MATH4302 Algebra II, HKU, 2022

Jiang-Hua Lu

The University of Hong Kong

Thursday March 24, 2022

Outline

Today's topics:

1. §2.1.6 : Ruler-and-Compass construction

To answer some questions from ancient Greek time: can one trisect an angle using a ruler and a compass?

infinitly long legs

stick, no marks

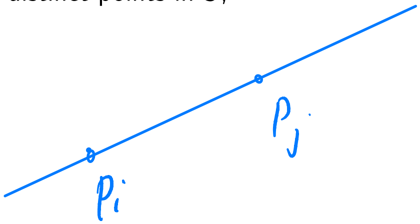
Setting up the problem:

Starting from two distinct points on a blank paper, what can one construct using a pencil, a ruler, and a compass?

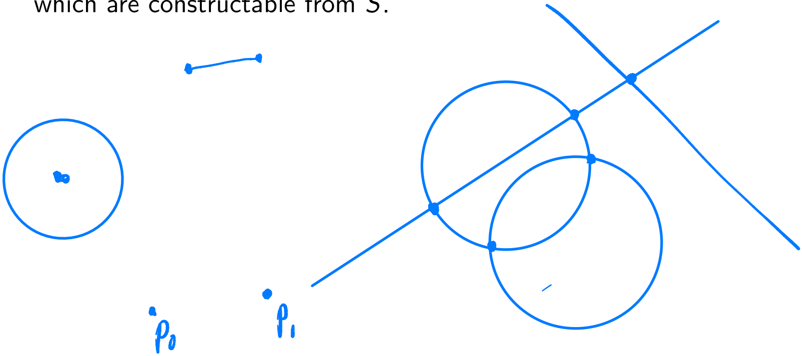
Definitions. Need to define the term "construct."

Given a set of points $S = \{P_0, P_1, P_2, \ldots, P_n\}$ on the paper,

- a (straight) line on the paper is said to be constructable from S if it passes two distinct points in S;



- a circle on the paper is said to be constructable from S if it is centered at a point in S and its radius is the distance between two distinct points in S;
- a point P on the paper is said to be constructable from S if P is the intersection of two lines, or one line and a circle, or two circles, which are constructable from S.



Definition. A point P on the paper is said to be constructable by a ruler and a compass if either $P = P_0$ or $P = P_1$, or if there exists a sequence

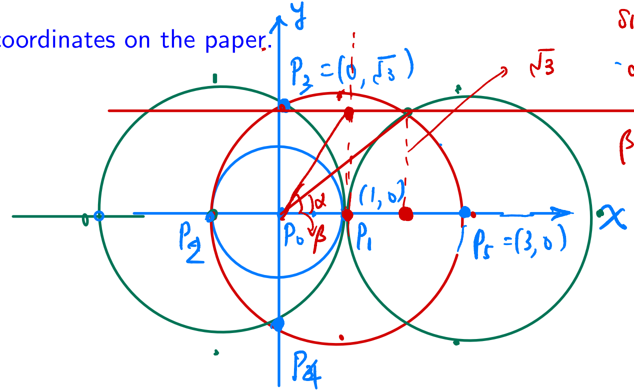
$$P_0, P_1, P_2, \ldots, P_n = P$$

of points with $n \geq 2$ such that for each $1 \leq j \leq n$, P_{j+1} is constructable from the set $S_j = \{P_0, P_1, \ldots, P_j\}$.

$d(P_0, P_1) = 1$

Question. Is every point on the paper constructable?

Putting coordinates on the paper.

