Revista Eletrônica Paulista de Matemática

ISSN 2316-9664
v. 24, 2024
Artigo de Iniciação Científica

Jorge Corrêa de Araújo
Faculdade de Formação de Professores
Universidade do Estado do Rio de Janeiro
jcaraujo_55@yahoo.com.br

Rosa García Márquez
Faculdade de Formação de Professores
Universidade do Estado do Rio de Janeiro
rosagmarquez@yahoo.com.br

Extensões algébricas de corpos: algumas aplicações práticas

Algebraic extensions of fields: Some practical applications

Resumo

Neste trabalho, nosso objetivo principal é apresentar de forma simples, o processo de construção do corpo de raízes de um polinômio $f(x) \in K[x]$ através da adjunção de raízes, onde K é um subcorpo dos números complexos $\mathbb{C}$. São explorados alguns casos de racionalização da Álgebra Elementar, por meio de extensões algébricas simples do corpo dos números racionais, usando duas abordagens metodológicas distintas derivadas da Álgebra Abstrata. O caso especial das raízes n-ésimas da unidade do polinômio $p(x) = x^n - 1$ é analisado do ponto de vista geométrico e da obtenção de seu corpo de raízes. Além disso, é apresentada de modo didático uma conexão entre as raízes n-ésimas da unidade e sua aplicação em processamento de sinais digitais.

Palavras-chave: Álgebra Abstrata. Racionalização Algébrica. Processamento de Sinais.

Abstract

In this work, our main objective is to present, in a simple manner, the process to construct the polynomial root field $f(x) \in K[x]$ through the root's adjunction, where K is the $\mathbb{C}$ complex numbers subfield. Some cases of rationalization in Elementary Algebra are explored through simple algebraic extensions of the rational numbers of fields, adopting two distinct methodological derived from Abstract Algebra. The special case of the nth unity roots of the $p(x) = x^n - 1$ polynomial is analyzed from a geometric viewpoint and to obtain the roots field. Furthermore, a didactic connection between the nth roots of unity and their application in digital signal processing is presented.

Keywords: Elementary Algebra. Abstract Algebra. Algebraic Rationalization. Signal Processing.

Artigo recebido em nov. 2023 e aceito em jun. 2024

1 Introdução

O "Teorema Fundamental da Álgebra" foi proposto pelo matemático francês Jean Baptiste Joseph Fourier e demostrado de forma completa pelo matemático alemão Carl Friedrich Gauss em 1799, em sua tese de doutoramento na Universidade de Helmstadt [1]. Esse teorema nos diz que o corpo $\mathbb{C}$ é algebricamente fechado, isto é, os únicos polinômios irredutíveis e unitários do domínio euclidiano $\mathbb{C}[x]$ são os fatores lineares da forma $x-a,\ \ a\in\mathbb{C}$. Sabemos que dado um corpo K e um polinômio $f(x)\in K[x]$ pode acontecer que $f(x)$ não admita raízes em K. Portanto, o problema de obtenção de raízes passa pela construção de outro corpo F que contenha o subcorpo K e $f(x)$ admita pelo menos uma raiz sobre F, ou seja, F é uma extensão do corpo K (veja [2]). Essa abordagem "construtivista" é obtida pela adjunção de raízes e pode nos levar ao corpo de decomposição de $f(x)\in K[x]$, sobre K. Isso acontece quando $K\subset\mathbb{C}$.

Nesse artigo daremos ênfase às extensões algébricas simples da forma $K\subset F=K(x)=\{f(\alpha)/\ f(x)\in K[x]\}\subset\mathbb{C}$, ou seja, por uma só etapa com a adjunção da raiz $\alpha\in F$ ao corpo K. Em decorrência dessa adjunção simples é que $IR(\alpha=i)=\mathbb{C}$, ou de modo equivalente, o corpo dos números complexos é isomorfo ao corpo gerado por IR e $i=\sqrt{-1}$, onde i é a forma dos "imaginários", ou na terminologia atual, unidade imaginária de $\mathbb{C}$. Os primeiros resultados sobre a forma dos "imaginários" podem ser encontrados, em 1747 na dissertação de D'Alembert [3]. O estudo de extensões algébricas de corpos que será brevemente tratada nesse artigo, é a base da teoria de Galois, a qual segundo Dean [4] relaciona a estrutura de subcorpo de uma extensão algébrica F contendo K, à estrutura de subgrupo do grupo $G(F/K)$ dos automorfismos de F que deixam fixados os elementos do corpo K. Desse modo, o conhecimento dos subgrupos do grupo $G(F/K)$ leva ao conhecimento dos subcorpos de F contendo K e, desse modo, resolver equações do tipo $f(x)=0$ e mostrar quais delas são ou não solúveis por radicais [2]. Obter corpo de raízes de um polinômio $f(x)$, ou da equação $f(x)=0$ pode ser relevante em particular, em problemas práticos. Por exemplo, o oscilador harmônico (MHS) simples para o estudo de pequenas vibrações mecânicas em torno de uma posição de equilíbrio, tem como modelo à equação dada por $\frac{d^2x}{dt^2}+p^2x=0;\quad p\in IR$ [5], que tem por equação característica um polinômio quadrático, cujas raízes, podem ser resolvidas facilmente por radicais. Segundo Bassanezi e Ferreira Junior [6] o desenvolvimento da Física Atômica, foi baseada em grande parte nesse modelo mecânico.

Portanto, devido à relevância desse tema, o objetivo desse artigo é abordar de forma resumida a porta de entrada para o estudo do grupo de Galois, que são os corpos de raízes de um polinômio irredutível sobre um corpo K, aqui associada a importantes aplicações práticas da dita "Álgebra Abstrata". A noção de extensões de corpos é realizada integralmente na seção 2. Em seguida são apresentadas as seções das aplicações todas dependentes da seção 2, mas não necessariamente apresentando conexões entre si. Por exemplo, na aplicação 3.1 obtém-se o corpo de decomposição do polinômio x^2-3 sobre $\mathbb{Q}$, o qual será usado na aplicação 3.3 e no problema grego da duplicação do cubo.

As aplicações 3.3 e 3.4 são importantes, pois mostram três métodos distintos de racionalização, dois deles usando o corpo de extensão e, outro, usando a Álgebra Elementar. Nesse sentido, estabelecemos aqui uma proposição original baseada na teoria de extensões, de modo

que uma classe de frações com denominadores irracionais pode ser efetivamente resolvida por meio de sistemas lineares invertíveis. Acreditamos que essa metodologia devido a sua simplicidade, possa vir a ser adotada a partir do nono ano do Ensino Fundamental.

A seção 4.1 mostra o corpo de raízes da unidade dado pela equação $x^n - 1 = 0$. Na seção 4.2 são apresentados os polinômios ciclotômicos que apanham às suas raízes como mostrado na seção 4.1. Finalmente na seção 4.3 tem-se o corpo de decomposição do polinômio $x^n - c$ sobre o corpo dos números complexos. A seção 4.4 é uma aplicação sobre processamento de sinais digitais que utiliza fortemente a seção 4.1, a qual contém a base teórica necessária para a fundamentação dos conceitos da teoria de sinais digitais. O desenvolvimento da seção 4.4 que trata da obtenção da matriz de Fourier em processamento de sinais digitais foi realizado com detalhes que não consta das referências aqui citadas. Como por exemplo, a construção da base ortonormal para o espaço dos sinais discretos periódicos que combinado com o teorema da decomposição ortogonal permite a um público mais amplo entender a origem da matriz de Fourier que é uma ferramenta importante segundo Kim [7] para transformar informações entre a frequência e o tempo. Tal detalhamento não constam das referências aqui citadas. Na pesquisa bibliográfica foram poucas as publicações disponibilizadas com ênfase nos temas aqui analisados, exceto Rezende [8] que utilizou o corpo de raízes da unidade em aplicações particulares do Teorema de Dirichlet para progressões aritméticas em reticulados com ênfase na teoria de informação e, na história da resolução do último Teorema de Fermat. Também o problema de duplicação do cubo pode ser encontrado no texto reportado por Miguel [9], mas com poucos detalhes.

2 Extensões algébricas de corpos

Seja K um corpo e $L \supset K$ uma extensão de K. Diz-se que $\alpha \in L$ é algébrico sobre K se existe um polinômio não nulo $f(x) \in K[x]$, tal que $f(\alpha) = 0$. Por exemplo, $\alpha = \sqrt{2}$ é algébrico sobre $\mathbb{Q}$, pois $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ se anula em $\alpha = \sqrt{2}$. Se para todo $\alpha \in L \supset K$, α é algébrico sobre K, então $L \supset K$ diz-se uma extensão algébrica [1].

Proposição 1: Seja $p(x) \in K[x]$ unitário e de menor grau tal que $p(\alpha) = 0$, isto é, α é algébrico sobre K. Tal polinômio (único) é irredutível em $K[x]$, ou seja, se $p(x) = g(x)h(x)$, com $g(x); h(x) \in K[x]$ então $g(x)$ ou $h(x)$ pertence a K.
Demonstração: De fato, como $p(\alpha) = 0$ tem-se que $p(\alpha) = g(\alpha)h(\alpha) = 0 \Rightarrow g(\alpha) = 0$ ou $h(\alpha) = 0$, pois $K(\alpha) = \{ f(\alpha) / f(x) \in K[x] \}$ é um subdomínio de L que contém K (veja [1]). Pela minimalidade do grau de $p(x)$, então $g(x)$ ou $h(x)$ deve ter grau zero, ou seja, $g(x)$ ou $h(x)$ é um polinômio escalar. Indicaremos esse polinômio unitário e irredutível por $p(x) = irr(\alpha, K)$ onde $p(\alpha) = 0$ [1]. Para ver que $K(\alpha) \supset K$, basta fazer $f(x) \in K$ aplicado em α o que resultará que todos os elementos do corpo base estão também em $K(\alpha)$.

