleceu a propriedade de que um número irracional seria um corte, o qual dividiria os números racionais em duas classes: uma inferior e outra superior a ele.

Portanto, com a definição de Georg Cantor para um número real, estabelecida sobre uma classe de equivalência de sequências de Cauchy de números racionais, e os "cortes" de Dedekind, que a caracterização da continuidade fora resolvida. Logo, com o estabelecimento de uma correspondência biunívoca entre pontos em uma reta e tais "cortes", dada por Dedekind, criou-se os números reais.

Ainda no contexto dos números reais, trataremos também, de forma breve, de sua classificação em algébricos e transcendentes, cujos tópicos terão uso fundamental no contexto desse trabalho. Além disso, falaremos um pouco sobre a correlação entre a irracionalidade dos números e as raízes de polinômios.

3.1 Os Números Racionais

Os historiadores apontam que o conceito numérico tenha se desenvolvido bem antes dos registros mais antigos existentes, pois o homem primitivo percebia a diferenciação entre um boi e um rebanho ou entre um peixe e um cardume; bem como o que apresentam em comum, a unidade. E que a noção de acrescentar ou retirar objetos de uma coleção já era um senso comum, se baseando em correspondências biunívocas – sejam usando os dedos, pedras, ranhuras em madeira ou nós em cordas – e seguido posteriormente pelo surgimento de alguns vocais para tal associação.

Nesse sentido, é possível citar Eves:

> Nos mais remotos estágios do período de contagem vocal, usavam-se sons (palavras) diferentes para, por exemplo, *dois* carneiros e *dois* homens. (Considere, por exemplo, em português: *parelha* de cavalos, *junta* de bois, *par* de sapatos, *casal* de coelhos.) A abstração da propriedade comum *dois*, representada por algum som considerado

> independentemente de qualquer associação concreta, provavelmente levou muito tempo para acontecer [...]. (EVES, 2008, p.26)

Assim, a história dos números nos conta que a ideia primitiva dos mesmos estava voltada para a contagem de objetos e coleções finitas e, também, para mensuração de terras. No intuito de entender e sistematizar tais conceitos, surgiram a Geometria e a Aritmética – uma relaciona as medidas e formas geométricas (as mais diversas possíveis) e a outra trata das operações com as grandezas em forma de números, respectivamente.

Diante de um contexto de desenvolvimento da matemática cronologicamente, havemos de convir com Garbi:

> "De qualquer maneira, todos concordam que o estudo das formas e dos números faz parte da Matemática e podemos tentar imaginar quando isso começou a ser feito, ainda que rudimentarmente. [...] Como se vê, a história é muito antiga e nos dá importantíssima lição: ninguém deve sentir-se frustrado ou desanimar se não conseguir aprender alguma coisa de Matemática na primeira tentativa. Afinal, demoramos muitos milênios para chegar até aqui." (GARBI, 2007, p.8)

Embora exista uma diferença entre contagem (uma equivalência de objetos de coleções distintas) e número (ideia abstrata, um símbolo), foi mediante as necessidades básicas durante o aparecimento de problemas reais do cotidiano que surgiram as definições de conjuntos numéricos. Nesse aspecto citamos Lima:

> "As necessidades provocadas por um sistema social cada vez mais complexo e as longas reflexões, possíveis graças à disponibilidade de tempo trazida pelo progresso econômico, conduziram, através dos séculos, ao aperfeiçoamento do extraordinário instrumento de avaliação que é o conjunto dos números naturais.
> Decorridos muitos milênios, podemos hoje descrever concisa e precisamente o conjunto $\mathbb{N}$ dos números naturais, valendo-nos da notável síntese feita pelo matemático italiano Giuseppe Peano no limiar do século 20." (LIMA, 2017, p.23)

Assim, tais conceitos e agrupamentos organizados dentro de uma especificidade de noções estabelecidas categoricamente pelo matemático ***Peano***, teoria essa eternizada nos textos matemáticos como ***Os Axiomas de Peano***, deu-se origem aos números naturais ($\mathbb{N}$).

O surgimento dos demais conjuntos que já temos conhecimento – Inteiros ($\mathbb{Z}$), Racionais ($\mathbb{Q}$), Irracionais ($\mathbb{R} - \{\mathbb{Q}\}$ ou $\mathbb{I}$), Reais ($\mathbb{R}$) e Complexos ($\mathbb{C}$) – foi um processo de certa forma lento e deu-se a partir do surgimento de novas definições nesse campo, como: Anéis, Domínios, Corpos e outras. Para exemplificar essa morosidade no surgimento desses

conjuntos citamos Ifrah, em que o mesmo relaciona o interstício dos naturais para a iniciação do aparecimentos dos inteiros:

> [...] Durante muito tempo, ela [humanidade] viveu também na impossibilidade de conceber os números "negativos" (-1, -2, -3, -4, etc), dos quais nos servimos correntemente hoje em dia para exprimir, por exemplo, uma temperatura abaixo de zero, ou ainda um saldo devedor numa conta bancária. Assim, durante muito tempo uma subtração como 3-5 foi considerada impossível. Sabemos como a descoberta do zero varreu este obstáculo e permitiu, de acordo com a famosa "regra de sinais" a extensão dos números aritméticos ordinários (ditos "naturais") até os números "relativos", por adjunção a eles de seus "simétricos" em relação a zero." (IFRAH, 1989, p.337)

Mas foi diante da teoria do matemático George Cantor e das construções dadas por Dedekind ("cortes de Dedekind") que as necessidades quanto aos números reais passaram a ser atendidas. Cantor foi quem primeiro utilizou um símbolo para representar os números reais; fez um trabalho sobre os conjuntos transfinitos e suas classificações; em seus estudos sobre a natureza do "contínuo", provou que o conjunto dos números reais é não-enumerável e, na "aritmetização da Análise", publicou, em 1874, um artigo relacionado à caracterização dos números reais.

Doravante, trataremos especificamente os números reais como números racionais e irracionais.

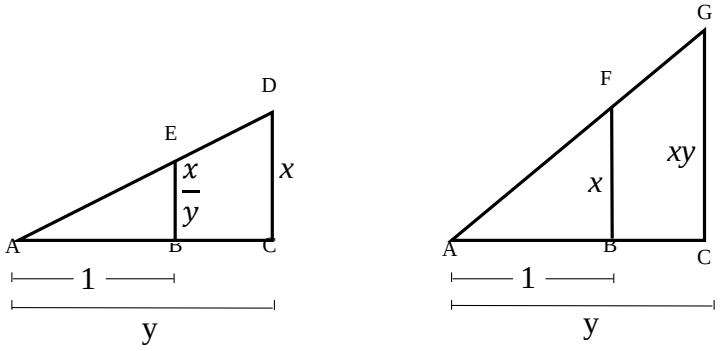
Historicamente, sabemos que os gregos foram responsáveis por grandes avanços nos conhecimentos matemáticos na antiguidade. Podemos citar Aristóteles, primeiro filósofo grego que sistematizou a observação empírica; Tales de Mileto, um comerciante que em suas andanças deslumbrou-se pelo conhecimento matemático, em especial a geometria, em que desenvolveu o ainda atual *Teorema de Tales*; Pitágoras, fundador da escola pitagórica e eternizado por seu notável *Teorema de Pitágoras*, dentre outros que poderíamos citar.

Todavia podemos salientar um grande feito dos gregos, que foram as medições de segmentos e as noções de segmentos comensuráveis e incomensuráveis.

Apropriados das técnicas euclidianas e utilizando-se de régua não graduada e compasso, os gregos sabiam realizar várias construções geométricas, uma forma de outorgar a existência de um número por sua representação geométrica. Dentre essas construções, estão os comprimentos do produto e do quociente de segmentos de comprimentos x e y, possivelmente a partir daí podemos intuitivamente compreender os números racionais através da geometria,

Figura 1, cujos resultados desenhamos são obtidos por semelhança de triângulos, ideia essa já formalizada por Tales.

Figura 1 – Representação geométrica do quociente e do produto, respectivamente, de segmentos de comprimentos *x* e *y*.



Fonte: Hefez e Villela (2018, com adaptações).

As construções são obtidas das seguintes formas: inicialmente tomemos três seguimentos – um de comprimento 1, outro de comprimento *x* (CD ≡ BF) e outro de comprimento *y* (AC, por conveniência AC > 1).

A primeira figura (a da esquerda), onde é obtido o quociente de *x* por *y*, sobre uma mesma reta, utilizando um compasso, marcamos o seguimento de comprimento 1 e o seguimento de comprimento *y*, ambos coincidindo em A. Em seguida, passando por C construímos uma perpendicular e assinalamos o seguimento *x* e, por conseguinte, construímos a semirreta AD. Agora, passando por B construímos uma perpendicular e marcamos o ponto E, seu ponto de interseção com o segmento AD. Daí, o segmento BE construído tem comprimento igual ao quociente de *x* por *y*. De fato, por critério de semelhança Lado – Ângulo – Lado (LAL), temos:

$$\frac{1}{y} = \frac{BE}{x},$$

que ocorrerá, se, e somente se, $BE = \frac{x}{y}$.

Na segunda figura (a da direita), demarcamos os segmentos de comprimentos 1 e *y* de modo análogo à figura anterior. E passando por B, construímos uma perpendicular e marcamos o segmento *x* (BF), construindo em seguida a semirreta AF. Agora, passando sobre

C construímos uma perpendicular e assinalamos o ponto G, interseção dela com a semirreta AF. Assim, o segmento CG terá comprimento igual ao produto de *x* por *y*. De fato, também por semelhança LAL, temos:

$$\frac{1}{y} = \frac{x}{CG},$$

que ocorrerá, se, e somente se, $CG = xy$.

Com isso, se conhecêssemos (dadas as medidas) os comprimentos de dois segmentos, certamente saberíamos o resultado do produto e do quociente entre eles, e suas representações geométricas – os seus comprimentos. E, os números ganhavam significado para os povos da antiguidade, por meio de construções geométricas realizadas pelos gregos.

Num contexto mais formal, definimos *número racional*[8] como todo número que pode ser expresso da forma $\frac{a}{b}$, em que *a* e *b* são números inteiros primos entre si e, $b \neq 0$. Cuja notação para o conjunto formado por todos os números racionais, dada por *Guiseppe Peano*, é:

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

Tal definição com as restrições sobre *a* e *b* são de fundamental importância e nos garante que cada número racional possa ser representado de forma única, pois sabemos que existem infinitas formas de expressar um mesmo número racional. Admitindo outras representações para o número racional $\frac{1}{2}$, o qual pode ser escrito de infinitas formas, como as expressões $\frac{2}{4}$, $\frac{-5}{-10}$, ..., ou $\frac{10^9}{2\times10^9}$, etc, percebemos que a representação em que os termos são relativamente primos entre si é única. Nesses casos, denominamos tais frações de frações equivalentes ao número racional $\frac{1}{2}$.

Suscintamente, podemos definir um número irracional como um número que não é racional, mas não haveria exatidão, visto que *i* (a unidade imaginária), por exemplo, não é um número real, muito menos um racional. Assim, temos mais clareza em definirmos os números irracionais como sendo o conjunto dos números reais que não são racionais. E denotamos por

[8] Uma definição algébrica para os Números Racionais pode ser obtida em **Apêndice A.**

$$\mathbb{R}\backslash\mathbb{Q} = \{a \in \mathbb{R};\ a \notin \mathbb{Q}\}.$$

Frações cujos denominadores são potencias de 10 são chamadas frações decimais e são de fundamental importância para representação decimal dos números racionais, além de podermos estender a elas também a representação decimal dos números naturais. Mas é na representação decimal dos números racionais que iremos explorar um pouco agora, fazendo a seguinte ressalva: para cada número decimal corresponderá uma única fração irredutível, que denominamos de fração geratriz.

A expressão decimal de um número racional é da forma

$$r = a_0, a_1 a_2 a_3 a_4 \dots a_m \dots, \tag{2.1}$$

onde a_0 é um número inteiro maior que ou igual a zero e é denominado de parte inteira de *r*; e $a_0, a_1, a_2, a_3, a_4, \dots, a_m, \dots$ são dígitos em que para todo m = 0, 1, 2, 3, 4, ..., m, ..., temos que $0 \leq a_m \leq 9$.

A expressão decimal de *r* em (2.1) pode ser reescrita em frações decimais da seguinte forma:

$$r = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \cdots + \frac{a_m}{10^m} + \cdots \tag{2.2}$$

Caso, a partir de um certo ponto, digamos todos os dígitos após a_m, podemos escrever (2.1) e (2.2) como, respectivamente,

$$r = a_0, a_1 a_2 a_3 a_4 \dots a_m \text{ e } r = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \cdots + \frac{a_m}{10^m}.$$

Exemplo 3.1 *– O número racional 1045,89 está na forma decimal e é escrito na forma de frações decimais como:*

$$1045{,}89 = 1045 + \frac{8}{10} + \frac{9}{10^2} = \frac{104589}{100}.$$

Uma igualdade que causa estranheza, uma igualdade entre um número natural e um número racional em sua forma decimal infinita, mas é facilmente observada ao aplicarmos a fórmula da soma de uma progressão geométrica infinita de razão 0 < q < 1, é a que 1 = 0,999..., isto é,

$$1 = 0{,}999\dots = \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \cdots. \tag{2.3}$$

Uma vez fixada tal igualdade, o processo de determinar a fração correspondente a um certo número decimal é facilitado.

Exemplo 3.2 *– Qual a fração correspondente ao número decimal 0,2222...?*

Solução:*Suponhamos que a fração correspondente seja f, isto é, f = 0,2222... .*

Ora, temos que

$$0{,}9999\ldots = \frac{9}{10} + \frac{9}{100} + \frac{9}{1000} + \cdots = 1$$

e, dividido por 9, obtemos

$$0{,}1111\ldots = \frac{1}{10} + \frac{1}{100} + \frac{1}{1000} + \cdots = \frac{1}{9}.$$

Logo,

$$f = 0{,}2222\ldots = 2\,(0{,}1111\ldots) = 2 \times \frac{1}{9} = \frac{2}{9}$$

Portanto, a fração geratriz do número decimal 0,2222... é $\frac{2}{9}$.

Exemplo 3.3 *– De modo similar ao apresentado no* ***Exemplo 2.2****, podemos concluir que para todo dígito d temos que:*

$$0,dddd\ldots = \frac{d}{9}.$$

Vejamos o resultado a seguir obtido da igualdade (2.3). Observamos que

$$\begin{aligned} 1 &= \frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \frac{9}{10^4} + \frac{9}{10^5} + \frac{9}{10^6} + \cdots \\ &= \left(\frac{9}{10} + \frac{9}{10^2}\right) + \left(\frac{9}{10^3} + \frac{9}{10^4}\right) + \left(\frac{9}{10^5} + \frac{9}{10^6}\right) + \cdots \\ &= \frac{99}{10^2} + \frac{99}{10^4} + \frac{99}{10^6} + \cdots \\ &= 99\left(\frac{1}{10^2} + \frac{1}{10^4} + \frac{1}{10^6} + \cdots\right), \end{aligned}$$

então,

$$\frac{1}{10^2} + \frac{1}{10^4} + \frac{1}{10^6} + \cdots = \frac{1}{99}.$$

Exemplo 3.4 *– Qual a fração geratriz do número decimal 0,151515...?*

Solução: *Segue que*

$$0{,}151515\ldots = \frac{15}{10^2} + \frac{15}{10^4} + \frac{15}{10^6} + \cdots = 15\left(\frac{1}{10^2} + \frac{1}{10^4} + \frac{1}{10^6} + \cdots\right) = \frac{15}{99}.$$

Portanto, a fração geratriz do número 0,151515... é $\frac{15}{99}$.

