

UNIVERSIDADE FEDERAL DE MINAS GERAIS

Construtibilidade com régua e compasso

Nomes dos alunos:

Erica Aparecida Correia Junqueira
Gustavo Alves de Souza
João Antônio Oliveira Ribeiro de Castro
Luan Victor Souza Santos
Sarah Azevedo Pereira
Vinícius Silveira Barros

Belo Horizonte, MG
julho de 2025

1 Introdução

Iniciaremos com a construção de qualquer segmento cujo comprimento é dado por um número racional. Para isso, precisaremos dos seguintes lemas:

Lema 1. *Dados uma reta L que passa por A e B , e um ponto C fora dela, podemos construir uma reta paralela à L que passa por C .*

Demonstração. Sem perda de generalidade vamos considerar A à esquerda de B . Usando o compasso, traçamos à direita de B o ponto D tal que $AB = BD$. À seguir traçamos as seguintes circunferências:

- C_1 de centro A e raio AC ;
- C_2 de centro B e raio BC ;
- C_3 de centro D e raio AC .

Seja $E = C_2 \cap C_3$. Observe que os triângulos $\triangle ABC$ e $\triangle BDE$ são congruentes, logo a reta $L' = CE$ é paralela à L e contém C . $\square$

Lema 2. *Dados um segmento de reta AB e um ponto C fora dela, podemos construir um segmento de reta CD que é paralelo a AB e possui o mesmo comprimento.*

Demonstração. Sem perda de generalidade vamos considerar A à esquerda de B . Seja L a reta que contém A e B . Com o auxílio do Lema 1 construímos a reta L' paralela à L que passa por C . Traçando a circunferência C de centro C e raio AB e tomando sua interseção com L' temos dois pontos, D e E . Os segmentos DC e CE ambos possuem comprimento AB e são paralelos à AB . $\square$

Perceba que com apenas estes dois lemas, podemos agora mover segmentos de reta livremente de um lugar para outro em um mesmo plano. E ainda, realizar operações com os comprimentos destes segmentos, à saber: soma (e subtração) e multiplicação (e divisão).

Definição 1. Dados dois segmentos de reta de comprimento a e b , respectivamente:

- **Somar** os segmentos a e b significa construir um segmento de reta com comprimento igual a $a + b$.
- **Subtrair** significa construir um segmento de comprimento $|a - b|$.
- **Multiplicar** significa construir um segmento de comprimento $a \cdot b$.
- **Dividir** significa construir um segmento de comprimento a/b (se $b \neq 0$).

Teorema 1. *Dados dois segmentos de reta AB e CD com comprimentos a e b , respectivamente, é possível com régua e compasso:*

1. Somar $(a + b)$ e subtrair $(|a - b|)$ seus comprimentos.

2. Multiplicar $(a \cdot b)$ e dividir (a/b) seus comprimentos.

Demonstração. Soma e Subtração:

Seja L a reta que contém AB . Trace:

- L_1 passando por B e C ,
- L_2 paralela a L_1 passando por D ,
- L_3 paralela a CD passando por B .

A interseção $L_2 \cap L_3$ define um ponto E . Com centro em B e raio BE , trace uma circunferência que intercepta L em F e G . Então, teremos $AG = a + b$ e $AF = |a - b|$

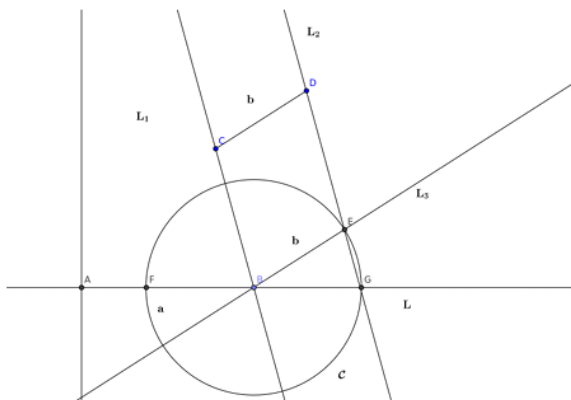


Figura 1: Soma e Subtração

Multiplicação e Divisão:

Posicione AB no eixo x ($A = (0, 0)$, $B = (a, 0)$) e CD no eixo y ($C = (0, 0)$, $D = (0, b)$). Para multiplicação:

- Trace a reta L_1 ligando D a $E = (1, 0)$.
- Trace L_2 paralela a L_1 passando por B .
- A interseção $L_2 \cap y$ define $F = (0, a \cdot b)$.

Para divisão, o processo é análogo, mas ajustando as posições iniciais. $\square$

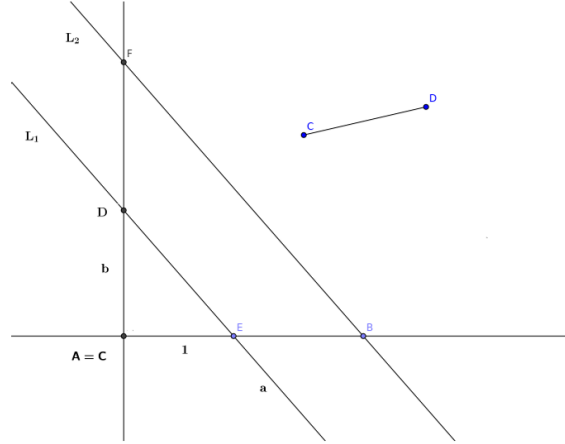


Figura 2: Multiplicação e Divisão

Teorema 2. *Dado um segmento AB de comprimento a , é possível construir um segmento de comprimento $\sqrt{a}$ com régua e compasso.*

Demonstração. Construa:

- $AC = a + 1$ (contendo B),
- D como ponto médio de AC ,
- Circunferência $\mathcal{C}$ com centro em D e raio AD .