Teorema 1: Seja $\langle p(x) \rangle = p(x).K[x]$ o ideal em $K[x]$ gerado por $p(x)$, onde $p(x) = irr(\alpha, K)$ é o polinômio mônico, irredutível e de menor grau em $K[x]$ que se anula α. Nessas condições tem-se

$$\bar{F} = \frac{K[x]}{\langle p(x)\rangle} \cong K(\alpha) = F \subset L. \tag{1}$$

Em outras palavras, $K(\alpha)\,(=F)$ é uma extensão de K onde $p(\alpha)=0,$ ou seja, $p(x)$ é redutível em $F[x]\,(=K(\alpha)[x])$.

Demonstração: Vamos provar o isomorfismo (1) usando uma abordagem sintética. Seja

$$\begin{aligned} \psi : K[x] &\to K(\alpha) = F \subset L \\ f(x) &\to \psi[f(x)] = f(\alpha). \end{aligned} \tag{2}$$

Essa função é um homomorfismo do domínio $K[x]$ no corpo F. Além disso, ψ é sobrejetiva pela própria definição, isto é, $\mathrm{Im}\psi = K[\alpha]$. Como $\psi[f(x)] = 0 \Rightarrow f(\alpha) = 0$, então ψ é injetiva. De fato, pela minimalidade do grau de $p(x)$ devemos ter $f(x) \in \langle p(x)\rangle$. Portanto $Nl(\psi) = \langle p(x)\rangle$ ou dito de outro modo, o núcleo de ψ é formado pelos polinômios de $K[x]$ que são divisíveis por $p(x)$. Desde que ψ é um homomorfismo sobrejetor com $Nl(\psi) = \langle p(x)\rangle$ resulta do teorema 3. A reportado por [10] que vale o isomorfismo (1), $\bar{F} = \frac{K[x]}{\langle p(x)\rangle} \cong K(\alpha) = F \subset L$ e que $p(x)$ admite α como raiz no corpo F.

Seja φ a função definida por

$$\begin{aligned} \varphi : K[x] &\to \bar{F} = \frac{K[x]}{\langle p(x)\rangle} \\ f(x) &\to \bar{f}(x) = f(x) + \langle p(x)\rangle, \end{aligned} \tag{3}$$

onde $\bar{f}(x)$ é a classe residual do ideal $\langle p(x)\rangle$ a qual $f(x)$ pertence.

Proposição 2: A função φ definida na eq. (3) é um homomorfismo canônico entre o domínio $K[x]$ e o corpo $\bar{F}$. Além disso, restrição de φ ao corpo $K,$ indicada por $\varphi_K = \varphi|_K$ é um isomorfismo dos polinômios escalares de $K[x],$ ou seja, de K sobre as classes residuais da forma $\bar{c} = c + \langle p(x)\rangle,$ com c pertencente a K.

Demonstração: De fato φ é sobrejetiva pela própria definição. Para verificarmos a injetividade basta fazer

$$\varphi|_K(c_1) = \varphi|_K(c_2) \Leftrightarrow \bar{c}_1 = \bar{c}_2 \Leftrightarrow \bar{c}_1 - \bar{c}_2 = \bar{0} = \langle p(x)\rangle \Rightarrow p(x) \mid (c_1 - c_2).$$

Como $c_1 - c_2$ tem grau zero e desde que $p(x)$ tem grau maior ou igual a um, o polinômio escalar $c_1 - c_2$ deve ser igual à zero, o que mostra que φ é também injetora. Segue que $\varphi|_K$ é um isomorfismo do corpo K sobre um subcorpo de $\bar{F}$ da forma $\bar{c} = c + \langle p(x)\rangle$. Nesse sentido podemos identificar $c \equiv \bar{c}$, para todo $c \in K$ e, com isso, $\bar{F} \supset K$.

Seja $p(x) = irr(\alpha, K)$ tal que $p(x) = c_0 + c_1 x + \ldots + c_n x^n \in K[x]$. Pelo algoritmo da divisão em $K[x]$ ([10]) existem únicos $q(x)$ e $r(x)$ ambos em $K[x]$ tais que $f(x) = p(x)q(x) + r(x)$, onde $grau(r(x)) < grau(p(x)) = n$, ou $r(x) = 0$. Usando essa decomposição para $f(x)$ e aplicando (3) tem-se $\bar{f}(x) = \varphi[f(x)]\varphi[p(x)] + \varphi[r(x)] = \bar{r}(x)$. Como $\varphi[p(x)] = 0$, isso significa dizer que cada classe $\bar{f}(x)$ em $\bar{F}$ tem seu único representante $r(x)$ de grau menor que *n*, o que nos leva a natureza do corpo $\bar{F}$ formada pelos elementos da forma

$$\bar{F} = \left\{ \bar{a}_0 + \bar{a}_1 \bar{x} + ... + \bar{a}_n \bar{x}^{n-1};\ a_i \in K \right\}, \tag{4}$$

onde $\bar{x} = x + \langle p(x) \rangle$. Como φ é um homomorfismo, φ leva 0 em 0. Logo temos que

$$\bar{0} = \varphi(0) = \varphi[p(x)] = \varphi(c_0) + \varphi(c_1)\varphi(x) + ... + \varphi(c_n)\varphi(x^n) = \bar{c}_0 + \bar{c}_1 \bar{x} + ... + \bar{c}_n \bar{x}^n \ \ (= \bar{p}(\bar{x})). \tag{5}$$

Resulta de (5) que $\bar{x}$ é um zero de $\bar{p}(x) \in \bar{F}[x]$. Portanto, o polinômio $p(x)$ irredutível em $K[x]$ tem como imagem pela φ, o polinômio $\bar{p}(x) \in \bar{F}[x]$ redutível em $\bar{F}[x]$ com zero $\bar{x} = x + \langle p(x) \rangle$.

Do isomorfismo (1) podemos estabelecer as seguintes identificações $c \leftrightarrow \bar{c}$ e $\alpha \leftrightarrow \bar{x}$. Daí, e usando a eq. (4) tem-se a natureza dos elementos do corpo F na forma

$$F = K(\alpha) = \left\{ a_0 + a_1 \alpha + ... + a_{n-1} \alpha^{n-1};\ a_i \in K \right\}, \tag{6}$$

sujeito à relação $p(\alpha) = c_0 + c_1 \alpha + ... + c_n \alpha^n = 0$, isto é, $p(x) \in K[x]$ tem uma raiz α sobre F, ou seja, $p(x)$ é redutível sobre $F[x]$. Aqui $F = K(\alpha)$ é uma extensão algébrica do corpo K onde $p(x)$ admite uma raiz α.

Proposição 3: Seja $p(x)$ um polinômio irredutível de grau *n* ($n > 0$) em $K[x]$. Se identificarmos *K* como um subcorpo de $\bar{F} = \dfrac{K[x]}{\langle p(x) \rangle}$, então $\bar{F} = \dfrac{K[x]}{\langle p(x) \rangle}$ é um subespaço vetorial sobre K.

Demonstração: De fato, resulta da eq. (4) que o conjunto $\left\{ \bar{1}, \bar{x}_1, ..., \bar{x}_{n-1} \right\}$ gera $\bar{F}$. Para verificarmos a independência de seus elementos basta fazer $\sum_{i=0}^{n-1} \bar{a}_i \bar{x}^i = \bar{0} = \langle p(x) \rangle \Rightarrow p(x) \mid g(x)$, onde $g(x) = \sum_{i=0}^{n-1} a_i x^i$, onde $grau(g(x)) < n$. Daí, pela minimalidade de $grau(p(x))$ devemos ter $g(x) = 0$, o que resulta em $a_i = 0$, $i = 1, 2, ..., n-1$. Logo do isomorfismo (1) o conjunto $\left\{ 1, \alpha, ..., \alpha^{n-1} \right\}$ é uma base para $F = K(\alpha)$ como um espaço vetorial sobre K.

Definição: Uma extensão $F \supseteq K$ é chamada uma extensão *finita* de K de grau *n*, se F é um espaço vetorial de dimensão finita *n* sobre K. Em caso contrário F é dito uma extensão *infinita* de *K* onde escreveremos $[F : K]$ para designar o grau de F sobre K (veja [4]).

Definição: Chamamos corpo de decomposição de um polinômio $f(x) \in K[x]$ sobre K ao menor subcorpo de $\mathbb{C}$ que contem K e todas as raízes de $f(x)$ em $\mathbb{C}$. Tal menor subcorpo existe e, será representado por $Gal(f, K) = K(\alpha_1, ..., \alpha_r)$, onde $\alpha_1, ..., \alpha_r$ são todas as raízes distintas de $f(x)$ em $\mathbb{C}$ (veja [1]).

3 Extensões algébricas e racionalização de frações algébricas

Nesta seção, são analisadas cinco aplicações envolvendo a racionalização de certas frações com denominadores irracionais e o problema da duplicação do cubo.

Para a racionalização dessas frações, duas metodologias foram adotadas com base na extensão algébrica de corpos, as quais puderam ser comparadas com a racionalização da Álgebra Elementar. Uma proposição foi aqui estabelecida pelos autores para que uma classe mais geral de frações irracionais pudesse ser racionalizada por meio de um sistema linear inversível e, desse

modo, esse conhecimento possa ser também acessível a estudantes do fim do ciclo Fundamental e do Ensino Médio.

3.1 Aplicação

Considere o polinômio $p(x)=x^2-3$, sobre o corpo $\mathcal{Q}$. Como $\alpha=\sqrt{3}\notin\mathcal{Q}$, $p(x)=x^2-3$ é irredutível em $\mathcal{Q}[x]$. Daí, usando a eq. (6) e fazendo $K=\mathcal{Q}$ tem-se

$$F=\left\{a_0+a_1\alpha;\ a_i\in\mathcal{Q},\alpha^2-3=0\right\}=\mathcal{Q}(\alpha)=\mathcal{Q}\left(\sqrt{3}\right)$$

Logo $p(x)$ captura as raízes $\pm\alpha$ sobre $F\left(a_0=0,a_1=\pm1\right)$. A Fig. 1 mostra $\mathcal{Q}(\alpha)$ como uma extensão algébrica de $\mathcal{Q}$ com $\left[\mathcal{Q}(\alpha):\mathcal{Q}\right]=2$.

