

Construção com régua e compasso

Prof. George Lucas

1 Introduzindo o problema

Definição 1.1. Dados pontos $z_1, z_2 \in \mathbb{C}$ e $r \geq 0$ definimos

$L(z_1, z_2) = \{tz_1 + (1-t)z_2 : t \in \mathbb{R}\}$ a reta que passa por z_1 e z_2

$C(z_1, r) = \{w \in \mathbb{C} : |w - z_1| = r\}$ o círculo de centro z_1 e raio r

Definição 1.2. Dado um conjunto finito $S \subset \mathbb{C}$ com $\{0, 1\} \subset S$ e S fechado por conjugação (isto é $\bar{z} \in S$ para todo $z \in S$), defina a sequência de conjuntos dada por $\mathcal{P}_0 = S$ e para $n \geq 0$:

$$\mathcal{L}_{n+1} = \{L(z_1, z_2) : z_1, z_2 \in \mathcal{P}_n\}, \mathcal{C}_{n+1} = \{C(z_1, |z_2 - z_3|) : z_1, z_2, z_3 \in \mathcal{P}_n\}$$

$$\mathcal{P}_{n+1} = \{z \in \mathbb{C} : z \text{ está em duas retas distintas de } \mathcal{L}_{n+1}\} \cup$$

$$\{z \in \mathbb{C} : z \text{ está em dois círculos distintos de } \mathcal{C}_{n+1}\} \cup$$

$$\{z \in \mathbb{C} : z \text{ está em uma reta de } \mathcal{L}_{n+1} \text{ e em um círculo de } \mathcal{C}_{n+1}\}.$$

Chamamos os elementos do conjunto $\mathcal{P}_n$ o conjunto dos pontos n -construtíveis a partir de S . Chamamos o conjunto $\bigcup_{n \geq 0} \mathcal{P}_n$ de conjunto dos pontos construtíveis a partir de S .

Verifique que os conjuntos $\mathcal{P}_n, \mathcal{L}_n, \mathcal{C}_n$ são finitos, $\mathcal{P}_n$ é fechado por conjugação e que ainda $\mathcal{P}_n \subset \mathcal{P}_{n+1}, \mathcal{L}_n \subset \mathcal{L}_{n+1}$ e $\mathcal{C}_n \subset \mathcal{C}_{n+1}$ para todo $n \in \mathbb{N}$.

Definição 1.3. Dizemos que $K \subset \mathbb{C}$ é um corpo se satisfas os seguintes axiomas:

- $0 \in K$ e $1 \in K$;
- Se $a, b \in K$ então $a - b \in K$;
- Se $a, b \in K$ com $b \neq 0$, então $\frac{a}{b} \in K$.

Note que por essa definição obtemos facilmente que se $a, b \in K$ então $a + b, ab \in K$, ou seja, um corpo é fechado para adição, subtração, multiplicação e divisão (contanto que o divisor seja $\neq 0$).

Lema 1.4. Dado uma família de corpos $\{K_i : i \in I\}$, temos que $\bigcap_{i \in I} K_i$ é um corpo.

Lema 1.5. Se K é um corpo, então $\mathbb{Q} \subset K$.

2 O conjunto dos pontos construtíveis

Nessa seção demonstraremos que dado um conjunto inicial S , então o conjunto dos pontos construtíveis a partir de S é o menor corpo que contém S e é fechado para raiz quadrada, isto é, é o conjunto $\bigcap_{K \in \mathcal{K}} K$, onde $\mathcal{K}$ é a família de corpos K

que contém S tais que se $z \in K$ então $\pm\sqrt{z} \in K$. Note que $\mathcal{K} \neq \emptyset$ pois $\mathbb{C} \in \mathcal{K}$.

Para isso, defina $\mathbb{Q}(S)^{py}$ tal menor corpo que contém S e é fechado para raiz quadrada. Dividamos a demonstração em 2 partes:

- (i) $\mathcal{P}_n \subset \mathbb{Q}(S)^{py}$ para todo $n \in \mathbb{N}$;
- (ii) $\bigcup_{n \geq 0} \mathcal{P}_n$ é um corpo fechado para raiz quadrada.

