Revista Eletrônica
Paulista de Matemática

ISSN 2316-9664
v. 22, n. 1, jul. 2022

Construções com régua e compasso: uma abordagem elementar

Constructions with ruler and compass: an elementar approach

Allan Kenedy Santos Silva
Instituto de Matemática
Ufal - Universidade Federal de Alagoas
allan.santos@im.ufal.br

Resumo

Os primeiros séculos da matemática grega tiveram três grandes linhas de desenvolvimento: O desenvolvimento do material que se organizou nos *Elementos* de Euclides; o desenvolvimento das noções de infinitésimos e infinitos; e a Geometria Superior. A Geometria Superior surgiu das tentativas de resolver alguns problemas de construção com régua e compasso que estavam em aberto. Dentre eles se destacam a Duplicação do Cubo, a Trissecção do Ângulo e a Quadratura do Círculo. A impossibilidade de solução desses problemas foi demonstrada somente no século XIX com os trabalhos de Wantzel e Lindemann. Os livros atuais de álgebra que tratam desse assunto o fazem por meio de conceitos de polinômios irredutíveis, extensões de corpos, grau de extensão dentre outros correlatos. O intuito deste artigo é apresentar uma abordagem elementar da prova da impossibilidade de solução dos problemas citados, isto é, sem recorrer àqueles conceitos mais avançados.

Palavras-chave: Régua e compasso. Duplicação do cubo. Trissecção do ângulo. Quadratura do círculo. Elementar.

Abstract

The first centuries of Greek mathematics had three major lines of development: The development of material that was organized in Euclid's *Elements*; the development of the notions of infinitesimals and infinites; and Superior Geometry. Superior Geometry arose from the attempts to solve some construction problems with a ruler and compass that were still open. Among them, the Duplication of the Cube, the Trisection of the Angle and the Square of the Circle stand out. The impossibility of solving these problems was only demonstrated in the 19th century with the works of Wantzel and Lindemann. Current algebra books dealing with this subject do so through the concepts of irreducible polynomials, field extensions, degree of extension, among other correlates. The purpose of this article is to present an elementary approach to the proof of the impossibility of solving the aforementioned problems, that is, without resorting to those more advanced concepts.

Keywords: Ruler and compass. Cube duplication. Angle trisection. Squaring the circle. Elementary.

Artigo recebido em nov. 2021 e aceito em mai. 2022

Este artigo está licenciado com uma Licença Creative Commons Attribution 4.0 International, podendo ser usado, distribuído e reproduzido, sem restrições, desde que o trabalho original seja devidamente citado.

1 Introdução

1.1 Linhas de desenvolvimento da matemática grega

Os primeiros séculos da matemática grega iniciaram com os esforços de Tales por uma geometria demonstrativa (600 a.C.) e culminaram na obra *Elementos* de Euclides (300 a.C.) (EVES, 2011). Durante esse período houveram três grandes linhas de desenvolvimento da matemática grega:

1. Desenvolvimento do material que se organizou nos *Elementos*;
2. Desenvolvimento de noções relacionadas com os infinitésimos e infinitos (limites, séries, processos infinitos) que foram formalizados no Cálculo;
3. Geometria Superior, isto é, a geometria de curvas que não são as retas, circunferências, planos, nem esferas.

A Geometria Superior surgiu das tentativas de resolver alguns problemas de construção com régua e compasso que estavam em aberto.

1.2 Construções com régua e compasso e os três famosos problemas

Os instrumentos utilizados são uma régua sem escala (sem marcas de medida) e um compasso. Com a régua podemos traçar uma reta que passa por dois pontos dados, e com o compasso podemos traçar um círculo cujo centro é um ponto dado e cujo raio é a distância entre dois pontos dados. Uma construção com régua e compasso é uma sequência de operações em que, dados um conjunto finito de pontos e utilizando uma régua e um compasso, traçamos novos pontos de uma das maneiras seguintes:

C1: Intersecção de duas retas;

C2: Intersecção de uma reta e uma circunferência;

C3: Intersecção de duas circunferências.

Exemplo 1 *Dado um ângulo $A\hat{B}C$, traçar o seu bissetor.*
Seguimos o passo-a-passo abaixo (ver Figura 1):

1. *Com a ponta seca do compasso*[1] *no vértice B e abertura BA (ou BC, tanto faz), trace uma circunferência c;*
2. *A circunferência c intersecta as semi-retas r e s nos pontos A e D;*
3. *Com abertura do compasso AD e a ponta seca em D, trace a circunferência d. Com a mesma abertura mas agora com a ponta seca em A trace a circunferência e;*
4. *As circunferências d e e se intersectam no ponto F;*
5. *Com a régua trace a semi-reta h que passa pelos pontos B e F. Ela será a bissetriz do ângulo $A\hat{B}C$.*

[1] É a ponta com a agulha.

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.
DOI: 10.21167/cqdv22n12022010026 Disponível em: www.fc.unesp.br/departamentos/matematica/revista-cqd

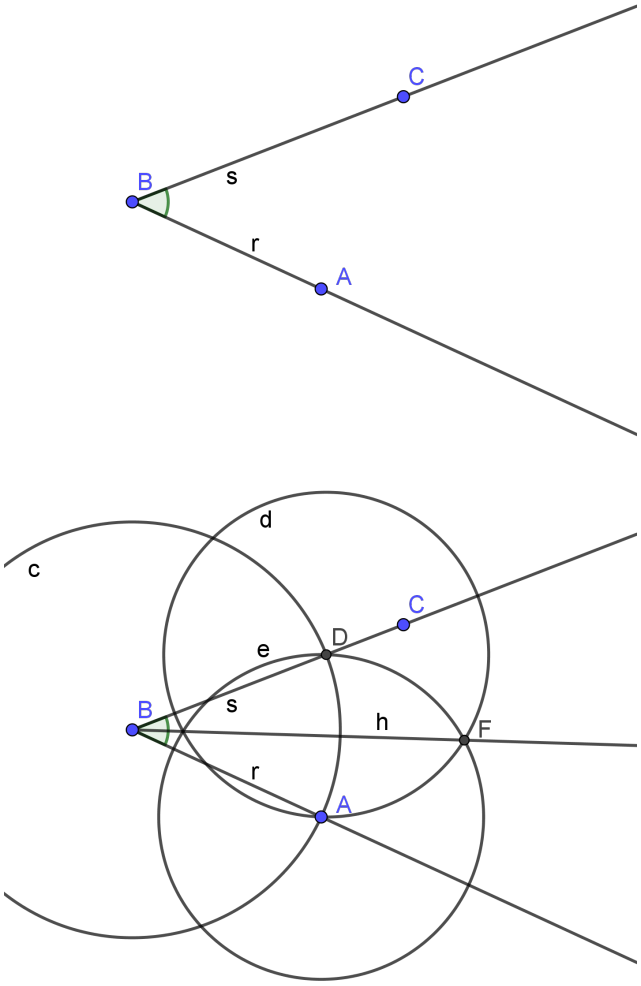

Figura 1: Bissecção do ângulo $A\hat{B}C$ com régua e compasso.

