Brazilian Electronic Journal of Mathematics, v.3 - n.5, jan/jun, 2022. ISSN: 2675-1313

Construções geométricas com Origami e a teoria de Galois

Geometric constructions with Origami and the Galois theory

Patrícia Borges dos Santos[1]

Resumo. A surpreendente conexão entre construções geométricas feitas com Origami e a teoria de Galois será explorada. Assim como as construções clássicas, as construções com Origami possuem uma interpretação algébrica por meio da teoria de Galois, e em ambos contextos ela se mostra uma poderosa ferramenta geométrica. Neste sentido será necessário assimilar alguns dos conceitos básicos da teoria de Galois, além das construções geométricas feitas com régua e compasso para, posteriormente, analisar e compreender como as construções geométricas feitas com Origami resolvem alguns dos problemas clássicos da geometria que são insolúveis via régua e compasso. Além disso, foi também objetivo deste texto introduzir a teoria de Galois da maneira mais acessível possível para um público de graduação.

Palavras-chave. Construções geométricas. Origami. Teoria de Galois.

Abstract. The surprising connection between geometric constructions made with Origami and Galois Theory will be explored. Like classic constructions, Origami constructions have an algebraic interpretation through the Theory of Galois, and in both contexts it proves to be a powerful geometric tool. In this sense it will be necessary to assimilate some of the basic concepts of Galois Theory, in geometric constructions made with ruler and compass to later analyze and understand how the geometric constructions made with Origami solve some of the classic geometry problems that are insoluble via ruler and compass. Moreover, was also a goal of this text to introduce Galois theory in as accessible a manner as possible for an undergraduate audience.

Keywords. Geometric constructions. Origami. Galois theory.

[1]Instituto de Ciências Exatas e Naturais do Pontal, Universidade Federal de Uberlândia, patriciabs@ufu.br

Mathematics Subject Classification (MSC). primary 12F10; secondary 51M15.

1 Introdução

Desde a Grécia antiga alguns problemas de construção geométrica desafiaram gerações de matemáticos. Os Três Problemas Clássicos, como são conhecidos, estão enunciados abaixo:

I. A quadratura do círculo: dada uma circunferência, construir um quadrado com a mesma área desta circunferência.

II. A duplicação do cubo: dado um cubo, construir um novo cubo com volume igual ao dobro do volume do primeiro.

III. A trissecção do ângulo: dado um determinado ângulo, construir um novo ângulo com um terço de sua amplitude.

Tais construções deveriam ser executadas utilizando-se apenas uma régua sem marcações, para desenhar retas e, um compasso, para desenhar círculos. Foi a teoria de Galois que permitiu transcrever esses problemas geométricos para problemas algébricos por meio de conceitos como, por exemplo, os conceitos de corpos, de extensões de corpos, e de números construtíveis. Uma questão importante que é provada utilizando-se resultados algébricos é que nenhum dos Três Problemas Clássicos tem solução utilizando-se apenas régua e compasso. Referências acessíveis sobre isso são, por exemplo, [4], [6] e [9].

A busca por uma ferramenta mais eficiente do que as construções clássicas (via régua e compasso) que solucione os Três Problemas Clássicos levaram muitos matemáticos a buscarem variações. Recorrendo-se ao uso de régua com marcação, ao uso de cônicas e curvas mecânicas e ao uso de outras ferramentas além do compasso alguns dos problemas clássicos da geometria grega foram resolvidos. Mas sem dúvida, uma das mais interessantes variações é uso de Origami ou dobraduras para executar tais construções geométricas.

Para muitos o Origami, é apenas uma arte de transformar folhas de papel sem cortes, através da execução de dobraduras, em formas interessantes e bonitas. Mesmo que aparentemente, o Origami seja um produto artístico, ele tem chamado atenção, devido às suas interessantes propriedades algébricas e geométricas (vide [16]). Veremos na seção 5 que as construções com Origami constituem uma ferramenta mais eficiente na resolução dos problemas geométricos clássicos. Por meio delas é possível trissectar qualquer ângulo

dado e duplicar qualquer cubo dado, o que não é possível de ser executado com régua e compasso. Já o problema da quadratura do círculo, mesmo no contexto de Origami, continua insolúvel.

Em seu site [11], Thomas Hull (2015) dá um excelente panorama da relevância desta relação entre Matemática e Origami:

> [...] a matemática do Origami, vem sendo extensivamente estudada por origamistas, matemáticos, cientistas e artistas. O matemático italiano-japonês Humiaki Huzita formulou uma lista de axiomas que definem o Origami geometricamente. O físico Jun Maekawa descobriu alguns teoremas fundamentais sobre Origami e usa tais teoremas para projetar modelos de Origami numa elegância surpreendente. O matemático Toshikazu Kawasaki tem um número de teoremas de Origami com seu nome e tem generalizado algum deles para descrever dobradura de papeis em dimensões maiores (Origami na quarta dimensão!). Robert Lang, da Califórnia, tem desenvolvido um método engenhoso de algoritmizar o processo de projetar Origamis, usando o computador para ajudá-lo a inventar modelos de complexidade espetacular. O educator Shuzo Fujimoto e o artista Chris Palmer descobriram paralelos maravilhosos entre Origami e pavimentação. E um grande número de professores tem desenvolvido inúmeros jeitos de usar o Origami para ensinar conceitos de matemática, química, física e arquitetura. (tradução livre da autora)

Mais informações sobre o trabalho dos autores citados no parágrafo acima podem ser encontradas respectivamente em [13], [14], [15], [16], [7] e [18]. Referência adicionais sobre as técnicas utilizadas no Origami para criar incríveis figuras de Origami podem ser vistas em [16], e sobre alguns aspectos matemáticos do Origami podemos citar [1] e [2].

2 Conceitos Preliminares

Para começarmos a explanação do assunto, iremos definir alguns elementos da teoria de Galois que serão utilizados no decorrer do texto. A maioria deles podem ser encontrados em qualquer livro de álgebra abstrata, veja por exemplo [12].

Um corpo L é dito uma extensão de F, se L contém F como um subcorpo. Neste caso denotaremos $F \subset L$. O corpo F será chamado de corpo base da extensão $F \subset L$.

A dimensão de L, quando considerado como um espaço vetorial sobre F, é o grau da extensão de corpos $F \subset L$, e será denotado por $[L : F]$. Dizemos que a extensão $F \subset L$ é finita quando o grau $[L : F]$ for finito.

Num curso de Álgebra linear básica já nos deparamos com extensões de corpos, por exemplo, vimos que $\mathbb{C}$ é um espaço vetorial real de dimensão 2. No contexto de extensões de corpos esta mesma afirmação seria escrita como $\mathbb{R} \subset \mathbb{C}$ é uma extensão finita de grau $[\mathbb{C} : \mathbb{R}] = 2$.

Se $F \subset L$ uma extensão de F, um elemento $\alpha \in L$ é algébrico sobre F se existe $f(x) \in F[x] \setminus \{0\}$ tal que $f(\alpha) = 0$. Caso contrário, dizemos que α é transcendente sobre F. Se todo $\alpha \in L \supset F$ é algébrico sobre F, então $F \subset L$ diz-se uma extensão algébrica.

Observe que $\sqrt[3]{2}$ é um elemento algébrico sobre $\mathbb{Q}$ enquanto π é um elemento transcendente sobre $\mathbb{Q}$. Evidentemente, se $\alpha \in F$ então α é algébrico sobre F já que é raiz de $p(x) = x - a \in F[x]$.

Se $F \subset L$ é uma extensão de corpos e $\alpha \in L$ algébrico sobre F. O polinômio mínimo de α sobre F, denotado por $m(\alpha, F)(x)$, é o polinômio mônico de menor grau em $F[x]$ que possui α como raiz.

Se observarmos que $x^3 - 2$ é o polinômio de menor grau com coeficientes racionais que tem $\alpha = \sqrt[3]{2}$ como raiz, deduzimos que o polinômio mínimo de $\alpha = \sqrt[3]{2}$ sobre $\mathbb{Q}$ será $m(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$. Analogamente, pode-se concluir que $m(i, \mathbb{R}) = x^2 + 1$.

O polinômio mínimo de α sobre F também pode ser pensado como o gerador do núcleo do homomorfismo entre $F[x]$ e L definido por $f(x) \mapsto f(\alpha)$. Por isso, pode-se mostrar que este polinômio é irredutível em $F[x]$, ou seja, $m(\alpha, F)(x)$ é um polinômio que não pode ser fatorado, em $F[x]$, no produto de dois polinômios não constantes.