Quando uma certa expressão decimal de um número racional $r = a_0, a_1 a_2 a_3 \ldots a_m \ldots$ tem os *n* primeiros dígitos após a vírgula se repetindo indefinidamente, isto é, $a_1 a_2 a_3 \ldots a_p$, dizemos que esses dígitos formam a dízima periódica do racional r e são denominados de período.

De modo geral, a geratriz de uma dízima periódica simples é uma fração cujo numerador é o período e o denominador é o número formado por tantos noves quantos forem a quantidade de dígitos do período.

3.2 Números Irracionais: identificação mediante as raízes de polinômios

Falando agora de números irracionais, sabemos que os mesmos já eram do conhecimento dos gregos, os quais demonstravam suas existências por meio de justificativas geométricas. A história nos afirma que o primeiro número irracional conhecido por eles foi o número $\frac{\sqrt{5}-1}{2}$ (razão entre a diagonal e o lado de um pentágono regular unitário). Mas por muito tempo, acreditava-se que $\sqrt{2}$ – interpretado geometricamente como a diagonal de um quadrado de lado unitário – era o primeiro número irracional de conhecimento dos gregos.

Faremos aqui uma demonstração algébrica sobre a *irracionalidade de* $\sqrt{2}$[9]. De fato, tal número real é um número irracional, pois, do contrário, poderíamos escrevê-lo da seguinte forma

$$\sqrt{2} = \frac{a}{b} \quad \text{(i)}$$

em que *a e b* são primos entre si e b ≠ 0. Assim, elevando à potência 2 ambos os lados da igualdade em (i), obtemos

[9] Outras demonstrações podem ser encontradas em [MARQUES, Diego, *pp. 16-22*].

$$2 = \frac{a^2}{b^2}$$

e, consequentemente

$$a^2 = 2b^2 \qquad \text{(ii)}$$

Ora, essa última igualdade nos diz que a^2 é um número par e, com isso, a é um número par. Assim, digamos que se $a = 2d$, com d um inteiro, daí substituindo na equação (ii), obtemos

$$(2c)^2 = 2b^2 \Rightarrow 4c^2 = 2b^2, \text{ logo } 2c^2 = b^2$$

O termo $2c^2$ é um inteiro par, então b^2 também é um inteiro par e, portanto, b é par. Então chegamos à conclusão de que a e b são ambos pares, o que contradiz o fato de serem primos entre si.

Portanto, $\sqrt{2}$ é um número irracional.

■

De modo geral os gregos sabiam construir geometricamente um segmento de comprimento $\sqrt{a}$, dado um segmento de comprimento a e uma unidade de medida. Tal segmento seria a altura relativa à hipotenusa de um triângulo retângulo cujas as projeções dos lados sobre a hipotenusa seriam os segmentos a e 1. Um esboço de tal construção está representada na **Figura 2**, obtida a partir dos seguintes procedimentos:

1) Traçamos uma reta r;

2) Sobre r, marcamos o ponto A e, com o compasso e a ponta seca fixada em A, marcamos o ponto B, também sobre r, de modo que o segmento AB tenha comprimento a;

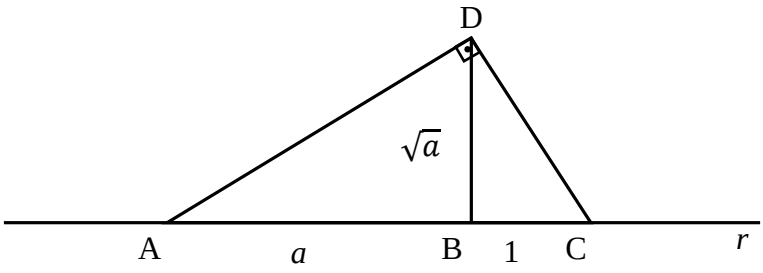
3) Ainda sobre r, com a ponta seca do compasso fixada em B, marcamos o ponto C em r, tal que BC tenha comprimento 1;

4) Com o compasso assinalamos o ponto médio do segmento AC e construímos uma circunferência de centro nesse ponto médio e de raio $(a + 1)/2$;

5) Agora, sobre B traçamos uma perpendicular que intersecta em D a circunferência construída em 4). E, com isso, o segmento BD terá o comprimento desejado, $\sqrt{a}$. De fato, pelas relações métricas de um triângulo, haja vista que o triângulo ACD é retângulo em D e tem altura

BD, segue que o quadrado da altura é igual ao produto das projeções dos lados AD e DC, isto é, o produto AB por BC.

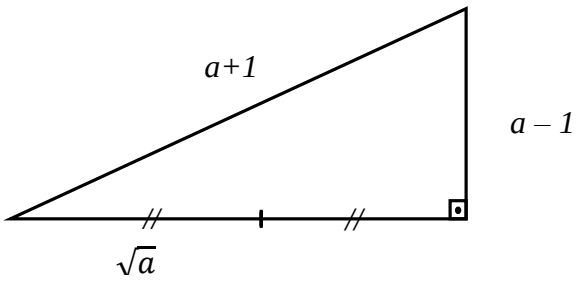
Figura 2 – Representação geométrica grega para um segmento de comprimento $\sqrt{a}$



Fonte: Elaborada pelo autor.

Sabemos ainda, por meio dos historiadores, por exemplo, que Teodoro de Cirene (470 a.C.) demonstrou geometricamente $\sqrt{a}$, usando um triângulo retângulo de hipotenusa *a + 1*, metade de um cateto como sendo $\sqrt{a}$ e o outro cateto *a – 1*. Observe a **Figura 3** abaixo,

Figura 3 – Representação geométrica de Teodoro de Cirene para um segmento de comprimento $\sqrt{a}$



Fonte: Elaborada pelo autor.

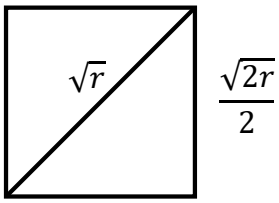
A justificativa algébrica para a ideia de Teodoro é facilmente verificada na igualdade abaixo,

$$(a+1)^2 = (a-1)^2 + \left(2\sqrt{a}\right)^2.$$

A ideia utilizada na demonstração algébrica para irracionalidade de $\sqrt{2}$ pode ser estendida para mostrar que a raiz quadrada de todo número racional positivo que não é um

quadrado perfeito é um número irracional. Assim, para representar geometricamente a $\sqrt{r}$, em que r é um número racional satisfazendo tais condições, apresentamos, na **Figura 4**, o comprimento de tal segmento, que é a diagonal de quadrado de lado $\frac{\sqrt{2r}}{2}$.

Figura 4 - Representação geométrica para $\sqrt{r}$



Fonte: Elaborada pelo autor.

Antes de demonstrarmos algebricamente esse fato, apresentaremos a definição de números primos e um lema importantíssimo na teoria dos números, denominado Lema de Euclides, que nos dará subsídios a essa demonstração.

Definição 3.1 – *Um número natural maior do que 1 que só possui dois divisores positivos, isto é, ele mesmo e 1, será denominado de número primo. Caso tal número não seja primo, ele será denominado de número composto.*

***Lema 3.1* – (Lema de Euclides**) *Sejam a, b, c ∈ ℤ, com c um número primo. Se c|ab, então c|a ou c|b.*

Demonstração:

É suficiente mostrarmos que, se c|ab e c não divide a, então c|b. Porém, como c não divide a e c é um número primo por hipótese, segue que a e c são primos entre si, ou seja, mdc(a, c) = 1. E, pelo Teorema de Bachet-Bézout[10], existem x e y inteiros tais que,

$$ax + cy = 1.\text{(i)}$$

Agora, como de c|ab, temos, por definição de divisibilidade[11], que existe um d ∈ ℤ tal que ab = cd.

[10] MARTINEZ, Fábio Brochero; at al, 2018.
[11] MARTINEZ, Fábio Brochero; at al, 2018.

Assim, em (i)*, multiplicando ambos os lados da igualdade por b, obtemos:*

$$abx + cby = b. \quad \text{(ii)}$$

Como ab = cd e substituindo ab por cd em (ii)*, segue que,*

$$cdx + cby = b,$$

e colocando c em evidência, temos que

$$c(dx + by) = b.$$

Como (dx + by) é inteiro, segue da definição de divisibilidade que c divide b. Portanto, c|b.

■

Agora, retomando a demonstração da irracionalidade de $\sqrt{r}$, sob as condições já citadas.

Consideremos, por contradição, que $\sqrt{r}$ *seja racional, isto é,*

$$\sqrt{r} = \frac{p}{q}$$

em que p e q são números inteiros e primos entre si e $q \neq 0$*. Assim, elevando à potência 2 ambos os lados da igualdade, obtemos*

$$r = \frac{p^2}{q^2}$$

e, consequentemente

$$p^2 = rq^2 \quad (i)$$

Da igualdade (i), observamos, pelo Lema de Euclides, que $q^2|p^2$ *e, consequentemente, q|p, o que é uma contradição haja vista que p e q são primos entre si. Portanto* $\sqrt{r}$ *é irracional quando r é um número racional positivo que não é um quadrado perfeito.*

■

O fato de $\sqrt{r}$ ser um número real irracional quando *r* é um número racional que não é quadrado perfeito, nos fornecem uma infinidade de números irracionais.

Podemos demonstrar a irracionalidade de $\sqrt{r}$ de outra forma não menos contundente, mas para isso necessitaremos enunciar alguns resultados algébricos. Iniciaremos com um corolário, seguindo pelo Teorema Fundamental da Aritmética.

Corolário 3.1 – *Se p, p_1, p_2, ..., p_k são números primos e, se p| p_1p_2 ... p_k, então p = p_i para algum i = 1, 2, ...,k.*

Demonstração:

Faremos a demonstração por indução. O caso k = 1, é óbvio.

Para o caso k = 2, consideremos que p | p_1p_2 e p ∤ p_2, com mdc (p, p_1) = d.

Como d | p, logo d = 1 ou d = p. Mas, pelo fato de d | p_2 e p ∤ p_2, segue que d ≠ p e, portanto, d = 1.

Daí, pelo Lema de Euclides e pelo fato de p ∤ p_2, então p | p_2, isto é, p = 1 ou p = p_2. Que pela definição de número primo, concluímos que p = p_2.

O caso geral é totalmente análogo ao caso k = 2.

■

Teorema 3.1 – (Teorema Fundamental da Aritmética) – *Todo número natural maior que 1 ou se escreve de modo único como produto de fatores primos (a menos da ordem dos fatores) ou é um número primo.*

Demonstração:

Vide [HEFEZ, Abramo. **Aritmética**, *p. 123*].

Se, no Teorema acima, agruparmos os fatores primos que se repetem, podemos escrever univocamente um determinado número inteiro $n \notin \{-1, 0, 1\}$ como

$$n = \pm {p_1}^{a_1} \cdots {p_k}^{a_k}$$

em que a_i são números naturais e p_i são números primos distintos para todo $i \in \{1, 2, ..., k\}$.

Tomando um número natural $m = {p_1}^{a_1} \cdots {p_k}^{a_k}$ e denotando o número de divisores positivos de *m* por *d*(*m*), por uma contagem simples, concluímos que

$$d(m) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

Daí, afirmamos e é de fácil verificação, se a quantidade de divisores positivos de *m* for ímpar então *m* é um quadrado perfeito.

Portanto, a partir desses resultados podemos verificar se um número natural é quadrado perfeito ou não.

Vejamos nos exemplos seguintes alguns números irracionais expressos por radicais de números reais que não são quadrados perfeitos. Cujas demonstrações estarão dentro do contexto já apresentado.

Exemplo 3.5 – *Mostre que* $\sqrt{5}$ *é irracional.*

Solução: *Poderíamos apenas usar o argumento de que 5 não é um quadrado perfeito, logo sua raiz quadrada trata-se de um número irracional. No entanto iremos fazer uma demonstração desse fato semelhante ao caso anterior da irracionalidade de* $\sqrt{2}$.

De fato, suponhamos, por absurdo, que $\sqrt{5}$ *é racional, ou seja,*

$$\sqrt{5} = \frac{a}{b}$$

com a e b sendo primos entre si e $b \neq 0$. *Agora, elevando ao quadrado a equação acima, obtemos*

$$5 = \frac{a^2}{b^2}, \text{ o que implica em } 5b^2 = a^2$$

O termo $5b^2$ *é um múltiplo de 5, logo* a^2 *também é um múltiplo de 5 e, com isso, a é um múltiplo de 5, isto é, a = 5c, com c um número inteiro. Substituindo a na equação* $5b^2 = a^2$, *obtemos*

$$(5c)^2 = 5b^2 \Rightarrow 25c^2 = 5b^2, \text{ logo } 5c^2 = b^2.$$

Ora, o termo $5c^2$ *é um múltiplo de 5, então* b^2 *é múltiplo de 5 e, consequentemente, b é um múltiplo de 5. Mas chegamos à conclusão de que a e b são ambos múltiplos de 5, contrariando o fato de serem primos entre si. Portanto* $\sqrt{5}$ *é irracional.*

■

Todavia, no estudo da racionalidade ou irracionalidade dos números escritos ou não sob radicais, para minimizar o trabalho nas demonstrações, devemos ser perspicazes em entendermos e usarmos esses argumentos adequados. Uma observação bastante valiosa é que

certas propriedades no ***Corpo dos números racionais***[12] não são válidas para os números irracionais.

Apresentaremos a seguir algumas demonstrações de racionalidade e irracionalidade de alguns números sob radicais.

Exemplo 3.6 *– Prove que* $\sqrt{10}$ *é irracional.*

Solução: *Ora, como argumento, temos que 10 não é um quadrado perfeito logo* $\sqrt{10}$ *é irracional.*

Bem simples a demonstração do exemplo anterior. Trataremos em outra óptica a prova (ou uma ideia da mesma) desse exemplo pois nem todos os reconhecimentos dos irracionais são triviais, mas antes vamos esclarecer algumas coisas.

Poderíamos usar um argumento falacioso, dizendo que pelo ***Exemplo 5.1*** do **Apêndice A**, temos que os números racionais são fechados para adição e multiplicação. E como $\sqrt{10} = \sqrt{2 \times 5} = \sqrt{2} \times \sqrt{5}$, em que $\sqrt{2}$ e $\sqrt{5}$ são ambos irracionais (já provado anteriormente como exemplos), portanto, $\sqrt{10}$ é irracional. Contudo, temos que $(\sqrt{3} - 1)$ e $(\sqrt{3} + 1)$ são ambos irracionais (veja ***Exemplo 2.5***) mas o resultado de seu produto é racional, isto é, $(\sqrt{3} - 1)(\sqrt{3} + 1) = 8$, mostrando-nos que o produto de irracionais nem sempre é irracional, ou seja, é fácil ver que os irracionais não é fechado para multiplicação. E, consequentemente, que esse fato não é válido para os números irracionais, isto é, nem sempre faz sentido – embora a afirmação seja verdadeira de que $\sqrt{10}$ é irracional – simplesmente justificarmos tal irracionalidade dessa forma. Então seria mais um caso a ser analisado separadamente.