Com esses dois instrumentos é possível realizar uma infinidade de construções geométricas (bissecção do ângulo, traçar polígonos regulares, construir qualquer segmento de medida racional etc.). Contudo existiam problemas ainda sem solução, dos quais três se destacam:

Duplicação do cubo: dado um cubo, construir um cubo cujo volume é o dobro do volume do cubo dado;

Trissecção do ângulo: dado um ângulo, construir a sua terça parte;

Quadratura do círculo: dado um círculo, construir um quadrado cuja área é igual a área do círculo dado.

Estes problemas podem ser traduzidos em linguagem algébrica atual como segue.

Duplicação do cubo: Dado um cubo de aresta a, seu volume é $V = a^3$. Queremos construir a aresta x do cubo de volume $2V$: $x^3 = 2V = 2a^3 \Rightarrow x = \sqrt[3]{2}a$. Então o problema é equivalente a construir $\sqrt[3]{2}$.

Trissecção do ângulo: Dado um ângulo α, construir $\alpha/3$. Usando o círculo trigonométrico, isto equivale a construir $\cos(\alpha/3)$ ou $\operatorname{sen}(\alpha/3)$.

Quadratura do círculo: Dado um círculo de raio r, sua área é $A = \pi r^2$. Queremos construir o lado l do quadrado de área A: $l^2 = A = \pi r^2 \Rightarrow l = \sqrt{\pi} r$. Então o problema é equivalente a construir

π já que, como veremos, a raiz quadrada de um número construtível é construtível.

Somente no século XIX foi demonstrado que estes problemas e alguns outros são impossíveis de serem solucionados somente por uma régua sem escala e compasso: a duplicação do cubo e a trissecção do ângulo por Wantzel (1837) e a quadratura do círculo por Lindemann (1882).

1.3 Organização do texto

A Seção 2 mostra como podemos traduzir o processo de construção com régua e compasso para a linguagem algébrica usando números complexos. A Seção 3 é dedicada a definir um tipo de estrutura algébrica chamada corpo (este é o único conceito mais avançado em todo o texto; todas as outras ferramentas matemáticas que serão utilizadas são acessíveis a um aluno no início de um curso de graduação em matemática). É também mostrado nessa seção que o conjunto dos pontos construtíveis possui a estrutura de corpo. A Seção 4 dá uma caracterização dos números construtíveis, mostrando que um número é construtível se puder ser escrito como uma combinação finita de somas, diferenças, produtos, quocientes e raízes quadradas sucessivas de números racionais. Na Seção 5 é demonstrada a impossibilidade de solução dos problemas da duplicação do cubo, da trissecção do ângulo e da quadratura do círculo.

2 Algebrizando a geometria

Perceba pelo exemplo na introdução que qualquer ponto é construído a partir dos pontos anteriores, e estes a partir dos anteriores a eles e assim por diante até os pontos iniciais A, B e C. Enumerando os pontos iniciais $A = P_0$, $B = P_1$ e $C = P_2$, e os pontos construídos $D = Q_1$ e $F = Q_2$, vemos que Q_1 foi construído a partir de P_0, P_1 e P_2, e Q_2 foi construído a partir de P_0, P_1, P_2 e Q_1. Com isto em mente podemos formalizar o conceito de construção com régua e compasso.

Um ponto P é *construtível com régua e compasso* a partir de um conjunto de pontos $S_0 = \{P_0, P_1, \ldots, P_n\}$ $(n \geq 1)$ se existe uma sequência de pontos $Q_1, \ldots, Q_k = P$ tais que Q_1 é obtido a partir do conjunto S_0 e Q_j, $j \geq 2$, é obtido a partir do conjunto $S_{j-1} = S_0 \cup \{Q_1, \ldots, Q_{j-1}\}$ de um dos seguintes modos:

C1: Q_j é o ponto de intersecção de duas retas que passam por pontos de S_{j-1};

C2: Q_j é o ponto de intersecção entre uma reta que passa por pontos de S_{j-1} e uma circunferência cujo centro é um ponto de S_{j-1} e cujo raio é a distância entre dois pontos de S_{j-1};

C3: Q_j é o ponto de intersecção entre duas circunferências cujos centros são pontos de S_{j-1} e cujos raios são as distâncias entre pares de pontos de S_{j-1};

Podemos traduzir o processo descrito acima para a linguagem algébrica utilizando os números complexos: associamos os pontos $P_0, P_1, \ldots, P_n$ aos complexos $z_0, z_1, \ldots, z_n$; escolhemos o sistema de coordenadas (efetuando rotações, translações e escalas) de modo que $z_0 = 0$ e $z_1 = 1$. As retas e circunferências são representadas por equações algébricas, de maneira que as operações C1, C2 e C3 são reformuladas como soluções de sistemas de equações conforme veremos adiante. Denotamos por $C(z_0, z_1, \ldots, z_n)$ o conjunto dos números complexos construtíveis a partir de $z_0, z_1, \ldots, z_n$.

3 O que é um corpo?

O que faremos agora é dar a $C(z_0, z_1, \ldots, z_n)$ uma estrutura algébrica, de maneira que possamos somar, subtrair, multiplicar, dividir e tirar raiz quadrada de seus elementos. Para isso precisamos dizer o que é uma operação.

Um *operador unário* (ou uma *operação unária*) sobre um conjunto A é uma função $* : A \to A$, que associa cada elemento x de A a outro elemento $*x$ de A. Por exemplo, a extração de raiz quadrada é uma operação unária no conjunto dos números reais não-negativos. Um *operador binário* (ou uma *operação binária*) sobre um conjunto A é uma função $* : A \times A \to A$ que associa a cada par x, y de elementos de A um outro elemento $z = x * y$ de A. Por exemplo, a soma e a multiplicação são operações binárias no conjunto dos números complexos. Um subconjunto B de A é *fechado* para a operação $*$ se, caso $*$ seja unário, para qualquer x em B, $*x$ está em B ou, caso $*$ seja binário, para quaisquer x, y em B, $x * y$ está em B. Por exemplo, o conjunto dos números racionais (que é um subconjunto dos números reais) é fechado para as operações de adição e multiplicação.