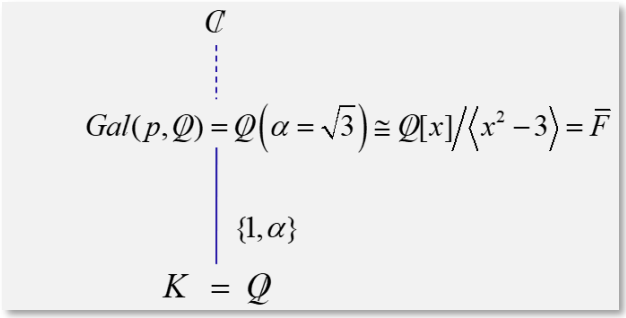

Figura 1: Visualização de $\mathcal{Q}(\alpha)\supset K=\mathcal{Q}$.

3.2 Aplicação

Seja $K=IR[x]$ e $p(x)=x^2+1\in IR[x]$. Esse polinômio não tem raiz sobre o corpo IR. Do isomorfismo (1) e de (6) tem-se $\bar{F}=\dfrac{IR[x]}{\left\langle x^2+1\right\rangle}\cong IR(\alpha=i)=F=\left\{a_0+a_1\alpha;\quad a_j\in IR,\ \alpha^2+1=0\right\}$.

A Fig. 2 mostra o conjunto dos números complexos $\mathbb{C}$ como uma extensão algébrica dos reais onde $\left[IR\left(\alpha=i\right):IR\right]=2$.

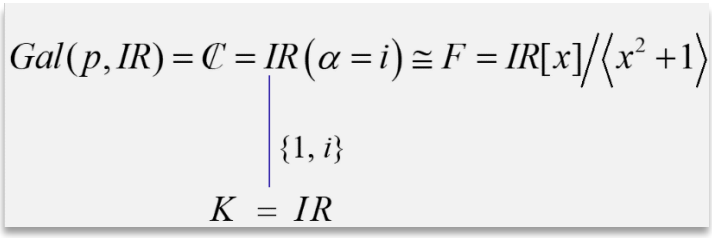

Figura 2: $\mathbb{C}=IR(i)$ como uma extensão algébrica de IR.

Um isomorfismo natural entre esses corpos deve levar $\alpha=i\to\bar{x}$ e $a\to\bar{a}$.

Observação: Nas aplicações 3.3 e 3.4 a seguir, são exploradas algumas formas de "racionalização" de frações algébricas. A primeira delas usa o conceito de elemento inverso em um corpo de extensão, a segunda, é a racionalização elementar propriamente dita, enquanto a terceira faz o uso de congruências polinomiais usando também o corpo de extensão. Antes de vermos as aplicações com esses métodos, vamos lembrar que o processo de racionalização de frações algébricas no Ensino Médio é utilizado somente em casos especiais, como por exemplo, frações do tipo $\dfrac{1}{a\pm\sqrt{b}}$, onde $\alpha=\sqrt{b}$ é algébrico sobre o corpo dos racionais $\mathcal{Q}$.

Como $\alpha = \sqrt[n]{b}$ é algébrico sobre os racionais Q, a racionalização de expressões do tipo $\frac{1}{c_o + c_1\alpha + ... + c_k\alpha^k}$ com $k < n$, sendo k e n ambos inteiros e positivos, podem-se mostrar impraticáveis ou mesmo impossíveis de serem obtidas pelo método de conjugação adotado na Álgebra Elementar. Entretanto, formularemos aqui uma proposição especial baseada na extensão algébrica de corpos e, que atende a esse tipo de expressão e cuja metodologia, acreditamos que possa ser adotada a estudantes do Ensino Médio.

Proposição 4. Considere $p(x) = x^n - b \in Q[x]$ irredutível sobre Q, onde $p(x)$ apanha uma raiz $\alpha = \sqrt[n]{b}$ sobre $F = Q(\alpha)$, então $\frac{1}{c_o + c_1\alpha + ... + c_k\alpha^k} \neq 0$ com $k < n, \quad k, n \in \mathbb{Z}^+$, pode ser determinado livre de frações no denominador.

Demonstração. Como $p(x)$ é redutível sobre $F = Q(\alpha)$, da eq. (6) tem-se que a natureza dos elementos desse corpo é dada por

$$F = Q(\alpha) = \left\{ a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : a_i \in Q, \ i = 0, ..., n-1 \right\},$$

sujeito a restrição $\alpha^n - b = 0$. Como $\frac{1}{c_o + c_1\alpha + ... + c_k\alpha^k} \neq 0$, existe um único $\beta = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$ em F, tal que

$$\left(c_o + c_1\alpha + ... + c_k\alpha^k\right)\left(a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}\right) = 1 (= 1 + 0\alpha + ... + 0\alpha^{n-1}) \ .$$

Fazendo a multiplicação entre os termos do lado esquerdo da equação e agrupando os fatores comuns em função das potências de α obtemos a igualdade

$$d_0 + d_1\alpha + ... + d_{n-1}\alpha^{n-1} = 1 + 0\alpha + ... + 0\alpha^{n-1},$$

onde cada d_i, com $i = 0, ..., n-1$, conterá somas finitas de produtos envolvendo termos em a_j´s e c_r´s com $j = 0, ..., n-1; \quad r = 0, .., k$ resultante dos agrupamentos de termos semelhantes nas respectivas potências de α. Portanto, o resultado será um sistema linear inversível de ordem $n \times n$ que resolvido fornecerá todos os a_j´s e, desse modo, $\beta = \frac{1}{c_o + c_1\alpha + ... + c_k\alpha^k}$ é livre de radicais no denominador.

Observação: Uma consequência direta desse resultado é que se β é livre de radicais, então *A*β também é livre de radicais, onde *A* é qualquer real que não tenha denominador irracional, a menos que tal denominador seja também uma potência de α.

3.3 Aplicação: racionalizar a fração $\frac{1}{2+\sqrt{3}}$

Denotando por $\alpha = \sqrt{3}$, devemos obter $(2+\alpha)^{-1} = \frac{1}{2+\alpha}$.

1º Método: "Racionalização" considerando o corpo $F = Q(\alpha)$ que foi obtido na aplicação 3.1 com $\alpha = \sqrt{3}$. Usando (6) e sabendo que $\alpha^2 = 3$, basta resolver a equação,

$$(2+\alpha)(a_0 + a_1\alpha) = 2a_0 + 2a_1\alpha + a_0\alpha + a_1\alpha^2 = (2a_0 + 3a_1) + (a_0 + 2a_1)\alpha = 1 + 0\alpha. \qquad (8)$$

Da eq. (8) obtém-se as seguintes equações lineares $2a_0 + 3a_1 = 1$ e $a_0 + 2a_1 = 0$ que pode ser escrito como um sistema linear, dado por

$$\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} 2 \\ -1 \end{bmatrix}, \tag{9}$$

onde $a_0 = 2$ e $a_1 = -1$. Portanto, pela Proposição 4 tem-se que

$$\frac{1}{2+\alpha} = \beta = a_0 + a_1\alpha = 2 - \alpha. \tag{10}$$

2º Método: Racionalização usando a álgebra elementar por multiplicação pelo conjugado,

$$(2+\alpha)^{-1} = \frac{1}{2+\alpha} = \frac{1}{2+\sqrt{3}} = \frac{2-\sqrt{3}}{\left(2+\sqrt{3}\right)\left(2-\sqrt{3}\right)} = \frac{2-\sqrt{3}}{4-3} = 2-\sqrt{3} = 2-\alpha. \tag{11}$$

3º Método: Obter $(2+\alpha)^{-1}$ em $F = \mathbb{Q}(\alpha)$ é equivalente a resolver em $F[x]$ uma equação de congruência polinomial. De fato, do isomorfismo (1) tem-se

$$(2+\alpha)s(\alpha) = 1 \Leftrightarrow \left(\overline{2}+\overline{x}\right)\overline{s}\left(\overline{x}\right) = \overline{1} \Leftrightarrow (2+x)s(x) \equiv 1 \bmod\left(x^2-3\right). \tag{12}$$

Usando o algoritmo da divisão em $\mathbb{Q}[x]$ pode-se escrever o polinômio escalar 1 como uma combinação linear de $2+x$ e x^2-3 para obter $s(x)$.

$$\begin{aligned} x^2-3 &= (2+x)(x-2)+1, \\ (x^2-3)(-1) &= (2+x)(2-x)-1, \\ (x^2-3)\ldots(1) &+ (2+x)(2-x) = 1, \end{aligned} \tag{13}$$

onde $s(x) = 2-x$, ou seja, $(2+\alpha)^{-1} = s(\alpha) = 2-\alpha.$

3.4 Aplicação: Racionalizar $\dfrac{1}{1+\sqrt[5]{2}+\sqrt[5]{2}^3}$

Seja $\alpha = \sqrt[5]{2}$, devemos obter $\left(1+\alpha+\alpha^3\right)^{-1} = \dfrac{1}{1+\alpha+\alpha^3}$. Esse problema foi proposto e resolvido por [4] usando o método de congruência polinomial.