Agora, do contrário, argumentar que o produto de racionais é racional é válido, pois trata-se de um ***corpo***, e pode ser uma saída magistral na resolução de um problema, como é o que se segue:

Exemplo 3.7 *– Mostre que* $\sqrt{2}+\sqrt{5}$ *é irracional.*

Solução*:* *Suponhamos que* $\sqrt{2}+\sqrt{5}$ *seja um número racional, digamos n, logo*

$$n = \sqrt{2}+\sqrt{5}\ .$$

[12] A definição de ***Corpo*** encontra-se no **Apêndice A**

Elevando ao quadrado ambos os lados da igualdade, obtemos $n^2 = 7+\sqrt{10}$*, que podemos escrever como*

$$n^2 - 7 = \sqrt{10}$$

Note-se que os números racionais são fechados para soma e multiplicação, pois trata-se de um corpo. Ou mais informalmente, podemos dizer que os racionais são fechados para as quatro operações. Dessa forma, o lado esquerdo da igualdade trata-se de um número racional, mas o lado direito da igualdade é um número irracional. Assim chegamos a uma contradição. Portanto está provada a irracionalidade de $\sqrt{2}+\sqrt{5}$*.*

■

Ainda que pareça viável demonstrar a irracionalidade de um número por técnicas similares às apresentadas até aqui, discorre-se enfadonho analisar caso a caso. Logo, há de se convir que uma estratégia mais abrangente terá grande contribuição para a matemática na resolução de problemas, isto é, ter um método que podemos generalizar e aplicar a um grande leque dos casos.

Diante de algumas situações, podemos também mostrar a irracionalidade de $\sqrt{r}$, quando *r* é um número racional positivo e não é um quadrado perfeito, recorrendo às soluções de equações polinomiais (ou às raízes de polinômios). Seguimos desse fato o exemplo que se segue:

Exemplo 3.8 *– Mostre que* $\left(\sqrt{3}-1\right)$ *e* $\left(\sqrt{3}+1\right)$ *são ambos irracionais.*

Solução*:* *Suponhamos, por absurdo, que ambos os números dados, isto é,* $\sqrt{3}-1=x$ e $\sqrt{3}+1=y$*, são números racionais. Daí, tomando o primeiro caso,* $\sqrt{3}-1=x$*, segue que*

$$\sqrt{3}-1=x \;\Rightarrow\; \sqrt{3}=x+1 \underset{1}{\Rightarrow} \left(\sqrt{3}\right)^2=(x+1)^2 \;\Rightarrow\; x^2+2x-2=0$$

Ora, aplicando o Critério de Eisenstein à equação quadrática resultante, observamos que a mesma não possui raízes racionais, portanto x não é um número racional. A prova para y é análoga à prova para x, então ambos são irracionais.

■

Logo, recorrermos às soluções de equações polinomiais que surgem das manipulações algébricas na resolução do problema de responder se um dado número expresso

por radicais é ou não um número racional é uma estratégia bem viável. Como apresentaremos nos exemplos a seguir.

Exemplo 3.9 *– Decidir se* $\sqrt{12-6\sqrt{3}}+\sqrt{12+6\sqrt{3}}$ *é racional ou irracional. Justifique.*

Apresentaremos duas soluções:

Solução 1: *Na resolução desse problema identificamos que:*

$$\sqrt{12-6\sqrt{3}}=\sqrt{\left(3-\sqrt{2}\right)^2}=3-\sqrt{2}\ e\sqrt{12+6\sqrt{3}}=\sqrt{\left(3+\sqrt{2}\right)^2}=3+\sqrt{2}$$

Então, $\sqrt{12-6\sqrt{3}}+\sqrt{12+6\sqrt{3}}=3-\sqrt{2}+3+\sqrt{2}=6.$

Portanto, a soma é um número racional.

■

Solução 2: *Agora abordaremos de uma forma diferente, manipularemos algebricamente até chegarmos a uma equação polinomial.*

Suponhamos que $\sqrt{12-6\sqrt{3}}+\sqrt{12+6\sqrt{3}}=k$*, com k racional. Assim, elevando ao quadrado ambos os lados da igualdade, teremos*

$$\left(\sqrt{12-6\sqrt{3}}+\sqrt{12+6\sqrt{3}}\right)^2=k^2\ \Rightarrow\ 12-6\sqrt{3}+6+12+6\sqrt{3}=k^2\ \Rightarrow\ k^2=30,$$

isto é, $k=-\sqrt{30}$ *ou* $k=\sqrt{30}$*. Mas 30 não é um quadrado perfeito, logo k é irracional.*

Portanto, $\sqrt{12-6\sqrt{3}}+\sqrt{12+6\sqrt{3}}$ *é um número irracional.*

■

Nos exemplos seguintes, determinaremos se os números expressos por radicais são racionais ou irracionais usando apenas a estratégia de manipulação algébrica até chegarmos a uma equação polinomial.

Exemplo 3.10 *– Mostre que* $\sqrt[3]{7+\sqrt{50}}+\sqrt[3]{7-\sqrt{50}}$ *é um número inteiro.*

Solução*: Suponhamos que* $\sqrt[3]{7+\sqrt{50}}+\sqrt[3]{7-\sqrt{50}}=x\in Z$*. Daí, elevando ao cubo ambos os lados da igualdade, teremos*

$$\left(\sqrt[3]{7+\sqrt{50}}+\sqrt[3]{7-\sqrt{50}}\right)^3 = x^3,$$

isto é,

$$7+\sqrt{50}+3\left(\sqrt[3]{7+\sqrt{50}}\right)^2\left(\sqrt[3]{7-\sqrt{50}}\right)+3\left(\sqrt[3]{7+\sqrt{50}}\right)\left(\sqrt[3]{7-\sqrt{50}}\right)^2+7-\sqrt{50}=x^3$$

de onde obtemos

$$14+3\left(\sqrt[3]{7+\sqrt{50}}\right)\left(\sqrt[3]{7-\sqrt{50}}\right)\left(\sqrt[3]{7+\sqrt{50}}+\sqrt[3]{7-\sqrt{50}}\right)=x^3.$$

Ora, por hipótese, $\sqrt[3]{7+\sqrt{50}}+\sqrt[3]{7-\sqrt{50}} = x \in Z$*, que substituindo na equação ligeiramente acima e desenvolvendo-a, teremos*

$$14+3\left(\sqrt[3]{(7+\sqrt{50})(7-\sqrt{50})}\right)x = x^3.$$

Resultando, assim, numa resolução de uma equação cúbica $x^3+3x-14=0$.

Portanto, como as soluções da equação cúbica $x^3+3x-14=0$ *são* $-1+i\sqrt{6}$, $-1-i\sqrt{6}$ *e 2 (utilizando o* ***Teorema 4.3****), onde apenas o 2 é inteiro (racional), segue que* $\sqrt[3]{7+\sqrt{50}}+\sqrt[3]{7-\sqrt{50}}=2\in\mathbb{Z}$*. E, por conseguinte,* $p(x)=x^3+3x-14$ *possui uma única raiz racional, e a observação feita acima segue.*

■

Exemplo 3.11 *– Se* $x=\sqrt{8+2\sqrt{10+2\sqrt{5}}}+\sqrt{8-2\sqrt{10+2\sqrt{5}}}$ *então x é igual a:*

(a) $\sqrt{10}+\sqrt{2}$*(b)* $2\sqrt{5}+2$*(c) 4*

(d) $2\sqrt{5}-2$*(e)* $\sqrt{10}-\sqrt{2}$

Solução*:* *Vamos elevar ao quadrado ambos os lados da igualdade, logo*

$$x^2=\left(\sqrt{8+2\sqrt{10+2\sqrt{5}}}+\sqrt{8-2\sqrt{10+2\sqrt{5}}}\right)^2,$$

o que implica em

$$x^2 = 8 + 2\sqrt{10 + 2\sqrt{5}} + 8 - 2\sqrt{10 + 2\sqrt{5}} + 2\sqrt{8^2 - \left(2\sqrt{10 + 2\sqrt{5}}\right)^2},$$

daí segue que

$$x^2 = 16 + 4\sqrt{6 - 2\sqrt{5}} \Rightarrow x^2 - 16 = 4\sqrt{6 - 2\sqrt{5}}.$$

E, nesta última, elevamos ao quadrado ambos os lados

$$(x^2 - 16)^2 = \left(4\sqrt{6 - 2\sqrt{5}}\right)^2 \Rightarrow x^4 - 32x^2 + 160 = -32\sqrt{5}.$$

Ora, se elevarmos ao quadrado mais uma vez e desenvolvermos, obteremos a seguinte equação polinomial: $x^8 - 64x^6 + 1344x^4 - 10240x^2 + 20480 = 0$.

Mas estudar as possíveis de raízes racionais para o polinômio dado por $p(x) = x^8 - 64x^6 + 1344x^4 - 10240x^2 + 20480$ *é tremendamente trabalhoso, onde se vê viabilidade em apenas avaliar as opções de soluções de tal equação pelos itens propostos como resposta. Além disso, é mais vantajoso utilizarmos o polinômio*

$$p(x) = x^4 - 32x^2 + 160 = -32\sqrt{5},$$

por apresentar potências menores e os cálculos irão se mostrar menos trabalhosos e determinarmos a partir daí, obter o valor para x' de modo que tenhamos $p(x') = -32\sqrt{5}$.

Portanto, avaliando as opções pela a substituição direta, concluímos que a opção correta é o item (a).

■

Embora pareçam estranhas as igualdades apresentadas, como no ***Exemplos 3.9***, isto é, $\sqrt[3]{7 + \sqrt{50}} + \sqrt[3]{7 - \sqrt{50}} = 2$, percebemos que as soluções de equações polinomiais (ou as raízes de um polinômio) é uma boa estratégia para demonstração da racionalidade ou irracionalidade dos números.

4 DIAGRAMA DE NEWTON E O CRITÉRIO DE DUMAS

Fazendo um *feedback* do que abordamos até aqui, no Capítulo 2 nos apropriamos de uma teoria elementar sobre os polinômios, nos fornecendo meios necessários para desenvolvermos esse capítulo, em que abordaremos teoremas mais específicos sobre a possibilidade de decomposição de um polinômio, que nos ajudarão a compreender melhor a ideia de irredutibilidade dos polinômios com coeficientes racionais e suas conexões com os números irracionais, que é o objetivo principal de nossa pesquisa. Em que apresentaremos os mecanismos – técnicas de verificações rápidas - para previamente detectarmos se um polinômio é redutível ou não.

E foi o que iniciamos falando no Capítulo 3, ao tratarmos dos números reais – racionais e irracionais – e a correlação entre os polinômios (semelhantemente a solucionar equações polinomiais) – suas raízes e a irracionalidade dos números reais.

Daí, avanços adicionais na leitura e representação dos polinômios estão relacionados à possibilidade de traduzir as características da irredutibilidade no idioma das imagens geométricas. Na primeira seção apresentaremos a representação dos polinômios mediante diagramas, conhecidos por ***Diagramas de Newton***.

E, finalmente abordaremos o principal teorema o qual nosso estudo está focado, o ***Teorema de Dumas***, também pensado para detectar polinômios irredutíveis tendo como estratégia a ideia de Newton de representar polinômios por meio das construções de seus respectivos diagramas. Que surge como peça de um quebra-cabeça incompleto no âmbito dado pelas limitações do ***Critério de Eisenstein*** sobre a irredutibilidade de polinômios.

4.1 Diagrama de Newton para representação de polinômio em $\mathbb{Z}[X]$

O estudo sobre a irredutibilidade tornou-se o foco de atenção de muitos matemáticos célebres. Na busca por propriedades gerais, eles se sentiram desconfortáveis com o critério de Eisenstein e suas limitações. Parecia que deveria haver algo por trás disso. A

sensação geral era de que, uma vez que algo fosse revelado, uma série de novos critérios mais gerais apareceria. Isso provou-se ser verdade.

O fundamento para tais métodos iniciou-se com o estudo da representação geométrica dos polinômios no plano cartesiano, cuja ideia foi estabelecida pelo grande matemático Isaac Newton – Diagrama de Newton para representação de polinômio –, duzentos anos antes dos tempos sobre os quais estamos falando. *A posteriori*, o estudo dos Polígonos de Newton foi utilizado durante certo tempo para estudar as singularidades de curvas.

Definiremos a seguir, como fazer a representação por diagramas de um polinômio por meio do Diagrama de Newton.

Definição 4.1 – *O Diagrama de Newton do polinômio*

$$p(X) = \sum_{k=1}^{n} a_k X^k \in \mathbb{Q}[X],$$

que denotaremos por $\Delta(p)$ *em relação a um primo q, é a região delimitada pela união dos segmentos* s_i *, com* $0 \leq i \leq n$*, tal(is) que:*

(i)Os pontos dos segmentos tem como coordenadas (i, y_i)*, em que i é o grau da variável correspondente ao coeficiente* a_i *e a coordenada* y_i *é o maior expoente que devemos elevar o primo q tal que* q^{y_i} *divide* a_i*. O diagrama tem que iniciar e terminar, respectivamente, em* $(0, y_0)$ *e* (n, y_n)

(ii)O segmento s_0 *tem como pontos extremos: inicial em* $(0, y_0)$ *e final em* (j, y_j)*, com* $0 < j \leq n$ *– se* $y_j < y_0$*, para o menor* $j > 0$ *adequado para que ocorra (i), quando* $a_0 > a_n$*; ou, inicial em* $(0, y_0)$ *e final em* (j, y_j) *– se* $y_j > y_0$*, para o menor* $j > 0$ *adequado para que ocorra (i), com* $0 < j \leq n$*, quando* $a_0 < a_n$*.*

(iii)Cada segmento s_k*, com* $1 \leq k \leq n-1$*, subsequente à* s_0*, caso exista, tem pontos extremos – inicial em* (k, y_k) *e final em* $(k+l, y_{k+l})$ *– isto para o menor de valor* $l > 0$ *tal que* $k + l \leq n-1$*, em que ocorre* $y_{k+l} \leq y_k$ *,* y_{k+l+1}*.*

(iv)O último segmento a ser traçado tem como pontos extremos – ponto inicial como sendo o ponto final do penúltimo segmento traçado e final em (n, y_n)*, quando (ii) e (iii) ocorrerem.*

Assim, vamos construir o diagrama de Newton de um polinômio $p(X)$ em relação a um número primo q, a partir da definição.

Exemplo 4.1) *Construa o diagrama de Newton para o primo p = 3 do polinômio a seguir* $f(X) = X^4 + 13X^3 - 4X^2 + 36X + 12$.

Solução:

Seguindo os itens da definição acima, temos:

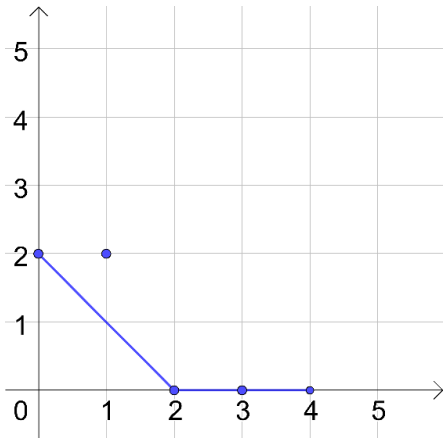
(i) Os pontos dos segmentos: O termo constante, $a_0 = 12$*, é divisível por* q^2*, mas não por* q^3*, então marcamos o ponto (0, 2). E seguimos procedendo da mesma forma para os demais coeficientes. O coeficiente* $a_1 = 36$ *é divisível por* q^2*, logo temos o ponto (1, 2); o coeficiente* $a_2 = -4$ *é divisível por* q^0*, e obtemos o ponto (2, 0); o coeficiente* $a_3 = 13$ *é divisível por* q^0*, então teremos o ponto (3, 0) e, o coeficiente* $a_4 = 1$*, o coeficiente líder, é divisíveis por* q^0*, portanto temos o ponto (4, 0).*

(ii) O segmento s_0*: O segmento* s_0 *tem como pontos extremos (0, 2) e (2, 0) e não (0, 2) e (1, 2) – pois nesse caso temos que* $y_0 = y_1$*, onde deveria ser* $y_0 < y_1$ *para (1, 2) ser o ponto extremo final.*

(iii) Os segmentos subsequentes: O segmento s_1 *tem como pontos extremos (2, 0) e (3, 0), visto que* $y_3 \leq y_2, y_4$*. O segmento* s_2 *tem como pontos extremos (3, 0) e (4, 0). (iv) Que será nosso último segmento, pois tem como um extremo o ponto referente ao coeficiente líder.*

Portanto, o diagrama para essa situação está representado a seguir:

Figura 5 – O diagrama de Newton para o polinômio $f(X) = X^4 + 13X^3 - 4X^2 + 36X + 12$



Fonte: Elaborada pelo autor.