As operações de adição e multiplicação nos números reais (ou mesmo os complexos) satisfazem uma série de propriedades: comutativa, associativa, distributiva, elemento neutro dentre outras. Um conjunto que satisfaz essas propriedades é chamado de corpo. Mais precisamente, um *corpo* é um conjunto A com duas operações binárias $+ : A \times A \to A$ (que chamaremos de adição) e $\cdot : A \times A \to A$ (que chamaremos de multiplicação) que satisfazem as seguintes propriedades:

Comutativa da adição: Para quaisquer x, y em A, $x + y = y + x$;

Associativa da adição: Para quaisquer x, y, z em A, $x + (y + z) = (x + y) + z$;

Elemento neutro da adição: Existe um elemento 0 em A, chamado *zero*, tal que para qualquer x em A, $x + 0 = x$;

Simétrico aditivo: Para cada x em A, existe um $-x$ em A tal que $x + (-x) = 0$;

Comutativa da multiplicação: Para quaisquer x, y em A, $x \cdot y = y \cdot x$;

Associativa da multiplicação: Para quaisquer x, y, z em A, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;

Elemento neutro da multiplicação: Existe um elemento 1 em A, chamado *um*, tal que para qualquer x em A, $1 \cdot x = x$;

Inverso multiplicativo: Para cada x em A, com $x \neq 0$, existe um x^{-1} em A tal que $x \cdot x^{-1} = 1$;

Distributiva: Para cada x, y, z em A, $x \cdot (y + z) = x \cdot y + x \cdot z$.

Por exemplo, o conjunto dos números complexos é um corpo.

Dado um corpo A, um *subcorpo* é um subconjunto B de A que também é um corpo com as operações de A. Por exemplo, o conjunto $\mathbb{Q}$ dos números racionais é um subcorpo do conjunto $\mathbb{R}$ dos números reais, e este por sua vez é um subcorpo do conjunto $\mathbb{C}$ dos números complexos.

Observação 2 *Para $B \subset A$ ser um subcorpo de A não é preciso verificar todas aquelas propriedades listadas anteriormente; é suficiente apenas verificar que para quaisquer $x, y \in B$, $x - y \in B$ e $x \cdot y^{-1} \in B$ para $y \neq 0$. De fato, se B satisfaz estas duas condições, fazendo $y = x$, teremos que $0 = x - x$ e $1 = x \cdot x^{-1}$ pertencem a B; por consequência, dado $x \in B$, $-x = 0 - x \in B$ e $x^{-1} = 1 \cdot x^{-1} \in B$; com isso $x + y = x - (-y) \in B$ e $x \cdot y = x \cdot (y^{-1})^{-1} \in B$, isto é, B é fechado para $+$ e $\cdot$. Por fim, todas as propriedades de corpo listadas anteriormente valem para B, pois elas já valem para A e $B \subset A$.*

Finalizadas as definições, vamos para o primeiro teorema:

Teorema 3 *$C(z_0, z_1, \ldots, z_n)$ é um subcorpo de $\mathbb{C}$ fechado para as operações de conjugação e extração de raiz quadrada.*

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.
DOI: 10.21167/cqdv22n12022010026 Disponível em: www.fc.unesp.br/departamentos/matematica/revista-cqd

Prova: Pela Observação 2 basta provar que para quaisquer $z, w \in C(z_0, z_1, \ldots, z_n)$, $z - w$ e $z \cdot w^{-1}$ pertencem a $C(z_0, z_1, \ldots, z_n)$; além disso, que para qualquer $z \in C(z_0, z_1, \ldots, z_n)$, $\sqrt{z}$ e $\overline{z}$ pertençam a $C(z_0, z_1, \ldots, z_n)$.

Dados $z, w \in C(z_0, z_1, \ldots, z_n)$, iremos representá-los pelos vetores $\overrightarrow{OA}$ e $\overrightarrow{OB}$ (ver Figura 2). Traçamos uma reta que passa por suas extremidades A e B e, pela origem O, traçamos uma reta paralela a reta AB. Marcamos nessa reta o ponto C no sentido BA cuja distância até O é igual a distância entre A e B. O vetor $\overrightarrow{OC}$ representa $z - w$. Como todas essas construções geométricas podem ser feitas usando régua e compasso, concluímos que $z - w \in C(z_0, z_1, \ldots, z_n)$.

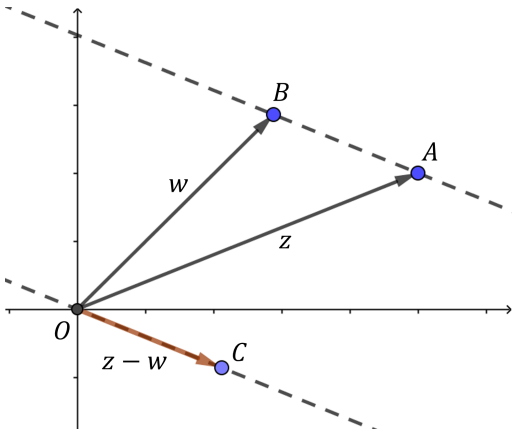

Figura 2: Diferença entre números complexos construtíveis.

Vamos representar z e w na forma polar $z = |z|(\cos\theta + i \operatorname{sen}\theta)$ e $w = |w|(\cos\phi + i \operatorname{sen}\phi)$. Então para $w \neq 0$,

$$\frac{z}{w} = \frac{|z|}{|w|}[\cos(\theta - \phi) + i \operatorname{sen}(\theta - \phi)]$$

Uma vez que $|z|$ e $|w|$ são construtíveis (pois z e w o são), podemos construir o quociente $|z|/|w|$ por meio da Figura 3. Como os ângulos θ e ϕ são construtíveis, é fácil ver que a diferença $\theta - \phi$ também é construtível. Portanto z/w é construtível, logo pertence a $C(z_0, z_1, \ldots, z_n)$. Isto prova que $C(z_0, z_1, \ldots, z_n)$ é um subcorpo de $\mathbb{C}$.

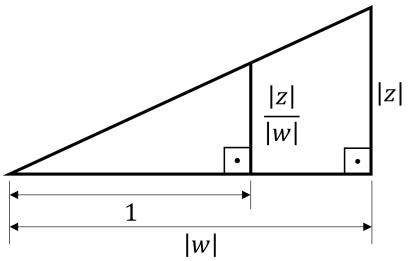

Figura 3: Divisão entre números construtíveis.