Trace uma reta perpendicular a AC passando por B , interceptando $\mathcal{C}$ em E . Então $BE = \sqrt{a}$. $\square$

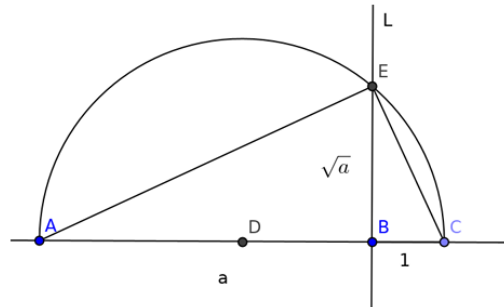


Figura 3: Comprimento $\sqrt{a}$ com régua e compasso.

2 Conclusão sobre os problemas clássicos

2.1 Definições e teoremas importantes

A partir do Teorema 1, concluímos que o conjunto $X := \{a \in \mathbb{R} : \text{é possível construir com régua e compasso um segmento de comprimento } a\}$ é um corpo. Com efeito, o conjunto é fechado para as operações de soma/subtração e de multiplicação. Além disso, como podemos dividir comprimentos, qualquer elemento não nulo do conjunto possui inverso. Outro ponto é que, do Teorema 2, tiramos que $\forall a \in X : \sqrt{a} \in X$. Assim, $\mathbb{Q} \subset X$.

Definição 2. Sejam $S \subset X$ e $a \in \mathbb{R}$. Dizemos que a é **construtível em n passos a partir de S** se podemos obter a por meio de n operações com régua e compasso aplicadas sobre elementos de S .

Lema 3. *Seja $S \subset X$. Se $\alpha \in X$ é construtível em 1 passo a partir de S , então $[\mathbb{Q}(S, \alpha) : \mathbb{Q}(S)] \leq 2$.*

Demonstração. Se α é construído a partir de adição / subtração ou multiplicação / divisão de elementos de S , então $\alpha \in \mathbb{Q}(S)$ e, assim, $\mathbb{Q}(S, \alpha) = \mathbb{Q}(S)$ e, logo, $[\mathbb{Q}(S, \alpha) : \mathbb{Q}(S)] = 1 < 2$.

Caso contrário, a única operação restante para gerar α é a extração da raiz quadrada de algum elemento de S . Assim, $\exists \beta \in S : \alpha = \sqrt{\beta}$. Logo, α é raiz do polinômio $p(x) = x^2 - \beta \in \mathbb{Q}(S)$. Dessa forma, $[\mathbb{Q}(S, \alpha) : \mathbb{Q}(S)] = 2$. $\square$

Lema 4. *Se S_k é o conjunto de números reais que podem ser construídos com até k passos a partir de um segmento de comprimento 1, então $\exists m \in \mathbb{N} : [\mathbb{Q}(S_k) : \mathbb{Q}] = 2^m$.*

Demonstração. • **Caso base:** Se $k = 1$, então, temos que os únicos elementos que podem ser contruídos com 1 passo a partir de $\{1\}$ são: $1 + 1 = 2; 1 - 1 = 0; \sqrt{1} = 1; 1 \times 1 = 1; 1/1 = 1$. Assim, $S_1 \subset \mathbb{Q}$ e, logo, $[\mathbb{Q}(S_1) : \mathbb{Q}] = 1 = 2^0$.

• **Passo indutivo:** Suponha que $[\mathbb{Q}(S_{k-1}) : \mathbb{Q}] = 2^m$. Do Lema anterior, temos que, para qualquer $a \in S_k$, $[\mathbb{Q}(S_{k-1}, a) : \mathbb{Q}] \leq 2$. Além disso, como S_k é um conjunto finito, para cada k existe uma quantidade finita de elementos $a_1, \dots, a_n \in S_k - S_{k-1}$. Assim, $[\mathbb{Q}(S_k) : \mathbb{Q}(S_{k-1})]$

$$\begin{aligned} &= [\mathbb{Q}(S_{k-1}, a_1, \dots, a_n) : \mathbb{Q}(S_{k-1})] \\ &= [\mathbb{Q}(S_{k-1}, a_1, \dots, a_n) : \mathbb{Q}(S_{k-1}, a_1, \dots, a_{n-1})] \dots [\mathbb{Q}(S_{k-1}, a_1) : \mathbb{Q}(S_{k-1})]. \end{aligned}$$

Como o grau de cada adjunção é menor ou igual a 2, temos que $[\mathbb{Q}(S_k) : \mathbb{Q}] = [\mathbb{Q}(S_k) : \mathbb{Q}(S_{k-1})][\mathbb{Q}(S_{k-1}) : \mathbb{Q}] = 2^l 2^m = 2^{l+m} \implies N = l + m$ $\square$

Teorema 3. $\forall a \in \mathbb{R}, (a \in X \implies (\exists N \in \mathbb{N} : [\mathbb{Q}(a) : \mathbb{Q}] = 2^N))$

Demonstração. Aplicando o Lema 4, o resultado segue, já que $\mathbb{Q} \subset \mathbb{Q}(a) \subset \mathbb{Q}(S_k)$ (para algum $k \in \mathbb{N}$.) $\square$

2.2 A impossibilidade da duplicação do cubo

O problema se consiste em: dado um cubo de volume V , podemos construir um cubo de volume $2V$?

Sabemos que o volume de um cubo de aresta a é dado por a^3 . Sem perda de generalidade, podemos assumir que $V = 1$. Assim, o problema se resume em mostrar não existe $a \in \mathbb{R}$ tal que $a^3 = 2$ e a é construtível, ou seja, $\sqrt[3]{2}$ não é construtível.

Demonstração:

Observe que $x^3 - 2$ é irredutível em $\mathbb{Q}$ por Eisenstein usando $p = 2$. Além disso, $\sqrt[3]{2}$ é raiz de $x^3 - 2$, logo $p_{\sqrt[3]{2}|\mathbb{Q}} = x^3 - 2$.

Desse modo, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e como 3 não pode ser fatorado como potência de 2, pelo teorema visto anteriormente, $\sqrt[3]{2}$ não é construtível.