Uma observação importante a se fazer é que para segmentos colineares consecutivos consideramos apenas um segmento, cujas extremidades são: o ponto inicial do primeiro segmento e o ponto final do último segmento. Assim, os segmentos s_1 e s_2 são representados por apenas um segmento s cujos extremos são *(2, 0)* e *(4, 0).*

Exemplo 4.2) *Construa o diagrama de Newton para o primo p = 2 do polinômio a seguir* $f(X) = 12X^3 - 8X^2 + 2X + 1$.

Solução: *Seguindo os itens da definição acima, temos:*

(i) Os pontos dos segmentos: O termo constante, $a_0 = 1$, *é divisível por* q^0, *então marcamos o ponto (0, 0). O coeficiente* $a_1 = 2$ *é divisível por* q^1, *logo temos o ponto (1, 1); o coeficiente* $a_2 = -8$ *é divisível por* q^3, *e obtemos o ponto (2, 3) e o coeficiente líder,* $a_3 = 12$, *é divisível por* q^2, *então teremos o ponto (3, 2).*

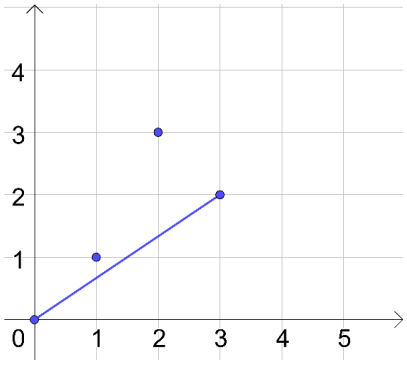
(ii) O segmento s_0*: O segmento* s_0 *teria como pontos extremos (0, 0) e (1, 1). Mas o ponto (1, 1) não é adequado e a justificativa está em (iii), o que também implicaria no diagrama não finalizar em (3, 2).*

(iii) Os segmentos subsequentes: Tais segmentos não serão traçados, haja vista que: o segmento com pontos extremos (1, 1) e (3, 2), não ocorre $y_1 \leq y_0, y_2$ *e nem o segmento com pontos extremos (1, 1) e (2, 3), pois não temos* $y_2 \leq y_1, y_3$.

(iv) Com isso o segmento s_0 *terá extremos (0, 0) e (3, 2), que também será nosso último segmento.*

Portanto, o diagrama para essa situação está representado a seguir:

Figura 6 – O diagrama de Newton para o polinômio $f(X) = 12X^3 - 8X^2 + 2X + 1$



Fonte: Elaborada pelo autor.

Agora, para construir o diagrama de Newton de um polinômio $p(X)$ em relação a um primo q, de um outro modo, precisamos das seguintes ferramentas:

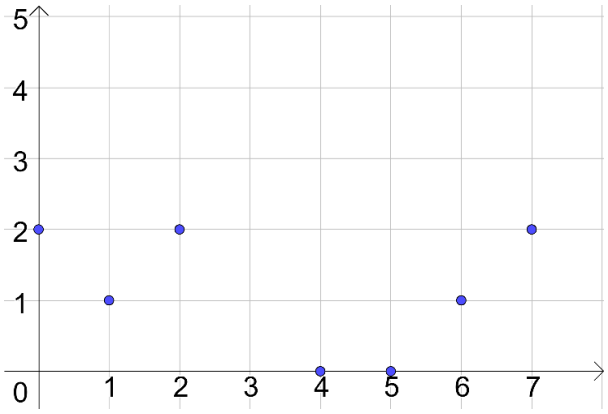
1. Um plano de coordenadas OXY (OX sendo o eixo horizontal e OU o eixo vertical).

2. Uma régua, um martelo e alguns pregos.

Começamos desenhando a base do diagrama, os pontos, análoga ao que foi feito nos exemplos acima, que é iniciada do termo constante até o coeficiente líder. Para cada termo $a_k X^k \in p(X)$ do polinômio $p(X)$, atribuímos um ponto no plano com coordenadas (k, l), onde l é o grau máximo de q (um número primo escolhido) de modo que a_k é divisível por q^l. O conjunto de todos esses pontos é o que chamamos de base. Caso a_k não seja divisível por q, então o ponto é dado por $(k, 0)$.

Na **Figura 7**, você pode ver a representação dos pontos do diagrama referente ao polinômio $p(X) = 4X^7 + 2X^6 + X^5 + X^4 + 4X^2 + 2X + 12$ em relação ao primo $q = 2$. A obtenção das coordenadas ocorre semelhantemente ao que vimos nos exemplos acima, tomamos o termo constante $a_0 = 12$ que é divisível por q^2, mas não por q^3, então marcamos o ponto (0, 2). Os coeficientes $a_1 = a_6 = 2$ são divisíveis por q^1, logo temos os pontos, respectivamente, (1, 1) e (6, 1). O coeficiente $a_3 = 0$ não produz nenhum ponto. E assim por diante, e temos para os coeficientes $a_4 = a_5 = 1$ os pontos, respectivamente, (4, 0) e (5, 0). E, por fim, os coeficientes $a_2 = a_7 = 4$ produzem, respectivamente, os pontos (2, 2) e (7, 2).

Figura 7 – Os pontos referente ao diagrama do polinômio $p(X) = 4X^7 + 2X^6 + X^5 + X^4 + 4X^2 + 2X + 12$



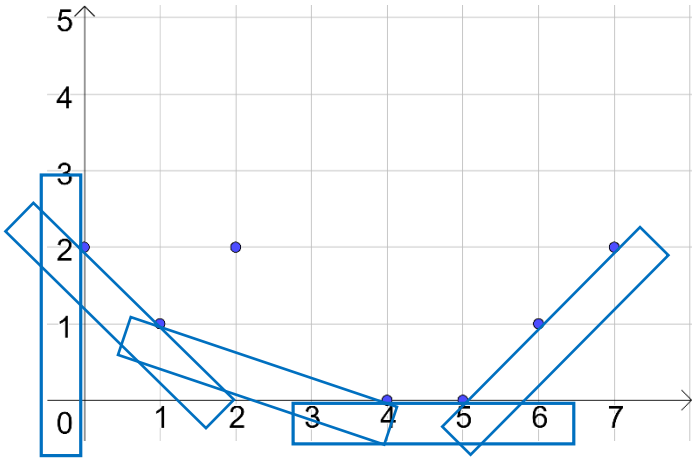
Fonte: Elaborada pelo autor.

A partir de agora, sempre admitiremos que não só o coeficiente líder seja sempre não nulo, mas também o termo constante também não seja zero. Caso contrário, se o termo independente de *X* for nulo, teremos sempre que o polinômio *p(X)* será redutível, o que não nos interessa. Portanto, temos pelo menos dois pontos no plano *OXY*: o ponto básico inicial (em nosso exemplo, (0,2)), que se refere ao termo constante, e o ponto básico final (em nosso exemplo (7,2)), que se refere ao termo do coeficiente líder.

Agora vamos ao trabalho construtivo.

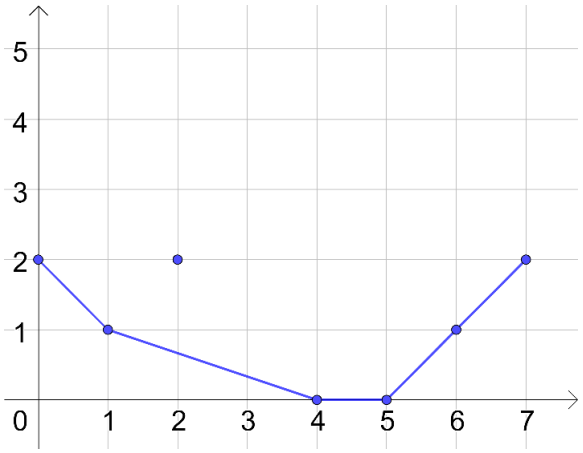
Primeiro, pegue o martelo, e pregue um prego no ponto básico inicial (o (0, 2)) e assim proceda, pregando pregos nos demais pontos até o ponto básico final (o (7, 2)). E com uma régua (grande o suficiente para alinhar o primeiro ao último ponto se necessário) alinhada ao eixo *OY* e fixada no ponto básico inicial, será girada no sentido anti-horário até encontrar outro prego (no nosso exemplo, este será o prego em (1,1)). O segmento reto que une esses dois pontos é o primeiro link do diagrama. Para obter o segundo link, gire a régua agora ao redor do segundo prego até encontrar outro prego, que será o ponto (4, 0). E iterando dessa forma, encontraremos todos os links, conforme o procedimento – com o auxílio de uma régua – de marcar na **Figura 8** e os links marcados na **Figura 9**.

Figura 8 – Processo para obter os links do diagrama de $p(X) = 4X^7 + 2X^6 + X^5 + X^4 + 4X^2 + 2X + 12$



Fonte: Elaborada pelo autor.

Figura 9 – Os links do diagrama de $p(X) = 4X^7 + 2X^6 + X^5 + X^4 + 4X^2 + 2X + 12$



Fonte: Elaborada pelo autor.

Pode acontecer que a régua acerte mais de um "prego" simultaneamente. Neste caso, desenhamos um alongamento sobre todas conexões (pontos). Com isso vimos que traçamos os links um a um até finalmente chegarmos ao ponto básico final e desenhar o último link, como mostrado nas **Figuras 8 e 9**.

Vamos exemplificar mais tal procedimento de obtermos um ***diagrama de Newton*** para um polinômio, porém, não usaremos a ideia de "girar a régua ao redor do prego", substituiremos por "girar a régua sobre o ponto de tangência".

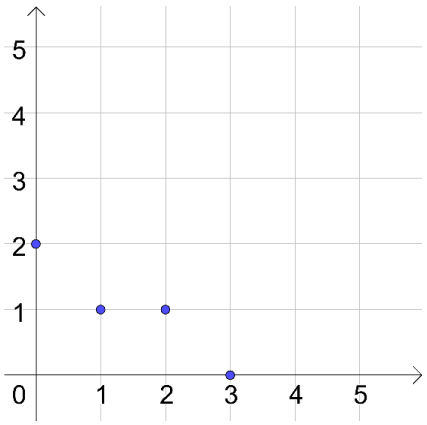
Exemplo 4.3 – *Sendo* $p(X) = X^3 - 6X^2 - 3X - 18$, *vamos construir o diagrama correspondente a tal polinômio.*

Solução: *Para a construção do* ***diagrama*** *de* $p(X)$ *consideremos o primo* $p = 3$, *logo os pontos pertencentes a ele serão: para o coeficiente* $a_0 = -18$, *temos que* $p^2 = 9$ *o divide, assim temos o ponto* $(0, 2)$ *correspondente a tal coeficiente; para o coeficiente* $a_1 = -3$, *temos que* $p^1 = 3$ *o divide, logo temos o ponto* $(1,1)$ *correspondente a ele; para o coeficiente* $a_2 = -8$, *temos que* $p^1 = 3$ *o divide, então o ponto correspondente a ele é* $(2,1)$*; e, para o coeficiente líder,* $a_3 = 1$, *segue que* $p^0 = 1$ *o divide, com isso teremos como ponto corresponde o* $(3,0)$.

Iniciando a construção do ***diagrama*** *de* $p(X)$:

Vamos assinalar os pontos, conforme a **Figura 10**:

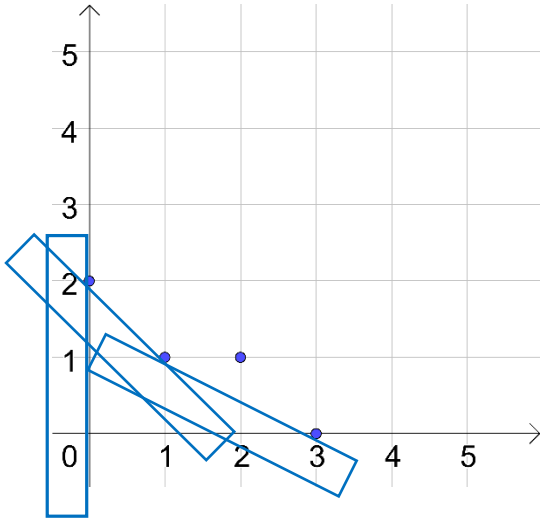
Figura 10 - Os pontos referente ao diagrama do polinômio $p(X) = X^3 - 6X^2 - 3X - 18$



Fonte: Elaborada pelo autor.

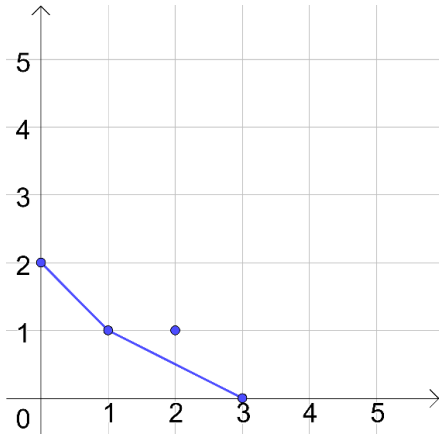
Na figura a seguir, **Figura 11**, *marcamos os links, onde faremos os seguinte procedimentos (nessa ordem): posicionamos uma régua paralela ao eixo Y e tangente ao primeiro ponto,* (*0,2*), *em seguida a giramos no sentido anti-horário até encontrar o próximo ponto* (*1,1*) *e marcamos nosso primeiro link, o seguimento de extremos* (*0,2*) *e* (*1,1*)*; em seguida, posicionamos a régua tangente ao ponto* (*1,1*) *e repetimos o procedimento de girar no sentido anti-horário até encontrar o próximo ponto, que é* (*2,1*) *e marcamos mais um link, o segmento de extremos* (*1,1*) *e* (*2,1*)*; e, em seguida, encerrando o processo de construção dos links, posicionamos agora a régua tangente ao ponto* (*2,1*) *e também giramos no sentido anti-horário até encontrar o ponto* (*3,1*) *e marcamos o último link, o segmento de extremos* (*2,1*) *e* (*3,1*)*. Daí obtemos o* ***diagrama****, exposto na* **Figura 12**, *para o polinômio em questão.*

Figura 11 - Processo para obter os links do diagrama de $p(X) = X^3 - 6X^2 - 3X - 18$



Fonte: Elaborada pelo autor.

Figura 12 - O diagrama de $p(X) = X^3 - 6X^2 - 3X - 18$



Fonte: Elaborada pelo autor.