Para $\sqrt{z}$ temos pela fórmula de De Moivre que

$$\sqrt{z} = \pm\sqrt{|z|}\left(\cos\frac{\theta}{2} + i \operatorname{sen}\frac{\theta}{2}\right)$$

$\sqrt{|z|}$ pode ser construído da seguinte maneira: marcamos sobre uma mesma reta segmentos OA de comprimento 1 e AB de comprimento $|z|$ (Figura 4), depois construímos uma circunferência

cujo diâmetro é OB; pelo ponto A traçamos um segmento perpendicular a reta OB que intersecta a circunferência no ponto C. O segmento AC tem comprimento[2] $\sqrt{|z|}$. Todas essas construções podem ser feitas com régua e compasso, logo $\sqrt{|z|}$ é construtível. Como o ângulo $\theta/2$ é a bissetriz de θ, o qual é, como visto no Exemplo 1, construtível, concluímos que $\sqrt{z}$ é construtível, logo $\sqrt{z} \in C(z_0, z_1, \ldots, z_n)$.

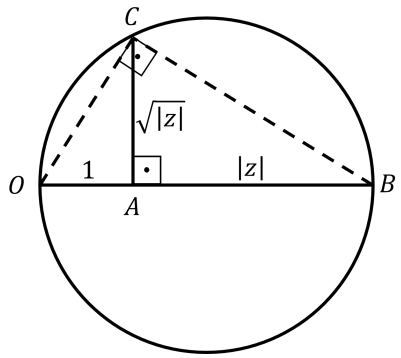

Figura 4: Raiz quadrada de um número construtível.

Por fim, lembre que o conjugado de um número complexo $z = a + bi$ é $\overline{z} = a - bi$, isto é, $\overline{z}$ é a reflexão de z em torno do eixo real (Figura 5), e isso pode ser feito com régua e compasso, logo $\overline{z} \in C(z_0, z_1, \ldots, z_n)$, o que conclui a prova do teorema. □

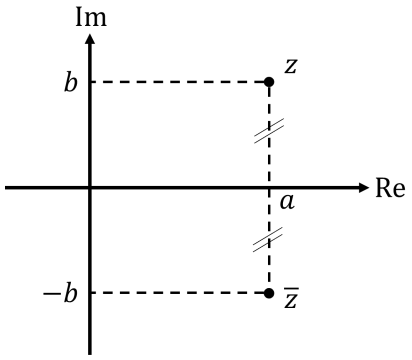

Figura 5: Conjugado de um número complexo construtível.

Corolário 4 *Todo número racional é construtível, isto é,* $\mathbb{Q} \subset C(z_0, z_1, \ldots, z_n)$.

Prova: De fato, como $z_0 = 0$ e $z_1 = 1$, qualquer inteiro p é obtido por meio de p segmentos de comprimento 1 desenhados no sentido positivo ou negativo conforme p seja positivo ou negativo, logo $p \in C(z_0, z_1, \ldots, z_n)$, isto é, $\mathbb{Z} \subset C(z_0, z_1, \ldots, z_n)$. Dados quaisquer pares de inteiros p e q, como $C(z_0, z_1, \ldots, z_n)$ é um corpo, o quociente p/q é construtível. Como todo racional é o quociente entre dois inteiros, é construtível. □

O corolário a seguir afirma que podemos resolver uma equação do segundo grau usando régua e compasso.

[2]Esta construção se justifica pois o triângulo OBC é retângulo (já que um dos lados é o diâmetro da circunferência e então a medida do ângulo $O\hat{C}B$ é a metade do arco OB que vale 180°, assim $O\hat{C}B = 180/2 = 90°$). Por semelhança entre os triângulos OAC e ABC, $OA/AC = AC/AB$, logo $AC = \sqrt{OA \cdot AB}$.

Corolário 5 *Se a, b, e c são construtíveis, com $a \neq 0$, então as raízes da equação $ax^2 + bx + c = 0$ são construtíveis.*

Prova: Basta ver que as raízes da equação são

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{e} \quad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

logo são construtíveis. □

Corolário 6 *O pentágono regular é construtível.*

Prova: O ângulo de 360° é equivalente a 2πrad, então construir o pentágono regular é equivalente a construir o ângulo de $2\pi/5$ (dividir a circunferência completa em 5 partes iguais). Por meio do círculo trigonométrico, isso é equivalente a construir o número complexo $\zeta = \cos(2\pi/5) + i\,\mathrm{sen}(2\pi/5)$. Como $\zeta^5 = 1$, então ζ é solução da equação $x^5 - 1 = 0$. Como 1 é uma solução da equação, o polinômio $x^5 - 1$ pode ser fatorado como

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1), \tag{1}$$

logo ζ é uma solução de $x^4 + x^3 + x^2 + x + 1 = 0$. Considere

$$\alpha = \zeta + \zeta^4 \quad \text{e} \quad \beta = \zeta^2 + \zeta^3.$$

Então

$$\alpha + \beta = \zeta + \zeta^4 + \zeta^2 + \zeta^3 = -1$$

e

$$\alpha\beta = \zeta^3 + \zeta^4 + \zeta^6 + \zeta^7 = \zeta^3 + \zeta^4 + \zeta + \zeta^2 = -1$$

por conta de (1), logo α e β são soluções de

$$x^2 - (\alpha + \beta)x + \alpha\beta = x^2 + x - 1 = 0,$$

portanto α e β são construtíveis pelo Corolário 5. Agora

$$(x - \zeta)(x - \zeta^4) = x^2 - (\zeta + \zeta^4)x + \zeta \cdot \zeta^4 = x^2 - \alpha x + 1$$

que é um polinômio do 2º grau cujos coeficientes são construtíveis, logo ζ é construtível pelo Corolário 5. □

Resolvendo as equações acima encontraremos

$$\zeta = \frac{-1 + \sqrt{5}}{4} + \frac{i}{2}\sqrt{\frac{5 + \sqrt{5}}{2}},$$

o que fornece um método para traçar o pentágono: construir $(-1 + \sqrt{5})/4$ e levantar a perpendicular ao eixo x nesse ponto até intersectar a circunferência unitária. Daí basta marcar os vértices sucessivamente (Figura 6).

Corolário 7 *Um número complexo $z = a + bi$ é construtível se, e somente se, a e b são construtíveis.*