2.3 A impossibilidade da quadratura do círculo

Outro problema clássico seria a possibilidade de, dado um círculo de raio r , conseguirmos construir com régua e compasso um quadrado de mesma área?

Sabemos que a área de um círculo de raio r é πr^2 , ou seja, o problema se resume em definir se existe um número construtível a tal que $a = \pi r^2$. Portanto queremos saber se $\sqrt{\pi}r$ é construtível.

Demonstração:

Sem perda de generalidade, olhemos para o caso em que $r = 1$. Veja que se $\sqrt{\pi}$ é construtível, $\sqrt{\pi}\sqrt{\pi} = \pi$ também é (o conjunto dos construtíveis é fechado para multiplicação). Entretanto, pelo teorema visto anteriormente, existiria $N \in \mathbb{N}$ tal que $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^N$, mas, sabemos que π é transcendente sobre $\mathbb{Q}$ e, portanto, $\mathbb{Q}(\pi) \mid \mathbb{Q}$ deve ser infinita. Logo, $\sqrt{\pi}$ não é construtível.

2.4 A trissecção do ângulo

Queremos agora analisar o problema em que dado um ângulo α , conseguirmos determinar com régua e compasso um ângulo β tal que $\alpha = 3\beta$?

Vejamos, primeiro, que construir um ângulo é equivalente a determinar se o cosseno desse ângulo é construtível analisando a figura de um círculo unitário.

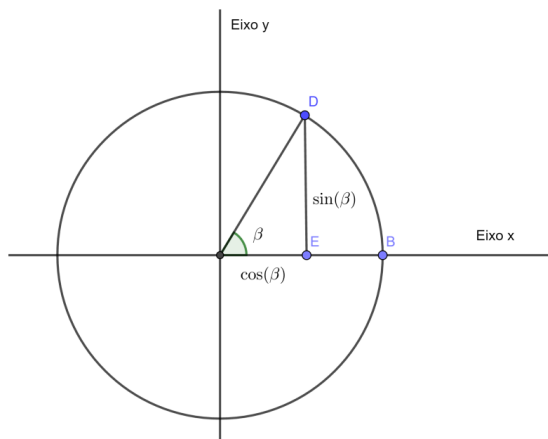


Figura 4: Círculo unitário

Na imagem percebemos que determinar um ângulo β é equivalente a determinar um ponto de coordenada $(\cos(\beta), \sin(\beta))$. Além disso, observe que marcando um ponto E sobre o eixo x de comprimento $\cos(\beta)$ a partir da origem e desenhando uma reta perpendicular ao eixo y que cruza esse ponto (já vimos que fazer tal reta é possível). O ponto que essa reta cruza o círculo unitário por cima determina o o ponto $(\cos(\beta), \sin(\beta))$.

Assim, temos a seguinte equivalência:

β é construtível $\Leftrightarrow \cos(\beta)$ é construtível.

Primeiro observe que existem ângulos que podem ser trissectados. Dado $\alpha = \frac{\pi}{2}$ temos $\beta = \frac{\alpha}{3} = \frac{\pi}{6}$, logo $\cos(\beta) = \frac{\sqrt{3}}{2}$. Como vimos anteriormente, sabemos fazer divisões e tirar raízes quadradas, portanto $\cos(\beta)$ é construtível e, assim, β também é.

Agora olhemos para um caso em que o ângulo não pode ser trissectado.

Escolha $\alpha = \frac{\pi}{3}$. Por propriedade de soma de arcos:

$$\begin{aligned} \frac{1}{2} &= \cos(\alpha) = \cos(3\beta) = \cos(2\beta + \beta) = \cos(2\beta)\cos(\beta) - \sin(2\beta)\sin(\beta) \\ &= (\cos^2(\beta) - \sin^2(\beta))\cos(\beta) - 2\sin^2(\beta)\cos(\beta) \\ &= \cos^3(\beta) - 3\sin^2(\beta)\cos(\beta) = \cos^3(\beta) - 3(1 - \cos^2(\beta)) \\ &= 4\cos^3(\beta) - 3\cos(\beta) \end{aligned}$$

Logo, $\cos(\beta)$ é raiz do polinômio $4x^3 - 3x - \frac{1}{2}$ e, portanto, do polinômio $p(x) = 8x^3 - 6x - 1$. Como esse polinômio é de grau 3 ele é irredutível em $\mathbb{Q}$ se e só se ele não possui raízes racionais. Pelo Teorema das Raízes Racionais temos as seguintes possíveis raízes: $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8}$.

$$\begin{aligned} p(1) &= 8(1)^3 - 6(1) - 1 = 1 \\ p(-1) &= 8(-1)^3 - 6(-1) - 1 = 6 \\ p(\frac{1}{2}) &= 8(\frac{1}{2})^3 - 6(\frac{1}{2}) - 1 = -3 \\ p(-\frac{1}{2}) &= 8(-\frac{1}{2})^3 - 6(-\frac{1}{2}) - 1 = 1 \\ p(\frac{1}{4}) &= 8(\frac{1}{4})^3 - 6(\frac{1}{4}) - 1 = -\frac{19}{8} \\ p(-\frac{1}{4}) &= 8(-\frac{1}{4})^3 - 6(-\frac{1}{4}) - 1 = \frac{3}{8} \\ p(\frac{1}{8}) &= 8(\frac{1}{8})^3 - 6(\frac{1}{8}) - 1 = -\frac{111}{64} \end{aligned}$$

$$p(-\frac{1}{8}) = 8(-\frac{1}{8})^3 - 6(-\frac{1}{8}) - 1 = \frac{-17}{64}$$

Portanto, $p(x)$ é irreduzível em $\mathbb{Q}$ e, assim, $p_{\cos(\beta)|\mathbb{Q}} = p$. Temos então que $[\mathbb{Q}(\cos(\beta)) : \mathbb{Q}] = 3$ e como 3 não pode ser fatorado como potência de 2, $\cos(\beta)$ não é construtível e, portanto, nem β .

3 O Teorema de Gauss

Nessa seção provaremos o Teorema de Gauss, que fornece uma condição necessária e suficiente para que um polígono regular de n lados seja construtível.