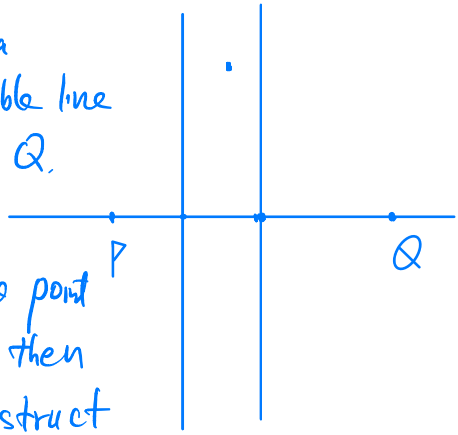


$\sin\alpha = \frac{\sqrt{3}}{2}$

$\alpha = \frac{\pi}{6}$

$\beta = \frac{\pi}{3}$

Claim: If ℓ is a constructable line through P & Q, and R is a constructable point not on ℓ, then we can construct



the line passing through R and parallel to ℓ.

Definition. A point $(x, y) \in \mathbb{R}^2$ is said to be **constructible** if the corresponding point P on the paper is.

Let $S = \{P_0, P_1, \ldots, P_n\} \subset \mathbb{R}^2$, where $P_j = (x_j, y_j)$, $1 \leq j \leq n$. Let

$$K = \mathbb{Q}(x_1, y_1, \ldots, x_n, y_n).$$

Lemma. Assume $P_{n+1} = (x_{n+1}, y_{n+1}) \in \mathbb{R}^2$ is constructible from S. Let

$$L = K(x_{n+1}, y_{n+1}) = \mathbb{Q}(x_1, y_1, \ldots, x_n, y_n,\ x_{n+1}, y_{n+1}).$$

Then $[L : K] = 1$ or 2.

Proof: Three cases.

- P_{n+1} is the intersection of two existing lines: solve for (x_{n+1}, y_{n+1}) from

$$\begin{cases} a\,x_{n+1} + b\,y_{n+1} + c = 0, \\ d\,x_{n+1} + e\,y_{n+1} + f = 0, \end{cases}$$

with $a, b, c, d, e, f \in K$. So $x_{n+1} \in K, y_{n+1} \in K$, thus $L = K$.

- P_{n+1} is the intersection of a line and a circle: solve

$x_{n+1} = \frac{1}{a}(-c-by_{n+1})$

$$\begin{cases} a\,x_{n+1} + b\,y_{n+1} + c = 0, \\ x_{n+1}^2 + y_{n+1}^2 + 2d\,x_{n+1} + 2e\,y_{n+1} + f = 0, \end{cases}$$

Solve quadratic equation for y_{n+1}

with $a, b, c, d, e, f \in K$. So $x_{n+1} \in K, y_{n+1} \in K$, or in a quadratic extension of K, i.e., $|L : K| = 1$ or 2.

- P_{n+1} is the intersection of two circles: solve

$$\begin{cases} x_{n+1}^2 + y_{n+1}^2 + 2a\,x_{n+1} + 2b\,y_{n+1} + c = 0, & (1) \\ x_{n+1}^2 + y_{n+1}^2 + 2d\,x_{n+1} + 2e\,y_{n+1} + f = 0, & (2) \end{cases}$$

with $a, b, c, d, e, f \in K$. Same as second case, $|L : K| = 1$ or 2.

Q.E.D.

Theorem

If $P = (x, y) \in \mathbb{R}^2$ is a constructible point, then $[\mathbb{Q}(x, y) : \mathbb{Q}], [\mathbb{Q}(x), \mathbb{Q}]$ and $[\mathbb{Q}(y) : \mathbb{Q}]$ are all powers of 2.

Proof. Assume that $P = (x, y) \in \mathbb{R}^2$ is constructible.

- By Lemma, there exist sequence of field extensions

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_n$$

  with $[L_j : L_{j-1}] = 1$ or 2 for each j, such that $(x, y) \in L_n$.

- By the Tower theorem, $[L_n : \mathbb{Q}] = 2^m$ for some integer $m \geq 0$.