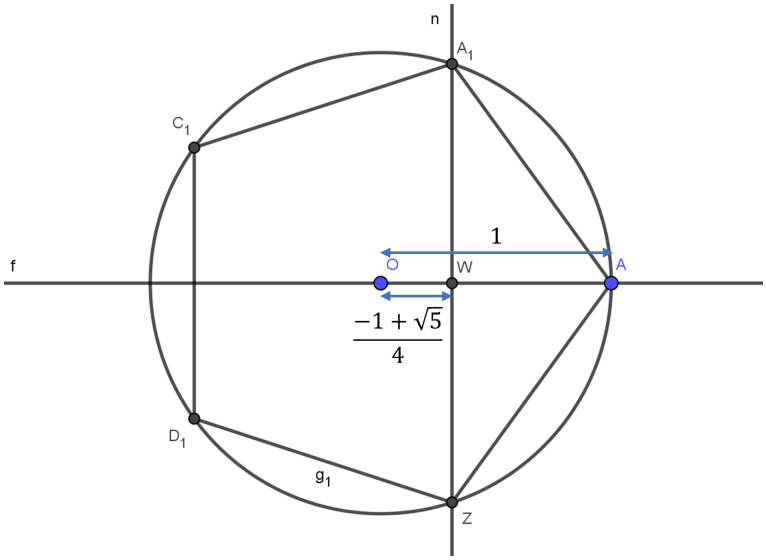

Figura 6: Construção do pentágono regular

Prova: O complexo $z = a + bi$ representa o ponto (a, b) do plano cartesiano. Se a e b são construtíveis obviamente z o será. Reciprocamente, se z é construtível, como os seus coeficientes a e b podem ser obtidos das relações

$$a = \frac{z + \overline{z}}{2} \quad \text{e} \quad b = \frac{z - \overline{z}}{2}$$

e $\overline{z}$ é construtível, vemos que a e b são construtíveis. □

Da Figura 5 tiramos o seguinte corolário.

Corolário 8 *Se $z = a + bi$ e $\overline{z} = a - bi$ forem dados, então as coordenadas a e b são construtíveis somente com régua.*

4 Caracterização dos números construtíveis

Dado um subcorpo F de $\mathbb{C}$ e uma lista de números $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, denotamos por $F[\alpha_1, \ldots, \alpha_n]$ o *menor* subcorpo de $\mathbb{C}$ que contém F e os $\alpha_1, \ldots, \alpha_n$. Menor no sentido que qualquer subcorpo de $\mathbb{C}$ que contém F e os $\alpha_1, \ldots, \alpha_n$ contém também $F[\alpha_1, \ldots, \alpha_n]$. O conjunto $F[\alpha_1, \ldots, \alpha_n]$ pode ser visto também como a intersecção de todos os subcorpos de $\mathbb{C}$ que contêm F e os $\alpha_1, \ldots, \alpha_n$. De fato, se G é um subcorpo de $\mathbb{C}$ que contêm F e $\alpha_1, \ldots, \alpha_n$, como $F[\alpha_1, \ldots, \alpha_n]$ é a intersecção de G com todos os outros subcorpos de $\mathbb{C}$ que contêm F e $\alpha_1, \ldots, \alpha_n$, obviamente $F[\alpha_1, \ldots, \alpha_n] \subset G$ e em todos os outros corpos. Podemos enxergar isso como uma maneira de adicionar a F os elementos $\alpha_1, \ldots, \alpha_n$ que não necessariamente estão nele, de modo a manter ainda a estrutura de corpo. O corpo $F[\alpha_1, \ldots, \alpha_n]$ é dito ser uma *extensão* de F. Note que se os $\alpha_1, \ldots, \alpha_n \in F$, então $F[\alpha_1, \ldots, \alpha_n] = F$.

A partir de $z_0 = 0$ e $z_1 = 1$ podemos, pelo Corolário 4, construir $\mathbb{Q}$. Os demais números $z_2, \ldots, z_n$ adicionamos a $\mathbb{Q}$ juntamente com os seus conjugados $\overline{z}_2, \ldots, \overline{z}_n$, formando o corpo $F_0 = \mathbb{Q}[z_2, \ldots, z_n, \overline{z}_2, \ldots, \overline{z}_n]$ pelo processo explicado no parágrafo anterior. A razão para a definição de F_0 tem dois motivos: 1º, o Corolário 8, pois construções somente com régua nos manterão ainda em F_0 como veremos adiante, assim não precisaremos construir pontos extras; 2º,

F_0 é o menor subcorpo de $\mathbb{C}$ que contém $\mathbb{Q}$ e os pontos $z_2, \ldots, z_n, \overline{z}_2, \ldots, \overline{z}_n$, o que significa que F_0 não contém pontos que não podem ser obtidos a partir dos pontos dados por meio de uma quantidade finita de operações algébricas, e nem pontos que não têm relação com os pontos dados.

O ponto Q_1 é obtido pela aplicação de uma das operações C1, C2 e C3 ao conjunto $S_0 = \{P_0, \ldots, P_n\}$. O ponto Q_2 é obtido por meio de uma das operações C1, C2 e C3 sobre o conjunto $S_1 = S_0 \cup \{Q_1\}$. O ponto Q_3 é obtido a partir de $S_2 = S_1 \cup \{Q_2\}$ ... O ponto Q_k é obtido a partir de $S_{k-1} = S_{k-2} \cup \{Q_{k-1}\}$.

Representando os pontos $Q_1, \ldots, Q_k$ pelos números complexos $w_1, \ldots, w_k$, temos a seguinte tradução para a álgebra: w_1 é obtido pela aplicação de uma das operações C1, C2 e C3 ao conjunto F_0, gerando o conjunto F_1. O ponto w_2 é obtido pela aplicação de uma das operações C1, C2 e C3 ao conjunto F_1, gerando o conjunto F_2. w_3 é obtido a partir de F_2 ... w_k é obtido a partir de F_{k-1} aplicando uma das operações C1, C2 e C3 ao conjunto F_{k-1}, gerando F_k.

Vamos raciocinar por indução em j. Por definição, F_0 é um corpo. Suponha que F_{j-1} $(j \geq 1)$ é um corpo. w_j é obtido pela aplicação de uma das operações C1, C2 e C3 ao conjunto F_{j-1}.

A operação C1 consiste na intersecção entre duas retas que passam por pontos de F_{j-1}. Se $p_1 = x_1 + iy_1$ e $p_2 = x_2 + iy_2$ são pontos de F_{j-1}, a equação da reta que passa por p_1 e p_2 é

$$\begin{vmatrix} x & y & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{vmatrix} = 0.$$

Calculando o determinante obteremos

$$(y_1 - y_2)x + (x_2 - x_1)y + (x_1y_2 - x_2y_1) = 0.$$

O Corolário 7 garante que $x_1, y_1, x_2, y_2 \in F_{j-1}$. Como F_{j-1} é um corpo, os coeficientes $y_1 - y_2$, $x_2 - x_1$ e $x_1y_2 - x_2y_1$ estão em F_{j-1}. Assim a equação de uma reta que passa por pontos de F_{j-1} é da forma

$$ax + by + c = 0$$

com $a, b, c \in F_{j-1}$. Portanto a operação C1 consiste em resolver um sistema do tipo

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}$$

onde $a, b, c, a', b', c' \in F_{j-1}$ (achar os pontos de intersecção entre curvas é o mesmo que resolver o sistema de equações dessas curvas). Resolvendo o sistema de equações acima encontramos

$$x = \frac{bc' - b'c}{ab' - a'b} \quad \text{e} \quad y = \frac{a'c - ac'}{ab' - a'b}$$

Como as frações acima envolvem somente operações algébricas entre elementos de F_{j-1} concluímos que $x, y \in F_{j-1}$, isto é, $w_j \in F_{j-1}$ e então $F_j = F_{j-1}$. A operação C1 nos mantém ainda em F_{j-1}.