Teorema 4. *Seja $n \in \mathbb{N}$. Um polígono regular de n lados é construtível se, e somente se, n é da forma $n = 2^a p_1 p_2 p_3 \dots p_i$, onde $a \in \mathbb{N}_0$ e $p_1, \dots, p_i$ são primos de Fermat distintos.*

3.1 Os primos de Fermat

Um número de Fermat é um número inteiro positivo da forma $F_n = 2^{2^n} + 1$, onde $n \in \mathbb{N}_0$. O matemático francês Pierre de Fermat conjecturou que todos os números dessa forma são primos, no entanto, o matemático Leonard Euler provou mais tarde que a conjectura é falsa. De fato, sabemos que os seguintes números são primos de Fermat:

$$F_0 = 2^{2^0} + 1 = 3; \quad F_1 = 2^{2^1} + 1 = 5; \quad F_2 = 2^{2^2} + 1 = 17; \\ F_3 = 2^{2^3} + 1 = 257; \quad F_4 = 2^{2^4} + 1 = 65537.$$

Sabemos porém que os números $F_5, \dots, F_{32}$ são compostos.

Lema 5. *Se $n = 2^j + 1$, e j não é da forma 2^l , então n é composto. Em outras palavras, se um primo é da forma $2^j + 1$, então ele é um primo de Fermat.*

Demonstração: Suponha que j tenha um número inteiro positivo ímpar b na sua decomposição, isso é, $j = b \cdot 2^l$ com $l \in \mathbb{N}_0$. Logo, $n = 2^j + 1 = 2^{b \cdot 2^l} + 1 = (2^{2^l})^b + 1 = (2^{2^l} + 1) \cdot ((2^{2^l})^{b-1} - (2^{2^l})^{b-2} + (2^{2^l})^{b-3} - \dots - 2^{2^l} + 1)$. Como $j \neq 2^l$, segue que $n = 2^j + 1$ é composto.

3.2 Função Totiente de Euler

Definimos a função Totiente de Euler como sendo $\phi : \mathbb{N} \rightarrow \mathbb{N}$, onde:

$$\phi(n) = |\{k \in \{1, \dots, n\} : \text{mdc}(k, n) = 1\}|.$$

Ou seja, $\phi(n)$ é o número de números naturais entre 1 e n que são coprimos com n . É fácil ver que $\phi(1) = \phi(2) = 1$; $\phi(3) = \phi(4) = 2$; $\phi(5) = 4$.

Segue imediatamente da definição que se p é primo, $\phi(p) = p - 1$. Além disso, se $k \in \mathbb{N}$, $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$, pois $\{m \in \{1, \dots, p^k\} : \text{mdc}(m, p^k) = 1\} = \{1, \dots, p^k\} - \{1, p, p^2, \dots, p^{k-1}\}$.

Lema 6. *Sejam $m, n \in \mathbb{N}$ primos entre si. Então $\phi(mn) = \phi(m)\phi(n)$.*

Demonstração: Para cada $a \in \{0, 1, \dots, mn - 1\}$, escreva $a = q_m m + r_m = q_n n + r_n$, onde $r_m \in \{0, \dots, m - 1\}$ e $r_n \in \{0, \dots, n - 1\}$. Pelo Teorema Chinês dos Restos, a aplicação $\psi : \{0, \dots, mn - 1\} \rightarrow \{0, \dots, m - 1\} \times \{0, \dots, n - 1\}$, $a \mapsto (r_m, r_n)$, é uma bijeção.

Agora note que $\text{mdc}(r_n, n) = \text{mdc}(a, n)$, e $\text{mdc}(r_m, m) = \text{mdc}(a, m)$. Como $\text{mdc}(m, n) = 1$, segue que $\text{mdc}(a, mn) = \text{mdc}(a, m) \cdot \text{mdc}(a, n) = \text{mdc}(r_m, m) \cdot \text{mdc}(r_n, n)$. Logo, $\text{mdc}(a, mn) = 1 \iff \text{mdc}(r_m, m) = \text{mdc}(r_n, n) = 1$.

Restringindo a bijeção ψ para o conjunto $X = \{a \in \{0, \dots, mn - 1\} \mid \text{mdc}(a, mn) = 1\}$, obtemos uma bijeção $\psi|_X : X \rightarrow Y \times Z$, onde $Y = \{a \in \{0, \dots, m - 1\} \mid \text{mdc}(a, m) = 1\}$ e $Z = \{a \in \{0, \dots, n - 1\} \mid \text{mdc}(a, n) = 1\}$.

Lema 7. *Seja n um número inteiro com $n \geq 2$, e assumamos que $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ é sua decomposição em fatores primos distintos dois a dois. Então:*

$$\phi(n) = \prod_{i=1}^k \phi(p_i^{\alpha_i}) = \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1) = n \cdot \prod_{p|n} (1 - \frac{1}{p}).$$

Demonstração: Segue direto do Lema 6 e das observações anteriores.

3.3 A extensão $\mathbb{Q}(\zeta_n) | \mathbb{Q}$

Denotaremos por $\mathbb{K}_n = \mathbb{Q}(1, e^{2\pi i/n}, e^{2 \cdot 2\pi i/n}, \dots, e^{(n-1) \cdot 2\pi i/n})$ o corpo ciclotômico, e $\zeta_n = e^{2\pi i/n}$.

Em particular, ζ_n é raiz primitiva de $x^n - 1 \in \mathbb{Q}[x]$, e $\mathbb{K}_n = \mathbb{Q}(\zeta_n)$ é corpo de decomposição para $x^n - 1$ sobre $\mathbb{Q}$.

Definimos $(\mathbb{Z}_n)^* = \{i \in \mathbb{Z}_n \mid ij = 1 \text{ para algum } j \in \mathbb{Z}_n\}$. Note que $((\mathbb{Z}_n)^*, \cdot)$ é um grupo multiplicativo, e que $|(\mathbb{Z}_n)^*| = \phi(n)$ pois $i \in \mathbb{Z}_n$ tem inverso multiplicativo se, e somente se $\text{mdc}(i, n) = 1$.

