The Three Classical Problems

An Introduction to Constructible Numbers

Satvik Saha

25 February, 2023

Department of Mathematics and Statistics,
Indian Institute of Science Education and Research, Kolkata

1. Angle trisection. $\pi/9$
2. Doubling the cube. $\sqrt[3]{2}$
3. Squaring the circle. $\sqrt{\pi}$

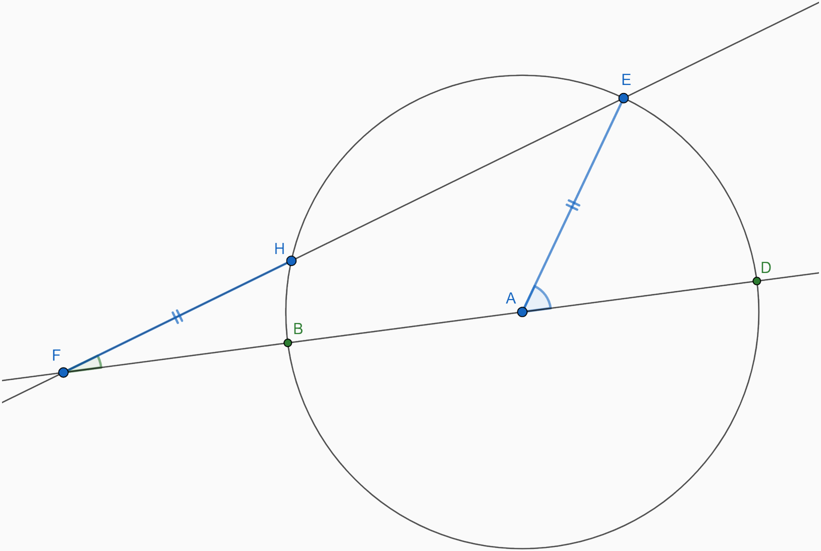

Figure 1: Archimedes’ method of trisecting an angle.

Outline

1. The Rules of the Game
2. The Language of Field Extensions
3. The Constructible Number Theorem
4. Bending the Rules

The Rules of the Game

Straightedge and compass

1. A line can be drawn through any two constructed points. $L(\alpha, \beta)$
2. A circle can be drawn centred at any constructed point, and with any previously constructed length as radius. $C(\gamma, R)$

The intersection points of constructed lines and circles are added to the collection of constructed points.

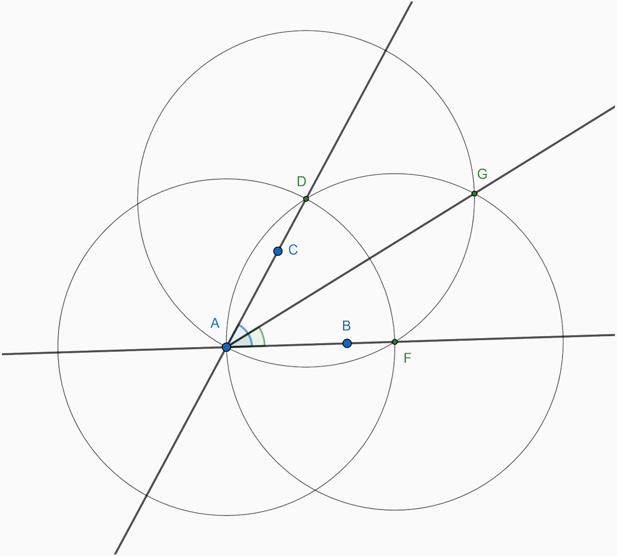

Figure 2: Any angle can be bisected.

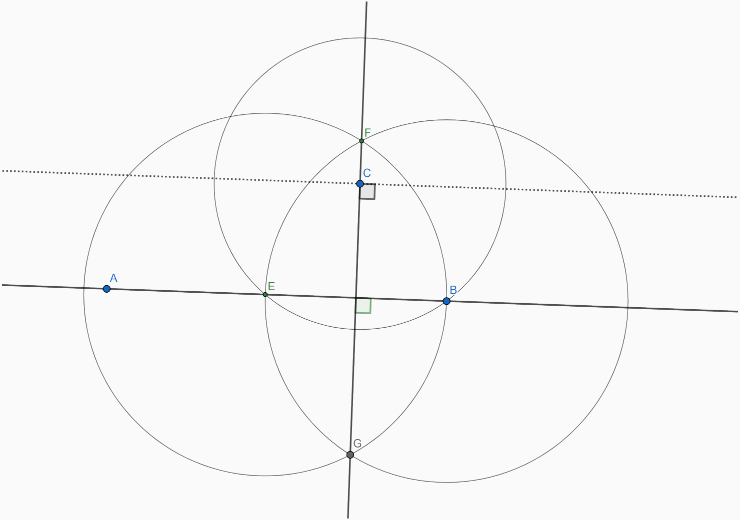

Figure 3: A perpendicular can be dropped onto a line from any point, and a parallel line can be drawn through the point.