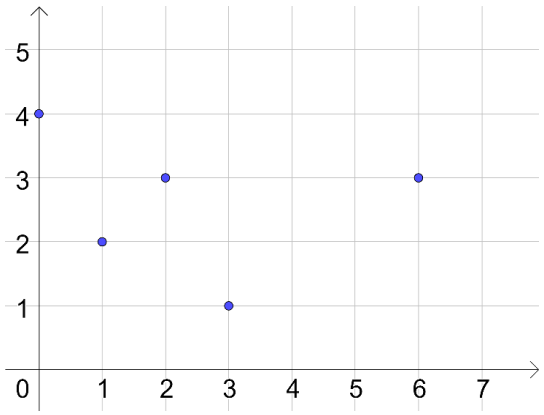
Exemplo 4.4 *– Construa o Diagrama de Newton do polinômio* $p(X) = 8X^6 + 2X^3 + 8X^2 + 4X + 16$ *em relação ao primo p = 2.*

Solução: *Inicialmente vamos determinar os pontos. Começamos pelo coeficiente constante, o* $a_0 = 16$*, onde segue que* p^4 *o divide, logo temos o ponto (0, 4); para o coeficiente* $a_1 = 4$ *temos que* p^2*o divide, logo teremos o ponto (1, 2); para os coeficientes nulos, que são os casos de* a_5 *e* a_4*, não teremos nenhum ponto; para os coeficientes* a_2*,* $a_6 = 8$*, obtemos os pontos (2, 3) e (6, 3), respectivamente, pois* p^3*os divide; já para o coeficiente* $a_3 = 2$*, segue que* p^1 *o divide e teremos o ponto (3, 1).*

Agora vamos à construção do Diagrama de Newton para o polinômio em questão, onde faremos uma sequência de figura para melhor compreensão do processo de construção.

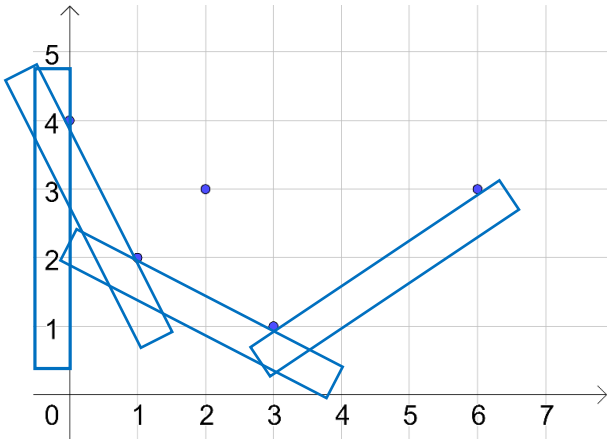
Então, na **Figura 13** *assinalaremos os pontos, na* **Figura 14** *marcaremos os links e, na* **Figura 15** *teremos o Diagrama de Newton em relação ao primo p = 2 para o polinômio* $p(X) = 8X^6 + 2X^3 + 8X^2 + 4X + 16$*.*

Figura 13 – Os pontos referente ao diagrama do polinômio $p(X) = 8X^6 + 2X^3 + 8X^2 + 4X + 16$



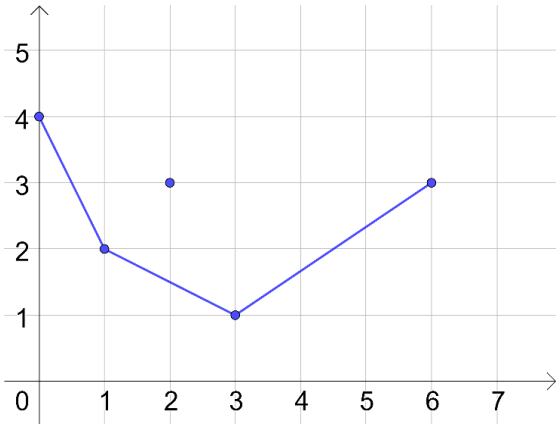
Fonte: Elaborada pelo autor.

Figura 14 – Obtendo os links para o diagrama do polinômio $p(X) = 8X^6 + 2X^3 + 8X^2 + 4X + 16$



Fonte: Elaborada pelo autor.

Figura 15 – O diagrama do polinômio $p(X) = 8X^6 + 2X^3 + 8X^2 + 4X + 16$



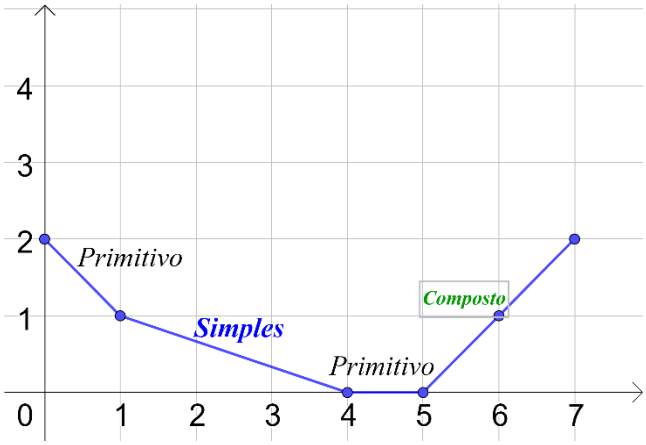
Fonte: Fonte: Elaborada pelo autor.

Podemos observar que alguns dos pontos básicos (como o ponto (2, 3) do exemplo em estudo e, o ponto (2, 1) do ***Exemplo 4.3***) não apareceram no diagrama. Mas isso não deve nos preocupar muito, pois a justificativa é que em qualquer empresa de valor, deve-se esperar um pouco de matéria-prima desperdiçada.

Agora sobre os links. Eles vêm em três categorias: ***Composto***, ***Simples*** e ***Primitivo***.

Um link do diagrama de Newton é ***Simples*** se não contiver pontos inteiros além de seus pontos finais (extremos). Um segmento que contém um ponto inteiro interior é chamado ***Composto***. Um link é dito ***Primitivo*** se sua projeção no eixo horizontal tiver comprimento 1. Para melhor exemplificar, tomemos a **Figura 16** abaixo e o observemos as classificações dos links conforme as categorias apresentadas:

Figura 16 – Classificação dos links em um diagrama de Newton



Fonte: Fonte: Elaborada pelo autor.

Agora concluímos um curso introdutório sobre a linguagem geométrica da representação de um polinômio e o ponta pé para a irredutibilidade, agora podemos começar a falar essa língua. Um resultado importante vindo da irredutibilidade dos polinômios, temos nesse sentido é que para um determinado número primo p, o diagrama de Newton do polinômio $p(X)$ não contém links primitivos, então $p(X)$ não tem raízes racionais.

Considere o polinômio do exemplo a seguir:

Exemplo 4.5 – *Seja a equação polinomial*

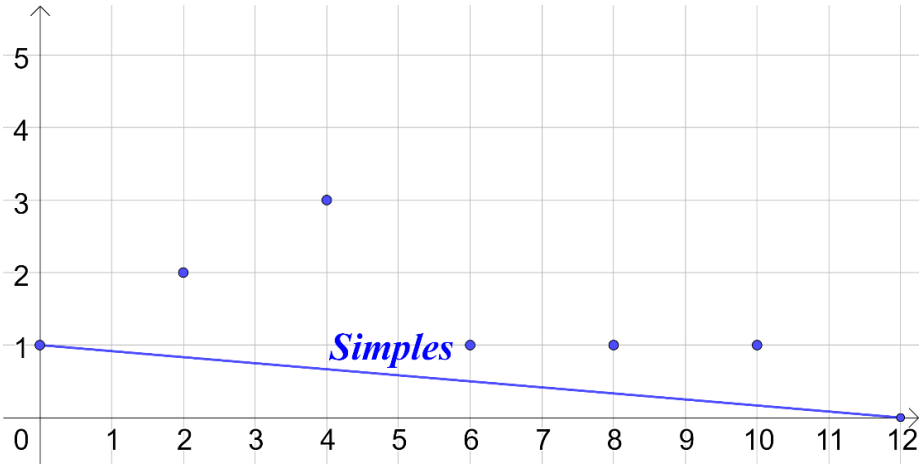
$$X^{12} - 6X^{10} + 15X^8 - 24X^6 + 27X^4 - 18X^2 + 3 = 0,$$

que, pelo exemplo ***Exemplo 2.15****, já sabemos que o mesmo não possui solução racional. Tomemos o polinômio* $p(X) = X^{12} - 6X^{10} + 15X^8 - 24X^6 + 27X^4 - 18X^2 + 3$*, vamos fazer a verificação da irredutibilidade de* $p(X)$ *sobre que* $\mathbb{Q}[X]$ *mediante* ***diagrama de Newton*** *para esse polinômio considerando o primo* $p = 3$*.*

Solução: *Vamos determinar os pontos e, começamos pelo coeficiente constante, o* $a_0 = 3$*, onde segue que* $p^1 = 3$ *o divide, logo temos o ponto (0, 1); para o coeficiente* $a_2 = -18$ *temos que* $p^2 = 9$ *o divide, logo teremos o ponto (2, 2); para o coeficiente* $a_4 = 27$ *temos que é divisível por* $p^3 = 27$*, e obtemos o ponto (4, 3); procedendo de mesmo modo, para os coeficientes* $a_6 = -24$*;* $a_8 = 15$*;* $a_{10} = 6$ *e* $a_{12} = 1$*, obtemos os respectivos pontos: (6, 1), (8, 1), (10, 1) e (12, 0); já os coeficientes* a_1*,* a_3*,* a_5*,* a_7*,* a_9 *e* a_{11} *são todos coeficientes nulos e por isso não produzem pontos.*

Esboçando o ***diagrama*** *para esse polinômio,* **Figura 17***, teremos:*

Figura 17 – Diagrama para o polinômio $p(X) = X^{12} - 6X^{10} + 15X^8 - 24X^6 + 27X^4 - 18X^2 + 3$



Fonte: Fonte: Elaborada pelo autor.

■

Mais adiante, veremos que quando o **diagrama** de um polinômio não possui link(s) primitivo(s) e/ou link(s) composto(s), diremos que $p(X)$ não possui raízes racionais, que será um fator comprobatório, para a irredutibilidade sobre $\mathbb{Q}[X]$.

E, como recompensa por todos os nossos esforços na construção do diagrama de Newton, temos um teorema que apresentaremos na próxima seção.

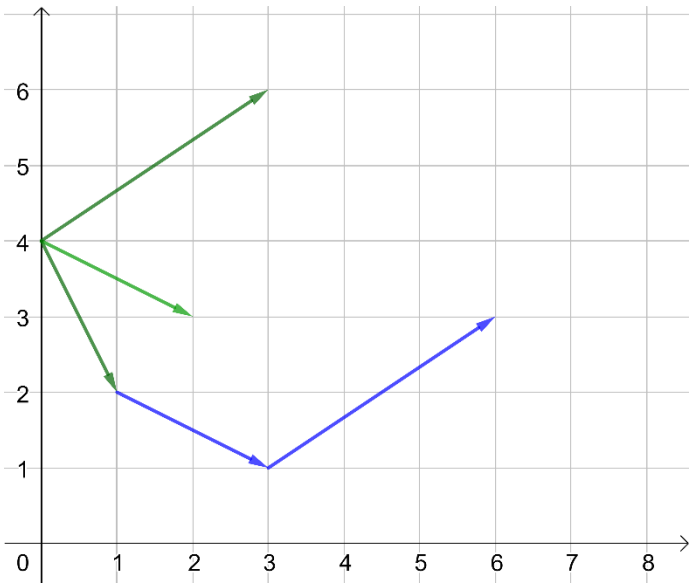
4.2 O Critério de Dumas na identificação de polinômios irredutíveis em $\mathbb{Q}[X]$

Gustave Dumas viveu na Suíça e trabalhou no problema da irredutibilidade no início do século XX. Ele obteve seu critério em 1906. Seu critério quanto à irredutibilidade de polinômios torna possível desenhar, com o auxílio dos diagramas de Newton para polinômios, um retrato do critério de Eisenstein e, portanto, nos ajuda a 67embra-lo e compreendê-lo mais completamente.

Antes de falarmos sobre o ***Critério de Dumas***, trataremos da ideia de ***montagem*** e ***desmontagem*** do ***Diagrama de Newton*** de um polinômio.

Para ***desmontagem***, considere o diagrama, **Figura 15**, do ***Exemplo 4.4***. O copiaremos, de modo que os links fornecidos serão como setas (vetores) com início na extremidade do vetor à esquerda e com extremidade à direita e, reproduzidos (transladados) para o ponto básico inicial (0, 4) (o obtido do coeficiente constante). Vale lembrar que o primeiro link será comum em ambas as situações. Com esse procedimento, construímos o que é denominado de ***pacote do módulo polinomial*** em relação a um número primo *p* dado (setas coloridas de verde). Observe a **Figura 18** a seguir:

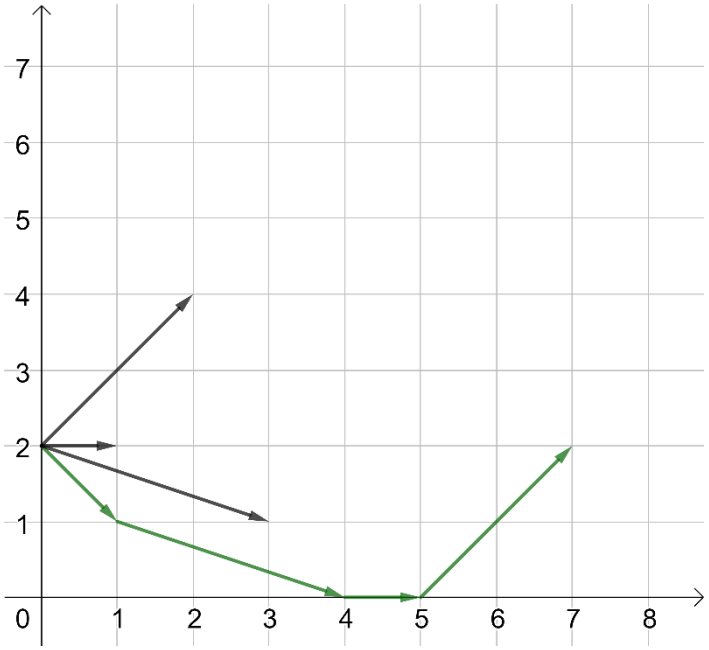
Figura 18 – Montagem e desmontagem do diagrama de Newton para um polinômio do exemplo 4.4



Fonte: Fonte: Elaborada pelo autor.

Agora, para o processo de ***montagem*** a partir de um ***pacote do módulo polinomial*** para um número primo *p*. Segue que, como a ***desmontagem*** e formação de um *pacote* é feita movendo-se os vetores para o ponto básico inicial e no sentido anti-horário de baixo para cima. Basta fazermos tal observação e recolocarmos os vetores do feixe no final um do outro, obedecendo essa ordem. E, daí, obtemos uma linha (a verde), que é o diagrama de Newton de um polinômio (observação de que o primeiro link estará presente tanto na ***desmontagem*** quanto na ***montagem***). Para ilustrar essa ideia, tomaremos o diagrama do polinômio representado na **Figura 9** representando cada link na forma de um vetor, como já vimos, e esboçado na desmontagem da **Figura 19** a seguir:

Figura 19 - Montagem e desmontagem do diagrama de Newton – pacote do módulo polinomial

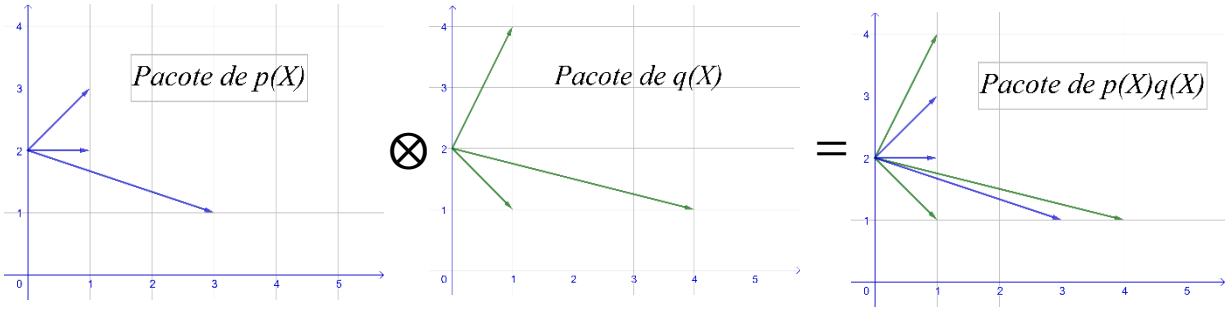


Fonte: Fonte: Elaborada pelo autor.