Lema 1. *Seja F um corpo de característica diferente de 2. Toda extensão $F \subset L$ de grau 2 é da forma $L = F(\beta)$ sendo $\beta \in L \setminus F$ e $\beta^2 \in F$.*

Demonstração. Como $[L : F] = 2$ existe $\alpha \in L \setminus F$ tal que $\{1, \alpha\}$ é F-base de L como espaço vetorial. Daí, $\alpha^2 = r + s\alpha$ com $r, s \in F$. Tome $\beta = \alpha - \frac{s}{2}$. Veja que $\beta \in L \setminus F$ e que $\{1, \beta\}$ também é F-base de L. Além disso,

$$\beta^2 = \left(\alpha - \frac{s}{2}\right)^2 = r + \frac{s^2}{4} \in F \tag{1}$$

Agora como $F(\beta)$ é subcorpo de L contendo F temos apenas as opções $[L : F(\beta)] = 1$ ou $[F(\beta) : F] = 1$. Esta última contraria a escolha de α. Logo $[L : F(\beta)] = 1$ e portanto $L = F(\beta)$.

O lema anterior garante que se F de característica diferente de 2 toda extensão de grau 2 de F é obtida ao se tomar raiz quadrada. Por esta razão extensões de grau 2 de um corpo F (de característica diferente de 2) são chamadas de extensões quadráticas.

A extensão $\mathbb{R} \subset \mathbb{C}$ é um exemplo de extensão quadrática pois além de $\mathbb{R}$ tem característica zero, $\mathbb{R} \subset \mathbb{C}$ é de grau dois e podemos escrever $\mathbb{C} = \mathbb{R}[i]$ sendo $\beta = i \in \mathbb{C} \setminus \mathbb{R}$ e

$\beta^2 \in \mathbb{R}$ como no lema 1.

Seja $f \in F[x]$ um polinômio de grau $n > 0$. Então a extensão $F \subset K$ é um corpo de decomposição de f sobre F se:

a) $f(x) = c(x - \alpha_1) \dots (x - \alpha_n)$, com $c \in F$ e $\alpha_i \in K$ e,

b) $K = F(\alpha_1, \dots, \alpha_n) = \left\{ \dfrac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} \ : \ \forall\, f,\, g \in F[x_1, \dots, x_n],\, g \neq 0 \right\}$.

O corpo de decomposição também pode ser pensado como sendo a menor extensão de F sobre a qual f se decompõe em um produto finito de fatores lineares.

Por exemplo, o corpo de decomposição do polinômio $f(x) = x^3 - 2$ não é $\mathbb{Q}(\sqrt[3]{2})$, pois em $\mathbb{Q}(\sqrt[3]{2})[x]$, f se fatora como $(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$. Entretanto, em $\mathbb{Q}(\sqrt[3]{2}, \omega)[x]$ temos a decomposição em fatores lineares, $(x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2)$, sendo ω uma raiz cúbica da unidade. Desta forma, $\mathbb{Q}(\sqrt[3]{2}, \omega)$ é o corpo de decomposição de $f(x) = x^3 - 2$.

Se temos uma extensão finita $F \subset L$ o grupo de Galois é o conjunto dos automorfismos de L que fixam F, a saber,

$$Gal(L/F) = \{\sigma : L \to L \,|\, \sigma \text{ é automorfismo, } \sigma(a) = a \text{ para todo } a \in F\}$$

munido com a operação de composição de funções. A cada subgrupo $H \subset Gal(L/F)$ associamos o subcorpo:

$$L_H = \{\alpha \in L \,|\, \sigma(\alpha) = \alpha, \text{ para todo } \sigma \in H\}.$$

Note que $F \subset L_H \subset L$. Isto justifica o porquê destes L_H serem chamados de subcorpos intermediários.

Se $L = F(\alpha_1, ..., \alpha_n)$, devido à definição de $Gal(L/F)$, pode-se verificar que todo $\sigma \in Gal(L/F)$ é unicamente determinado pelos valores que assume em $\alpha_1, ..., \alpha_n$. Além disto, se $\alpha \in L$ é raiz de um polinômio não constante então $\sigma(\alpha)$ também e raiz deste polinômio.

Diante disto, considere a extensão $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right) = L$. O polinômio minimal sobre $\mathbb{Q}$ é $x^3 - 2$, cuja única raiz real é $\sqrt[3]{2}$ e portanto ela é a única raiz em $\mathbb{Q}\left(\sqrt[3]{2}\right)$. Daí, todo $\sigma \in Gal(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q})$ deve satisfazer $\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$ e, já que σ é unicamente determinado por $\sigma\left(\sqrt[3]{2}\right)$, σ deve ser a identidade, $\mathbb{1}_L$. Assim, $Gal(\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}) = \{\mathbb{1}_L\}$.

Alguns resultados importantes deste grupo e que usaremos posteriormente serão listadas abaixo sem demonstração. Aos leitores curiosos sugerimos a leitura da Parte II de [5].

Teorema 1. *Se L é o corpo de decomposição de um polinômio em $F[x]$ que possui apenas raízes simples, então o grupo de Galois de $F \subset L$ possui ordem $|Gal(L/F)| = [L : F]$.*

Extensões algébricas também podem ser classificadas em normais e/ou separáveis. Uma extensão algébrica $F \subset L$ é normal se todo polinômio irredutível em $F[x]$ que tiver uma raiz em L deverá ter todas as outras raízes em L. Já as extensões separáveis são aquelas que além de serem algébricas satisfazem a propriedade de que todos elementos de L possuem seu polinômio minimal com todas raízes simples num corpo de decomposição.

Dizemos que uma extensão finita $F \subset L$ é galoisiana se e somente se uma das seguintes condições equivalentes forem satisfeitas:

- L é o corpo de decomposição de um polinômio separável em $F[x]$.
- $F \subset L$ é uma extensão normal e separável.
- $|Gal(L/F)| = [L : F]$.

Teorema 2. *Seja $F \subset L$ uma extensão finita e separável. Então existe uma extensão $L \subset M$ tal que $F \subset M$ é galoisiana.*

Apesar de $f(x) = x^3 - 2$ ser separável, vimos em um exemplo acima que $\mathbb{Q}(\sqrt[3]{2})$ não é o corpo de decomposição do polinômio $f(x) = x^3 - 2$ logo a extensão $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ não é galoisiana. Agora, como $\mathbb{Q}(\sqrt[3]{2}, \omega)$ é o corpo de decomposição de $f(x) = x^3 - 2$ então ela será uma extensão galoisiana.

Teorema 3 (Correspondência de Galois)**.** *Seja $F \subset L$ uma extensão galoisiana. Existe uma correspondência biunívoca os subcorpos intermediários $F \subset K \subset L$ e os subgrupos $H \subset Gal(L/F)$ dada por:*

$$\begin{array}{ccc} \{\textit{subcorpos } F \subset K \subset L\} & \rightleftharpoons & \{\textit{subgrupos } H \subset Gal(L/F)\} \\ K & \longrightarrow & Gal(L/K) \\ K_H & \longleftarrow & H \end{array} \tag{2}$$

Além disso, os mapas descritos acima revertem inclusões e são um o inverso do outro. Mais ainda, se K é o subcorpo correspondente ao subgrupo H por este mapa então $F \subset K$ é galoisiana se e somente se H é um subgrupo normal de $Gal(L/F)$ e, quando isto acontecer existe um isomorfismo natural $Gal(L/F)/H \simeq Gal(K/F)$.

Para ilustrar a correspondência de Galois descrita acima considere a extensão $\mathbb{R} \subset \mathbb{R}(i) = \mathbb{C}$. A conjugação complexa $\tau(z) = \overline{z}$ é um automorfismo de corpos que, restrito à $\mathbb{R}$, coincide com a identidade, ou seja, $\tau \in Gal(\mathbb{C}/\mathbb{R})$. Desta forma, $Gal(\mathbb{C}/\mathbb{R})$ tem pelo menos dois elementos, a saber, $\mathbb{1}_{\mathbb{C}}$ e τ. Agora como $\mathbb{R} \subset \mathbb{C}$ é galoisiana e $[\mathbb{C} : \mathbb{R}] = 2$,

$Gal(\mathbb{C}/\mathbb{R})$ consiste de exatamente dois elementos e portanto, $Gal(\mathbb{C}/\mathbb{R}) = \{\mathbb{1}_{\mathbb{C}}, \tau\}$. A correspondência de Galois neste caso é dada por:

$$\{\mathbb{R},\, \mathbb{C}\} \;\; \rightleftharpoons \;\; \{Gal(\mathbb{C}/\mathbb{R})\} = \{\mathbb{1}_L, \tau\}$$

Na tentativa de fazer um artigo o mais autocontido possível, incluiremos alguns resultados da teoria de grupos.

Um grupo finito G é dito solúvel se existirem subgrupos

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$$

tais que para todo $i \in \{1, \cdots, n\}$ temos:

1. G_i é normal em G_{i-1};
2. $|G_{i-1}/G_i| = [G_{i-1} : G_i]$ é primo.

Todos grupos abelianos são trivialmente solúveis, já que a série requerida acima será dada pelo próprio grupo e o grupo trivial.