Lema 8. *Seja $n \in \mathbb{N}$. Então $\mathbb{Q}(\zeta_n) | \mathbb{Q}$ é uma extensão de Galois, e $\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q}) \cong (\mathbb{Z}_n)^*$. Em particular, $[\zeta_n : \mathbb{Q}] = |\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q})| = |(\mathbb{Z}_n)^*| = \phi(n)$, e $\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q})$ é abeliano.*

Demonstração: Omitiremos a demonstração, mas pode ser encontrada no capítulo 9 do livro Galois Theory de David Cox, juntamente com os pré-requisitos para a mesma.

Lema 9. *Seja $\mathbb{L} | \mathbb{F}$ uma extensão de Galois. Se $G_1 \leq G_2 \leq \text{Gal}(\mathbb{L} | \mathbb{Q})$, então $[\mathbb{L}_{G_1} : \mathbb{L}_{G_2}] = |G_2 : G_1|$.*

Demonstração: Vamos mostrar que $[\text{Gal}(\mathbb{L} | \mathbb{F}) : H] = [\mathbb{L}_H : \mathbb{F}]$ para todo $H \leq \text{Gal}(\mathbb{L} | \mathbb{F})$. Como $\mathbb{L} | \mathbb{F}$ é de Galois, e $\mathbb{L} | \mathbb{L}_H$, temos que $\mathbb{L} | \mathbb{L}_H$ também é de Galois. Além disso, pela correspondência de Galois, temos que $H = \text{Gal}(\mathbb{L} | \mathbb{L}_H)$. Portanto, como $\mathbb{L} | \mathbb{L}_H$ é de Galois, temos que: $|H| = |\text{Gal}(\mathbb{L} | \mathbb{L}_H)| = [\mathbb{L} : \mathbb{L}_H]$. Por outro lado, como $\mathbb{L} | \mathbb{F}$ é de Galois:

$$|\text{Gal}(\mathbb{L} | \mathbb{F})| = [\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{L}_H] \cdot [\mathbb{L}_H : \mathbb{F}] = |H| \cdot [\mathbb{L}_H : \mathbb{F}].$$

$$\text{Por fim, pelo Teorema de Lagrange: } [\text{Gal}(\mathbb{L} | \mathbb{F}) : H] = \frac{|\text{Gal}(\mathbb{L} | \mathbb{F})|}{|H|} = \frac{|H| \cdot [\mathbb{L}_H : \mathbb{F}]}{|H|} =$$

$[\mathbb{L}_H : \mathbb{F}]$.

Em particular, $[Gal(\mathbb{L}|\mathbb{F}) : G_1] = [\mathbb{L}_{G_1} : \mathbb{F}]$, e $[Gal(\mathbb{L}|\mathbb{F}) : G_2] = [\mathbb{L}_{G_2} : \mathbb{F}]$. Segue que:

$$[\mathbb{L}_{G_1} : \mathbb{L}_{G_2}] = [\mathbb{L}_{G_1} : \mathbb{F}] / [\mathbb{L}_{G_2} : \mathbb{F}] = [Gal(\mathbb{L}|\mathbb{F}) : G_1] / [Gal(\mathbb{L}|\mathbb{F}) : G_2] = |G_2| / |G_1| = [G_2 : G_1].$$

3.4 O Lema principal

Lema 10. *Seja $n \in \mathbb{N}$, $n \geq 5$. Então $\cos(\frac{2\pi}{n})$ é construtível se, e somente se n é da forma $n = 2^a p_1 p_2 p_3 \dots p_s$, onde $a \in \mathbb{N}_0$ e $p_1, \dots, p_s$ são primos de Fermat distintos.*

Demonstração: Note primeiramente que para $n \geq 5$, $\cos(\frac{2\pi}{n}) > 0$, e portanto faz sentido falar em construir um segmento de reta com comprimento $\cos(\frac{2\pi}{n})$. Pelo Lema 8, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, onde $\zeta_n = e^{2\pi i/n} = \cos(\frac{2\pi}{n}) + i \cdot \sin(\frac{2\pi}{n})$.

Afirmo que $\mathbb{Q}(\cos(\frac{2\pi}{n})) \subseteq \mathbb{Q}(\zeta_n)$. De fato, $(\zeta_n)^{-1} = (e^{2\pi i/n})^{-1} = e^{(2\pi i/n) \cdot (-1)} = e^{-2\pi i/n} = \cos(-\frac{2\pi}{n}) + i \cdot \sin(-\frac{2\pi}{n}) = \cos(\frac{2\pi}{n}) - i \cdot \sin(\frac{2\pi}{n})$. Logo, $\frac{\zeta_n + (\zeta_n)^{-1}}{2} = \frac{\cos(\frac{2\pi}{n}) + i \cdot \sin(\frac{2\pi}{n}) + \cos(\frac{2\pi}{n}) - i \cdot \sin(\frac{2\pi}{n})}{2} = \frac{2 \cdot \cos(\frac{2\pi}{n})}{2} = \cos(\frac{2\pi}{n}) \implies \cos(\frac{2\pi}{n}) \in \mathbb{Q}(\zeta_n) \implies \mathbb{Q}(\cos(\frac{2\pi}{n})) \subseteq \mathbb{Q}(\zeta_n)$.

Logo, obtemos a torre de extensões $\mathbb{Q}(\zeta_n) | \mathbb{Q}(\cos(\frac{2\pi}{n})) | \mathbb{Q}$, e portanto segue que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(\frac{2\pi}{n}))] \cdot [\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}]$.