1º Método: "Racionalização" considerando o corpo $F = \mathbb{Q}(\alpha)$, com $\alpha = \sqrt[5]{2}$. Usando (6) basta resolver a equação no corpo $F = \mathbb{Q}(\alpha)$,

$$\left(1+\alpha+\alpha^3\right)\left(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4\right) = 1 \tag{14}$$

Desenvolvendo a eq. (14) e agrupando os termos como potências de α tem-se usado o fato que $\alpha^5 = 2$, $\alpha^6 = 2\alpha$ e $\alpha^7 = 2\alpha^2$ tem-se

$$\left(a_0 + 2a_2 + 2a_4\right) + \left(a_0 + a_1 + 2a_3\right)\alpha + \left(a_1 + a_2 + 2a_4\right)\alpha^2 + \left(a_0 + a_2 + a_3\right)\alpha^3 + \left(a_1 + a_3 + a_4\right)\alpha^4 = 1$$

Da igualdade acima, resulta o conjunto de equações lineares dadas por

$a_0 + 2a_2 + 2a_4 = 1;\ a_0 + a_1 + 2a_3 = 0,\ a_1 + a_2 + 2a_4 = 0,\ a_0 + a_2 + a_3 = 0$ e $a_1 + a_3 + a_4 = 0.$

Essas equações podem ser colocadas como um sistema linear de ordem 5×5 na forma

$$\begin{bmatrix} 1 & 0 & 2 & 0 & 2 \\ 1 & 1 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 & 2 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \tag{15}$$

A solução da eq. (15) é dada por $a_0 = 1,\ a_1 = -1, a_2 = -1, a_3 = 0$ e $a_4 = 1$. Portanto, pela Proposição 4, o inverso desejado é dado por

$$\left(1+\alpha+\alpha^3\right)^{-1} = \beta = 1-\alpha-\alpha^2+\alpha^4 = 1-\sqrt[5]{2}-\left(\sqrt[5]{2}\right)^2+\left(\sqrt[5]{2}\right)^4. \tag{16}$$

2º Método: Racionalização usando a álgebra elementar

$$\frac{1}{1+\alpha+\alpha^3}=? \tag{17}$$

Não conseguimos obter um conjugado de modo direto para a racionalização desse denominador. Então a ideia é obter um polinômio $N=ax^3+bx^2+cx+d$ que seja divisível pelo polinômio $D=x^{\frac{3}{5}}+x^{\frac{1}{5}}+1$ de modo que $P=\frac{N}{D}\Rightarrow\frac{1}{D}=\frac{P}{N}$. Usando o *software* Maple, foi obtido o polinômio $P=x^3-5x^2+6x+1$. Daí,

$$\frac{1}{D}=\frac{1}{x^{\frac{3}{5}}+x^{\frac{1}{5}}+1}=\frac{x^{\frac{12}{5}}-x^{\frac{10}{5}}-x^{\frac{9}{5}}+x^{\frac{8}{5}}-3x^{\frac{7}{5}}+2x+3x^{\frac{4}{5}}-2x^{\frac{3}{5}}+x^{\frac{2}{5}}-2^{\frac{1}{5}}+1}{x^3-5x^2+6x+1}. \tag{18}$$

Fazendo $x=2$ na eq. (18) tem-se $\left(1+\alpha+\alpha^3\right)^{-1}=1-\alpha-\alpha^2+\alpha^4=1-\sqrt[5]{2}-\left(\sqrt[5]{2}\right)^2+\left(\sqrt[5]{2}\right)^4$.

3º Método: Resolver $\left(1+\alpha+\alpha^3\right)^{-1}$ em F é equivalente a resolver em $\bar{F}$ a equação

$$\left(1+\alpha+\alpha^3\right)s(\alpha)=1\Leftrightarrow\left(\bar{1}+\bar{x}+\bar{x}^3\right)\bar{s}(\bar{x})=\bar{1}\Leftrightarrow\left(1+x+x^3\right)s(x)\equiv 1\bmod(x^5-2). \tag{19}$$

Fazendo uso do algoritmo da divisão em $F[x]$ tem-se

$$\begin{aligned}
x^5-2&=\left(x^3+x+1\right)\left(x^2-1\right)-\left(x^2-x+1\right),\\
x^3+x+1&=\left(x^2-x+1\right)(x+1)+x,\\
x^2-x+1&=x(x-1)+1.
\end{aligned} \tag{20}$$

Tem-se que o $M.D.C\left\{x^5-2,\ x^3+x+1\right\}=1$. Esse máximo divisor comum pode ser escrito como uma combinação linear dos polinômios x^5-2 e x^3+x+1 para obtermos o polinômio $s(x)\in F[x]$.

$$\begin{aligned}
1&=\left(x^2-x+1\right)-(x-1)x,\\
1&=\left(x^2-x+1\right)-(x-1)\left\{(x^3+x+1)-(x^2-x+1)(x+1)\right\},\\
&\vdots\\
1&=(x^3+x+1)(x^4-x^2-x+1)-(x^5-2)x^2.
\end{aligned} \tag{21}$$

A cadeia de equações (21) é obtida da eq. (20), onde a última igualdade da cadeia dada pela eq. (21) é equivalente a afirmar que x^5-2 divide $1-(x^3+x+1)(x^4-x^2-x+1)$, onde

$$s(x)=x^4-x^2-x+1,\ \text{ou seja,}\ s(\alpha)=\alpha^4-\alpha^2-\alpha+1=(\alpha^3+\alpha+1)^{-1}.$$

3.5 Aplicação: a duplicação do cubo é impossível usando apenas a régua e o compasso

A equação algébrica $x^3-2=0$ embora pareça "ingênua", nos dá a resposta para um problema clássico dos gregos originado no período de 430 a.C. relacionado à "duplicação do cubo", considerando apenas a construção geométrica usando a régua e o compasso. Conforme reportado por [11] o povo de Atenas nesse período passava por uma peste que assolava a cidade e, desse modo, procuraram o oráculo para saber como deviam proceder. "A resposta do oráculo foi que deveriam duplicar o tamanho do altar de Apolo que era em forma de um cubo". Como

o volume de um cubo de aresta unitária é igual à unidade, então o valor da aresta α para a "duplicação do cubo" seria a raiz da equação algébrica $x^3 - 2 = 0$.

Segundo [10] um número real α é dito construtível se, através do uso de apenas régua e compasso, pode-se construir um segmento de reta de comprimento α. Admite-se que seja dado um comprimento unitário fundamental. Ainda de acordo com [11], com a construção geométrica pode-se construir com a régua e o compasso uma reta perpendicular e uma reta paralela a uma dada reta, passando por um ponto dado. A partir disto é possível mostrar que o conjunto desses elementos construtíveis, $\wp$, forma um subcorpo do corpo dos números reais IR. É fácil de ver que $\wp \supset \mathbb{Q} \supset \mathbb{Z}$, pois todo inteiro é efetivamente construtível por meio da marca fundamental da régua. A resposta para a "duplicação do cubo", e de outros problemas clássicos analisados pelos gregos [1] e [12], é baseada no critério da não-construtibilidade, de novo, usando a régua e o compasso de um número real α.

Trata-se do corolário 2 reportado por [10]. Se o número real α satisfaz um polinômio irredutível de grau k sobre o corpo dos números racionais $\mathbb{Q}$ e se $k \neq 2^m$, sendo m um inteiro positivo, então α não é construtível. Portanto como $x^3 - 2$ é irredutível sobre $\mathbb{Q}$ e de grau $k = 3 \neq 2^m$, então $\alpha = \sqrt[3]{2}$ não é construtível, ou seja, é impossível a "duplicação do cubo unitário" usando somente a régua e o compasso.

4 Algumas aplicações das raízes n-ésimas

Nesta seção será mostrado como as raízes n-ésimas da unidade desempenham um papel importante na obtenção de corpo de raízes de polinômios da forma $x^n - c = 0$ e em processamento de sinais digitais.

4.1 Aplicação: as raízes n-ésimas da unidade

Consideramos o polinômio

$$x^n - 1 = 0 \tag{22}$$

tem-se $x^n - 1 \in \mathbb{Q}[x]$ onde n é um inteiro maior ou igual à unidade. Seja $x = \rho e^{i\theta} = \rho\left[\cos(\theta) + i\,\mathrm{sen}(\theta)\right]$ uma solução da equação $x^n - 1 = 0$. Da fórmula de Möivre e da igualdade de dois números complexos resulta que $x^n = \rho^n e^{in\theta} = 1$, então $\rho = 1$ e $n\theta = 2\lambda\pi$, $\lambda = 0, 1, ..., n-1$ sendo um número inteiro. Portanto, as n -ésimas raízes da unidade são dadas por

$$\xi_\lambda = e^{i\frac{2\pi\lambda}{n}} = \cos\left(\frac{2\pi\lambda}{n}\right) + i\,\mathrm{sen}\left(\frac{2\pi\lambda}{n}\right);\ \lambda = 0, ..., n-1. \tag{23}$$

Os zeros da equação (22) formam um subgrupo finito em relação à multiplicação dos números complexos, sendo esse grupo indicado por $T_n = \{\xi_\lambda;.\}_{\lambda=0,...,n-1}$. Além disso, esse grupo é cíclico e de ordem n [10]. Os geradores de T_n são chamados de n -ésimas raízes primitivas da unidade e são um número igual a $\phi(n) = \#\{0 < \lambda < n : mdc(\lambda, n) = 1\}$, isto é, $\phi(n)$ representa o número de inteiros λ, tais que $0 < \lambda < n$ com λ e n elementos primos entre si [13]. Por esse critério, $mdc(\lambda = 1, n) = 1$ e $\xi = \xi_1 = e^{i\frac{2\pi}{n}}$ é uma raiz geradora de T_n, ou seja, $T_n = \langle\xi\rangle = \{\xi^\lambda, \lambda = 0, ..., n-1\}$. As raízes $\xi^\lambda = e^{i\frac{2\pi\lambda}{n}}$, $\lambda = 0, ..., n-1$ podem ser interpretadas como sendo os vértices de um polígono regular de n lado inscritos no círculo unitário de centro em $x = 0$ e um vértice em $x = \xi^0 = 1$ [2].

4.2 Aplicação: polinômios ciclotômicos

Seja $\varphi_n(x) = \prod_{mdc(k,n)=1} \left(x - \xi^k\right)$ em $Q(\xi)[x]$, onde ξ é uma *n*-ésima raiz primitiva da unidade [4]. Portanto, $\varphi_n(x)$ é um polinômio cujos zeros são as raízes *n*-ésima primitivas da unidade onde o grau = $\varphi_n(x) = \phi(n)$. O polinômio $\varphi_n(x)$ é chamado apropriadamente de *n*-ésimo polinômio de ciclotômico. Note que $\varphi_1(x) = x - 1$, pois $mdc(1, n) = 1,$ ou seja, $\varphi_1(x)$ é de grau um, com $\xi^0 = 1$ sendo a 1-ésima raiz primitiva da unidade. Analogamente, $\varphi_2(x) = x + 1$ com o grau de $\varphi_2(x) = \varphi(2) = 1$ e $\xi = -1$ sendo 1-ésima raiz primitiva de unidade $\left(\xi^0 = 1, \xi = -1\right)$. Segundo [4] é possível escrever $x^n - 1$ na forma

$$x^n - 1 = \varphi_n(x) \prod_{\substack{d/n \\ d \neq n}} \varphi_d(x). \tag{24}$$

Da eq. (38) tem-se

$$\varphi_n(x) = \frac{x^n - 1}{\prod_{\substack{d/n \\ d \neq n}} \varphi_d(x)}. \tag{25}$$

Assim por exemplo, podemos construir

$$\varphi_3(x) = \frac{x^3 - 1}{\varphi_1(x)} = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 = \left(x - \xi\right)\left(x + \xi\right),$$

onde $\xi = e^{i\frac{2\pi}{3}}$ é a 3-ésima raiz primitiva da unidade da aplicação 2.2, em seguida,

$$\varphi_4(x) = \frac{x^4 - 1}{\varphi_1(x)\varphi_2(x)} = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1 = \left(x - \xi\right)\left(x + \xi\right),$$

sendo $\xi = i,$ etc.