A parte (i) consiste de fazer indução em n . Com efeito para $n = 0$ o resultado é óbvio. Agora assumindo válido para $n \geq 0$ desejamos provar que $\mathcal{P}_{n+1} \subset \mathbb{Q}(S)^{py}$ o que é equivalente a provar que:

- $\{z \in \mathbb{C} : z \text{ está em duas retas distintas de } \mathcal{L}_{n+1}\} \subset \mathbb{Q}(S)^{py}$;
- $\{z \in \mathbb{C} : z \text{ está em dois círculos distintos de } \mathcal{C}_{n+1}\} \subset \mathbb{Q}(S)^{py}$;
- $\{z \in \mathbb{C} : z \text{ está em uma reta de } \mathcal{L}_{n+1} \text{ e em um círculo de } \mathcal{C}_{n+1}\} \subset \mathbb{Q}(S)^{py}$.

Se z é a intersecção de duas retas, então existem $\alpha, \beta \in \mathbb{R}$ e $z_1, z_2, z_3, z_4 \in \mathcal{P}_n \subset \mathbb{Q}(S)^{py}$ tais que $z = \alpha z_1 + (1 - \alpha)z_2 = \beta z_3 + (1 - \beta)z_4$. Fazendo a conta obtemos $\alpha = \frac{z_2(z_4 - z_3) + \bar{z}_2(z_3 - z_4) - z_3\bar{z}_4 + z_4\bar{z}_3}{(z_1 - z_2)(z_3 - z_4) + (z_4 - z_3)(z_1 - z_2)} \in \mathbb{Q}(S)^{py}$ (pois $z_1, z_2, z_3, z_4, \bar{z}_1, \bar{z}_2, \bar{z}_3, \bar{z}_4 \in \mathcal{P}_n \subset \mathbb{Q}(S)^{py}$) e assim $z \in \mathbb{Q}(S)^{py}$.

Se z é a intersecção de dois círculos, então existem $z_1, z_2, z_3, z_4, z_5, z_6 \in \mathcal{P}_n \subset \mathbb{Q}(S)^{py}$ tais que $|z - z_1| = |z_2 - z_3|$ e $|z - z_4| = |z_5 - z_6|$... fazendo as contas obtemos $z \in \mathbb{Q}(S)^{py}$.

Se z é a intersecção de uma reta e um círculo, então existem $z_1, z_2, z_3, z_4, z_5 \in \mathcal{P}_n \subset \mathbb{Q}(S)^{py}$ e $\alpha \in \mathbb{R}$ tais que $z = \alpha z_1 + (1 - \alpha)z_2$ e $|z - z_3| = |z_4 - z_5|$. Fazendo a conta obtemos $z \in \mathbb{Q}(S)^{py}$.

A prova da parte (ii) é mais extensa e precisamos do seguinte lema:

Lema 2.1. *Seja $n \geq 0$, então*

1. *Se $z, w \in \mathcal{P}_n$, então $\frac{z+w}{2} \in \mathcal{P}_{n+2}$;*
2. *Se $a, b, c \in \mathcal{P}_n$, então a bissetriz do ângulo entre os segmentos $L[a, b]$ e $L[a, c]$ está em $\mathcal{L}_{n+3}$;*
3. *Se $a, b \in \mathcal{P}_n$ então a reta perpendicular a $L(a, b)$ por a está em $\mathcal{L}_{n+3}$;*
4. *Se $a, b, c, p, q \in \mathcal{P}_n$ e θ é o ângulo entre os segmentos $L[a, b]$ e $L[a, c]$, então as retas que passam por p e fazem ângulo θ com $L(p, q)$ estão em $\mathcal{L}_{n+3}$;*
5. *Se $a, b, c \in \mathcal{P}_n$, então a reta paralela a $L(a, b)$ que passa por c está em $\mathcal{L}_{n+3}$;*

6. Se $a, b, c, p, q \in \mathcal{P}_n$ tais que a, b, c não são colineares, então os pontos r tais que os triângulos $\triangle abc$ e $\triangle pqr$ são semelhantes estão em $\mathcal{P}_{n+7}$.

Nota. Aqui, se $z_1, z_2 \in \mathbb{C}$ definimos $L[z_1, z_2] = \{tz_1 + (1-t)z_2 : t \in [0, 1]\}$ o segmento que une z_1 e z_2 .

Demonstração. em sala. □

Teorema 2.2. *Sejam $z, w \in \bigcup_{n \geq 0} \mathcal{P}_n$, então:*

1. $z - w \in \bigcup_{n \geq 0} \mathcal{P}_n$;
2. Se $w \neq 0$ então $\frac{z}{w} \in \bigcup_{n \geq 0} \mathcal{P}_n$;
3. $\pm\sqrt{z} \in \bigcup_{n \geq 0} \mathcal{P}_n$.