Vemos que um dado diagrama de Newton corresponde a um pacote único de vetores e, inversamente, o diagrama é recuperado exclusivamente de seu pacote. O teorema a seguir, já idealizado por ***Dumas*** em quem direcionamos nosso estudo sobre polinômios, trata do produto de pacotes de dois polinômios, que nos dá uma ideia, similar ao ***Lema de Gauss***, de irredutibilidade nesse campo de representação geométrica dos polinômios.

Teorema 4.1 (Teorema de Dumas). *O pacote do produto p(X)q(X) de dois polinômios é a união de dois pacotes, o de p(X) e o de q(X). (conforme indica a* **Figura 20***)*

Figura 20 – Produto de pacotes dos módulos polinomiais



Fonte: Oleinikov (1999, com adaptações).

Demonstração:

Sejam os polinômios $p(X) = \sum_{k\geq 0}^{n} a_k X^k$ *e* $q(X) = \sum_{j\geq 0}^{m} b_j X^j$ *e considere o primo p. Suponhamos que para o diagrama de p(X) tenhamos os seguintes pontos: (0,* k_0*), (1,* k_1*), ... (n,* k_n*) e, com eles formemos n links; e, para o diagrama de q(X) tenhamos os seguintes pontos: (0,* j_0*), (1,* j_1*), ... (n,* j_m*) e, com eles formemos m links.*

Temos por definição (ver ***Definição 2.3****) do produto de polinômios a seguinte relação:*

$$p(X) \times q(X) = \sum_{l\geq 0}^{m+n} c_l X^l, \text{ onde } c_l = \sum_{k,j\geq 0}^{k+j=l} (a_k b_j).$$

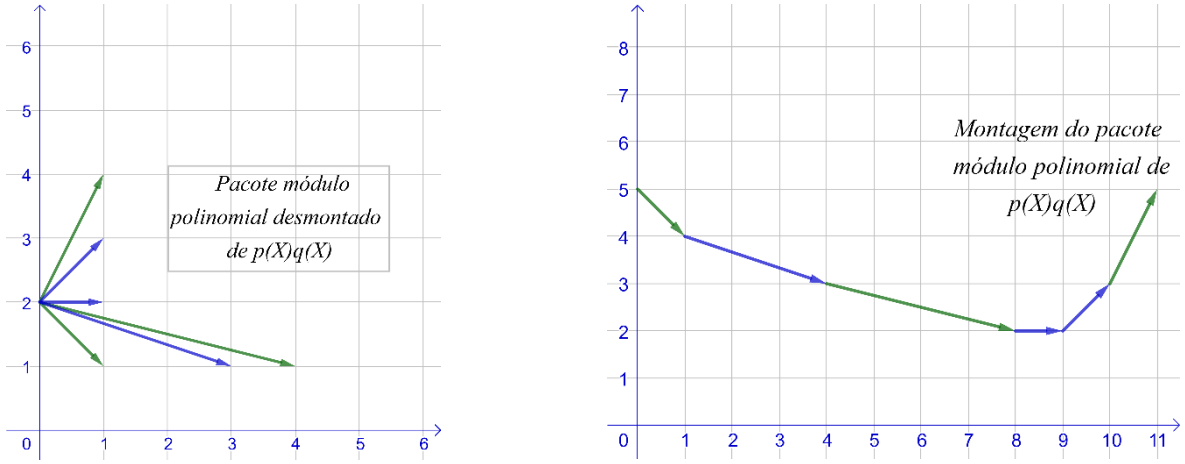
Então, ao efetuar o produto $p(X) \times q(X)$*, para seu diagrama teremos os pontos a seguir: para* $c_0 = a_0 b_0$*, temos que a potência de p que o divide tem expoente* $k_0 + j_0$*, visto que* $p^{k_0} | a_0$ *e* $p^{j_0} | b_0$*, logo obtemos o ponto (0,* l_0*) = (0,* $k_0 + j_0$*); para* $c_1 = a_0 b_1 + a_1 b_0$ *temos que a coordenada* l_1*, do ponto (1,* l_1*), corresponde à maior potência de p que divide a soma, que será a potência de p que divide um dos fatores da soma; e iterando a construção dos pontos, teremos para último ponto (m+n,* l_{m+n}*), relativo ao coeficiente* $c_{n+m} = a_n b_m$*, e que a potência de p que o divide tem por expoente* $k_n + j_m$*, pois por hipótese* $p^{k_n} | a_n$ *e* $p^{j_m} | b_m$*.*

Portanto, após a obtenção de todos os pontos do produto $p(X) \times q(X)$*, são eles: (0,* l_0*), (1,* l_1*), ..., (m+n,* l_{m+n}*); podemos formar m+n links, isto é, a soma dos links de p(X) e q(X). O que prova o teorema.*

■

A montagem do diagrama a partir do *pacote de p*(*X*)*q*(*X*), conforme **Figura 20**, é dada, como já especificamos, recolocando os vetores do feixe (**Figura 21**, *Pacote de p(X)q(X)*) no final um do outro (**Figura 21**, *Montagem do pacote módulo polinomial de p(X)q(X)*), no sentido anti-horário e obedecendo a ordem em que se encontram os vetores. Vejamos:

Figura 21 – Desmontagem e montagem do pacote módulo polinomial



Fonte: Elaborada pelo autor.

Algumas considerações: a primeira é que, para o pacote módulo polinomial montado (Imagem à direita, **Figura 21**) podemos transladá-la verticalmente de modo que o vetor de pontos inicial (8,2) e final (9,2), por exemplo, fique sobre o eixo horizontal, bastando dividir o polinômio *p*(*X*)*q*(*X*) por r^2, supondo que o diagrama tenha sido construído em relação ao primo *r*; a segunda observação é que existindo vetores que coincidam total ou parcialmente, os mesmos, devem ser colocados um após o outro.

Teorema 4.2 (Critério de Dumas). *Se, para algum número primo p, o diagrama do polinômio p*(*X*) *consiste exatamente em um link simples, o polinômio é irredutível.*

Demonstração:

Seja o polinômio $f(X)=\sum_{k=0}^{n} a_k X^k$ *nos racionais.*

Consideremos que o diagrama de Newton para f(X), em relação a um número primo p, seja apenas um link simples e, suponhamos por contradição, que f(X) seja redutível sobre os racionais, isto é, existe r ∈ ℚ, tal que f(r) = 0.

Então, pelo ***Teorema 2.2****, como r é uma raiz de f(X), segue, como consequência, que podemos escrever f(X) como*

$$f(X) = (X - r)\, q(X),$$

em que q(X) ∈ ℚ[X]\{ℚ} é o quociente da divisão.

Mas, pelo ***Teorema 4.1****, temos que o pacote módulo polinomial de f(X) é a união dos pacotes módulo polinomiais de (X – r) e de q(X), ou seja, no diagrama de Newton para f(X), em relação ao primo p, estão os links de (X – r) e de q(X). No entanto, no diagrama de Newton para (X – r), em relação ao primo p, consta apenas um link primitivo; e, no diagrama de Newton para q(X), em relação ao primo p, consta um ou mais links. Logo, nessas condições, o diagrama de Newton para f(X), em relação a um número primo p, não será de apenas um link simples, o que contradiz a hipótese.*

Portanto, se para algum número primo p, o diagrama de um polinômio p(X) consistir em exatamente um link simples, o polinômio é irredutível.

■

Exemplo 4.6 *– Verifique se o polinômio* $k(X) = X^5 + 7X^4 + 16X^3 + 8X^2 - 16X - 16$ *é irredutível sobre ℚ[X].*

Solução: *Ora, não podemos aplicar o* ***Critério de Eisenstein*** *visto não termos como escolher um primo p tal que cumpra todos os requisitos como diz tal critério.*

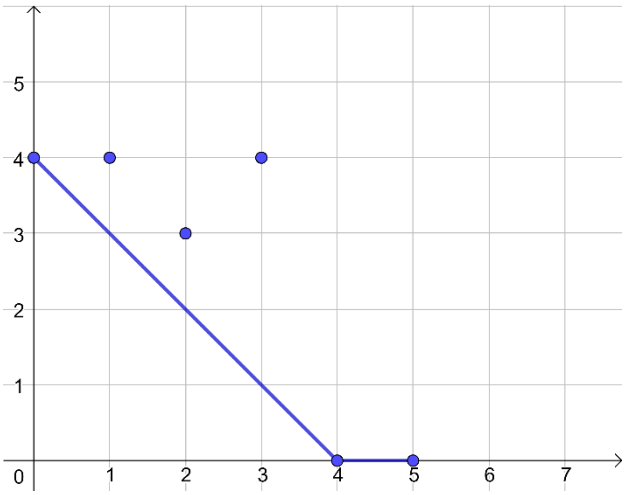
Então uma maneira de solucionar, porém, enfadonha, seria testar todas as possíveis raízes racionais de k(X), isto é, aplicarmos a ideia do ***Teorema 2.4****, avaliarmos se pelo menos algum dos racionais – ± 1, ± 2, ± 4, ± 8, ± 16 – é raiz do polinômio em questão. Mas, nesse sentido, nos pouparemos desse trabalho, o qual faremos se verdadeiramente soubermos se o mesmo é redutível ou não, que para afirmarmos esboçaremos o* ***diagrama*** *de k(X) e analisaremos sobre a óptica do* ***Critério de Dumas****.*

Os pontos correspondentes à k(X) em relação ao primo p = 2 são: pelo coeficiente constante, o $a_0 = -16$*, como* $p^4 = 16$ *o divide, logo temos o ponto (0, 4); para o coeficiente*

$a_1 = -16$ *temos que* $p^4 = 16$ *o divide, logo teremos o ponto (1, 4); para o coeficiente* $a_2 = 8$ *obtemos o ponto (2, 3); para o coeficiente* $a_3 = 16$*, temos o ponto (3, 4); já para os coeficientes* a_4 *e* a_5*não são divisíveis por nenhuma potência de p, exceto* p^0*, então teremos, respectivamente, os pontos (4, 0) e (5, 0).*

Agora, esboçando o ***diagrama*** *correspondente a k*(*X*),

Figura 22 – Diagrama de Newton para o polinômio $k(X) = X^5 + 7X^4 + 16X^3 + 8X^2 - 16X - 16$



Fonte: Fonte: Elaborada pelo autor.

Como no diagrama de k(*X*) *não temos apenas um link simples conforme* ***Critério de Dumas****, logo o polinômio não é irredutível sobre* $\mathbb{Q}[X]$*. De fato, sua forma fatorada, após testarmos suas raízes racionais, é k*(*X*) *=* $(X+2)^4(X-1)$*.*

Vejamos alguns outros exemplos que comprovam a eficácia das concepções dadas por ***Dumas*** quanto a irredutibilidade de polinômios e, supostamente, uma ideia da existência de números irracionais.

Exemplo 4.7 (Critério de Eisenstein) *Seja* $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ *um polinômio com coeficientes inteiros tais que, para um p primo, o coeficiente líder não seja divisível por p, e os demais coeficientes são divisíveis por p e o coeficiente constante não é divisível por* p^2*. Então f é irredutível.*

Solução: *O diagrama de Newton para o polinômio f*(*X*) *consiste de apenas um link simples, onde os pontos centrais, correspondentes aos outros coeficientes não formaram links – não havendo pontos de coordenadas inteiras –, excetuando o líder e o independente da variável,*

isto é, consiste de um segmento de extremos (0, 1) e (n, 0), respectivamente, pontos inicial e final do segmento.

Portanto, pelo ***Critério de Dumas****, o polinômio f(X) é irredutível.*

■

Exemplo 4.8 *- Seja p um primo, (c, p) = 1 e (m, n) = 1. Então o polinômio* $X^n + cY^m$ *é irredutível.*

Solução: *O diagrama de Newton para o polinômio considerado, em relação ao primo p, é um segmento com os pontos finais (0, m) e (n, 0). Como (m, n) = 1, não há pontos com coordenadas inteiras dentro deste segmento.*

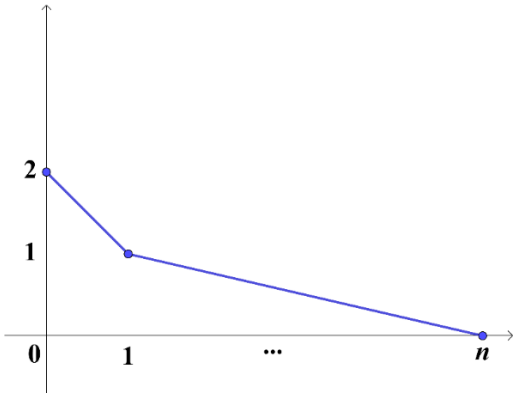
Portanto, pelo ***Critério de Dumas****, o polinômio é irredutível.*

■

Exemplo 4.9 *– Sejam p um primo e o polinômio* $w(X) = aX^n + pX + bp^2$*, onde* $(b, p) = 1$*, p não divide a e* $p(X)$ *não possui raízes inteiras, então o polinômio é irredutível.*

Solução: *Ao construir o diagrama de Newton para w tomando o primo p, temos que o mesmo consiste da união do segmento com os pontos finais (0, 2) e (1, 1) e do segmento com os pontos finais (1, 1) e (n, 0), que dentro desses segmentos, não há pontos com coordenadas inteiras. Portanto, a fatoração não trivial de w sobre* $\mathbb{Z}$ *(*$\mathbb{Q}$*) pode consistir apenas em um fator linear e um fator de grau "n – 1"; como podemos observar no diagrama abaixo,* **Figura 23***:*

Figura 23 – Diagrama de Newton para o polinômio $w(X) = aX^n + pX + bp^2$



Fonte: Elaborada pelo autor.

Portanto, é irredutível.