Em particular se *p* é um número primo, o único d positivo, divisor de *p* e menor que *p* é $d = 1.$ Daí e da eq. (38) obtém-se

$$\varphi_p(x) = \frac{x^p - 1}{\varphi_1(x)} = \frac{x^p - 1}{x - 1} = x^p + \ldots + x + 1 \tag{26}$$

O polinômio $\varphi_p(x)$ é denominado $p-$ésimo polinômio ciclotômico [11] tendo como raízes a unidade e, as $p-$ésimas raízes primitivas da unidade na forma $\xi_\lambda = e^{\frac{i2\pi}{p}\lambda}$, $\lambda = 1, \ldots, p-1$, já que $\phi(p) = p - 1.$ De (26) tem-se $g(x) = x^{p-1} + \ldots + x + 1,$ onde $g(x) = irr(\xi, Q),$ daí o conjunto $\beta = \left\{1, \xi, \ldots, \xi^{p-2}\right\}$ é uma base de $Q(\xi)$ como um espaço vetorial sobre Q onde $Q(\xi) = \left\{a_0 + a_1\xi + \ldots + a_{p-2}\xi^{p-2}; a_i \in Q\right\}$ com $\left[Q(\xi) : Q\right] = p - 2.$ Poderíamos igualmente obter a natureza dos elementos desse corpo fazendo a divisão euclidiana de $f(x)$ por $g(x),$ ambos em $Q[x]$.

De fato, existem únicos $q(x)$ e $r(x)$ em $Q[x]$ de modo que $f(x) = g(x)q(x) + r(x)$, onde $grau\left(r(x)\right) < p - 2$ ou $r(x) = 0$ sendo $Q(\xi) = \left\{f(\xi) : f(x) \in Q[x]\right\}$. Como $r(\xi) \neq 0,$ pois caso contrário, haveria contradição na minimalidade do grau de $g(x)$. Logo devemos ter $r(x) = a_0 + a_1\xi + \ldots + a_{p-2}$ e desde que $g(\xi) = 0,$ então

$$Q(\xi) = \left\{f(\xi) = 0 \cdot q(\xi) + r(\xi) : f(x) \in Q[x]\right\}, \text{ isto é, } Q(\xi) = \left\{r(\xi)\right\}.$$

4.3 Aplicação: a equação $x^n - c$ no corpo dos números complexos

Se $x^n - c\ (0 \neq c \in K)$ se decompõem em $F \supseteq K$, então existe $\xi \in F$, onde ξ é uma raiz *n*-ésima primitiva da unidade [4]. Seja $\omega \in F$ uma raiz *n*-ésima da equação $x^n - c = 0$. É fácil de ver que $\omega, \xi\omega, ..., \xi^{n-1}\omega$ são todos os n zeros de $x^n - c$ no corpo *F*. Em particular, seja $c = a + ib$ um número complexo, então sua forma polar é dada por $c = |c|e^{i\beta}$, onde $\beta = tg^{-1}\left(\frac{b}{a}\right) = \arg c.$ Seja $\omega = re^{i\theta}$, com $r > 0$ uma solução dessa equação. Usando a fórmula de Möivre tem-se $\omega^n = r^n e^{in\theta} = |c|e^{i\beta}$, $\beta = n\theta.$ Dessas considerações obtemos que $\omega = |c|^{\frac{1}{n}} e^{i\left(\frac{1}{n}\right)\beta} = |c|^{\frac{1}{n}} e^{i\theta}$, ou seja, $\omega = \cos(\theta) + i\,\mathrm{sen}(\theta)$, sendo $\theta = \frac{\beta}{n}\left[= \frac{1}{n} tg^{-1}\left(\frac{b}{a}\right)\right]$.

Da identidade $\log|\omega| = \log|c|^{\frac{1}{n}} = \log(a^2 + b^2)^{\frac{1}{n}}$ tem-se pela bijetividade da função logarítmica que $|\omega| = \left(a^2 + b^2\right)^{\frac{1}{2n}}$ e daí, $\omega = \left(a^2 + b^2\right)^{\frac{1}{2n}} e^{i\theta}$, ou ainda na forma algébrica

$$\omega = \left(a^2 + b^2\right)^{\frac{1}{2n}} e^{i\left(\frac{1}{n}\right)tg^{-1}\left(\frac{b}{a}\right)}. \tag{27}$$

Foi visto anteriormente que $\xi = e^{i\frac{2\pi}{n}}$ é uma raiz *n*-ésima primitiva da unidade, então $\xi^\lambda = e^{i\frac{2\pi}{n}\lambda}$, $\lambda = 0, ..., n-1$, são todas as *n* raízes da unidade, então as raízes *n*-ésimas de c são dadas na forma anteriormente descrita como $\xi^\lambda \omega$ na forma

$$\xi^\lambda \omega = (a^2 + b^2)^{\frac{1}{2n}} e^{i\left[\frac{2\pi}{n}\lambda + \left(\frac{1}{n}\right)tg^{-1}\left(\frac{b}{a}\right)\right]}; \quad \lambda = 0, ..., n-1, \tag{28}$$

com $\arg(\xi^\lambda \omega) = \frac{2\pi}{n}\lambda + \left(\frac{1}{n}\right)tg^{-1}\left(\frac{b}{a}\right)$, para cada λ inteiro dentro do intervalo de variação.

As raízes *n*-ésimas de *c* são também representadas como vértices de um polígono regular inscrito em um círculo de raio igual ao módulo de c e centrado em $x = 0$, sendo um de seus vértices $x = \omega$ [2]. Para compreender a natureza do corpo de decomposição $F = Gal\left(x^n - c, Q\right)$ faremos uso da proposição 4, reportada por [1], a qual mostra como obter uma base do corpo F como um espaço vetorial sobre o corpo base Q, usando as bases intermediários das extensões algébricas $F = Q(\omega, \xi) = K(\xi) \supset K = Q(\omega) \supset Q$. Veremos a seguir um teorema que trata sobre essa questão. Sejam $F \supset M \supset K$ corpos tais que os graus das extensões $[F : M]$ e $[M : K]$ são finitos, então o grau da extensão $[F : K]$ é finito e $[F : K] = [F : M][M : K]$.

O que afirma essa proposição é que a dimensão de *F* como um espaço vetorial sobre *K* é o produto das dimensões de *F* sobre *M* pela dimensão de *M* sobre *K*. A demonstração consiste em provar que o conjunto $\beta_K^F = \left\{v_i u_j\right\}_{\substack{i=1,..,r \\ j=1,..,s}}$ é uma base de F sobre K. Da hipótese da proposição podemos supor que o conjunto $\beta_M^F = \left\{v_i\right\}_{i=1,..,r}$ forma uma base para de F sobre M, enquanto $\beta_K^M = \left\{u_j\right\}_{j=1,..,s}$ forma uma base de M sobre o corpo base K. Com isso pode-se estabelecer $\dim F|_K = r \cdot s = \dim F|_M \cdot \dim M|_K$. Para provar que $\beta_K^F = \left\{v_i u_j\right\}_{\substack{i=1,..,r \\ j=1,..,s}}$ é uma base de F sobre K é preciso mostrar que esses vetores são linearmente independentes e que geram o espaço F. De

fato, seja $\sum_{\substack{i=1,...,r\\ j=1,..,s}} \lambda_{ij} v_i u_j = 0$, com escalares $\lambda_{ij} \in K$. Para cada índice i fixado de $1,...,r$, fazemos a variação do índice $j = 1,...,r$ para obter a expressão

$$\sum_{\substack{i=1...r\\ j=1...s}} \lambda_{ij} v_i u_j = \left[\sum_{j=1...s} \lambda_{1j} u_j \right] v_1 + ... \left[\sum_{j=1...s} \lambda_{sj} u_s \right] v_s = 0.$$

Os somatórios dentro dos colchetes são elementos de M e, como os $v_1,...,v_s$ são linearmente independentes em F sobre M, cada somatório $\sum_{j=1...s} \lambda_{ij} u_j$ deve ser zero. Analogamente, como u_j´s são linearmente independentes em M sobre K devemos ter $\lambda_{ij} = 0$ para todo para todo par i, j. Resta mostrar que β_K^F é um conjunto gerador de F sobre K. Seja $z \in F$ e usando o fato que $v_1,...,v_s$ formam uma base de F sobre M, existem escalares, $\alpha_1,...,\alpha_r \in M$ tais que $z = \sum_{i=1}^{r} \alpha_i v_i$. Agora considerando M como um espaço vetorial sobre K, existem escalares $\beta_{ij} \in K$, $j = 1,..,s$, onde $z = \sum_{i=1}^{r} \sum_{j=1}^{s} \beta_{ij} v_i u_j = \sum_{i,j} \beta_{ij} v_i u_j$. Ou seja, β_K^F é uma base de F sobre o corpo K. Portanto, a natureza dos elementos do corpo F como uma extensão do corpo base K é dada por

$$F = \left\{ \sum_{i,j} \beta_{ij} v_i u_j,\ \beta_{ij} \in K, i = 1,..., r,\ j = 1,..., s \right\} \tag{29}$$