- As $\mathbb{Q} \subset \mathbb{Q}(x, y) \subset L_n$, by the Tower Theorem again,

$$[\mathbb{Q}(x, y) : \mathbb{Q}] | 2^m,$$

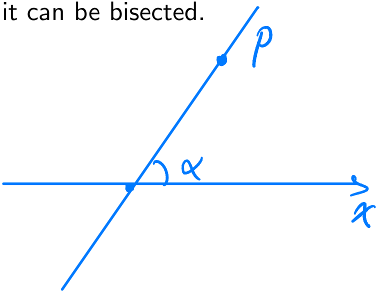
  so $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$ for some integer $r \geq 0$.

- Since $\mathbb{Q} \subset \mathbb{Q}(x) \subset \mathbb{Q}(x, y)$ and $\mathbb{Q} \subset \mathbb{Q}(y) \subset \mathbb{Q}(x, y)$, by Tower Theorem again, both $[\mathbb{Q}(x) : \mathbb{Q}]$ and $[\mathbb{Q}(y) : \mathbb{Q}]$ are powers of 2. //

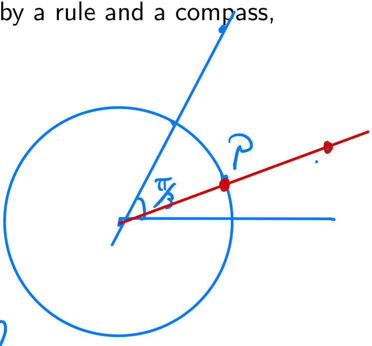
Definition. An angle α is said to be constructible if there is a constructible point $P \neq (0,0)$ on the half line $\underline{L}$ connecting $(0,0)$ and P that has angle α with L_x.

Example. The angle $\pi/3$ is constructible, and it can be bisected.

Exercise.



Theorem. The angle $\pi/3$ can not be trisected by a rule and a compass, i.e., the angle $\pi/9$ is not constructible.



Proof. Let $\alpha = \frac{\pi}{9}$, $3\alpha = \frac{\pi}{3}$

$P = (\cos\alpha, \sin\alpha)$

Consider $L = \mathbb{Q}(\cos\alpha)$

$\frac{1}{2} = \cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$

So $\cos\alpha = \beta$ is a root of

$$4x^3 - 3x - \frac{1}{2} = 0$$

$$8x^3 - 6x - 1 = 0$$

Check: $p(x) = 8x^3 - 6x - 1 \in \mathbb{Q}[x]$ is irreducible

so $|\mathbb{Q}(\cos\alpha) : \mathbb{Q}| = 3$. So P is not constructible //

Further statements:

Definition. A real number $a \in \mathbb{R}$ is said to be constructible if its absolute value $|a|$ is the distance between two constructible points in $\mathbb{R}^2$.

- The set of all constructible real numbers is a subfield of $\mathbb{R}$.
- A point $(x, y) \in \mathbb{R}^2$ is constructible if and only if both x and y are constructible numbers.
- A real number x is constructible iff $x \in K_n$ for a tower of real quadratic field extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \mathbb{R},$$

where $[K_{j+1} : K] = 2$ for all $0 \leq j \leq n-1$;

Further statements, cont'd

- A complex number $x + iy \in \mathbb{C} \cong \mathbb{R}^2$ is constructible iff $x + iy \in K_n$ for a tower of complex quadratic field extensions

$$\mathbb{Q}(i) = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \mathbb{C},$$

where $[K_{j+1} : K] = 2$ for all $0 \leq j \leq n-1$.

- The set of all constructible points in $\mathbb{R}^2 \cong \mathbb{C}$, being a subfield of $\overline{\mathbb{Q}}$, is countable.

Further statements, cont'd

- A complex number $x + iy \in \mathbb{C} \cong \mathbb{R}^2$ is constructible iff $x + iy \in K_n$ for a tower of complex quadratic field extensions

$$\mathbb{Q}(i) = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subset \mathbb{C},$$

  where $[K_{j+1} : K] = 2$ for all $0 \leq j \leq n - 1$.

- The set of all constructible points in $\mathbb{R}^2 \cong \mathbb{C}$, being a subfield of $\overline{\mathbb{Q}}$, is countable.