Demonstração. Se $w = 0$ então (1) é óbvio. Para $w \neq 0$ veja que $B(0, |w|)$ e $R(0, w)$ se intersectam em w e $-w$, assim $-w \in \bigcup_{n \geq 0} \mathcal{P}_n$ e portanto pelo lema

anterior $\frac{z+(-w)}{2} \in \bigcup_{n \geq 0} \mathcal{P}_n$. Assim $z - w \in R(0, \frac{z-w}{2}) \cap B(\frac{z-w}{2}, |\frac{z-w}{2}|) \subset \bigcup_{n \geq 0} \mathcal{P}_n$

provando (1).

Para (2), (3) assumiremos $z \neq 0$, caso contrário o resultado é óbvio.

Agora note que os triângulos $\triangle(0, z, w)$ e $\triangle(0, \frac{z}{w}, 1)$ são semelhantes e portanto, pelo lema anterior, $\frac{z}{w} \in \bigcup_{n \geq 0} \mathcal{P}_n$, concluindo (2). (Caso $0, z, w$ sejam colineares

deixamos esse caso a cargo do leitor).

Agora seja $z = re^{i\theta}$, $r > 0$. Bissectando o ângulo $\angle(1, 0, z)$ conseguimos traçar a reta $l = \{te^{\frac{i\theta}{2}} : t \in \mathbb{R}\}$. Conseguimos também construir o ponto $\frac{r-1}{2}$ pois ele é o ponto médio de $-1 \in R(0, 1) \cap B(0, 1)$ e $r \in R(0, 1) \cap B(0, |z|)$. Seja si ($s > 0$) uma das intersecções de $C(\frac{r-1}{2}, \frac{r+1}{2})$ e a perpendicular a $L(0, 1)$ por 0. Como a circunferência $C(\frac{r-1}{2}, \frac{r+1}{2})$ passa pelos pontos $-1, r, si, -si$, então aplicando potência de ponto obtemos $s \times s = r \times 1$ e portanto $s = \sqrt{r}$. Finalmente $\{\pm\sqrt{z}\} = B(0, |si|) \cap l$ e está provado (3). □

Este teorema conclui a demonstração de (ii) e portanto o resultado dessa seção segue.

3 Condição necessária para um ponto ser construtível

Inicialmente note que como $\mathcal{P}_n$ é finito, então o conjunto dos pontos construtíveis é enumerável. Assim "quase todo ponto" não é construtível, apesar de o conjunto dos pontos construtíveis ser denso em $\mathbb{C}$ (Basta notar que $a + bi$ é construtível para todos $a, b \in \mathbb{Q}$). Para provar que um ponto é construtível, basta exibir uma maneira de construí-lo, entretanto como provamos que um determinado ponto não é construtível? Iremos nessa seção ver uma propriedade importante dos pontos construtíveis.

Definição 3.1. *Um par (L, K) de corpos (subcorpos de $\mathbb{C}$) é chamada uma extensão de corpos se $K \subset L$. Denotaremos simplesmente por $L : K$.*

Note que L pode ser visto como um espaço vetorial sobre K e com isso vamos definir:

Definição 3.2. *Dada uma extensão de corpos $L : K$ defina seu grau $[L : K]$ como a dimensão de L vista como espaço vetorial sobre K . Se tal dimensão for infinita simplesmente escreva $[L : K] = \infty$.*

Teorema 3.3 (Lei da torre). *Sejam $M : L$ e $L : K$ duas extensões de corpos. Então*

$$[M : L][L : K] = [M : K].$$

Demonstração. Assuma que as três extensões tem grau finito.

Seja $\{x_1, x_2, \dots, x_m\}$ uma base de L sobre K e $\{y_1, y_2, \dots, y_n\}$ uma base de M sobre L . Então deixamos como exercício ao leitor provar que $\{x_i y_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ é uma base de M sobre K .

Se uma dessas 3 extensões tem grau infinito, o resultado também segue. $\square$

Definição 3.4. *Dado um corpo K e um conjunto $S \in \mathbb{C}$ definimos $K(S)$ como sendo o menor corpo que contém K e S , isto é, a intersecção de todos os corpos que contém K e S .*

Em particular $\mathbb{Q}(S)$ denota o menor corpo de contém S .