Observe que ζ_n é raiz do polinômio $f(x) = x^2 - 2\cos(\frac{2\pi}{n})x + 1 \in \mathbb{Q}(\cos(\frac{2\pi}{n}))[x]$, pois $f(\zeta_n) = (\zeta_n)^2 - 2\cos(\frac{2\pi}{n})(\zeta_n) + 1 = (e^{2\pi i/n})^2 - 2\cos(\frac{2\pi}{n})(e^{2\pi i/n}) + 1 = (e^{2\pi i/n})(e^{2\pi i/n} - 2\cos(\frac{2\pi}{n})) + 1 = (e^{2\pi i/n})(\cos(\frac{2\pi}{n}) + i \cdot \sin(\frac{2\pi}{n}) - 2\cos(\frac{2\pi}{n})) + 1 = -(e^{2\pi i/n})(\cos(\frac{2\pi}{n}) - i \cdot \sin(\frac{2\pi}{n})) + 1 = -(e^{2\pi i/n})(\cos(-\frac{2\pi}{n}) + i \cdot \sin(-\frac{2\pi}{n})) + 1 = -(e^{2\pi i/n})(e^{-2\pi i/n}) + 1 = -1 + 1 = 0$.

Logo, $p_{\zeta_n | \mathbb{Q}(\cos(\frac{2\pi}{n}))}$ divide f , e portanto $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(\frac{2\pi}{n}))] = \text{grau}(p_{\zeta_n | \mathbb{Q}(\cos(\frac{2\pi}{n}))}) \leq \text{grau}(f) = 2$. Mas se fosse $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(\frac{2\pi}{n}))] = 1$, teríamos $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\cos(\frac{2\pi}{n}))$, o que é absurdo pois $\mathbb{Q}(\cos(\frac{2\pi}{n})) \subseteq \mathbb{R}$ e $\zeta_n \notin \mathbb{R}$. Concluímos que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(\frac{2\pi}{n}))] = 2 \implies [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}]$.

Suponha primeiro que $\cos(\frac{2\pi}{n})$ é construtível. Pelo Teorema 3, existe $N \in \mathbb{N}$ tal que vale $[\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}] = 2^N$. Segue daí que $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}] = 2 \cdot 2^N = 2^{N+1} = 2^m$, tomando $m = N + 1$.

Seja $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ a decomposição de n em fatores primos distintos, temos pelo Lema 6 que $\phi(n) = \phi(p_1^{\alpha_1}) \dots \phi(p_r^{\alpha_r})$. Como cada $\phi(p_i^{\alpha_i})$ é inteiro, temos que $\phi(p_i^{\alpha_i})$ divide $\phi(n) = 2^m$ para cada $i \in \{1, \dots, r\}$. Portanto, dado $i \in \{1, \dots, r\}$, temos que: $\phi(p_i^{\alpha_i}) = 2^{k_i}$ para algum $k_i \in \{1, \dots, m\} \implies 2^{k_i} =$

$\phi(p_i^{\alpha_i}) = p_i^{\alpha_i} \cdot \prod_{p|p_i^{\alpha_i}} (1 - \frac{1}{p}) = p_i^{\alpha_i} \cdot (1 - \frac{1}{p_i}) = p_i^{\alpha_i-1} \cdot (p_i - 1)$. Logo, ou $p_i^{\alpha_i-1} | 2^{k_i} \implies p_i | 2^{k_i} \implies p_i = 2$, ou $(p_i - 1) | 2^{k_i} \implies \exists l_i \in \{1, \dots, k_i\}$ tal que $p_i - 1 = 2^{l_i} \implies p_i = 2^{l_i} + 1 \implies p_i$ é primo de Fermat pelo Lema 5. Mas se p_i é primo de Fermat, $p_i \neq 2 \implies p_i$ não divide $2^{k_i} = p_i^{\alpha_i-1} \cdot (p_i - 1) \implies p_i$ não divide $p_i^{\alpha_i-1} \implies \alpha_i - 1 = 0 \implies \alpha_i = 1$. Concluimos que se algum $p_i = 2$, vale que $n = 2^{\alpha_i} p_1 \dots p_{i-1} p_{i+1} \dots p_r$, e se nenhum $p_i = 2$, vale que $n = 2^0 p_1 \dots p_r$.

Reciprocamente, tome $n \in \mathbb{N}$, $n \geq 5$, tal que $n = 2^a p_1 p_2 p_3 \dots p_s$, onde $a \in \mathbb{N}_0$ e $p_1, \dots, p_s$ são primos de Fermat distintos. Segue que $\phi(n) = \phi(2^a p_1 p_2 p_3 \dots p_s) = \phi(2^a) \phi(p_1) \phi(p_2) \phi(p_3) \dots \phi(p_s)$. Para cada $i \in \{1, \dots, s\}$, temos que p_i é primo de Fermat, e portanto $p_i = 2^{t_i} + 1$ para algum $t_i \in \mathbb{N}_0$. Logo, $\phi(p_i) = p_i \cdot \prod_{p|p_i} (1 - \frac{1}{p}) = p_i \cdot (1 - \frac{1}{p_i}) = p_i - 1 = 2^{t_i} + 1 - 1 = 2^{t_i}$. Se $a = 0$, $n = p_1 \dots p_s \implies \phi(n) = \phi(p_1) \dots \phi(p_s) = 2^{t_1} \dots 2^{t_s}$. Se $a > 0$, $\phi(2^a) = 2^a \cdot \prod_{p|2^a} (1 - \frac{1}{p}) = 2^a \cdot (1 - \frac{1}{2}) = 2^{a-1} \cdot (2 - 1) = 2^{a-1}$, com $a - 1 \in \mathbb{N}_0$. Logo, $\phi(n) = \phi(2^a) \phi(p_1) \phi(p_2) \phi(p_3) \dots \phi(p_s) = 2^{a-1} \cdot 2^{t_1} \dots 2^{t_s}$. De todo jeito, $\phi(n) = 2^m$ para algum $m \in \mathbb{N}$.

Portanto, temos que: $2^m = \phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2 \cdot [\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}] \implies [\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}] = 2^{m-1}$. Além disso, como $\mathbb{Q}(\zeta_n) | \mathbb{Q}$ é de Galois, $|\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = 2^m$.