■

Exemplo 4.10 *– Prove que tg10º é irracional.*

Solução: *Temos pela identidade de arco duplo, que*

$$tg30° = tg(10° + 20°) = \frac{tg10° + tg20°}{1 - tg10° \cdot tg20°}. \quad (1)$$

Como,

$$tg20° = tg(10° + 10°) = \frac{2tg10°}{1 - tg^2 10°}. \quad (2)$$

Segue, substituindo o resultado em (*2*) *em* (*1*)*, que*

$$tg30° = \frac{tg10° + \frac{2tg10°}{1 - tg^2 10°}}{1 - tg10° \cdot \frac{2tg10°}{1 - tg^2 10°}} = \frac{-tg^3 10° + 3tg10°}{-3tg^2 10° + 1}. \quad (3)$$

Porém, $tg30° = \frac{\sqrt{3}}{3}$ *e fazendo* $tg10° = X$*, segue de* (*3*) *que*

$$\frac{-X^3 + 3X}{-3X^2 + 1} = \frac{\sqrt{3}}{3},$$

e elevando ao quadrado ambos os lados da igualdade, obteremos que

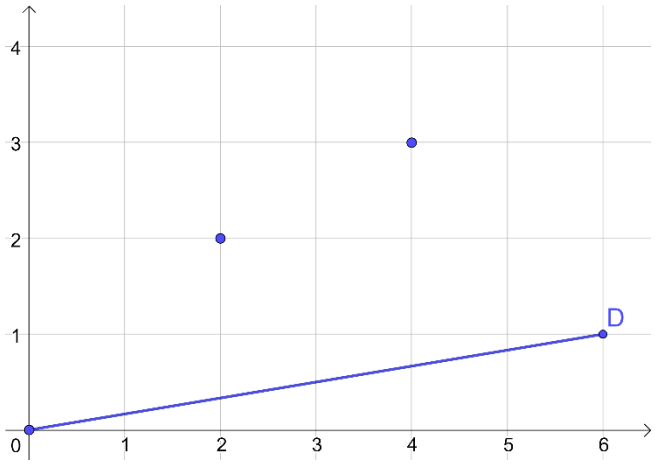
$$\left(\frac{-X^3 + 3X}{-3X^2 + 1}\right)^2 = \frac{1}{3},$$

em que, desenvolvendo chegamos à equação polinômio

$$3X^6 - 27X^4 + 36X^2 - 1 = 0. \quad (4)$$

Assim, avaliar que a equação em (*4*) *tem solução racional é equivalente verificar se o polinômio* $p(X) = 3X^6 - 27X^4 + 36X^2 - 1$ *é redutível sobre os racionais. Daí, antes de testarmos as possíveis raízes racionais, faremos o* ***diagrama de Newton*** *para tal polinômio,* **Figura 24***, tomando o primo p = 3 e, em seguida, o analisaremos à luz do* ***Critério de Dumas****.*

Figura 24 – Diagrama de Newton para o polinômio $p(X) = 3X^6 – 27X^4 + 36X^2 – 1$



Fonte: Elaborada pelo autor.

Note pela **Figura 24**, *que o diagrama do polinômio só consiste de um link simples, então, pelo* ***Critério de Dumas***, *segue que o polinômio* $p(X)$ *é irredutível sobre os racionais, que é equivalente a dizer que a equação em* (4) *não possui soluções racionais.*

Portanto, segue que, de fato, $tg10^o$ *é irracional.*

Exemplo 4.11 **(OCM-2000 - Modificada)** – *Sejam a, b, c e d as raízes (nos complexos) do polinômio* $X^4+6X^2+4X + 3$. *Encontre um polinômio* $p(X)$, *do quarto grau, que tenha como raízes* a^2, b^2, c^2 *e* d^2, *e mostre que tal polinômio não possui raízes racionais.*

Solução: *Seja* $f(X) = X^4+6X^2+4X + 3$. *Como a, b, c e d são raízes de* $f(X)$, *então*

$$f(X) = X^4+6X^2+4X + 3 = (X – a)(X – b)(X – c)(X – d).$$

O polinômio a determinar é tal que

$$p(X) = (X – a^2)(X – b^2)(X – c^2)(X – d^2).$$

Agora, tomando $X = Y^2$, *teremos que:*

$$p(Y^2) = (Y^2 – a^2)(Y^2 – b^2)(Y^2 – c^2)(Y^2 – d^2)$$

$$= (Y + a)(Y - a)(Y + b)(Y - b)(Y + c)(Y - c)(Y + d)(Y - d)$$

$$= (Y + a)(Y + b)(Y + c)(Y + d)(Y - a)(Y - b)(Y - c)(Y - d)$$

$$= (Y + a)(Y + b)(Y + c)(Y + d)(-Y + a)(-Y + b)(-Y + c)(-Y + d)$$

$$= p(Y)\,p(-Y)$$

$$= (Y^4+6Y^2+4Y+3)(Y^4+6Y^2-4Y+3)$$

$$= Y^8 + 12Y^6 + 42Y^4 + 20Y^2 + 9.$$

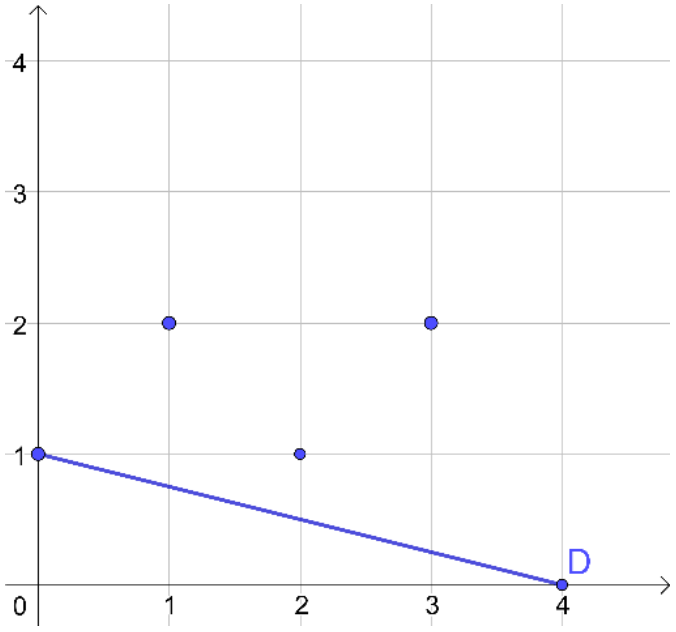
Logo, $p(Y^2) = Y^8 + 12Y^6 + 42Y^4 + 20Y^2 + 9$. *E como, para cada* $X \in \mathbb{C}$ *existe* $Y \in \mathbb{C}$, *tal que* $X = Y^2$, *então, teremos que*

$$p(X) = p(Y^2) = Y^8 + 12Y^6 + 42Y^4 + 20Y^2 + 9 = X^4 + 12X^3 + 42X^2 + 20X + 9.$$

Portanto, o polinômio procurado é $p(X) = X^4 + 12X^3 + 42X^2 + 20X + 9$.

Agora mostraremos que nenhuma das raízes de $p(X)$ *é racional. Poderíamos testar as possíveis raízes racionais de tal polinômio, mas seria um processo demorado e sem garantia de êxito, e o* ***critério de Eisenstein*** *não é possível aplicar. Então, para mostrar a irracionalidade das raízes, consideremos o diagrama de tal polinômio para um primo* $p = 2$ *esboçado na* **Figura 25:**

Figura 25 – Diagrama de Newton para o polinômio $p(X) = X^4 + 12X^3 + 42X^2 + 20X + 9$



Fonte: Elaborada pelo autor.

Portanto, como o ***diagrama*** *de* $p(X)$ *consiste de apenas um link simples, pelo* ***critério de Dumas****, segue que o mesmo não possui raiz racional.*

Nessa contextualização, a geometrização dos polinômios idealizada por ***Newton*** e a fantástica aplicação dos argumentos de ***Dumas*** dadas em seu critério sobre irredutibilidade, nos aparelha de forma a apresentar demonstrações mais simplificadas de problemas, como fizemos para o ***Critério de Eisenstein*** no ***Exemplo 4.7*** e a demonstração que ***tg10° é irracional***, ou até mesmo solucionar outros que outrora ainda eram enigmáticos, como é o caso do ***Exemplo 4.11***.

5 CONCLUSÃO

Após muitos anos entre a ideia primitiva de números e os conceitos atuais, em que se permeou por fracassos e sucessos em conjecturar-se ideias mais gerais, foram sem dúvida os gregos, com sua geometria e aritmética, que deram um alinhamento inicial por meio da contagem e das construções geométricas aos números.

A partir desse cenário, durante muitos anos buscou-se um procedimento mais geral para averiguação da racionalidade de certos números, ou equivalentemente, sua irracionalidade, mas estudar caso a caso tornou-se cansativo e desanimador. E foi diante desse contexto que coube aos polinômios, especificamente ao estudo de suas raízes, solucionar esse problema.

Assim, vários matemáticos pelo mundo incumbiram-se dessa missão, de estudar as raízes de polinômios, em especial para nós as raízes racionais para polinômios com coeficientes inteiros. E novo foco passou a existir, a irredutibilidade desses polinômios. Surgindo daí alguns critérios, dentre eles e objetos de nosso estudo – Teorema das Raízes Racionais, Critério de Eisenstein e Critério de Dumas.

O Teoremas das Raízes Racionais, certamente é determinante, pois se houver alguma raiz racional, a mesma terá a forma explicitada no teorema, e se caso exista, tal polinômio é redutível. Porém, é um desprendimento de tempo valioso em se testar as possíveis candidatas a raiz racional e mesmo assim nenhuma delas contemplar essa condição.

Então, fez-se e é de grande serventia, o surgimento de critérios de observação prévia se tal polinômio possui ou não raiz racional, e se a resposta for positiva, vale a pena encontrá-la utilizando-se a ideia do Teorema das Raízes Racionais. Caso contrário, as raízes reais de tal polinômio serão irracionais.

Com isso, estudaram-se dois critérios importantíssimos – de Eisenstein e de Dumas. Ambos se alicerçam na escolha de um certo número primo para iniciar a sondagem sobre a existência de raízes racionais em polinômios com coeficientes inteiros.

A aplicação do Critério de Eisenstein é mais simples, fazendo-se apenas a observação de certas divisibilidades dos coeficientes do polinômio em relação ao número primo escolhido. Contudo, a não abrangência a certos polinômios, como os Ciclotômicos, a tornou uma ferramenta menos eficiente.

No entanto, diante do exposto na nossa pesquisa afirmamos sem titubear, que o Critério de Dumas foi um avanço significativo no estudo das raízes de um polinômio com coeficientes inteiros – com a possibilidade de sua redutibilidade – e na conquista de possíveis novos números irracionais, na hipótese de irredutibilidade, que baseia-se de uma ideia de Newton na representação geométrica de polinômio, tal critério avalia a existência de raiz racional na construção geométrica do polinômio, cuja representação é obtida por meio de pontos em que as coordenadas de cada ponto obedecem a critérios de divisibilidades dos coeficientes em relação às potências do primo p escolhido.

REFERÊNCIAS

AABOE, Asger. **Episódios da História Antiga da Matemática**. Tradução de João Bosco Pitombeira de Carvalho. Rio de Janeiro: Editora S.B.M., 2002.

BASTOS, Gervasio Gurgel. **Notas de Álgebra**. Fortaleza: Edições Livro Técnico, 2002.

BOYER, Carl Benjamin. **História da Matemática**. São Paulo: Edgard Blucher, 1986.

CAMINHA, A. **Tópicos de Matemática Elementar, Volume 6**: Polinômios. Rio de Janeiro: Editora S.B.M., 2012.

CAMINHA, A. **Tópicos de Matemática Elementar, Volume 5**: Números Reais. 2. ed. Rio de Janeiro: Editora S.B.M., 2014.

EVES, Howard. **Introdução à História da Matemática**. Campinas: Editora UNICAMP, 2008.

GARBI, Gilberto G. **O romance das equações algébricas:** A História da Álgebra. 2. ed. - São Paulo: Makron Books, 2007.

GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de Álgebra**. Rio de Janeiro: IMPA, 2002. (Coleção Projeto Euclides).

GONÇALVES, Adilson. **Introdução à Álgebra**. Rio de Janeiro: IMPA, 1979. (Coleção Projeto Euclides).

HEFEZ, Abramo; VILELA, Maria L. T.. **Polinômios e Equações Algébricas**. Rio de Janeiro: Editora S.B.M., 2018. (Coleção PROFMAT).

HEFEZ, Abramo. **Aritmética**. 2. ed. - Rio de Janeiro: Editora S.B.M., 2016. (Coleção PROFMAT).

HEFEZ, Abramo. **Curso de Álgebra, volume 1**. 5. ed. - Rio de Janeiro: IMPA, 2016. (Coleção Matemática Universitária).

IFRAH, Georges. **Os números:** a história de uma grande invenção. 4. ed. – Rio de Janeiro: Editora Globo, 1989.

LIMA, Elon Lages. **Curso de Análise, volume 1**. Rio de Janeiro: IMPA, 1976. (Coleção Projeto Euclides).

LIMA, Elon Lages. **Números e Funções Reais.** 1. ed. - Rio de Janeiro: IMPA, 2017. (Coleção PROFMAT).

MARQUES, Diego. **Teoria dos Números Transcendentes**. Rio de Janeiro: Editora S.B.M., 2013. (Coleção Textos Universitários).

NETO, Aref A.; SAMPAIO, José L. P.; LAPA, Nilton; CAVALLANTTE, Sidney L. **Noções de Matemática, Volume 7**: Números Complexos e Polinômios. 1. ed. – Fortaleza: Editora Vestseller, 2011.

NIVEN, Ivan. **Números:** Racionais e Irracionais. Tradução de Renate Watanabe. Rio de Janeiro: Editora S.B.M., 2012. (Coleção Iniciação Científica).

OLEINIKOV, V. A. Irredutibility and Irrationality. *In*: Serge Tabachnikov (ed.). **Kvant selecta**: Algebra and analysis, II. Providence, R.I.: American Mathematical Society, c1999. (Mathematical Word, v. 15)

PRASOLOV, Victor V. **Polynomials**. Translated from the Russian by Dimitry Leites. 2nd ed. New York: Springer, 2001. Título original: Mnogochleny.

APÊNDICE A - ANÉIS, DOMÍNIO DE INTEGRIDADE E CORPO

Nos capítulos desse trabalho usamos algumas vezes certos termos da Álgebra, como os que estão citados no título desse apêndice, que em determinados momentos se fazem necessários citá-los. Agora, em momento oportuno, iremos defini-los nessa seção.

Vejamos tais definições baseados em (GONÇALVES, A., HEFEZ, A. e LEQUAIN, I.):

Antes de qualquer coisa, seja $\mathbb{B}$ um conjunto não vazio, em que a representação do produto cartesiano de *B* por ele próprio será denotado por $\mathbb{B} \times \mathbb{B}$. E uma operação $(*)$ em $\mathbb{B}$ é definida como uma função, isto é:

$$\begin{array}{rccc} * : & \mathbb{B} \times \mathbb{B} & \to & \mathbb{B} \\ & (k, w) & \mapsto & k * w \end{array}$$

Sejam duas operações, uma denominada de *adição* (denotada por +) e a outra denominada de *multiplicação* (denotada por •). Logo temos as seguintes definições:

Definição 6.1 – *Diremos que* $(\mathbb{B}, +, \bullet)$ *é um* ***anel comutativo*** *se as seguintes propriedades são satisfeitas para quaisquer* $k, w, t \in \mathbb{B}$.

P1) Associatividade das operações de adição e de multiplicação, respectivamente, isto é,

$$k + (w + t) = (k + w) + tek \bullet (w \bullet t) = (k \bullet w) \bullet t$$

P2) Comutatividade das operações de adição e de multiplicação, respectivamente, isto é,

$$k + w = w + kek \bullet w = w \bullet k$$

P3) Existe um único elemento neutro em relação à adição e um único elemento neutro em relação à multiplicação, respectivamente, isto é,

$$\exists 0 \in \mathbb{B}, tal\ que,\ para\ todo\ b \in \mathbb{B},\ tem\text{-}se\ que\ 0 + b = b\ e\ b + 0 = b$$

$$e$$

$$\exists 1 \in \mathbb{B},\ 0 \neq 1,\quad tal\ que,\ para\ todo\ b \in \mathbb{B},\ tem\text{-}se\ que\ 1 \bullet b = b\ e\ b \bullet 1 = b$$

P4) Distributividade da multiplicação em relação à adição, isto é,

$$k \bullet (w + t) = k \bullet w + k \bullet t \textit{(distributiva à esquerda)}$$

e

$$(w + t) \bullet k = w \bullet k + t \bullet k \textit{(distributiva à direita)}$$

Podemos concluir da definição acima que se todas as quatro propriedades forem satisfeitas, exceto à *P2*, então *(*$\mathbb{B}$*, +, •)* será chamado de ***anel não-comutativo***.