Vamos considerar $Gal\left(x^p - c, Q\right)$ onde p e c são números primos entre si maiores ou iguais a 2 com $\omega = \sqrt[p]{c} \in IR$ obtida de (27) e $\xi = e^{i\frac{2\pi}{p}}$ uma raiz p-ésima primitiva da unidade. Sabemos que o corpo de raízes de $x^p - c$ sobre Q deve conter $\omega, \xi\omega, ..., \xi^{p-1}\omega$ como zeros de acordo com (28). Desse modo, $x^p - c$ é irredutível sobre $Q(\omega)$. Portanto, $\left[K = Q(\omega) : Q\right] = p$, onde $\beta_Q^K = \left\{\omega^j\right\}_{j=0,..,p-1}$ é uma base de $M = Q(\omega)$ como um espaço vetorial sobre $K = Q$. A natureza dos elementos β_Q^K decorre do isomorfismo (1) já discutido anteriormente. Precisamos agora das raízes $\xi, \xi^2, ..., \xi^{p-1}$ do polinômio $\varphi_p(x) = x^{p-1} + ... + x + 1$ que é o p-ésimo polinômio ciclotômico irredutível sobre Q. Usando os corolários 2 e 3 reportados por [1] $\varphi_p(x)$ é também irredutível sobre $K = Q(\omega)$, ou seja, $\left[F = K\left(\xi\right) : K\right] = p - 1$. Analogamente $\beta_K^F = \left\{1, \xi, ..., \xi^{p-2}\right\}$ é uma base de $F = K\left(\xi\right)$ como um espaço vetorial sobre o corpo $K = Q\left(\omega\right)$. Temos, portanto, a seguinte cadeia de extensões algébricas $F = Gal\left(x^p - c, Q\right) = K\left(\xi\right) = Q\left(\omega, \xi\right) \supset K = Q(\omega) \supset Q.$

A natureza dos elementos do corpo de raízes F como uma extensão algébrica, pode ser descrita pela fórmula que relaciona o grau da extensão final F sobre Q com as extensões intermediárias K sobre Q (=p) e F sobre K (=p-1), isto é,

$$\left[F : Q\right] = [K : Q] \cdot [F : Q] = p\left(p - 1\right)$$

é dada por (29) como uma combinação finita de todos os produtos dos elementos, na realidade números das bases β_K^F e β_Q^K multiplicadas por escalares em Q na forma

$$F = Q\left(\omega, \xi\right) = \left\{ \lambda_{ij}\left(\omega^i \xi^j\right);\quad \lambda_{ij} \in Q, i = 0,..., p-1;\ j = 0,..., p-2 \right\} \tag{30}$$

A Fig. 3 ilustra os principais elementos envolvidos nas extensões dadas.

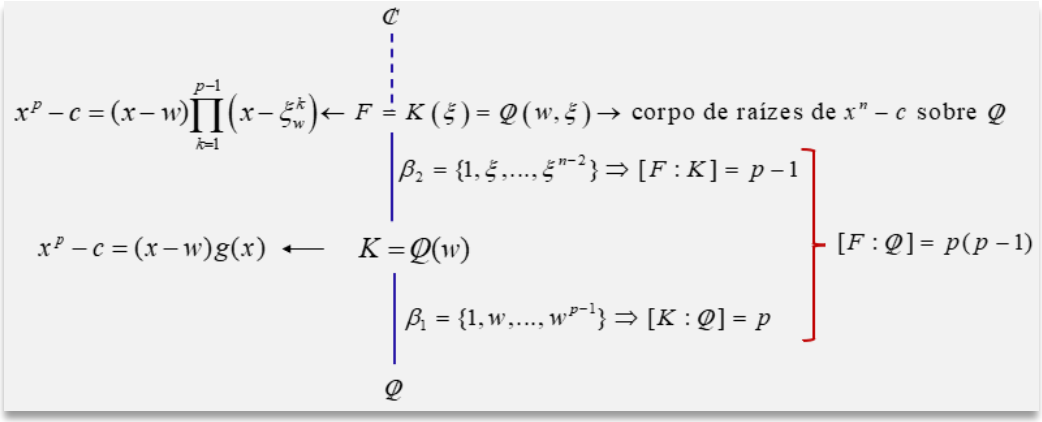

Figura 3. Visualização das extensões algébricas $F = K(\xi) = Q(\omega,\xi) \supset K = Q(\omega) \supset Q$.

Dentro desse contexto vamos considerar a equação cúbica $x^3 - 2 = 0$ em C. Usando (27) resulta $\omega = \sqrt[3]{2}\ (b=0, \beta=0)$ como sendo um zero real dessa equação.

Da aplicação 3.2; $\xi = e^{i\frac{2\pi}{3}}$ é uma raiz cúbica primitiva da unidade, então $\omega,\ \xi\omega,\ \xi^2\omega$, onde $\xi^2 = \overline{\xi}$ são as três raízes dessa equação. Portanto, usando (30) $F = Gal\left(x^3-2, Q\right) = \left\{\lambda_{ij}\left(\xi^i\omega^j\right);\quad \lambda_{ij} \in Q,\ 0 \le i \le 1,\ 0 \le j \le 2\right\}$. A Fig. 4 mostra as raízes cúbicas de $x^3 - 2$ comparadas com as raízes cúbicas da unidade, ambas como vértices de triângulos equiláteros de lados inscritos respectivamente em círculos de raio 1 e ω.

A transformação geométrica $\varphi: D_1 \to D_\omega$ definida por $\varphi(z) = \omega z$ é uma bijeção linear que expande o disco unitário D_1 de uma "extensão" ω, pois $|\omega z| = \omega$ e $\arg(\omega z) = \arg z$ no disco D_ω de raio ω.

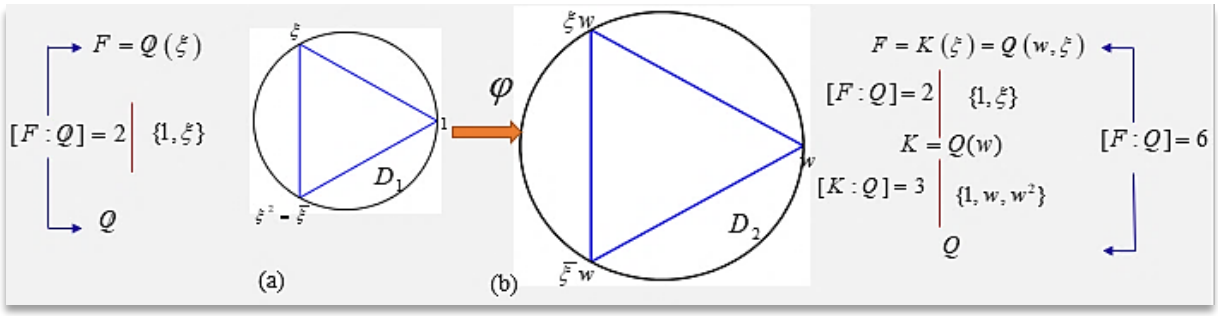

Figura 4. Representação dos zeros das equações ciclotômicas: (a) $x^3 - 1 = 0$. e (b) $x^3 - 2 = 0$ e suas torres de extensões sobre o corpo base Q.

4.4 Aplicação: sinais digitais

Uma aplicação importante das raízes da unidade é no processamento de sinais digitais. Segundo [14] um sinal trata-se muitas vezes de uma quantidade física que varia com o tempo, onde a temperatura é um bom exemplo, pois medida a cada hora, a temperatura flutuará. Também a posição de um móvel, com referência à sua posição no tempo, $M = M(t)$, ou no espaço $M = M(x,y,z)$. Outro exemplo de importância prática é o sinal senoidal $x(t) = \alpha\cos(2\pi ft + \varphi)$, onde $|\alpha| = \max\{|x(t)|\}$ é a amplitude ou magnitude do sinal, $f = \frac{1}{T}$ a

frequência ou o número de oscilações por segundo (Hz), T é o período, isto é, o intervalo de tempo antes que o sinal se repita e, φ a fase inicial do sinal.

Nessa aplicação estamos interessados nos sinais discretos ou digitais, isto é, aqueles cujos valores podem ser armazenados como números racionais em um computador digital. Portanto, ainda segundo [14] no âmbito digital, um sinal nada mais é do que uma lista de números ou seja, um vetor unidimensional. Os sinais que serão aqui analisados serão os sinais discretos, ou seja, aqueles que têm índice inteiro e valor discreto, isto é, que podem ser representados por um computador digital. Pode-se obter um sinal digital a partir de um sinal analógico por meio de um processo conhecido como *amostragem*, no qual os valores são medidos (amostrados) em intervalos regulares e armazenados [14]. Segundo [14] em um sinal digital a variável n se relaciona com a variável t por meio da equação $x[n]=x(nT_s)$, $n\in Z$, $x[*];x(*)\in IR$ sendo $T_s\in IR$ o tempo ou período de amostragem, isto é, o intervalo de tempo entre duas amostras que não precisa ser um número inteiro, pois sinais medidos em $T_S=0.001s$ são bastante comuns [14], enquanto $f_s=\dfrac{1}{T_s}$ é a frequência de amostragem que indica o número de leituras ou amostras lidas por segundo. Conforme dito anteriormente a equação $x[n]=x(nT_s)$ que descreve o processo de amostragem não é exatamente o mesmo que $x(t)$, na melhor das hipóteses, $x[n]$ é uma boa aproximação para $x(t)$ [14]. Vamos representar a *N*-ésima raiz da unidade por $W_N=e^{-i\frac{2\pi}{N}}$, onde N é um número inteiro positivo com frequência fundamental $f=\dfrac{2\pi}{N}$.

Seja $\phi_k(n)=W_N^{-kn}=e^{i\frac{2\pi}{N}kn}\left(=\xi^{kn}\right)$, então para cada inteiro k fixado, $k=0,...,N-1$, tem-se que $\varphi_k(n)$ é uma sequência periódica de período *N*, com n sendo um inteiro variando também de zero até $N-1$, isto é, $n=0,...,N-1$.