Como $\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q})$ é abeliano, todos os seus subgrupos são normais. Em particular:

$$\begin{aligned} \text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q}(\cos(\frac{2\pi}{n}))) &\trianglelefteq \text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q}), \text{ e} \\ \text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q}) / \text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q}(\cos(\frac{2\pi}{n}))) &\cong \text{Gal}(\mathbb{Q}(\cos(\frac{2\pi}{n})) | \mathbb{Q}) \\ \implies |\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q})| &= |\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q}) / \text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q}(\cos(\frac{2\pi}{n})))| \\ &= |\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q})| / |\text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q}(\cos(\frac{2\pi}{n})))| = 2^m / 2 = 2^{m-1}. \end{aligned}$$

Obtivemos que $|\text{Gal}(\mathbb{Q}(\cos(\frac{2\pi}{n})) | \mathbb{Q})| = 2^{m-1}$, e portanto aplicando o primeiro Teorema de Sylow repetidas vezes obtemos uma cadeia de subgrupos:

$\{e\} \leq G_1 \leq \dots \leq G_{m-2} \leq G_{m-1} = \text{Gal}(\mathbb{Q}(\cos(\frac{2\pi}{n})) | \mathbb{Q})$, onde cada G_i tem ordem 2^i . Utilizando o Teorema Fundamental da Teoria de Galois, obtemos uma Torre de extensões correspondente:

$$\mathbb{Q}(\cos(\frac{2\pi}{n})) = \mathbb{L}_0 | \mathbb{L}_1 | \dots | \mathbb{L}_{m-2} | \mathbb{L}_{m-1} = \mathbb{Q},$$

onde para cada $i \in \{1, \dots, m-1\}$ vale que $\mathbb{L}_i = \mathbb{Q}_{G_i}$, e pelo Lema 9,

$$[\mathbb{L}_{i-1} : \mathbb{L}_i] = [\mathbb{Q}_{G_i} : \mathbb{Q}_{G_{i-1}}] = [G_{i-1} : G_i] = |G_i| / |G_{i-1}| = 2^i / 2^{i-1} = 2.$$

Concluimos pelo exercício 6 que $\cos(\frac{2\pi}{n})$ é construtível.

3.5 A construção

Sabemos pelo Lema P que se $n \geq 5$, então $\cos(\frac{2\pi}{n})$ é construtível se, e somente se n é da forma $n = 2^a p_1 p_2 p_3 \dots p_s$, onde $a \in \mathbb{N}_0$ e $p_1, \dots, p_s$ são primos de Fermat distintos. Nessa subseção, vamos concluir a demonstração do Teorema de Gauss mostrando que $\cos(\frac{2\pi}{n})$ é construtível se, e somente se um polígono

regular de n lados é construtível.

3.5.1 O triângulo e o quadrado

Embora o Lema P não nos forneça informação para quando $n = 3$ ou $n = 4$, é fácil ver que tanto o triângulo equilátero quanto o quadrado são construtíveis:

Dado um segmento de reta AB de comprimento l , utilize o compasso para traçar duas circunferências C_1 , e C_2 de raio l , a primeira centrada em A , e a segunda centrada em B . Denotando por C um dos pontos de interseção entre C_1 e C_2 , obtemos o triângulo equilátero ABC .

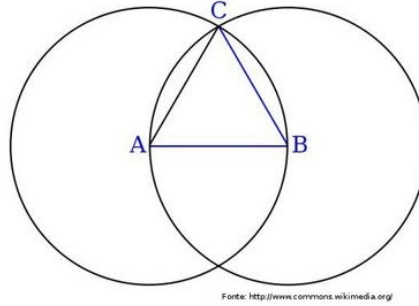


Figura 5: Construção do Triângulo Equilátero

É fácil ver que o reticulado obtido na Proposição 2 contém um quadrado de lado 1.

Note que $3 = 2^2 + 1$ é um primo de Fermat, e que $4 = 2^2$ é potência de 2, portanto a construtibilidade do triângulo equilátero e do quadrado são con-
dizentes com o Teorema de Gauss.

3.5.2 O caso $n \geq 5$

Se $n \geq 5$, o Lema P nos diz que $\cos(\frac{2\pi}{n})$ é construtível se, e somente se n é da forma $n = 2^a p_1 p_2 p_3 \dots p_s$, onde $a \in \mathbb{N}_0$ e $p_1, \dots, p_s$ são primos de Fermat distintos. Logo, para completar a demonstração do Teorema de Gauss, basta mostrar que $\cos(\frac{2\pi}{n})$ é construtível se, e somente se um polígono regular de n lados é construtível.

De fato, se temos construído um polígono regular de n lados, podemos obter um segmento de reta de comprimento $\cos(\frac{2\pi}{n})$ da seguinte forma:

Considere um vértice B do polígono que liga os lados AB e BC do mesmo. Seja r a reta que contém o segmento AB , e s a reta que contém o segmento BC , temos que o menor ângulo entre essas retas é $\pi - \frac{(n-2)\pi}{n} = \frac{n\pi - n\pi + 2\pi}{n} = \frac{2\pi}{n}$. Como vimos anteriormente, $\cos(\beta)$ é construtível se, e somente se o ângulo β é construtível. Logo, $\cos(\frac{2\pi}{n})$ é construtível.

Reciprocamente, se temos construído um segmento de reta AB de comprimento $\cos(\frac{2\pi}{n})$, podemos construir um polígono regular de n lados da seguinte forma: Trace uma circunferência C_1 de raio 1 centrada em A . Seja r_1 a reta perpendicular ao segmento AB , e que passa por B , denote por A_1 algum dos dois pontos de interseção entre C_1 e r_1 . Trace AA_1 , e note que o comprimento de AA_1 é 1, pois A_1 está em C_1 . Seja s_1 a reta paralela a AA_1 que passa por B , e t_1 a reta paralela a AB que passa por A_1 , denote por D_1 a interseção entre s_1 e t_1 . Note que o comprimento de A_1D_1 é o mesmo que o de AB , ou seja, é $\cos(\frac{2\pi}{n})$. Trace a circunferência C_2 centrada em A_1 e passando por D_1 , e note que C_2 tem raio $\cos(\frac{2\pi}{n})$. Denote por u_1 a reta contendo o segmento AA_1 , e denote por B_1 o ponto de interseção entre C_2 e u_1 tal que A_1 está entre A e B_1 . Em particular, o comprimento de A_1B_1 é $\cos(\frac{2\pi}{n})$. Repita o argumento para A_1B_1 , obtendo dois novos pontos A_2 e B_2 . Repetindo a construção n vezes por indução, temos que $AA_1A_2, \dots, A_{n-1}$ é um polígono regular de n lados.