A equação da circunferência cujo centro é um ponto $p = u + iv$ de F_{j-1} e cujo raio r é a distância entre dois pontos de F_{j-1} é

$$(x - u)^2 + (y - v)^2 = r^2.$$

Desenvolvendo as potências e reagrupando os termos, obtemos

$$x^2 + y^2 - 2ux - 2vy + (u^2 + v^2 - r^2) = 0.$$

Os coeficientes $-2u$, $-2v$ e $u^2+v^2-r^2$ pertencem a F_{j-1}, logo a equação de uma circunferência em F_{j-1} é

$$x^2+y^2+ax+by+c=0,$$

onde $a,b,c \in F_{j-1}$.

A operação C2 consiste em intersectar uma reta em F_{j-1} e uma circunferência em F_{j-1}, o que equivale a resolver o sistema

$$\begin{cases} ax+by+c=0 \\ x^2+y^2+a'x+b'y+c'=0 \end{cases}$$

onde $a,b,c,a',b',c' \in F_{j-1}$. Suponha que $b \neq 0$ (o caso $a \neq 0$ é análogo). Então

$$y=\frac{-ax-c}{b}. \tag{2}$$

Substituindo na segunda equação obtemos

$$x^2+\left(\frac{-ax-c}{b}\right)^2+a'x+b'\left(\frac{-ax-c}{b}\right)+c'=0,$$

o que dará após alguns cálculos

$$(a^2+b^2)x^2+(2ac-a'b^2-abb')x+(c^2-bb'c+b^2c')=0.$$

Escrevendo $A=a^2+b^2$, $B=2ac-a'b^2-abb'$ e $C=c^2-bb'c+b^2c'$ teremos

$$Ax^2+Bx+C=0$$

onde $A,B,C \in F_{j-1}$. Note que $A \neq 0$, assim

$$x=\frac{-B\pm\sqrt{B^2-4AC}}{2A}=-\frac{B}{2A}\pm\frac{1}{2A}\sqrt{B^2-4AC},$$

isto é, x é da forma

$$x=R+S\sqrt{T}$$

com $R,S,T \in F_{j-1}$. Substituindo isto em (2) obteremos

$$y=\frac{-a(R+S\sqrt{T})-c}{b}=-\frac{aR+c}{b}-\frac{aS}{b}\sqrt{T}$$

que é da forma

$$y=U+V\sqrt{T}$$

com $U,V,T \in F_{j-1}$. Portanto $w_j=x+iy$ é da forma

$$w_j=(R+S\sqrt{T})+i(U+V\sqrt{T})=(R+Ui)+(S+Vi)\sqrt{T},$$

isto é,

$$w_j=P+Q\sqrt{T}$$

onde $P,Q,T \in F_{j-1}$.

A operação C3 consiste na intersecção de duas circunferências cujos centros são pontos de F_{j-1} e cujos raios são as distâncias entre pontos de F_{j-1}. Como na discussão do caso C2, isso equivale a resolver o sistema

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0 \end{cases}$$

onde $a, b, c, a', b', c' \in F_{j-1}$. Subtraindo estas equações membro a membro encontramos

$$(a - a')x + (b - b')y + (c - c') = 0.$$

Supondo $b - b' \neq 0$ (o caso $a - a' \neq 0$ é análogo) teremos

$$y = \frac{-(a - a')x - (c - c')}{b - b'}. \tag{3}$$

Substituindo numa das equações do sistema e fazendo os cálculos obteremos uma equação da forma

$$Ax^2 + Bx + C = 0$$

onde $A, B, C \in F_{j-1}$. Como vimos no caso C2, sua solução é da forma

$$x = R + S\sqrt{T}$$

onde $R, S, T \in F_{j-1}$. Substituindo isto em (3) obteremos uma expressão do tipo

$$y = U + V\sqrt{T}$$

onde $U, V, T \in F_{j-1}$. Portanto $w_j = x + iy$ terá a forma

$$w_j = P + Q\sqrt{T}$$

onde $P, Q, T \in F_{j-1}$.

Em resumo, as operações C1, C2 e C3 produzem um $w_j = P + Q\sqrt{T}$ com $P, Q, T \in F_{j-1}$, podendo acontecer que $\sqrt{T} \in F_{j-1}$ ou não. De qualquer forma, o conjunto F_j será

$$F_j = \{P + Q\sqrt{T} | P, Q \in F_{j-1}\}$$

com $T \in F_{j-1}$. Observe que $F_{j-1} \subseteq F_j$ pois podemos escrever $P = P + 0\sqrt{T}$.

F_j é um subcorpo de $\mathbb{C}$. De fato, dados $a = P + Q\sqrt{T}$ e $b = R + S\sqrt{T}$ em F_j,

$$a - b = (P - R) + (Q - S)\sqrt{c} \in F_j$$

e se $b \neq 0$,

$$\frac{a}{b} = \frac{P + Q\sqrt{T}}{R + S\sqrt{T}} = \frac{P + Q\sqrt{T}}{R + S\sqrt{T}} \cdot \frac{R - S\sqrt{T}}{R - S\sqrt{T}} = \frac{PR - QST}{R^2 - S^2T} + \frac{QR - PS}{R^2 - S^2T}\sqrt{T} \in F_j,$$

o que mostra que F_j é fechado para a subtração e a divisão, logo é um subcorpo de $\mathbb{C}$.

Por indução concluímos que um número w é construtível com régua e compasso a partir de $z_0, z_1, \ldots, z_n$, isto é, $w \in C(z_0, z_1, \ldots, z_n)$ se, e somente se, partindo de $F_0 = \mathbb{Q}[z_2, \ldots, z_n, \overline{z}_2, \ldots, \overline{z}_n]$, for possível formar uma sequência de inclusões

$$F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k$$

com $w \in F_k$ tais que

$$F_j = \{a + b\sqrt{c} | a, b \in F_{j-1}\}$$

para cada $j = 1, \ldots, k$, onde $c \in F_{j-1}$.