Teorema 4 (Burnside)**.** *Se p e q são números primos distintos então todo grupo de ordem $p^n q^m$ é solúvel, para $n,\, m \geq 0$.*

A palavra "solúvel" surgiu a partir da teoria de Galois e da prova de que não existe solução geral para equações do quinto grau. Especificamente, uma equação polinomial é solúvel por radicais se e somente se o grupo de Galois correspondente é solúvel. Para mais informações sobre grupos solúveis sugiro a leitura de [8, Capítulo VII].

3 Construções Geométricas

Essencialmente, há duas maneiras de considerar pontos no plano. Podemos considerar um ponto P tendo coordenadas (x, y), ou que P é representado por um número complexo $\alpha = x + yi$. Se construímos o ponto P representado por $\alpha = x + yi$ então podemos construir retas perpendiculares aos eixos a fim de obter as partes real, x, e imaginária, y, de P. Reciprocamente, dados os números reais x e y é possível obter o ponto (x, y) correspondendo à $z = x + yi$. Também todas as operações aritméticas nos números complexos (adição, subtração, multiplicação e divisão) podem ser efetuadas por fazer operações com suas partes real e imaginária. Dessa forma podemos passar livremente entre estas duas descrições.

Além disto, recordamos que todo $\alpha \in \mathbb{C} \setminus \{0\}$ pode ser escrito na forma polar como $\alpha = re^{i\theta}$, com $r = |\alpha|$ e $0 \leq \theta < 2\pi$ onde $e^{i\theta} = \cos\theta + i\text{sen}\,\theta$. Note que os $e^{i\theta}$ são os pontos do círculo unitário e que $\zeta_n = e^{i\frac{2\pi}{n}}$ é uma raiz primitiva n-ésima da unidade.

Tendo isto em mente, antes de estabelecer os teoremas sobre construções geométricas, será preciso dar uma descrição detalhada do que se entende por construção geométrica. Considere dois pontos distintos α e β, entende-se por construção geométrica utilizando régua e compasso o que aqui nos referimos à:

C1. A partir de $\alpha \neq \beta$, podemos desenhar a reta ℓ que passa por α e β.

C2. A partir de $\alpha \neq \beta$ e γ, podemos desenhar o círculo C com centro em γ, cujo raio é a distância entre α e β.

Das intersecções entre retas e círculos surgirão novos pontos, a saber:

P1. O ponto de interseção das retas distintas ℓ_1 e ℓ_2 construídas como acima.

P2. Os pontos de interseção entre a reta e o círculo C construídos como acima.

P3. Os pontos de interseção entre os círculos distintos C_1 e C_2 construídos acima.

3.1 Números Construíveis

A questão a ser considerada agora é como traduzir tais problemas de construção geométrica na linguagem da teoria de corpos. Analisamos problemas de construção que investigam quando, dados alguns objetos geométricos iniciais (como pontos, retas ou círculos), podemos criar outros objetos geométricos com certas propriedades, usando apenas régua e compasso. Assumiremos que pelo menos dois pontos são dados, a saber, $0,\ 1 \in \mathbb{C}$. Se, um ponto pode ser construído via régua e compasso e com as operações descritas acima, dizemos que o ponto é construível.

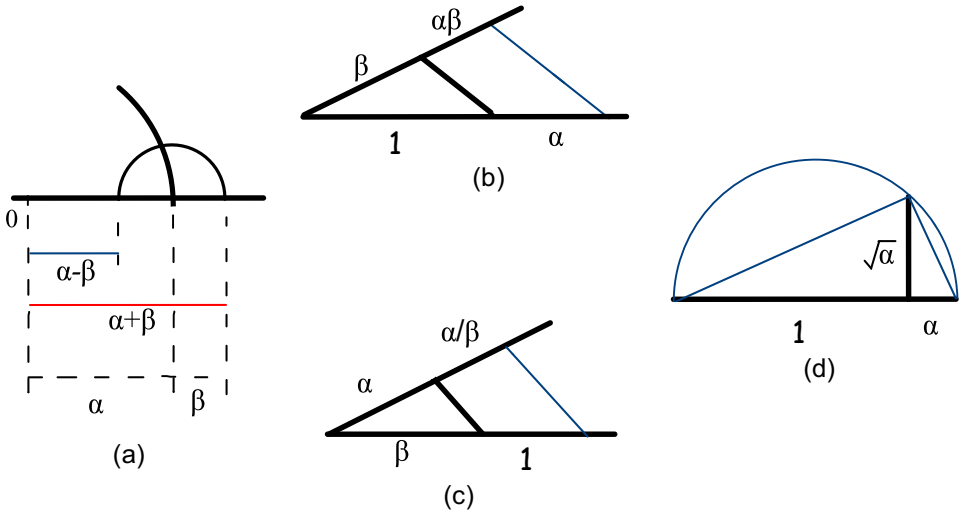
Deste modo, a definição formal que irá viabilizar fazer tal tradução é seguinte:

Definição 1. *Um número complexo α é construível se existir uma sequência finita de construções com régua e compasso usando C1, C2, P1, P2, P3, que começam em 0 e 1 e terminam em α.*

O conjunto dos números construíveis será denotado por $\mathscr{C} = \{\alpha \in \mathbb{C} \,|\, \alpha \text{ é construível }\}$. Por convenção, $0,\ 1 \in \mathscr{C}$. Observe que o número i e os eixos x e y também são construíveis.

Primeiro observe na figura 1 que é possível executar todas as operações aritméticas, além de extrair raiz quadrada (de um número real positivo), via régua e compasso.

Figura 1: Como as operações aritméticas básicas e a extração de raiz quadrada são executadas com régua e compasso



Com isso em mãos temos o resultado:

Teorema 5. *O conjunto $\mathscr{C}$ é um subcorpo de $\mathbb{C}$. Além disso:*

a. Para todos a e $b \in \mathbb{R}$, a e $b \in \mathscr{C}$ se, e somente se, $\alpha = a + ib \in \mathscr{C}$.

b. Se $\alpha \in \mathscr{C}$ então $\sqrt{\alpha} \in \mathscr{C}$.

Demonstração. Inicialmente provaremos que $\mathscr{C}$ é um subgrupo aditivo de $\mathbb{C}$. Dado $\alpha \in \mathscr{C} \setminus \{0\}$ desenhe, por C1, a reta que liga 0 à α e, por C2, o círculo de raio $|\alpha|$ centrado na origem. Estes objetos se interceptam em $\pm\alpha$, sendo portanto $-\alpha$ construível, por P2.

Agora suponha que α e β são construíveis. Podemos supor, sem perda de generalidade, que α, β e 0 não são colineares, use C2 duas vezes para construir o círculo de raio $|\alpha|$ centrado em β e, o círculo de raio $|\beta|$ centrado em α como no item (a) da figura 1. Um dos pontos de interseção será $\alpha + \beta$. Concluímos por P3 que $\alpha + \beta$ é construível. Já que, por definição, $0 \in \mathscr{C}$ segue que $\mathscr{C}$ é subgrupo aditivo de $\mathbb{C}$.

Provaremos agora a parte a.: dado $\alpha = a + bi \in \mathscr{C}$ podemos desenhar retas perpendiculares aos eixos x e y passando por α. Isto nos garante a, $bi \in \mathscr{C}$. Já que o círculo de raio $|bi|$ centrado na origem intercepta o eixo x em b, C2 e P2 garantem que $b \in \mathscr{C}$.

Reciprocamente, dados a, $b \in \mathscr{C} \cap \mathbb{R}$, aplicando C2 e P2 ao círculo de raio $|b|$ centrado em 0 vemos que bi é construível. Pelo parágrafo anterior, temos que $a + bi \in \mathscr{C}$. Desta

forma, a prova do item a. está completa.

Considere agora $a,\ b \in \mathscr{C} \cap \{x \in \mathbb{R} : x > 0\}$. Sabendo que $i \in \mathscr{C}$, observe o item (b) da figura 2 e veja como podemos construir bi. Usamos C1 para desenhar a reta l passando por a e por i. Usando construções básicas da geometria Euclidiana é possível traçar uma reta l' passando por bi e paralela à l. Então, por P1, temos que l' e o eixo x se intersectam em um ponto construível c. Segue por semelhança de triângulos que $\dfrac{c}{a} = \dfrac{bi}{i}$, ou seja, $c = ab$. Desta forma, ab é construível. De maneira análoga, a figura 2 item (c) nos mostra que $\dfrac{1}{a}$ também é construível. Isto nos permite concluir que $\mathscr{C} \cap \mathbb{R}$ é subcorpo de $\mathbb{R}$. Para provar que $\mathscr{C}$ é fechado para o produto e para inversão de elementos não nulos, considere $\alpha = a + bi$ e $\beta = c + di$ dois números construíveis. Daí,

$$\alpha\beta = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

Segue pela parte a. que $a,\ b,\ c,\ d \in \mathscr{C} \cap \mathbb{R}$, assim $ac - bd$ e $ad + bc$ estão em $\mathscr{C} \cap \mathbb{R}$ uma vez que este é subcorpo de $\mathbb{R}$. Agora, usando a recíproca da parte a. concluímos que $\alpha\beta \in \mathscr{C}$. Além disto, se $\alpha \neq 0$ temos:

$$\frac{1}{\alpha} = \frac{1}{a + bi}\left(\frac{a - bi}{a - bi}\right) = \frac{a}{a^2 + b^2} + \left(\frac{-b}{a^2 + b^2}\right) i.$$

Usando a parte a. e o fato de $\mathscr{C} \cap \mathbb{R}$ ser subcorpo de $\mathbb{R}$, vemos que $\dfrac{1}{\alpha} \in \mathscr{C}$. Desta forma, $\mathscr{C}$ é um subcorpo de $\mathbb{C}$.