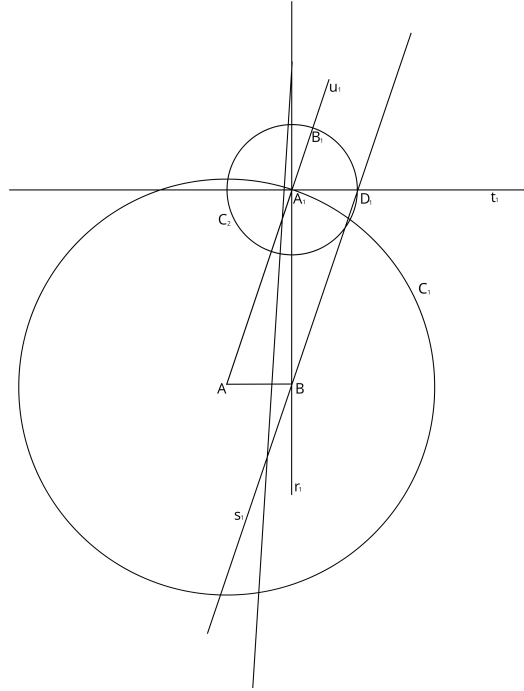


Figura 6: Primeiro Passo da Construção

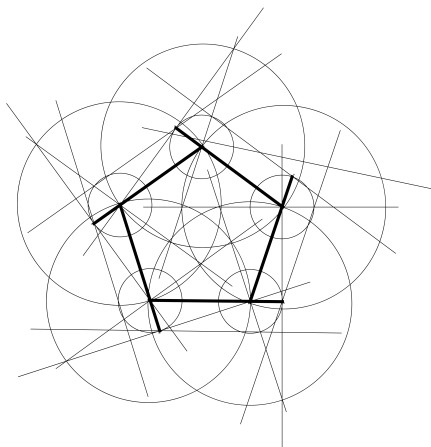


Figura 7: Construção final do pentágono regular

4 Exercícios

Exercício 1. Trace a mediatriz de um segmento qualquer, de extremos A e B . (Dica: use o fato de que A e B podem ser centros de circunferências distintas, mas de um mesmo raio r).

Exercício 2. Transportar um ângulo θ tal que

$$0 < \theta < \frac{\pi}{2}$$

apoando-o sobre uma semirreta seja qual for.

Exercício 3. Do Teorema 1, demonstre que a divisão pode ser feita utilizando régua e compasso.

Exercício 4. Já demonstramos que, dado um número real a , ($a \in X \implies (\exists N \in \mathbb{N} : [\mathbb{Q}(a) : \mathbb{Q}] = 2^N)$). A recíproca é verdadeira? Prove ou dê um contraexemplo

Exercício 5. Determine se o número $\alpha = \sqrt{1 + \sqrt[3]{2}}$ é construtível ou não

Exercício 6. Nesse exercício, vamos completar a demonstração do lema 10 da seção 3.4.

- (a) Mostre que toda extensão de grau 2 possui um elemento primitivo.
- (b) Considere a torre de extensões $\mathbb{R}|\mathbb{L}|\mathbb{Q}$ tal que todo elemento de $\mathbb{L}$ é construtível. Mostre que se $\alpha \in \mathbb{R}$ é tal que $[\mathbb{L}(\alpha) : \mathbb{L}] = 2$, então todo elemento de $\mathbb{L}(\alpha)$ é construtível.
- (c) Utilize o item (b) para provar que se $\alpha \in \mathbb{R}$ é tal que existe uma torre de extensões $\mathbb{Q}(\alpha) = \mathbb{F}_0|\mathbb{F}_1|\dots|\mathbb{F}_{m-1}|\mathbb{F}_m = \mathbb{Q}$ com $[\mathbb{F}_{i-1} : \mathbb{F}_i] = 2 \ \forall i \in \{1, \dots, m\}$, então α é construtível.
- (d) Conclua a demonstração do Lema 10 da seção 3.4.

Exercício 7. Nesse exercício, vamos construir um pentágono regular utilizando régua e compasso.

(a) Verifique utilizando o Teorema de Gauss, que um pentágono regular é construtível.

(b) Mostre que o polinômio minimal de $\cos(\frac{2\pi}{5})$ sobre $\mathbb{Q}$ é $f(x) = x^2 + (1/2)x - (1/4)$, e calcule o grau da extensão $\mathbb{Q}(\cos(\frac{2\pi}{5}))|\mathbb{Q}$. Conclua que $\cos(\frac{2\pi}{5}) = \frac{-1+\sqrt{5}}{4}$.

(Dica: Utilize $\cos(\frac{2\pi}{5}) = \frac{e^{2\pi i/5} + e^{-2\pi i/5}}{2}$).

(c) Partindo do reticulado obtido nos lemas 1 e 2, utilize o método obtido no Teorema 2 para construir um segmento de reta de comprimento $\sqrt{5}$.

(d) Utilize o método de subtração obtido no Teorema 1 para encontrar um segmento de reta de comprimento $\sqrt{5} - 1$.

(e) Utilize o método de divisão obtido no Exercício 3 para encontrar um segmento de reta de comprimento $\frac{\sqrt{5}-1}{2} = \cos(\frac{2\pi}{5})$.

(f) Utilize a construção descrita na seção 3.5. para construir um pentágono regular.