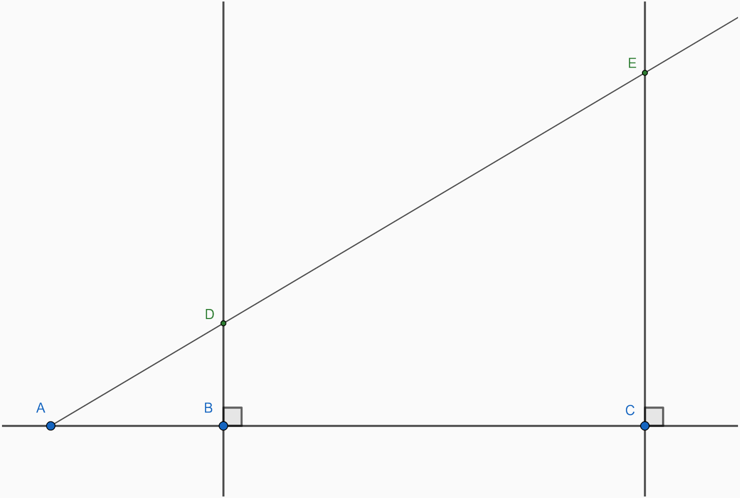

Figure 4: Any two lengths can be multiplied together or divided, via $DB = EC/AC$ with $AB = 1$.

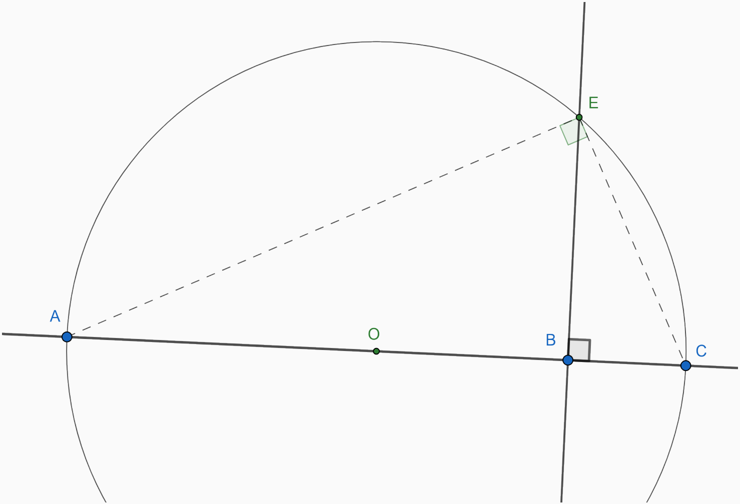

Figure 5: The square root of any length can be constructed, via $AB = EB^2$ with $BC = 1$.

Start by marking the points 0 and 1 on the complex plane. A number $\alpha \in \mathbb{C}$ is said to be constructible if and only if it can be constructed via straightedge and compass in finitely many steps.

Remark

If α is constructible, so are $-\alpha$, $\overline{\alpha}$, $i\alpha$, $|\alpha|$, $\sqrt{\alpha}$, $\mathrm{Re}(\alpha)$, $\mathrm{Im}(\alpha)$.

Constructible numbers

Constructible numbers form a field.

Proof

If α and β are constructible, so are $\alpha \pm \beta$, $\alpha\beta$, α/β.

Remark

The field of constructible numbers contains $\mathbb{Q}$, and is contained within $\mathbb{C}$.

The Language of Field Extensions

Field extensions

Let F, K be fields with $F \subseteq K$. We say that K/F is a field extension of F, also denoted $F \hookrightarrow K$.

With this, K can be seen as an F-vector space. Define

$$[K : F] = \dim_F(K).$$

We say that K/F is a *finite extension* if $[K : F]$ is finite.

Simple field extensions

Let K/F be a field extension. Suppose that $\alpha \in K \setminus F$. Then, we define $F(\alpha)$ to be the smallest subfield of K containing both F and α.

$$F(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} : p, q \in F[x],\ q(\alpha) \neq 0 \right\}.$$

Algebraic extensions

We say that α is *algebraic* over F when $f(\alpha) = 0$ for some polynomial $f \in F[x]$.

If f is monic and of minimal degree, then f is called the (unique) *minimal polynomial* of α.

Examples

The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.

The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$.

The minimal polynomial of $\cos(\pi/9)$ over $\mathbb{Q}$ is $x^3 - 3x/4 - 1/8$.