Finalmente mostraremos que $\sqrt{\alpha}$ é construível quando α o é. Podemos assumir que $\alpha \neq 0$. Se escrevemos $\alpha = re^{i\theta}$, $r = |\alpha| > 0$ então queremos provar que $\sqrt{\alpha} = \sqrt{r}e^{i\theta/2}$ é construível. Para tanto, faremos algumas considerações relativas à construtibilidade de α:

- Usando o eixo x e a reta contendo 0 e α (por C1) podemos construir o angulo θ, o qual podemos bissectar por construções usuais, via regua e compasso. Desta forma o angulo $\theta/2$ é construível.

- O círculo de raio $r = |\alpha|$ centrado em 0 (por C2) intersecta o eixo x em $\pm r$. Por P2 vemos que r é construível.

- Se podemos construir $\sqrt{r}$, então podemos traçar o círculo de raio $\sqrt{r}$ centrado na origem (por C2). Então P2 aplicado à este círculo e ao angulo $\theta/2$ construído acima garantem que $\sqrt{r}e^{i\theta/2}$ é construível.

Resta mostrar que $\sqrt{r}$ é construível quando $r > 0$ o é. Considere o diagrama (d) da figura 2. Pela geometria Euclidiana o triângulo de vértices 1, α e $1 + r$ é um triângulo retângulo.

Os triângulos que dividem o lado determinado por 1 e α são semelhantes, assim sendo d a distância de 1 à α temos:

$$\frac{1}{d} = \frac{d}{r}$$

Daí, $d^2 = r$ e, portanto $d = \sqrt{r}$. Já que d é construível concluímos que $\sqrt{r}$ é construível, o que finaliza a prova.

Teorema 6. *Seja α um número complexo. Então $\alpha \in \mathscr{C}$ se, e somente se, existem subcorpos:*

$$\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_{(n-1)} \subset F_n \subset \mathbb{C}$$

tais que $\alpha \in F_n$ e $[F_i : F_{i-1}] = 2$, para todo $1 \leq i \leq n$.

Demonstração. Primeiro iremos supor que existem subcorpos $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_{(n-1)} \subset F_n \subset \mathbb{C}$ tais que $\alpha \in F_n$ e $[F_i : F_{i-1}] = 2$, para todo $1 \leq i \leq n$. Como $[F_i : F_{i-1}] = 2$ segue do Lema 1 que $F_i = F_{i-1}(\sqrt{\alpha_i})$ para algum $\alpha_i \in F_i$. Vamos mostrar por indução em $0 \leq i \leq n$ que $F_i \subset \mathscr{C}$. O caso $F_0 = \mathbb{Q} \subset \mathscr{C}$ segue do fato de $\mathscr{C}$ ser subcorpo de $\mathbb{C}$. Agora suponha que $F_{i-1} \subset \mathscr{C}$ então $\alpha_i \in F_{i-1}$ é construível, o que implica em $\sqrt{\alpha_i} \in \mathscr{C}$ pelo Teorema 5. Assim $F_i = F_{i-1}(\sqrt{\alpha_i}) \subset \mathscr{C}$, como foi afirmado. Isto mostra que $F_n \subset \mathscr{C}$ e assim, em particular, $\alpha \in F_n$ é construível.

Reciprocamente, dado $\alpha \in \mathscr{C}$ precisamos exibir sucessivas extensões quadráticas que começam em $\mathbb{Q}$ e que eventualmente contem α. Iremos provar que existem extensões $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_{(n-1)} \subset F_n \subset \mathbb{C}$ satisfazendo $[F_i : F_{i-1}] = 2$ e tais que F_n contem as partes real e imaginária de todos os números construídos durante o processo de obtenção de α. O teorema seguirá daí, já que $a, b \in F_n$ implicará em $\alpha = a + bi \in F_n(i)$.

Faremos isto usando indução no número N de vezes que usamos P1, P2 e P3 na construção de α. Quando $N = 0$ teremos $\alpha = 0$ ou $\alpha = 1$ e neste caso temos $F_n = F_0 = \mathbb{Q}$. Agora suponha que α é construído em $N > 1$ etapas sendo que a última etapa usa P1, a interseção de duas reta distintas l_1 e l_2. Desta maneira, l_j foi construída, usando C1, a partir de pontos distintos α_j e β_j, para $j = 1, 2$. Pela hipótese de indução existem extensões $\mathbb{Q} = F_0 \subset ... \subset F_n \subset \mathbb{C}$ onde $[F_i : F_{i-1}] = 2$ tal que as partes real e imaginária de α estão em F_n. A reta l_1, que passa por $\alpha_1 \neq \beta_1$, tem equação da forma $a_1x + b_1y = c_1$. Já que as partes real e imaginárias de α_1 e β_1 estão em F_n, podemos considerar que os coeficientes a_1, b_1 e c_1 pertencem a F_n. Analogamente, l_2 tem equação da forma $a_2x + b_2y = c_2$ com a_2, b_2, $c_2 \in F_n$. Portanto as partes real e imaginárias de α são dadas pela única solução do sistema de equações lineares:

$$\begin{cases} a_1x + b_1y &= c_1 \\ a_2x + b_2y &= c_2 \end{cases} \tag{3}$$

Nesta situação, a matriz dos coeficientes é invertível e, portanto a solução será dada por:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \tag{4}$$

Segue disto que as partes real e imaginária de α pertencem à F_n.

Suponha agora que a última etapa da construção de α usa P2, a interseção de uma reta l e uma circunferência C. Assim, l é uma reta passando por $\alpha_1 \neq \beta_1$ (por C1) e C o círculo com centro γ_2 e raio $|\alpha_2 - \beta_2|$, por C2. Os cinco pontos α_1, α_2, β_1, β_2 e γ_2 vieram das etapas anteriores da construção, assim pela hipótese de indução existem extensões $\mathbb{Q} = F_0 \subset ... \subset F_n \subset \mathbb{C}$ onde $[F_i : F_{i-1}] = 2$ tais que as partes real e imaginária destes cinco pontos estão em F_n. Vamos mostrar que as partes real e imaginária de α estão em F_n, ou em uma extensão quadrática de F_n. Como acima l é dada pela equação

$$a_1 x + b_1 y = c_1 \tag{5}$$

com a_1, b_1, $c_1 \in F_n$. Podemos também descrever o círculo C por meio da equação:

$$x^2 + y^2 + a_2 x + b_2 y + c_2 = 0 \tag{6}$$

a_2, b_2, $c_2 \in F_n$. Suponha agora $a_1 \neq 0$, segue da equação (5) que $x = -b_1' y + c_1'$. Substituindo em (6), obtemos uma equação quadrática

$$\left(-b_1' y + c_1'\right)^2 + y^2 + a_2 \left(-b_1' y + c_1'\right) + c_2 = 0.$$

Pela fórmula quadrática, os valores de y envolve uma raiz quadrada de uma expressão em F_n. Se esta expressão pertencer à F_n então y e $x = -b_1' y + c_1'$ também irão pertencer. Daí as partes real e imaginária de α estão em F_n.

Por outro lado, se esta raiz quadrada não está em F_n então ela pertencerá à uma extensão quadrática $F_n \subset F_{n+1}$. Então y e $x = -b_1' y + c_1'$ também pertencerão à F_{n+1}, o que nos garante que as partes real e imaginária de α pertencem a uma extensão quadrática de F_n. Quando $a_1 = 0$ o argumento é bem semelhante (basta trocar os papéis de a_1 e b_1 pois neste caso $b_1 \neq 0$).

Finalmente suponha que a última etapa na construção de α usa P3, a interseção de dois círculos C_1 e C_2. Como foi feito acima podemos encontrar $\mathbb{Q} = F_0 \subset ... \subset F_n \subset \mathbb{C}$ com $[F_i : F_{i-1}] = 2$ tais que os círculos são dados pelas equações:

$$\begin{cases} x^2 + y^2 + a_1 x + b_1 y + c_1 &= 0 \\ x^2 + y^2 + a_2 x + b_2 y + c_2 &= 0 \end{cases} \tag{7}$$

com todos coeficientes em F_n. Além disto sabemos que as partes real e imaginária de α são dadas pela solução de (7). Se subtrairmos uma equação da outra obtemos a expressão:

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0. \tag{8}$$

Já que os círculos C_1 e C_2 são distintos mas não disjuntos podemos ver facilmente que os coeficientes de x e de y não se anulam simultaneamente. Assim, a equação (8) define uma reta. Além disto, se combinarmos esta equação com a primeira de (7) recaímos ao caso anterior de interseção de reta e círculo. Concluímos assim que as partes real e imaginária de α estão em F_n ou em uma extensão quadrática de F_n. Isto completa a prova.