Note que os valores de $\phi_k(n)$ são raízes *N*-ésimas raiz da unidade! Considere $U=\{u_N(n):n\in Z,\ n=0,...,N-1\}$ das sequências periódicas de período N, então esse conjunto forma um espaço vetorial sobre o corpo dos números complexos. Sejam $k,m=0,...,N-1$ inteiros e definamos

$$\langle\varphi_k(n),\varphi_m(n)\rangle=\sum_{n=0}^{N-1}\varphi_k(n)\,\varphi_m^*(n)=\sum_{n=0}^{N-1}e^{i\frac{2\pi}{N}kn}e^{-i\frac{2\pi}{N}mn}=\sum_{n=0}^{N-1}e^{-i\frac{2\pi}{N}(m-k)n}\ , \tag{31}$$

onde $\varphi_k(n)$ e $\varphi_m(n)$ são vistos como vetores em $\mathbb{C}^N$ como um $\mathbb{C}$ espaço vetorial onde $\varphi_m^*(n)$ representa a conjugação complexa. Note que a afirmação anterior é baseada no seguinte resultado: para todo $x,y\in\mathbb{C}^N\Rightarrow\langle x,y\rangle=\sum_{j=1}^{N}x_j\bar{y}_j$ define o produto interno canônico em $\mathbb{C}^N$ como um $\mathbb{C}$ espaço vetorial ou espaço unitário [15].

Vamos mostrar que $\{\varphi_k(n)\in U;n=0,...,N-1\}$, $k=0,...,N-1$ forma um subconjunto ortogonal de U com respeito a esse produto interno. De fato,

$$k\neq m\Rightarrow I_{k,m}=\sum_{n=0}^{N-1}e^{i\frac{2\pi}{N}(k-m)n}=\frac{1-q^N}{1-q}=\frac{1-e^{i2\pi(k-m)}}{1-q}=0,$$

ou seja, ϕ_k e ϕ_m são ortogonais, caso $k\neq m$ onde $q=e^{-i\frac{2\pi}{N}(m-k)}$ é a razão da soma da progressão geométrica finita decorrente do produto interno $I_{k,m}$. Além disso, o comprimento de cada vetor $\phi_k(n)$ pode ser diretamente obtido da igualdade abaixo,

$$\left\|\varphi_k(n)\right\|^2 = I_{k,k} = \left\langle \varphi_k(n), \varphi_k(n)\right\rangle = \sum_{n=0}^{N-1} \varphi_k(n)\varphi_k^*(n) = \sum_{n=0}^{N-1} e^{i\frac{2\pi}{N}kn} e^{-i\frac{2\pi}{N}kn} = \sum_{n=0}^{N-1} 1 = N, \tag{32}$$

ou simplesmente,

$$\left\|\varphi_k(n)\right\| = \sqrt{N}. \tag{33}$$

Podemos concluir que

$$\Im = \left\{ \frac{1}{\sqrt{N}}\varphi_k(n) \in U : n = 0,...,N-1 \right\} = \left\{ \frac{1}{\sqrt{N}} W_N^{-kn} : n = 0,...,N-1 \right\} \left(= \left\{ \frac{1}{\sqrt{N}} \xi^{kn} : n = 0,...,N-1 \right\} \right), k = 0,...,N-1$$

forma um conjunto ortonormal nesse espaço. Segundo [17] a matriz unitária $N \times N$, $F = \left\{ \frac{1}{\sqrt{N}} W_N^{kn} \right\}$, $k,n = 0,...,N-1$, onde $W_N^{kn} = e^{-i\frac{2\pi}{N}kn} \left(= \overline{\xi}^{kn} \right)$ é denominada *matriz de Fourier*. Cada sequência $\phi_k(n)$, com $n = 0,...,N-1$em pode ser vista como sendo um vetor no espaço C^N sendo $\phi_k = \left\{ \frac{1}{\sqrt{N}} W_N^{-kn}, 0 \le n \le N-1 \right\}^T$, $k = 0,...,N-1$, onde $W_N^{-kn} = e^{i\frac{2\pi}{N}kn} = \xi^{kn}$. Resulta que esses vetores são as colunas de $F^{*T} = F^*$ da matriz de Fourier F. Portanto, os vetores ϕ_k, $k = 0,...,N-1$ formam uma base ortonormal do espaço vetorial U de dimensão N. Então todo elemento $x_N = x_N(n) \in U$ pode ser escrito na forma $x_N = x_N(n) = \sum_{k=0}^{N-1} \left\langle x_N \mid \phi_k \right\rangle \phi_k$ [16]. Esse teorema é relativo à decomposição ortogonal da sequência ou vetor x_N nas direções dos vetores básicos ϕ_k. Desse modo podemos escrever

$$x_N = \sum_{k=0}^{N-1} \left\langle x_N \mid \phi_k \right\rangle \phi_k = \frac{1}{N} \left(\left\langle x_N, \phi_0 \right\rangle \phi_0 + ... + \left\langle x_N, \phi_{N-1} \right\rangle \phi_{N-1} \right), \tag{34}$$

ou ainda por

$$x_N = \sum_{k=0}^{N-1} \left\langle x_N \mid \phi_k \right\rangle \phi_k = \frac{1}{N} \left(\left(\sum_{n=0}^{N-1} x_N(n) \phi_0^* \right) \phi_0 + ... + \left(\sum_{n=0}^{N-1} x_N(n) \phi_{N-1}^* \right) \phi_{N-1} \right). \tag{35}$$

Como cada ϕ_k é expresso por W_N^{-kn}, então tomando a conjugação complexa na eq. (35) podemos escrever

$$x_N = \frac{1}{N} \left(\left(\sum_{n=0}^{N-1} x_N(n) W_N^0 \right) \phi_0 + ... + \left(\sum_{n=0}^{N-1} x_N(n) W_N^{(N-1)n} \right) \phi_{N-1} \right) = X(0) \frac{\phi_0}{\sqrt{N}} + ... + X(N-1) \frac{\phi_{N-1}}{\sqrt{N}}, \tag{36}$$

onde $W_N^{mn} = \overline{\xi}^{mn}$ com

$$X(m) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_N(n) W_N^{mn} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_N(n) \overline{\xi}^{mn}, \quad m = 0,...,N-1. \tag{37}$$

A eq. (37) é a transformada de Fourier discreta (TFD) de $x(n)$ [17], ou seja, em termos matriciais a eq. (37) pode ser escrita como

$$X = \frac{1}{\sqrt{N}} Fx. \tag{38}$$

Na TFD de $x_N(n)$ para cada saída $X(m)$ são utilizadas n frequências do tipo $\frac{2\pi}{N} m(n)$, com $n = 0,...,N-1$e, por isso, m determina a frequência das componentes de $X(m)$, ou seja, a TFD $X(m)$ é uma função caracterizada pelo conteúdo de sua frequência [18]. Por isso, o domínio (valores de m) para os quais $X(m)$, $m = 0,...,N-1$, ou seja, as componentes de frequência da transformada são calculadas, é denominado *domínio de frequência*.

Da eq. (38) tem-se a inversa da TFD dada por [17]

$$x_N = \frac{1}{\sqrt{N}} F^* X, \tag{39}$$

ou na forma

$$x_N(n) = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} X(m) W_N^{-mn} = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} X(m) \xi^{mn}. \quad (40)$$

As eqs. (37) e (40) costumam vir também na forma reportada por [14] trocando m por k e sem o fator $\frac{1}{\sqrt{N}}$, isto é,

$$X[k] = \sum_{n=0}^{N-1} x_N[n] e^{-i\frac{2\pi}{N}kn} \left(= \sum_{n=0}^{N-1} x_N[n] \overline{\xi}^{kn}, k = 0, ..., N-1 \right), \quad (41)$$

e

$$x_N[n] = \frac{1}{N} \sum_{k=0}^{N-1} X(k) e^{i\frac{2\pi}{N}kn} \left(= \frac{1}{N} \sum_{k=0}^{N-1} X(k) \xi^{kn} \right). \quad (42)$$

As eqs. (41) e (42) já se encontram na forma do processo de amostragem do sinal. Segundo [18], a localização do multiplicador $\frac{1}{N}$ não importa, o requisito é que se dois multiplicadores são usados o produto deve dar $\frac{1}{N}$. Pode ser notado das eqs. (40) ou (42) que o sinal $x_N(n)$ ou $x_N[n]$ é uma combinação linear finita de exponenciais complexas $e^{i\frac{2\pi}{N}kn} = \xi^{kn}$ que são múltiplas das raízes *n*-ésimas da unidade, ξ^k e com os $knf's$ múltiplos inteiros da frequência fundamental. Note que das eqs. (37) ou (41) $X(m)$ ou $X(k)$ nos dá à magnitude do *m* ou *k*-ésimo harmônico. Das eqs. (37) ou (41) pode ser visto que $X(m)$ ou $X(k)$ separa a *m*, ou a *k* ésima componente de frequência do sinal $x(n)$ ou $x[n]$, ou seja, usando a analogia proposta por [18], a TFD funciona como um "prisma matemático" que separa o sinal em suas várias componentes de frequência. Como em geral, $X(m)$ ou $X(k)$ são quantidades complexas pode-se, usando a análise complexa escrever $X(m) = |X(m)| e^{-i\phi(m)}$ em coordenadas polares, onde $\phi(m) = tg^{-1}\left[\frac{I(m)}{R(m)}\right]$, sendo $I(m)$ e $R(m)$ respectivamente a parte real e imaginária de $X(m)$ e $\phi(m)$ o ângulo de fase ou fase do espectro da transformada. Portanto, conhecendo o espectro e o ângulo de fase de cada componente de frequência pode-se obter o sinal original com base nas eqs. (37) e (38) ou eqs. (41) e (42).

A metodologia utilizada nesse artigo para a obtenção da TFD e a sua inversa, difere na forma de apresentação da utilizada por [14] onde, por exemplo, a magnitude complexa do *k*-ésimo harmônico $X(k)$ é obtido pela convolução de duas sequências discretas $X(l)$ e $\delta(k-l)$ conforme pode ser visto na eq. (3.27) reportada por [14]. Embora não seja nosso objetivo nos estendermos mais na teoria de sinais digitais, veremos uma aplicação do funcionamento da TFD em um caso particular.