Defina também $E_n = \mathbb{Q}(\mathcal{P}_n) = E_0(\mathcal{P}_n)$.

Definição 3.5. *Seja $K \subset \mathbb{C}$ um corpo. O polinômio minimal (se existir) de $\alpha \in \mathbb{C}$ é o polinômio mônico sobre K de menor grau que tem α como raiz. Se tal polinômio existir, dizemos que α é algébrico sobre K . Caso contrário dizemos que α é transcendental sobre K .*

Lema 3.6. *Seja $\alpha \in \mathbb{C}$ algébrico sobre K . Então $[K(\alpha) : K]$ é o grau do polinômio minimal de α sobre K .*

Demonstração. Seja m o grau do polinômio minimal de α sobre K . Note que por esse motivo $\{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ é um conjunto LI no espaço vetorial $K(\alpha)$ sobre K . Deixaremos como exercício ao leitor verificar que

$$\left\{ \sum_{i=0}^{m-1} a_i \alpha^i : a_0, \dots, a_{m-1} \in K \right\}$$

é um corpo (Dica: Obviamente isso é fechado para diferença e para produto pois podemos escrever qualquer potência de α como combinação linear de potências com expoente no máximo $m - 1$. Para provar que o inverso de cada elemento não-nulo está no conjunto use Bézout).

Assim, $K(\alpha) = \left\{ \sum_{i=0}^{m-1} a_i \alpha^i : a_0, \dots, a_{m-1} \in K \right\}$. □

Nota. Note que se $\alpha \in \mathbb{C}$ for transcendental sobre K , então $[K(\alpha) : K] = \infty$ pois $\{\alpha^n : n \geq 0\}$ é um conjunto LI.

Teorema 3.7. *Se $\alpha \in \bigcup_{n \geq 0} \mathcal{P}_n$, então $[E_0(\alpha) : E_0]$ é uma potência de 2.*

Demonstração. Se $\alpha \in \mathcal{P}_{n+1}$, então $E_0(\alpha) \subset E_{n+1}$. Vamos provar que $[E_{m+1} : E_m]$ é uma potência de 2 para todo $m \geq 0$ e portanto como $[E_{n+1} : E_n][E_n : E_{n-1}] \dots [E_1 : E_0] = [E_{n+1} : E_0] = [E_{n+1} : E_0(\alpha)][E_0(\alpha) : E_0]$, o resultado segue.

Começamos observando que $[E_n(\alpha) : E_n] = 1$ ou 2 . Com efeito, se $\alpha \in E_n$ tal grau é 1. Assuma $\alpha \notin E_n$. Pelas mesmas contas da parte (i) da seção anterior obtemos que existe um polinômio de grau ≤ 2 sobre E_n que zera α e portanto segue tal afirmação.

Agora note que se $\{\alpha_1, \alpha_2, \dots, \alpha_k\} = P_{m+1} \setminus P_m$ então $E_{m+1} = E_m(\alpha_1, \dots, \alpha_k)$ e assim

$$[E_{m+1} : E_m] = \prod_{i=1}^k [E_m(\alpha_1, \dots, \alpha_i) : E_m(\alpha_1, \dots, \alpha_{i-1})]$$

e como $[E_m(\alpha_1, \dots, \alpha_i) : E_m(\alpha_1, \dots, \alpha_{i-1})] \leq [E_m(\alpha_i) : E_m] = 1$ ou 2 , então segue o resultado.

A última desigualdade segue pelo seguinte fato: Seja Q o polinômio minimal de α_i sobre E_m , então tal polinômio também está sobre $E_m(\alpha_1, \dots, \alpha_{i-1})$. □

Note que, em particular, números transcendentais sobre E_0 não são construtíveis.

Exercícios

- (1) Prove que se $\mathcal{P}_0 = \{0, 1\}$, então não podemos construir o ponto $e^{\frac{i\pi}{9}}$. Isto é, dado uma reta r é impossível construir com régua e compasso uma reta que forme um ângulo de 20° com r .
- (2) Dado um segmento e seus dois extremos, é impossível construir um heptágono regular.

Referências

- [1] Stewart, Ian. Galois theory. Chapman and Hall/CRC, 2022.
- [2] Caminha, Antônio. Construções com Régua e Compasso, 2021.