Do Teorema supracitado pode-se observar que todo número construível é algébrico em $\mathbb{Q}$ e o grau de seu polinômio mínimo será uma potência de 2. Formalmente tem-se:

Corolário 1. *Se $\alpha \in \mathscr{C}$ então $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$, para $m \geq 0$.*

Demonstração. Se $\alpha \in \mathscr{C}$ o Teorema 6 nos garante a existência de extensões $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ onde $[F_i : F_{i-1}] = 2$ e $\alpha \in F_n$. Assim, pelo Teorema da torre temos:

$$[F_n : \mathbb{Q}] = [F_n : F_0] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_1 : F_0] = 2^n.$$

Entretanto também sabemos que $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset F_n$. Usando o Teorema da torre novamente concluímos que $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide $[F_n : \mathbb{Q}] = 2^n$. Portanto, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ para algum $m > 0$.

Teorema 7. *Seja $\alpha \in \mathbb{C}$ algébrico sobre $\mathbb{Q}$ e seja $\mathbb{Q} \subset L$ o corpo de decomposição do polinômio minimal de α sobre $\mathbb{Q}$. Então α é construível se e somente se $[L : \mathbb{Q}]$ é uma potência de 2.*

Demonstração. Inicialmente suponha que $[L : \mathbb{Q}]$ é uma potência de 2. Já que $\mathbb{Q} \subset L$ é galoisiana, segue que $|Gal(L/\mathbb{Q})| = [L : \mathbb{Q}]$ é uma potência de 2, digamos $|Gal(L/\mathbb{Q})| = 2^m$. Pelo Teorema 4 sabemos que $Gal(L/\mathbb{Q})$ é solúvel, ou seja, existem subgrupos

$$\{e\} = G_m \subset G_{m-1} \subset \cdots \subset G_1 \subset G_0 = G$$

tais que G_i é normal em G_{i-1} e de índice 2 já que $|Gal(L/\mathbb{Q})| = 2^m$. Isto nos garante que

$$\mathbb{Q} = L_{G_0} \subset L_{G_1} \cdots \subset L_{G_m} = L,$$

com $[L_{G_i} : L_{G_{i-1}}] = 2$ para todo i. Segue do Teorema 6 que α é construível. Para a recíproca mostraremos primeiro que $\mathbb{Q} \subset \mathscr{C}$ é uma extensão normal. Para tanto, tome $\alpha \in \mathscr{C}$, e seja f o polinômio minimal de α sobre $\mathbb{Q}$. Precisamos mostrar que f se fatora

completamente sobre $\mathscr{C}$ sabendo que α é construível. O Teorema 6 assegura a existência de extensões

$$\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_{(n-1)} \subset F_n \subset \mathbb{C}$$

tais que $\alpha \in F_n$ e $[F_i : F_{i-1}] = 2$, para todo $1 \leq i \leq n$. Pelo Teorema 2 existe uma extensão $F_n \subset \mathbb{Q}$ de modo que $\mathbb{Q} \subset M$ é galoisiana. Mais ainda, podemos assumir $M \subset \mathbb{C}$. Observe que f se fatora completamente em M, já que M é normal em $\mathbb{Q}$, f é irredutível em $\mathbb{Q}[x]$ e $\alpha \in F_n \subset M$ é uma raiz de f. Considere agora uma outra raiz β de f. É possível então exibir $\sigma \in Gal(M/\mathbb{Q})$ tal que $\sigma(\alpha) = \beta$. Avaliando as imagens por σ dos corpos $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ temos: $\mathbb{Q} = \sigma(\mathbb{Q}) \subset \sigma(F_1) \subset ... \subset \sigma(F_n)$ tais que $[\sigma(F_i) : \sigma(F_{i-1})] = 2$ para todo i. O Teorema 6 nos diz que $\beta = \sigma(\alpha) \in \sigma(F_n)$ é construível. Isto mostra que f se fatora completamente em $\mathscr{C}$. Segue daí que $\mathscr{C}$ contém um corpo de decomposição L de f sobre $\mathbb{Q}$. Pelo Teorema do Elemento Primitivo temos $L = \mathbb{Q}(\gamma)$ para algum $\gamma \in L$. Já que $\gamma \in \mathscr{C}$, o Corolário 1 implica em $[\mathbb{Q}(\gamma) : \mathbb{Q}] = [L : \mathbb{Q}]$ é uma potência de 2 o que completa a prova deste teorema.

4 Os três problemas clássicos

Na seção anterior destacamos como o mundo artificial das construções geométricas se relaciona com estruturas algébricas tais como grupos e corpos. Isto nos remete à base da história matemática e servirá para dar resposta a três questões geométricas com enunciado elementar e que os antigos gregos não souberam responder.

Os Três Problemas Clássicos, serão reescritos abaixo de maneira algébrica e a insolubilidade de cada um deles será justificada.

4.1 Trisecção do Ângulo:

O problema de trisectar um ângulo qualquer equivale à encontrar raízes de um polinômio irredutível de grau 3. Mas pelo Corolário 1 sabemos que os números construíveis são apenas raízes de polinômios de grau igual a uma potência de 2. De fato, considere $\phi = 3\theta$, pela identidade de Chebyshev $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$ temos que $\cos(\theta)$ é raiz do polinômio $4X^3 - 3X - \cos(\phi) \in \mathbb{Q}(\cos(\phi))$. Dessa forma, trissectar ϕ, via régua e compasso numa sequência finita de etapas, equivale a construir o ângulo θ e, se isso for possível, $\cos(\theta)$ também será construível. Mas pelo Corolário 1, $\cos(\theta) \in \mathscr{C}$ se, e somente se o polinômio $4X^3 - 3X - \cos(\phi)$ for redutível sobre $\mathbb{Q}(\cos(\phi))$ (do contrário, $[\mathbb{Q}(\cos(\phi)) : \mathbb{Q}]$ e, consequentemente $[\mathbb{Q}(\cos(\theta)) : \mathbb{Q}]$, seriam múltiplos de 3). Em particular, concluímos que $\frac{\pi}{3}$ não pode ser trissectado usando apenas régua e

compasso já que $8X^3-6X-1$ é irredutível[2] sobre $\mathbb{Q}$. É importante observar também que existem ângulos específicos que podem ser trissectados, por exemplo, $\theta = 0$ ou mesmo $\theta = \frac{\pi}{2}$.

4.2 Duplicação do Cubo:

O problema de duplicar o cubo consiste em dado um cubo qualquer construir outro com volume igual ao dobro do volume do primeiro. Se iniciarmos com um cubo de arestas de comprimento igual a 1, o volume também será 1, o que significa que precisamos construir um cubo com volume 2. Se isto for possível deveremos construir um número s de modo que $s^3 = 2$, isto é, $s = \sqrt[3]{2}$. Assim a duplicação do cubo com régua e compasso equivale a dizer que $s = \sqrt[3]{2}$ é um número construível. Mas $x^3 - 2$ é o polinômio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$, entretanto pelo Corolário 1 sabemos que $s = \sqrt[3]{2}$ não é construível. Esta contradição prova que não podemos duplicar o cubo usando apenas régua e compasso.

4.3 Quadratura do Círculo:

O problema consiste em construir um quadrado cuja área seja igual à área de um determinado círculo. Dado um círculo de raio 1, sua área será igual a π, então queremos construir um quadrado de lado l tal que $l^2 = \pi$, isto é, $l = \sqrt{\pi}$. Desta forma, a quadratura do círculo via régua e compasso equivale a dizer que $\sqrt{\pi}$ é um número construível. Como $\mathscr{C}$ é um corpo, a construção de $l = \sqrt{\pi}$ implicaria que $\pi = l^2$ também seria construível. Do Teorema 5.b. teríamos que π é algébrico sobre $\mathbb{Q}$. Entretanto uma consequência do Teorema de Lindemann é que π é transcendente sobre $\mathbb{Q}$. Essa contradição mostra que não podemos efetuar a quadratura do círculo via régua e compasso.