Começando com um $w = a + b\sqrt{c} \in F_k$, perceba que cada a, b, c é da forma $p + q\sqrt{r}$ com $p, q, r \in F_{k-2}$ de modo que, escrevendo $a = p_1 + q_1\sqrt{r_1}$, $b = p_2 + q_2\sqrt{r_2}$ e $c = p_3 + q_3\sqrt{r_3}$, então

$$w = p_1 + q_1\sqrt{r_1} + (p_2 + q_2\sqrt{r_2})\sqrt{p_3 + q_3\sqrt{r_3}}.$$

Agora cada p, q, r é da forma $u + v\sqrt{t}$ com $u, v, t \in F_{k-3}$, logo

$$\begin{aligned} w &= u_1 + v_1\sqrt{t_1} + (u_1' + v_1'\sqrt{t_1'})\sqrt{u_1'' + v_1''\sqrt{t_1''}} \\ &\quad + \left(u_2 + v_2\sqrt{t_1} + (u_2' + v_2'\sqrt{t_2'})\sqrt{u_2'' + v_2''\sqrt{t_2''}}\right)\sqrt{u_3 + v_3\sqrt{t_3} + (u_3' + v_3'\sqrt{t_3'})\sqrt{u_3'' + v_3''\sqrt{t_3''}}}. \end{aligned}$$

Procedendo assim até chegarmos em F_0 veremos que w é expresso como uma combinação finita de somas, diferenças, produtos, quocientes e raízes quadradas sucessivas de elementos de F_0. Isto nos fornece uma forma de perceber se um dado número é construtível com régua e compasso.

Exemplo 9 *Saber se*

$$z = \frac{\sqrt{6} + \sqrt{\sqrt{1 + \sqrt[4]{2} + \sqrt{3}} + 5}}{1 - \sqrt{3}}$$

é construtível.

Partindo de $F_0 = \mathbb{Q}$ construímos

$$F_1 = \{a + b\sqrt{2} | a, b \in F_0\}$$

para que $w_1 = \sqrt{2} \in F_1$. Defina agora

$$F_2 = \{a + b\sqrt{w_1} | a, b \in F_1\}$$

para que $w_2 = \sqrt[4]{2} = \sqrt{\sqrt{2}} \in F_2$. Defina

$$F_3 = \{a + b\sqrt{3} | a, b \in F_2\}$$

para que $w_3 = 1 + \sqrt[4]{2} + \sqrt{3} \in F_3$. Ponha

$$F_4 = \{a + b\sqrt{w_3} | a, b \in F_3\}$$

para que $w_4 = \sqrt{1 + \sqrt[4]{2} + \sqrt{3}} + 5 \in F_4$. Defina agora

$$F_5 = \{a + b\sqrt{w_4} | a, b \in F_4\}.$$

Como $\sqrt{6} = \sqrt{2}\sqrt{3}$, $\sqrt{2} \in F_1$ e $\sqrt{3} \in F_3$ e ambos F_1 e F_3 estão contidos em F_5, então $\sqrt{6} \in F_5$, logo $\sqrt{6} + \sqrt{\sqrt{1 + \sqrt[4]{2} + \sqrt{3}} + 5} \in F_5$. Por fim, como $1 - \sqrt{3} \in F_3 \subset F_5$, concluímos que $z \in F_5$, logo z é construtível.

5 Insolubilidade dos problemas clássicos

Os problemas da duplicação do cubo e da trissecção do ângulo são equivalentes, conforme veremos, a resolver equações do terceiro grau. Queremos então saber se uma solução de uma equação do 3º grau pode ser expressa como uma combinação finita de operações algébricas envolvendo a extração de raízes quadradas. A resposta é, em geral, não, conforme dita o teorema a seguir (COURANT; ROBBINS, 2000).

Teorema 10 *Se uma equação algébrica do terceiro grau com coeficientes em F_0 não tem raiz em F_0, então nenhuma de suas raízes é construtível com régua e compasso.*

Prova: O teorema pode ser reformulado da seguinte maneira: se alguma raiz x da equação

$$P(x) = ax^3 + bx^2 + cx + d = 0 \tag{4}$$

com $a, b, c, d \in F_0$ é construtível, então $x \in F_0$.

Faremos a prova por contradição. Suponha que $x \notin F_0$. Como x é construtível, existe uma sequência de inclusões de corpos

$$F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{k-1} \subseteq F_k$$

com $x \in F_k$ tais que

$$F_j = \{a + b\sqrt{c} | a, b \in F_{j-1}\}$$

para cada $j = 1, \ldots, k$, onde $c \in F_{j-1}$. Escolha k para ser o menor inteiro no qual alguma raiz de $P(x)$ está em F_k. Como $x \notin F_0$, $k \geq 1$.

Pela minimalidade de k temos que $x \notin F_{k-1}$, logo x pode ser escrito como

$$x = p + q\sqrt{r}$$

onde $p, q, r \in F_{k-1}$, $q \neq 0$ e $\sqrt{r} \notin F_{k-1}$. Substituindo-o na equação (4) teremos

$$\begin{aligned}
P(x) &= ax^3 + bx^2 + cx + d \\
&= a(p + q\sqrt{r})^3 + b(p + q\sqrt{r})^2 + c(p + q\sqrt{r}) + d \\
&= a(p^3 + 3p^2q\sqrt{r} + 3pq^2r + q^3r\sqrt{r}) + b(p^2 + 2pq\sqrt{r} + q^2r) + c(p + q\sqrt{r}) + d \\
&= (ap^3 + 3apq^2r + bp^2 + bq^2r + cp + d) + (3ap^2 + aq^2r + 2bp + c)q\sqrt{r} \\
&= u + vq\sqrt{r}
\end{aligned}$$

onde $u, v \in F_{k-1}$. Mas como $P(x) = 0$, temos que $u = 0$ e $vq = 0$. Como $q \neq 0$, então $v = 0$. Porém, chamando $\tilde{x} = p - q\sqrt{r}$, teremos ao substitui-lo em (4) que

$$P(\tilde{x}) = u - vq\sqrt{r} = 0,$$

logo $\tilde{x}$ é também raiz de $P(x)$.[3]

Para encontrar a 3ª raiz y da equação usamos a relação de Girard

$$x + \tilde{x} + y = -\frac{b}{a} \Rightarrow y = -\frac{b}{a} - x - \tilde{x} = -\frac{b}{a} - 2p,$$

logo $y \in F_{k-1}$, o que contradiz a minimalidade de k. Isto ocorreu pois no início supomos que $x \notin F_0$, portanto $x \in F_0$. □

Podemos finalmente solucionar os problemas clássicos.

[3]Essa afirmação vale em geral: se $x = p + q\sqrt{r}$ é raiz de um polinômio $P(x)$ de grau ≥ 2, então $\tilde{x} = p - q\sqrt{r}$ é também raiz de $P(x)$.