Por outro lado, um ***anel*** que que satisfizer a definição a seguir será denominado de ***corpo***, nesse sentido dizemos que todo elemento não nulo de um ***corpo*** possui um inverso.

Definição 6.2 – *Diremos que um **anel comutativo** é um **corpo** se ele satisfizer a propriedade a seguir:*

P5) Todo $b \in \mathbb{B}$*, com* $b \neq 0$*, existe* $\exists b' \in \mathbb{B}$*, tal que* $b \bullet b' = 1$*.*

Agora definiremos ***domínio de integridade***.

Definição 6.3 – *Um anel comutativo (*$\mathbb{B}$*, +, •) é dito **domínio de integridade** se ele satisfizer a seguinte propriedade:*

P6) Para todo $k,w \in \mathbb{B}$*, com* $k \bullet w = 0$*, então* $k = 0$ *ou* $w = 0$*.*

Pela definição imediatamente acima, dizemos que um ***domínio de integridade*** é um ***anel comutativo*** com unidade e que não possui divisores de zero.

De modo a facilitar a compreensão, quando não ocasionar ambiguidade, denotaremos $a \bullet b$ *por ab e,* b' em *P6* apenas por b^{-1} ou por $\frac{1}{b}$.

Uma observação importante, relacionado à **Definição 4.3**, enunciaremos no teorema seguir:

Teorema 6.1 (Lei do Corte) – *Seja* $\mathbb{B}$ *um* ***corpo*** *e* $b \in \mathbb{B}$ *um elemento não nulo. Então, dados* $a, c \in \mathbb{B}$*, segue-se que:*

$$ab = cb \Rightarrow a = c \quad (1)$$

Demonstração:

Ora, como $\mathbb{B}$ *é um* ***corpo*** *e* $b \neq 0$*, logo existe um* $b^{-1} \in \mathbb{B}$*, tal que* $bb^{-1} = 1$*. Daí, multiplicando à esquerda ambos os lados por* b^{-1}*, teremos que*

$$abb^{-1} = cbb^{-1} \overset{P6}{\Rightarrow} a1 = c1 \overset{P3}{\Rightarrow} a = c$$

Portanto, sob as condições dadas, a equação (1) é válida.

■

Assim, nos sentimos motivados para mais duas definições, onde definiremos ***subanel*** e ***subcorpo***.

Definição 6.4 – *Um subconjunto não vazio* $\mathbb{A}$ *de um anel* $\mathbb{B}$ *será dito um subanel de* $\mathbb{B}$ *se, com as operações de adição e multiplicação em* $\mathbb{B}$*, ainda continuar sendo um anel.*

De modo a reduzir a demonstração se um dado subconjunto é um ***subanel*** enunciaremos a proposição à seguir que nos dará esse alento. Mas vale notar que: *-b* é o simétrico de *b* em $\mathbb{A}$.

Proposição 6.1 – *Dado o anel* $(\mathbb{A}, +, \cdot)$ *e seja* $\mathbb{B}$ *um subconjunto não vazio de* $\mathbb{A}$*. São equivalentes:*

(i) $\mathbb{B}$ *é subanel de* $\mathbb{A}$*;*

(ii) $a, b \in \mathbb{B}$*, então* $a - b \in \mathbb{B}$ *e* $ab \in \mathbb{B}$*.*

Prova:

(i) $\Rightarrow$ *(ii). Como* $\mathbb{B}$ *é um subanel, então, por definição,* $\mathbb{B}$ *é um anel. Assim, se dados* $a,b \in \mathbb{B}$ *temos que* $-b \in \mathbb{B}$*, daí segue que* $a - b \in \mathbb{B}$ *e* $ab \in \mathbb{B}$*.*

(ii) ⇒ (i). Por hipótese, temos que a multiplicação é fechada em $\mathbb{B}$*. E, além disso, por definição, que as propriedades P1 e P2 são válidas em* $\mathbb{B}$*. Logo devemos mostrar que a adição é fechada em* $\mathbb{B}$ *e que,* $\mathbb{B}$ *possui elemento neutro e elemento simétrico da adição. De fato,*

(1) O elemento neutro da adição.

Como $\emptyset \neq \mathbb{B} \subseteq \mathbb{A}$*, logo podemos tomar* $b \in \mathbb{B}$*, que por hipótese* $0 = b - b \in \mathbb{B}$*, que é o elemento neutro para adição em* $\mathbb{A}$*. Portanto,* $\mathbb{B}$ *possui elemento neutro para adição.*

(2) Elemento simétrico.

Ora, por (1), dados $0, b \in \mathbb{B}$*, temos por hipótese que* $0 - b \in \mathbb{B} \subseteq \mathbb{A}$*, isto é,* $-b \in \mathbb{B} \subseteq \mathbb{A}$ *. Desde que -b seja o simétrico de b em* $\mathbb{A}$*, o que implicará em -b ser o simétrico de b em* $\mathbb{B}$*.*

Agora, mostraremos que a Adição é fechada em $\mathbb{B}$*, isto é, dados* $a,b \in \mathbb{B}$ *teremos que* $a + b \in \mathbb{B}$*. De fato, como por (2), dados* $a,b \in \mathbb{B}$ *temos que* $-b \in \mathbb{B}$*, então por hipótese segue que* $a - (-b) = a + b \in \mathbb{B}$*. Portanto garantimos que a Adição é fechada em* $\mathbb{B}$*.*

■

Exemplo 6.1 *– Assim, com as operações usuais:* $(\mathbb{Z}, +, \cdot)$ *é subanel de* $(\mathbb{Q}, +, \cdot)$ *e* $(\mathbb{Q}, +, \cdot)$ *é subanel de* $(\mathbb{R}, +, \cdot)$*.*

Exemplo 6.2 *– O anel* $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p},\ a, b, p \in \mathbb{Z} \text{ e } p \geq 2 \text{ primo}\}$*, chamado de anel* $\mathbb{Z}$ *adjunção* $\sqrt{p}$*, é um subanel de* $\mathbb{Q}[\sqrt{p}] = = \{a + b\sqrt{p},\ a, b, p \in \mathbb{Q} \text{ e } p \geq 2 \text{ primo}\}$ *e, por sua vez ambos são subanéis de* $\mathbb{R}$*.*

Definição 6.5 *– Um subconjunto não vazio L de um corpo K será chamado de subcorpo de K se, com as operações de adição e multiplicação de K, ainda continuar sendo um corpo.*

Exemplo 6.3 *– No corpo das frações, temos que o conjunto dos números racionais Q* $= \left\{{}^{a}/_{b}\,; a \text{ e } b \text{ são números inteiros e } b \neq 0\right\}$ *munido das operações:*

$$Adição\ (+)\colon \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{e} \qquad Multiplicação\ (\cdot)\colon \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

é um corpo das frações nos inteiros.

Demonstração:

De fato, o conjunto dos números racionais é um corpo. Sejam $^{a}/_{b}, ^{c}/_{d}, ^{e}/_{f} \in Q$, *observemos que os racionais gozam das seguintes propriedades:*

P1) Associatividade das operações de adição e de multiplicação, respectivamente, isto é,

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{adf+bcf+bde}{bdf}=\frac{adf+b(cf+de)}{bdf}$$
$$=\frac{adf}{bdf}+\frac{b(cf+de)}{bdf}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)$$

e,

$$\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f}=\frac{ac}{bd}\cdot\frac{e}{f}=\frac{ace}{bdf}=\frac{a}{b}\cdot\frac{ce}{df}=\frac{a}{b}\cdot\left(\frac{c}{d}\cdot\frac{e}{f}\right).$$

P2) Comutatividade das operações de adição e de multiplicação, respectivamente, isto é,

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}\underset{1}{=}\frac{bc+ad}{bd}=\frac{bc}{bd}+\frac{ad}{bd}=\frac{c}{d}+\frac{a}{b}$$

e,

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}\underset{2}{=}\frac{c}{d}\cdot\frac{a}{b}.$$

Note que as igualdades 1 e 2 são válidas pois os inteiros gozam da comutatividade na adição e multiplicação, respectivamente.

P3) Existe um único elemento neutro em relação à adição e um único elemento neutro em relação à multiplicação, respectivamente, isto é,

$\exists 0 \in Q$, *pois basta tomarmos* $^{0}/_{b} = 0$ *tal que, para todo* $^{a}/_{b} \in Q$, *tem-se que*

$$0+{}^{a}/_{b}={}^{0}/_{b}+{}^{a}/_{b}={}^{(0b+ab)}/_{bb}={}^{ab}/_{bb}={}^{a}/_{b}$$

e

$\exists 1 \in Q$, *bastando tomarmos* $^{b}/_{b}=1$, *de modo que, para todo* $^{a}/_{b} \in Q$, *tem-se que*

$$1\bullet\ {}^{a}/_{b} = {}^{a}/_{b}\ e\ {}^{a}/_{b}\bullet\ 1 = {}^{a}/_{b}$$

Quanto a unicidade do elemento neutro em relação à adição, podemos supor a existência de dois elementos neutros, 0 e 0', daí segue que

$$\frac{0}{b} \underset{1}{\underset{\smile}{=}} \frac{0}{b} + \frac{0'}{b} \underset{2}{\underset{\smile}{=}} \frac{0\prime}{b}$$

onde a igual 1 ocorre pois $\frac{0'}{b}$ *é elemento neutro e a igualdade 2 ocorre pois* $\frac{0}{b}$ *também é elemento neutro. Portanto a unicidade está provada.*

Com a mesma ideia da existência de dois elementos neutro da multiplicação, podemos usar para provar a unicidade também.

P4) Distributividade da multiplicação em relação à adição, isto é,

$$\left(\frac{a}{b} + \frac{c}{d}\right)\cdot\frac{e}{f} = \frac{ad+bc}{bd}\cdot\frac{e}{f} = \frac{(ad+bc)\cdot e}{bdf} \underset{1}{\underset{\smile}{=}} \frac{ade+bce}{bdf} = \frac{ade}{bdf} + \frac{bce}{bdf} = \frac{ae}{bf} + \frac{ce}{df} = \frac{a}{b}\cdot\frac{e}{f} + \frac{c}{d}\cdot\frac{e}{f}$$

(distributiva à esquerda)

e

$$\frac{e}{f}\cdot\left(\frac{a}{b} + \frac{c}{d}\right) = \frac{e}{f}\cdot\frac{ad+bc}{bd} = \frac{e\cdot(ad+bc)}{fbd} \underset{1}{\underset{\smile}{=}} \frac{ead+ebc}{fbd} = \frac{ead}{fbd} + \frac{ebc}{fbd} = \frac{ea}{fb} + \frac{ec}{fd} = \frac{e}{f}\cdot\frac{a}{b} + \frac{e}{f}\cdot\frac{c}{d}$$

(distributiva à direita)

P5) Note que para todo $\frac{a}{b} \in Q\backslash\{0\}$*, temos que existe* $\exists\frac{b}{a} \in Q$*, que é seu inverso multiplicativo. E ele é único. De fato, suponha que existam dois inversos multiplicativos para* $\frac{a}{b}$ *, sejam eles* $\frac{b}{a}$ *e* $\frac{e}{f}$*, daí segue que*

$$\frac{b}{a} = \frac{b}{a}\cdot 1 = \frac{b}{a}\cdot\left(\frac{a}{b}\cdot\frac{e}{f}\right) = \left(\frac{b}{a}\cdot\frac{a}{b}\right)\cdot\frac{e}{f} = 1\cdot\frac{e}{f} = \frac{e}{f}.$$

Onde concluímos a unicidade do inverso multiplicativo nos racionais.

E, portanto, demonstramos que o conjunto dos números racionais é um ***corpo****.*

■

Exemplo 6.4 *– Temos que* $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p},\ a, b, p \in \mathbb{Z}\ e\ p \geq 2\ primo\}$ *é um anel mas não é um corpo. Já* $\mathbb{Q}[\sqrt{p}] = = \{a + b\sqrt{p},\ a, b, p \in \mathbb{Q}\ e\ p \geq 2\ primo\}$ *nos dá uma infinidade de corpos, tais que,* $\mathbb{Q} \subset \mathbb{Q}[\sqrt{p}] \subset R$.

Podemos ainda, mediante o fato dos racionais ser um corpo, afirmar que o mesmo é algebricamente fechado para as operações de adição e multiplicação. Haja vista que para todo racional, $r \in \mathbb{Q}$, existe um polinômio $p(X) \in \mathbb{Q}(X)$, tal que $p(r) = 0$. É o que nos afirmar a definição a seguir:

Definição 6.6 *– Seja K um corpo. Dizemos que K é um corpo* ***algebricamente fechado*** *se para todo* $p(X) \in K[X]$ *existe* $a \in K$ *tal que* $p(a) = 0$.

APÊNDICE B - EXTENSÕES DE CORPOS

Nessa seção abordaremos, de modo suficiente para embasamento desse trabalho, extensões de corpos relacionados com as raízes de polinômios. O que nos proporciona de bônus a solução de problemas geométricos clássicos de certas construções com régua não graduada e compasso.

No contexto de extensão de corpos temos por objetivo principal a adjunção de raízes de polinômios a corpos já existentes, e com isso construirmos corpos *K*. Assumiremos previamente algumas noções em Álgebra Linear, tais como: espaço e subespaço vetorial, dimensão e base.

Definição 7.1 – *Sejam dois corpos K e L, tais que L é um subcorpo de K, e as operações de adição e multiplicação em K se restringem às respectivas operações em L. Assim, denominamos K de uma extensão de L e, denotamos por* $K \mid L$, *ou ainda por,*

$$\begin{matrix} K \\ | \\ L \end{matrix}$$

No caso da definição acima, consideramos *K* como um *L*-espaço vetorial. E temos a seguinte definição:

Definição 7.2 – *O grau da extensão* $K \mid L$ *denotamos por* $[K : L]$ *e é igual à dimensão de K como L-espaço vetorial. Logo se o grau da extensão for* $n < \infty$ *diremos que K é uma extensão finita de L e, além disso, se ω é uma base do L-espaço vetorial K, então ω também é uma base da extensão.*

Exemplo 7.1 – *São exemplos de extensões de corpos os seguintes:* $\mathbb{R} \mid Q, C \mid Q, Q \mid \mathbb{Z}$, $Q\sqrt{p} \mid Q$ *e* $K(x) \mid K$, *em que x é uma indeterminada em K* ($x \in K$) *e K é um dos corpos* $\mathbb{Q}, \mathbb{R}$ *ou* $\mathbb{C}$ (*ou uma de suas adjunções*).

Definição 7.3 – *Seja K um corpo qualquer, definimos de um polinômio sobre K na indeterminada x à expressão* $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$, *em que* $a_i \in K$ *para todo i natural e, existe n natural tal que* $a_j = 0$ *para todo* $j \geq n$. *E denotamos por K*[*x*] *o conjunto de todos os polinômios sobre K na indeterminada x.*

Em se tratando de dois polinômios $p(x), q(x) \in K[x]$, dizemos que $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$ e $q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m + \cdots$ são iguais quando ocorrer que $a_k = b_k$ em *K* para todo *k* natural.

Entretanto, se para $p(x) \in K[x]$ acontecer que *p*(*x*) = *a*, com $a \in K$, isto é, $a_0 = a$ e $a_i = 0$ para todo $i \geq 1$, chamamos tal polinômio de *polinômio constante*. E ocorrendo que *p*(*x*) = 0, isto é, $a_i = 0$ para todo $i \geq 0$, chamamo-lo de *polinômio nulo*.