5 Números de Origami

No Origami, os artistas usam interseções de dobraduras como pontos de referência para novas dobraduras. Este tipo de construção pode ser estendida a pontos do plano complexo. Isto é, dado um conjunto de pontos de referência e um conjunto de retas pode-se executar dobraduras a fim de se obter novos pontos de referência por adicionar interseções de retas ao nosso conjunto inicial. Neste capítulo formalizamos a noção de

[2]Caso contrário esse polinômio seria escrito como produto dois polinômios de grau estritamente maior do que zero, ou seja, existiriam $f(x)$, $g(x) \in \mathbb{Q}[x]$ tais que $8X^3 - 6X - 1 = f(x)g(x)$. Sem perda de generalidade podemos supor $\partial(f(x)) = 1$ e $\partial(g(x)) = 2$. Isto nos diz que $f(x)$ tem uma raiz racional, consequentemente, $8X^3 - 6X - 1$ deveria também ter uma raiz racional, o que é impossível.

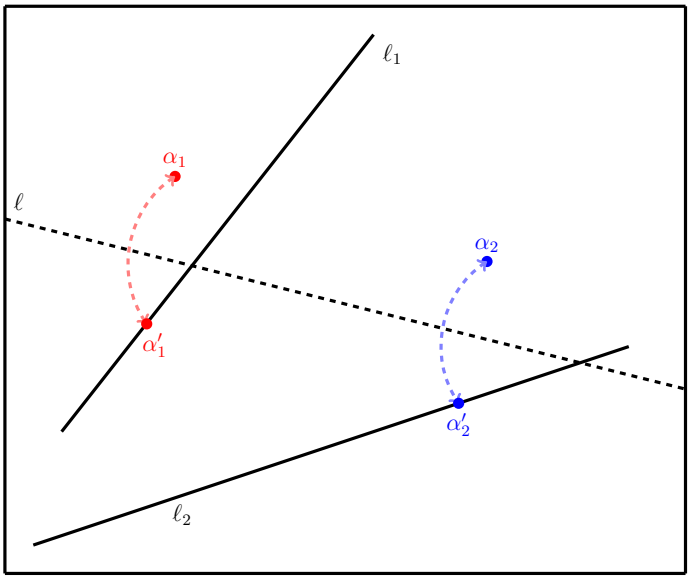
construção com Origami e apresentamos alguns resultados já conhecidos. Todo o trabalho deste capítulo é inspirado em [5], entretanto, as demonstrações foram reescritas nas minhas próprias palavras e alguns detalhes foram preenchidos. Além disto, todas as as imagens que aqui aparecem foram por mim criadas.

A conexão entre os três problemas clássicos e dobraduras ou Origami é bem recente. Uma das primeiras referências foi [17], publicada em Madras no ano de 1893. A trissecção do ângulo dada aqui usando Origami foi descoberta nos anos 70 por Hisashi Abe e foi inspirada no artigo de Hull [10]. Mais referências sobre Origami podem ser encontradas em [1], [3], [10].

Nossa próxima tarefa é dar uma descrição cuidadosa dos números que são obtidos quando adicionamos o movimento de dobrar, às construções C1 e C2 definidas anteriormente. Aqui podemos destacar a diferença entre os números construtíveis e os números de Origami. Essencialmente ela reside na inserção da dobradura como construção geométrica permitida e é por isto que estes números receberam este nome. Em termos matemáticos a dobradura se descreve a partir da seguinte construção:

C3. Dados $\alpha_1 \neq \alpha_2$ fora das retas $\ell_1 \neq \ell_2$, podemos desenhar a reta ℓ que reflete α_1 em um ponto de ℓ_1 e α_2 em um ponto de ℓ_2.

Figura 2: Representação da construção C3

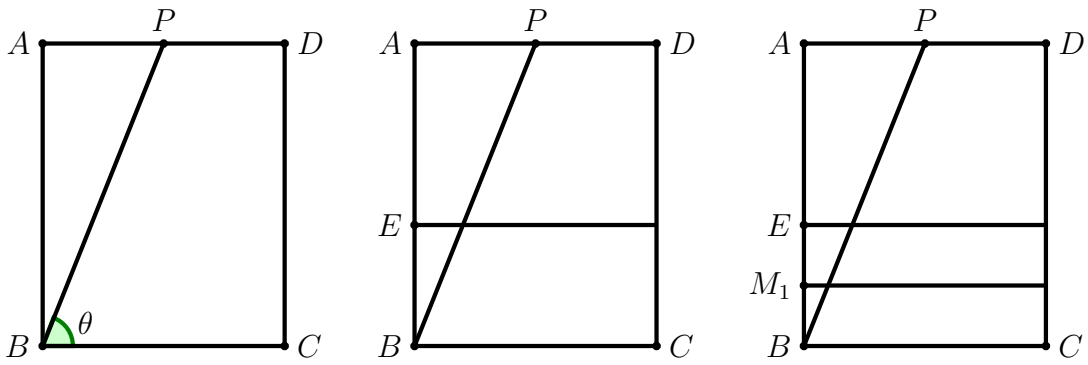


Definição 2. *Um número complexo α é um número de origami se houver uma sequência finita de construções usando C1, C2, C3, P1, P2, P3 que começam em 0 e 1 e terminam em α.*

5.1 Trissecção de ângulo via Origami

Nesta seção iremos mostrar através de todas as construções e definições que foram feitas na seção anterior como será feita a trissecção de um ângulo. Começamos com um papel retangular e denotaremos os cantos desta folha de papel (começando pelo canto superior esquerdo e enumerando no sentido anti-horário) por A, B, C, D, respectivamente. Além disso, assumiremos que já existe uma dobra começando no ponto B que encontra o segmento de reta AD em um ponto P como na figura 3(a):

Figura 3: Etapas iniciais da trissecção do ângulo via Origami.



A fim de trissectar o ângulo $\theta = \sphericalangle CBP$ executaremos as seguintes etapas:

1. Faça um vinco ao dobrar e desdobrar o lado BC paralelo à AD até um certo ponto da folha, o ponto obtido em AB pela interseção do vinco com AB será denotado por E (Figura 3(b));

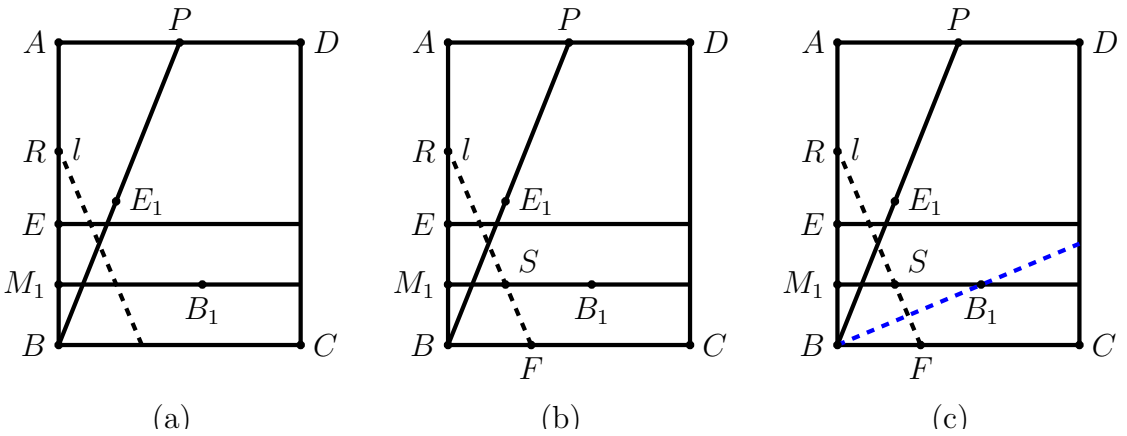
2. Dobre o lado BC até o vinco feito na etapa 1. e desdobre, o ponto encontrado em AB será denotado por M_1 e é o ponto médio do segmento BE (Figura 3(c));

3. Faça uma dobra de modo que o ponto E pare em cima do vinco BP e, simultaneamente, o ponto B pare sobre o vinco obtido na etapa 2., denote por l a linha imaginária obtida e R o ponto em AB (Figura 4(a));

4. Denote por F o ponto obtido pela interseção do vinco obtido em 3. com BC, e denote por S a interseção deste mesmo vinco com o vinco que passa por M_1 (Figura 4(b));

5. Faça uma dobra de modo que o ponto F pare sobre o ponto S e estenda este vinco até encontrar o ponto B e desdobre(Figura 4(c));

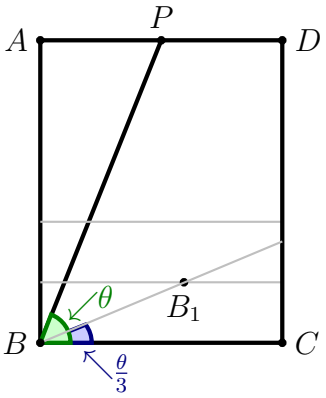
Figura 4: Etapas finais da trissecção do ângulo via Origami.



6. Denote por B_1 o ponto obtido pela interseção do vinco obtido em $5.$ com o vinco que passa por M_1;

7. O ângulo θ está trissectado por $\sphericalangle(CBB_1)$(Figura 5).

Figura 5: Representação do ângulo trissectado.