Uma vez conhecido o conteúdo de frequência k vamos ver por meio de um exemplo prático como a TFD atua sobre ele. Vamos usar o exemplo de um sinal de entrada simples proposto por [18], a saber um sinal senoidal da forma $x(t) = 2\cos(2\pi ft)$ cuja versão digital é dada por $x_N[n] = 2\cos(2\pi nT_s)$. Em vez de usar a TFD diretamente em $x[n]$ vamos usar a igualdade $\cos(\theta) = \frac{1}{2}\left(e^{i\theta} + e^{-i\theta}\right)$ que facilitará a aplicação da TFD resultando no sinal $x_N[n] = e^{i2\pi fnT_s} + e^{-i2\pi fnT_s}$. Se nos ativermos apenas às frequências positivas, podemos escrever $x_N[n] = e^{i2\pi fnT_s}$. Para obter o espectro de frequências basta usar a eq. (41) nesse sinal para obter

$$X[k]=\sum_{n=0}^{N-1}x[n]\,e^{-i\frac{2\pi}{N}kn}=\sum_{n=0}^{N-1}e^{i2\pi fnT_s}\,e^{-i\frac{2\pi}{N}kn}=\sum_{n=0}^{N-1}e^{i2\pi\left(fnT_s-\frac{kn}{N}\right)}. \tag{43}$$

A frequência de análise amostral é dada segundo [14] por $f_{análise}[k]=\dfrac{k\,f_s}{N}$. Vamos supor que a frequência real f seja um múltiplo de $\dfrac{f_s}{N}$, na forma $\dfrac{k\,f_s}{N}$, então a frequência $f=f_{análise}[k]=\dfrac{k\,f_s}{N}$, ou seja, a frequência real do sinal coincide com a frequência de análise. Nesse caso desde que $f_sT_s=1$, tem-se que

$$X[k]=\sum_{n=0}^{N-1}x[n]e^{-i\frac{2\pi}{N}kn}=\sum_{n=0}^{N-1}e^{i2\pi\left(\frac{kf_snT_s}{N}-\frac{kn}{N}\right)}=\sum_{n=0}^{N-1}e^{i2\pi\left(\frac{kn}{N}-\frac{kn}{N}\right)}=\sum_{n=0}^{N-1}1=N. \tag{44}$$

E a TFD para os demais pontos? Vamos examinar $X[k+1]$ a luz da eq. (41). Nesse caso resulta que

$$X[k+1]=\sum_{n=0}^{N-1}e^{i2\pi\left(fnT_s-\frac{[k+1]n}{N}\right)}=\sum_{n=0}^{N-1}e^{i2\pi\left(\frac{kn}{N}-\frac{[k+1]n}{N}\right)}=\sum_{n=0}^{N-1}e^{i2\pi\left(-\frac{n}{N}\right)}=0, \tag{45}$$

pois esse somatório é a soma de uma progressão geométrica finita de razão $e^{-i\frac{2\pi}{N}}$. Com isso, todo o espectro de frequência só tem um único pico em $f=\dfrac{kf_s}{N}$ (Hz) de magnitude N e zero quando diferente de f.

Vamos considerar um sinal senoidal da forma $x(t)=2\cos(2\pi 30t)$, onde $f=30$ com a seguinte amostragem simulada: $N=200$ (amostras) número de amostras coletadas à taxa de $f_s=400$ (amostras por segundo). Em $k=15$, tem-se que $f_{análise}[k=15]=k\cdot\dfrac{f_s}{N}=15\cdot\dfrac{400}{200}=30=f$, ou seja, $X[30]=200$ e, fora de $k=15$, $X[k+1]=0$.

A Fig. 5(a) mostra 56 das $N=200$ amostras do sinal senoidal coletadas no tempo de 0.14 s, enquanto a Fig. 5(b) é o gráfico da magnitude de frequências do sinal amostrado. Em $k=30$, o sinal tem magnitude igual à 200 e, fora dele, todas as magnitudes são nulas.

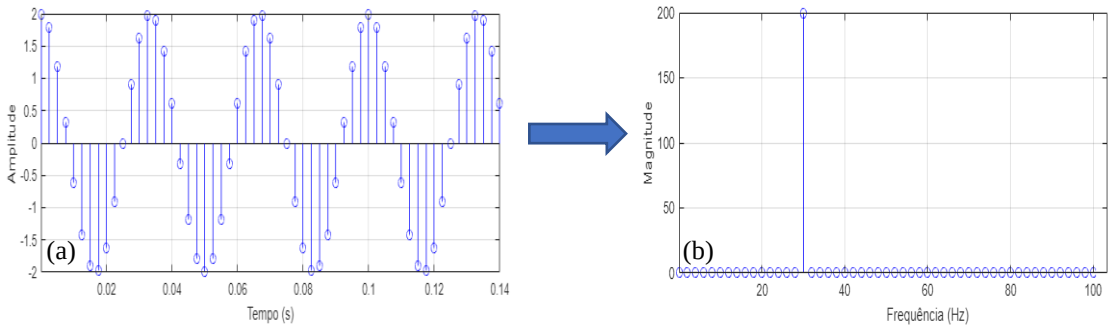

Figura 5: (a) Sinal amostrado no intervalo de 0.14s e (b) TFD do sinal $x(t)=2\cos(2\pi 30t)$ com a amostragem simulada na faixa de 0 a 100 Hz no domínio de frequência.

Essa teoria unidimensional de processamento de sinais digitais, pode ser estendida para imagens digitais bidimensionais onde a TFD sobre uma $N\times N$ imagen $\{u(m,n)\}$ é dada segundo [1] por $v(k,l)=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}u(m,n)\,W_N^{km}W_N^{\ln}$, $0\le k,\,l\le N-1,$, que nada mais é do que uma generalização da eq. (40) para duas dimensões.

Toda a tecnologia de processamento de sinais depende da matriz de Fourier F. O sinal é digitalizado, seja de origem da fala, imagens, sonar, telecomunicações ou de exploração de petróleo. O sinal x é transformado pela matriz F, isto é, Fx e, depois transformado de volta após algum tipo de processamento, como por exemplo, uma filtragem no domínio de frequência ou mesmo no domínio temporal. De acordo com [1] a TFD é uma das mais importantes transformadas do processamento de sinais e imagens digitais.

6 Conclusões

As aplicações envolvendo a racionalização de frações algébricas elementares via extensão de corpos se mostrou eficaz para exemplos mais complexos quando comparada ao método tradicional que utiliza o conjugado. A proposição aqui estabelecida para a racionalização de certas frações irracionais com base na teoria da extensão de corpos, amplia significativamente a possibilidade de exemplos mais complexos que podem ser apresentados para turmas do fim do ciclo do Ensino Fundamental e do Ensino Médio.

O problema da duplicação do cubo de matemáticos gregos da Grécia antiga foi analisado a luz dessa teoria. As raízes n-ésimas da unidade foram utilizadas para a construção de uma base ortonormal no espaço de sequências discretas e periódicas estabelecendo uma conexão entre a teoria das extensões algébricas e a teoria de processamento de sinais digitais com base na matriz de Fourier. As aplicações aqui analisadas, tem por objetivo mostrar a importância da teoria da Álgebra Abstrata em problemas de interesse matemáticos e científicos.

Referências

[1] GONÇALVES, A. **Introdução à álgebra**. Rio de Janeiro: IMPA, 1979. (Projeto Euclides; 7).

[2] BIRKHOFF, G.; MACLANE, S. **Álgebra moderna básica**. 4. ed. Rio de Janeiro: Guanabara Dois, 1977.

[3] ROQUE, T.; CARVALHO, J. B. P. **Tópicos de história da matemática.** 2. ed. Rio de Janeiro: SBM, 2012. (Coleção PROFMAT; 3).

[4] DEAN, R. A. **Elementos de álgebra abstrata**. Rio de Janeiro: Livros Técnicos e Científicos, 1974.

[5] SYNGE, J. L; GRIFFITH, B. A. **Mecânica racional**. Tradução de Nelson França Furtado. 2. ed. Porto Alegre: Globo, 1968.

[6] BASSANEZI, R. C.; FERREIRA JUNIOR, W. C. **Equações diferenciais com aplicações**. São Paulo: Paulo: Harbra, 1988.

[**7**] KIM, K. **Conceptual digital signal processing with Matlab**. Singapore: Springer, 2020.

[8] REZENDE, J. de C. **Um estudo sobre as raízes da unidade e suas aplicações em matemática**. 2017. Dissertação (Mestrado em Matemática) - Universidade Estadual Paulista a "Júlio de Mesquita Filho", Instituto de Geociências e Ciências Exatas, Rio Claro, 2017.

[9] MIGUEL, M. J. **Construções com régua e compasso**. 2018. Dissertação (Mestrado em Matemática) - Universidade Federal Rural de Pernambuco, Recife, 2018.

[10] HERSTEIN, I. N. **Tópicos em álgebra.** Editora polígono com a colaboração da editora USP. 1970.

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

[12] SILVA, A. K. S. Construções com régua e compasso: uma abordagem elementar. **C.Q.D. – Revista Eletrônica Paulista de Matemática**, Bauru, v. 22, n. 1, p. 10–26, jul. 2022. Disponível em: https://sistemas.fc.unesp.br/ojs/index.php/revistacqd/index. Acesso em: 10 julho 2024.

[13] HEFEZ, A. **Curso de álgebra**. 5. ed. Rio de Janeiro: IMPA, 2016. v. 1. (Coleção matemática universitária).

[14] WEEKS, M. **Processamento digital de sinais utilizando Matlab e Wavelets.** 2. ed. Rio de Janeiro: LTC, 2012.

[15] BRONSON, R.; COSTA, G. **Equações diferenciais**. 3. ed. Porto Alegre: Bookman, 2008. *E-book.*

[16] DAVIS, H. F. **Fourier series and orthogonal functions.** New York: Dover Publications, 1963.

[17] ANIL, K. J. **Fundamentals of digital image processing:** Englewood Cliffs: Prentice Hall, c1989. (Prentice Hall information and system sciences series).

[18] GONZALEZ R. C., WOODS, R. E. **Digital image processing**. 2nd ed. Upper Saddle River: Prentice Hall, 2002.