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.
DOI: 10.21167/cqdv22n12022010026 Disponível em: www.fc.unesp.br/departamentos/matematica/revista-cqd

5.1 Duplicação do cubo

Partimos de um segmento de comprimento l para construir um segmento de comprimento $\sqrt[3]{2}l$. Como l é dado a partir de dois pontos, podemos assumir que esses pontos são z_0 e z_1, logo $F_0 = \mathbb{Q}$. $\sqrt[3]{2}$ é uma solução da equação $x^3 - 2 = 0$. Suas outras raízes são

$$\sqrt[3]{2} \cdot \frac{-1 \pm \sqrt{3}i}{2}.$$

Como nenhuma raiz está em $\mathbb{Q}$, o Teorema 10 garante que nenhuma delas é construtível. Em particular $\sqrt[3]{2}$ não é construtível. Portanto o problema da duplicação do cubo é impossível somente com régua e compasso.

5.2 Trissecção do ângulo

Naturalmente alguns ângulos, como 90° ou 180°, podem ser trissectados com régua e compasso. O problema consiste em saber se existe um procedimento geral para a trissecção. Vamos provar que o ângulo de 60° não pode ser trissectado com régua e compasso apenas.

Considere as identidades trigonométricas

$$\cos(\alpha + \beta) = \cos\alpha\cos\beta - \operatorname{sen}\alpha\operatorname{sen}\beta$$

e

$$\operatorname{sen}(\alpha + \beta) = \operatorname{sen}\alpha\cos\beta + \operatorname{sen}\beta\cos\alpha.$$

Então

$$\cos 2\theta = \cos(\theta + \theta) = \cos^2\theta - \operatorname{sen}^2\theta$$

e

$$\operatorname{sen} 2\theta = \operatorname{sen}(\theta + \theta) = 2\operatorname{sen}\theta\cos\theta.$$

Assim

$$\begin{aligned}
\cos 3\theta &= \cos(2\theta + \theta) = \cos 2\theta\cos\theta - \operatorname{sen} 2\theta\operatorname{sen}\theta \\
&= (\cos^2\theta - \operatorname{sen}^2\theta)\cos\theta - 2\operatorname{sen}\theta\cos\theta\operatorname{sen}\theta \\
&= (\cos^2\theta - \operatorname{sen}^2\theta)\cos\theta - 2\operatorname{sen}^2\theta\cos\theta
\end{aligned}$$

Da relação $\cos^2\theta + \operatorname{sen}\theta^2 = 1$ extraímos $-\operatorname{sen}^2\theta = \cos^2\theta - 1$, logo

$$\begin{aligned}
\cos 3\theta &= (2\cos^2\theta - 1)\cos\theta + 2(\cos^2\theta - 1)\cos\theta \\
&= 4\cos^3\theta - 3\cos\theta
\end{aligned}$$

Escrevendo $3\theta = \alpha$ encontramos

$$\cos\alpha = 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}.$$

O ângulo de 60°=$\pi/3$ pode ser construído a partir de dois pontos, logo $F_0 = \mathbb{Q}$. Tomando $\alpha = \pi/3$ temos que $\cos\alpha = 1/2$, logo

$$\frac{1}{2} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9}.$$

Escrevendo $\cos \pi/9 = x$ teremos

$$\frac{1}{2} = 4x^3 - 3x \Rightarrow 8x^3 - 6x - 1 = 0.$$

Para saber se a equação acima tem alguma solução racional usaremos o seguinte teorema que aprendemos no ensino médio (IEZZI et al., 1977):

Teorema 11 *Se uma equação algébrica*

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

de coeficientes inteiros admite uma raiz racional p/q com p e q primos entre si, então p é um divisor de a_0 e q é um divisor de a_n.

Pelo teorema, as possíveis raízes racionais de $8x^3 - 6x - 1 = 0$ são

$$\left\{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}\right\},$$

mas nenhuma delas é de fato raiz da equação anterior como o leitor poderá checar, o que nos leva a concluir que a equação não possui raízes em $\mathbb{Q}$. Pelo Teorema 10 nenhuma raiz de $8x^3 - 6x - 1 = 0$ é construtível. Em particular $\cos \pi/9$ não é construtível e, portanto, o ângulo de 60° não pode ser trissectado somente usando régua e compasso.

5.3 Quadratura do círculo

Um círculo é determinado por dois pontos, logo $F_0 = \mathbb{Q}$. O problema da quadratura do círculo é equivalente a construir $\sqrt{\pi}$. Lindemann (1882) demonstrou que π não pode ser solução de equação algébrica de coeficientes racionais, isto é, que π é um número *transcendente*.[4] Ora, se π não é algébrico, então não pode ser construído a partir de $\mathbb{Q}$ uma vez que números construtíveis são obtidos através de operações algébricas. Já que π não é construtível, tampouco $\sqrt{\pi}$ o é. Isto demonstra a impossibilidade da quadratura do círculo somente com régua e compasso.

6 Referências Bibliográficas

COURANT, R.; ROBBINS, H. **O que é matemática?** Rio de Janeiro: Ciência Moderna, 2000.

EVES, H. **Introdução à história da matemática**. 5 ed. Campinas: Unicamp, 2011.

FIGUEIREDO, D. G. de. **Números irracionais e transcendentes**. Rio de Janeiro: SBM, 1985.

GONCALVES, A. **Curso de álgebra**. Rio de Janeiro: Impa, 1979.

HEFEZ, A. **Curso de álgebra**. [*S. l.: s.n.*], 2002. v. 2. (versão preliminar). Disponível em: https://docplayer.com.br/175412716-Curso-de-algebra-volume-ii-versao-preliminar-abramo-hefez.html. Acesso em: 4 nov. 2021.

[4] A prova disso é longa e utiliza ferramentas matemáticas avançadas, o que foge do escopo deste texto. O leitor interessado pode encontrar a prova no próprio artigo do Lindemann ou em Stewart (2004, p. 274-276) ou no capítulo 7 de Figueiredo (1985).

IEZZI, G. *et. al*. **Fundamentos de matemática elementar**: complexos, polinômios, equações. 2. ed. São Paulo: Atual, 1977. v. 6.

LINDEMANN, F. Ueber die zahl π. **Mathematische Annalen**, v. 20, p. 213–225, 1882. Disponível em: http://www.digizeitschriften.de/dms/img/?PID=GDZPPN002246910. Acesso em: 4 nov. 2021.

RAGHAVAN, K. N. **Constructions with ruler and compass**: an application of algebra to geometry. Bangalore: The Institute of Mathematical Sciences, 2017. Disponível em: https://www.isibang.ac.in/ jay/MC/Raghavan%202.pdf. Acesso em: 4 nov. 2021.

STEWART, I. **Galois theory**. 3rd. ed. Boca Raton: Chapman & Hall/CRC, 2004.

WANTZEL, M. L. Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas. **Journal de Mathématiques Pures et Appliquées**, v. 2, n. 1, p. 366–372, 1837. Disponível em: http://eudml.org/doc/234865. Acesso em: 4 nov. 2021.