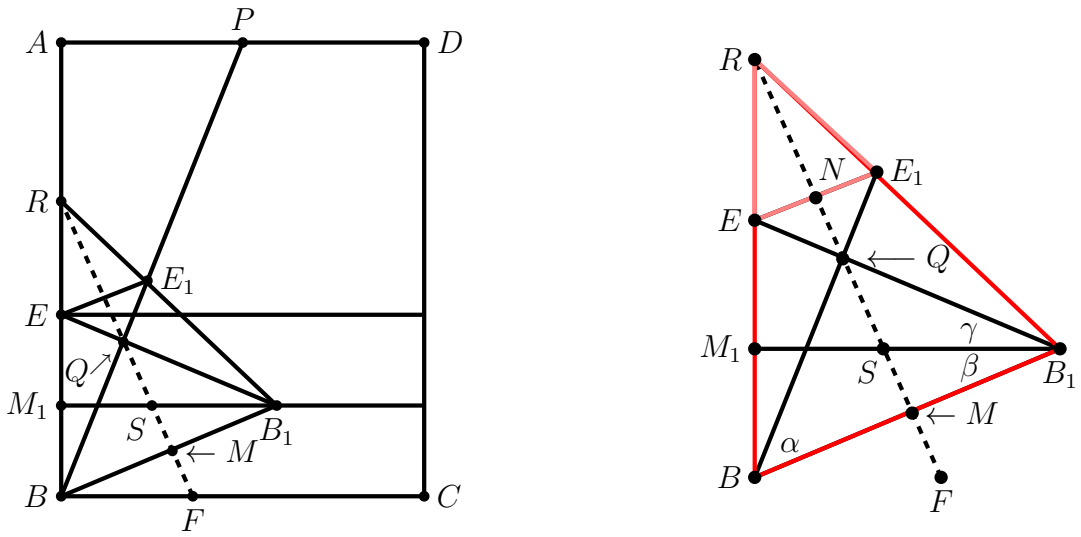
Iremos demonstrar agora porque o ângulo θ está trissectado por $\sphericalangle(CBB_1)$:
Segue da construção que os triângulos BRB_1 e ERE_1 são isósceles (Figura 6), então:

$$\overline{BE} \cong \overline{B_1E_1} \tag{9}$$

Seja N o ponto médio da base do triângulo ERE_1:

$$\widehat{REN} \cong \widehat{RE_1N} \Rightarrow \widehat{NEB} \cong \widehat{NE_1B_1} \tag{10}$$

Figura 6: Recorte



$$\widehat{RBM} \cong \widehat{RB_1M} \tag{11}$$

Daí, segue do caso de congruência de triângulos L.A.L e pelas equações (1) e (2) que:

$$\triangle BEE_1 \cong \triangle B_1E_1E \Rightarrow \widehat{E_1BE} \cong \widehat{EB_1B}$$

Por (3) temos que:

$$\widehat{E_1BB_1} \cong \widehat{EB_1B} \Rightarrow \widehat{QBB_1} \cong \widehat{QB_1B}$$

Pela recíproca do Teorema do Triângulo Isósceles, segue que: $\triangle QBB_1$ é isósceles e daí:

$$\overline{QB} \cong \overline{QB_1}$$

Como $\triangle BQB_1$ é isósceles, e sendo $\alpha = \widehat{QBB_1}$, $\beta = \widehat{PB_1B}$ e $\gamma = \widehat{PB_1E}$, temos que

$$\alpha = \beta + \gamma \tag{12}$$

a reta que passa por BF é paralela à que passa por PB_1 (por construção) está cortada pela transversal $\overrightarrow{BB_1}$, logo os ângulos β e $\widehat{CBB_1}$, são alternos internos e por isso são congruentes, ou seja $\beta \cong \widehat{CBB_1}$.

Agora, sendo

$$\alpha + \widehat{CBB_1} = \theta \Rightarrow$$

$$\alpha + \beta = \theta \tag{13}$$

Como $\triangle EPB_1$ e $\triangle BPB_1$ são congruentes pelo 1° caso de congruência de triângulos

(L.A.L) segue que os ângulos β e γ são congruentes. Segue de (1) que

$$\alpha = 2\beta \tag{14}$$

Substituindo (6) em (5) tiramos que

$$3\beta = \theta \Rightarrow \beta = \theta/3 = \widehat{CBB_1}$$

como queríamos.

Teorema 8. *O conjunto $\mathscr{O} = \{\alpha \in \mathbb{C} \,|\, \alpha$ é um número de origami $\}$ é um subcorpo de $\mathbb{C}$. Além disso:*

a. Se $\alpha = a + ib$, onde $a, b \in \mathbb{R}$, então $\alpha \in \mathscr{O}$ se, e somente se $a, b \in \mathscr{O}$.

b. Se $\alpha \in \mathscr{O}$ então $\sqrt{\alpha}$, $\sqrt[3]{\alpha} \in \mathscr{O}$.

c. Um número complexo α está em $\mathscr{O}$ se, e somente se existem subcorpos

$$\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_{(n-1)} \subset F_n \subset \mathbb{C}$$

tais que $\alpha \in F_n$ e $[F_i : F_{(i-1)}]$ = 2 ou 3 para todo $1 \leq i \leq n$.

Demonstração. Para mostrar que $\mathscr{O}$ é subcorpo de $\mathbb{C}$ usaremos 12.

A demonstração da parte a. é muito semelhante à que fizemos no Teorema 5 para o conjunto dos números construíveis $\mathscr{C}$ e será omitida.

Para provar o item b. escreva α na forma polar como $\alpha = re^{i\theta}$. Podemos assumir $r > 0$. Usando régua e compasso podemos transferir r ao eixo x e então a mesma construção dada no Teorema 5 nos garante que $\sqrt{r} \in \mathscr{O}$. Já que podemos bissectar θ via régua e compasso temos que: $\sqrt{\alpha} = \pm\sqrt{r}e^{i\frac{\theta}{2}} \in \mathscr{O}$.

Para a raiz cúbica podemos trissectar θ usando a construção da figura 4. Já a construção de $\sqrt[3]{r}$ requer a construção de uma reta tangente simultaneamente às parábolas de equações:

$$y^2 = -2rx \qquad y = \tfrac{1}{2}x^2$$

Os focos α_1 e α_2 e as diretrizes l_1 e l_2 destas parábolas estão definidas em $\mathbb{R}$ contendo r e portanto podem ser construídas a partir de r usando régua e compasso. Aplicando C3 à α_1, α_2, l_1 e l_2 podemos construir uma reta l simultaneamente tangente à estas duas parábolas. Pode-se mostrar facilmente que l tem inclinação $m = \sqrt[3]{r}$, isto nos permite dizer $\sqrt[3]{r} \in \mathscr{O}$. Já que $w = e^{i\frac{2\pi}{3}} \in \mathscr{O}$ segue que:

$$\sqrt[3]{\alpha} = w^i\sqrt[3]{r}e^{i\frac{\theta}{3}} \in \mathscr{O}, \quad \forall\ i = 1,\ 2,\ 3.$$

Para a parte c. vamos dizer que os corpos $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ formam uma $2-3$-torre quando $[F_i : F_{(i-1)}] = 2$ ou 3 para todo $i \in \{1, \cdots, n\}$. Agora para uma $2-3$-torre vamos mostrar que $F_n \subset \mathscr{O}$ usando indução em n. Já que o caso $n = 0$ é trivial, vamos assumir que $F_{n-1} \subset \mathscr{O}$. Assim dado $\alpha \in F_n$ sabemos que α é raiz de um polinômio $f \in \mathscr{O}[x]$ de grau no máximo 3, já que $[F_i : F_{(i-1)}] = 2$ ou 3. Se f tiver grau 1 automaticamente $\alpha \in \mathscr{O}$ e, se f tiver grau 2 ou 3 a fórmula quadrática de Cardano, garante que α pode ser expresso em termos de raízes quadradas, raízes cúbicas e elementos de $\mathscr{O}$. Segue do item b. que $\alpha \in \mathscr{O}$.

Teorema 9. *Seja $\alpha \in \mathbb{C}$ algébrico sobre $\mathbb{Q}$ e seja $\mathbb{Q} \subset L$ o corpo de decomposição de um polinômio mínimo de α sobre $\mathbb{Q}$. Então α é um número de origami se, e somente se $[L : \mathbb{Q}] = 2^a 3^b$ para inteiros a,b ≥ 0.*

Demonstração. Aqui o argumento é bem semelhante à prova do Teorema 7. Resumidamente, dado $\alpha \in \mathscr{O}$ a ideia é mostrar primeiro que $\mathbb{Q} \subset \mathscr{O}$ é uma extensão normal e consequentemente temos $L \subset \mathscr{O}$. Daí a fórmula para $[L : \mathscr{O}]$ segue por aplicar o Teorema 8 a um elemento primitivo de $\mathbb{Q} \subset L$. Para a recíproca usaremos o Teorema 4 para mostrar que $Gal(L/\mathbb{Q})$ é solúvel já que $|Gal(L/\mathbb{Q})| = [L : \mathbb{Q}] = 2^a 3^b$. A $2-3$ torre desejada será construída usando o Teorema 3 e da definição de grupo solúvel.

Conforme foi observado, os problemas de trissectar um ângulo e duplicar um cubo equivalem à encontrar raízes de um polinômio irredutível de grau 3. O Teorema anterior garante que as raízes de polinômios de grau da forma $2^a 3^b$ são números de Origami. Em particular, as raízes de um polinômio irredutível de grau 3 serão números de Origami, ou seja, podem ser construídos usando uma sequência finita de construções seguindo C1, C2, C3, P1, P2, P3.

No início desta seção vimos como era possível trissectar um ângulo via régua, compasso e dobradura. Na próxima seção mostraremos como é feita, geometricamente, a duplicação do cubo e o porquê desta construção funcionar.

5.2 Duplicação do Cubo

A fim de duplicar o cubo, como no caso anterior, começamos com um papel quadrangular e denotaremos os cantos desta folha de papel (começando pelo canto superior esquerdo e enumerando no sentido anti-horário) por A, B, C, D, respectivamente. A seguir, executaremos as seguintes etapas:

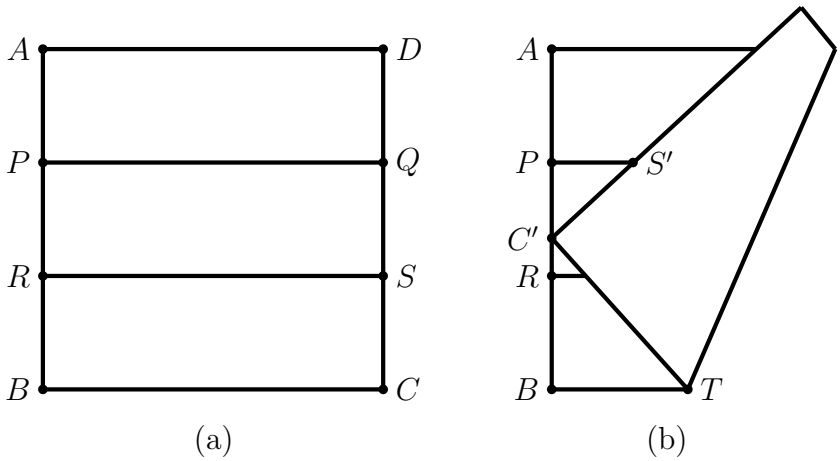
1. Divida-a em três partes iguais, paralelamente à BC. Teremos duas linhas, o ponto de encontro da linha inferior com o segmento CD será denotado por S (Figura 7(a));

2. Faça uma dobra de modo que o vértice denominado C fique sobre o segmento AB e o ponto S fique sobre a linha superior que divide a folha em três partes (Figura 7(b));

3. A proporção dos comprimentos AC' por $C'B$ é $\sqrt[3]{2}$;

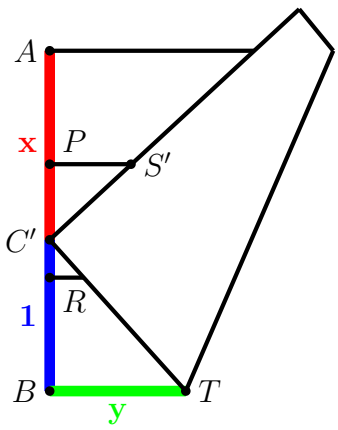
Todas essas etapas podem ser observadas nas Figuras 7(a) e 7(b).

Figura 7: representação d



Provaremos agora que com esta construção é possivel duplicar o cubo, ou seja, achar $x = \sqrt[3]{2}$:

Figura 8: Construção de $x = \sqrt[3]{2}$



Na figura 7(b), marque o vértice que formou pelo vinco feito em 2. por T. Seja $AC' = x$ e $C'B = 1$, então $AB = 1 + x$ e todos os demais lados do quadrado valem

$1+x$. Seja $BT = y$, então $TC' = 1+x-y$. Usando o Teorema de Pitágoras temos que:

$$1+y^2 = (1+x-y)^2 = 1+x^2+y^2+2x-2y-2xy.$$

ou

$$y = \frac{x^2+2x}{2x+2}. \tag{15}$$

Sendo $AP = \dfrac{1+x}{3}$, temos que:

$$PC' = x - \frac{1+x}{3} = \frac{2x-1}{3}.$$

Além disso, $C'S' = \dfrac{1+x}{3}$. Pelo caso de semelhança AA observamos que os triângulos $PC'S'$ e BTC' são semelhantes, daí:

$$\frac{(1+x)/3}{(2x-1)/3} = \frac{C'S'}{PC'} = \frac{C'T}{BT} = \frac{1+x-y}{y}.$$

então

$$\frac{(1+x)}{(2x-1)} = \frac{1+x}{y} - 1 \qquad \Rightarrow \qquad \frac{(1+x)}{y} = \frac{1+x}{2x-1} + 1 = \frac{3x}{2x-1}$$

ou ainda,

$$y = \frac{(1+x)(2x-1)}{3x} \qquad \Rightarrow \qquad y = \frac{2x^2+x-1}{3x}. \tag{16}$$

De (15) e (16),

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

$$4x^3+6x^2-2 = 3x^3+6x^2.$$

e portanto

$$x^3 = 2 \Rightarrow x = \sqrt[3]{2}.$$

6 Conclusão

Vimos que a resolução dos Três Problemas Clássicos depende de quais construções geométricas são permitidas. Observamos através do presente trabalho que é possível, por meio da teoria de Galois e da técnica de Origami, resolver estes problemas que são insolúveis via régua e compasso. Fornecemos uma explicação detalhada de como trissectar um ângulo arbitrário e como duplicar um cubo usando apenas régua, compasso e dobradura.

Assim, esse método que foi proposto inicialmente por H. Abe em 1980, se mostra mais potente que os métodos Euclidianos ordinários. O extraordinário aqui reside no processo da sobreposição simultânea de dois pontos distintos em duas retas, o que é feito por meio da dobradura. Além disso, o fato de acrescentar a dobradura nos permite desenhar objetos geométricos (como as parábolas) que vão além das construções ordinárias via régua e compasso.

Referências

[1] ALPERIN, R. A mathematical theory of origami constructions and numbers, **New York J. Math.** v.6, p. 119–133, 2000.

[2] ALPERIN, R. One-, Two- and Multi-Fold Origami Axioms. **Origami 4**, p. 371–393.

[3] AUCKLY, D.; CLEVELAND, J. Totally real origami and impossible paper folding. **The American mathematical monthly**, v. 102, n. 3, p. 215-226, 1995.

[4] BUNT, L. N. H.; JONES, P. S.; BEDIENT, J. D. **The historical roots of elementary mathematics**. Courier Corporation, 1988.

[5] COX, A. D. **Galois Theory**. Wiley. 2004.

[6] COURANT, H. R. R., COURANT, R., ROBBINS, H., & STEWART, I. **What is Mathematics?**: an elementary approach to ideas and methods. Oxford University Press, 1996.

[7] FUJIMOTO, S.; NISHIWAKI, M. **Seizo Soru Origami Asobi no Shotai (Creative Invitation to Paper Play)**. 1982.

[8] GARCIA, A.; LEQUAIN, I. **Elementos de Álgebra**. Rio de Janeiro. IMPA. 2003.

[9] HADLOCK, C. R. **Field theory and its classical problems**. Washington, DC: Mathematical Association of America, 1978.

[10] HULL, T. A note on "impossible" paper folding. **American Mathematical Monthly**, v. 103, n. 3, p. 240–241, 1996.

[11] HULL, T. Disponível em: http://mars.wne.edu/ thull/origamimath.html. Acesso em 04 de março de 2022.

[12] HUNGERFORD, T. W. **Algebra**. Springer-Verlag. GTM 73. 2003.

[13] HUZITA, H.; SCIMEMI, B. The algebra of paper folding (origami). In: Proceedings of the First International Meeting of Origami Science and Technology. University of Padova, Padova, 1989. p. 215-222.

[14] KASAHARA, K.; MAEKAWA, J. **Viva! Origami**. Sanrio, Tokyo, Japan, 1983.

[15] KAWASAKI, T. **Roses, Origami** & **Math**. Japan Publications Trading, 2005.

[16] LANG, R. J. Artworks, Disponível em https://langorigami.com/artworks/. Acesso em 04 de março de 2022.

[17] RAO, T. S.; ROW, T. S. **Geometric exercises in paper folding**. Open Court Publishing Company, 1917.

[18] RUTZKY, J.; PALMER, C. K. **Shadowfolds: surprisingly easy-to-make geometric designs in fabric**. New York: Kodansha International, 2011.

Submetido em dez. 2021
Aceito em mar. 2022