Algebraic extensions

If α is algebraic over F, then

$$F(\alpha) = \{p(\alpha) : p \in F[x]\} = F[\alpha].$$

It follows that $[F(\alpha) : F]$ is precisely the degree of the minimal polynomial of α over F.

Examples

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2. \qquad [\mathbb{Q}(\cos(\pi/9)) : \mathbb{Q}] = 3.$$

Proof

The numbers $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ form a basis of $F(\alpha)$.

Chaining simple field extensions

Let K/F be a field extension. Suppose that $\alpha_1, \ldots, \alpha_k \in K \setminus F$. Then, we define $F(\alpha_1, \ldots, \alpha_k)$ to be the smallest subfield of K containing F and all $\alpha_1, \ldots, \alpha_k$.

$$\begin{aligned} F(\alpha_1, \ldots, \alpha_k) &= F(\alpha_1, \ldots, \alpha_\ell)(\alpha_{\ell+1}, \ldots, \alpha_k) \\ &= F(\alpha_1)(\alpha_2)\ldots(\alpha_k). \end{aligned}$$

Tower Lemma

Let K/F and L/K be finite field extensions. Then, L/F is a finite field extension, with

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

Example

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$
$$= 3 \times 2 = 6.$$

Proof

If $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of K/F and $\{\beta_1, \ldots, \beta_m\}$ is a basis of L/K, then $\{\alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_n\beta_m\}$ is a basis of L/F.

Constructible numbers form a field $\mathscr{C}$, with

$$\mathbb{Q}(i) \subseteq \mathscr{C} \subseteq \mathbb{C}.$$

Remark

If α is constructible, then so is $\sqrt{\alpha}$. Thus, $\mathscr{C}$ is a *quadratically closed field* – in particular, $\mathscr{C}$ is the *quadratic closure* of $\mathbb{Q}$.

The Constructible Number Theorem

Minimal polynomials of constructible numbers

If a number $\alpha \in \mathbb{C}$ is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ for some integer n.

Equivalently, the degree of the minimal polynomial of α over $\mathbb{Q}$ must be a power of 2.

Example

The number $\cos(\pi/9)$, hence the angle $\pi/9$, is not constructible.

The number $\sqrt[3]{2}$ is not constructible.

The number $\sqrt{\pi}$ is not even algebraic!

Lines and circles

If α lies at the intersection of some lines $L(\beta_i, \delta_i)$ and/or circles $C(\gamma_i, R_i)$ for some $\beta_i, \delta_i, \gamma_i, R_i \in F$ where the field $F \supseteq \mathbb{Q}$ is closed under conjugation, then

$$[F(\alpha) : F] \leq 2.$$

In other words, there exist $\xi, \zeta \in F$ such that

$$\alpha^2 - 2\xi\alpha + \zeta = 0 \iff \alpha = \xi \pm \sqrt{\xi^2 - \zeta}.$$

The lines $\beta_i + (\delta_i - \beta_i)x \equiv \beta_i + \gamma_i x$ intersect at

$$\beta_1 + \gamma_1 \frac{v_2(s_2 - s_1) + u_2(t_1 - t_2)}{u_1 v_2 - u_2 v_1},$$

where $\beta_i = s_i + it_i$, $\gamma_i = u_i + iv_i$.

Proof

Solve the system

$$s_1 + u_1 x_1 = s_2 + u_2 x_2, \qquad t_1 + v_1 x_1 = t_2 + v_2 x_2.$$

Intersection of a line and a circle

The line $\beta + \delta x$ and the circle $|z - \gamma|^2 = R^2$ intersect at

$$\beta + \delta x$$

where x is a real root of the quadratic

$$|\delta|^2 x^2 + \left[(\beta - \gamma)\overline{\delta} + \overline{(\beta - \gamma)}\delta\right] x = R^2 - |\beta - \gamma|^2.$$

Proof

Expand

$$|(\beta - \gamma) + \delta x|^2 = R^2.$$

Intersection of two circles

The circles $|z - \gamma_i|^2 = R_i^2$ intersect at

$$x + iy$$

where

$$2(u_1 - u_2)x + 2(v_1 - v_2)y = R_2^2 - R_1^2 + |\gamma_1|^2 - |\gamma_2|^2,$$

and $\gamma_i = u_i + iv_i$.

This reduces to the previous case!

Building a tower

Let α be constructible. There is a finite sequence of lines and circles such that the final diagram has α at some intersection.

Look at the diagram at step m. There are finitely many intersections of lines and circles present, say $\alpha_1, \ldots, \alpha_k$. Thus, they all lie in the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_k) = F_n$.

In the next step, a line or circle is drawn using these existing points, so any new intersection α_{k+i} must lie in $F_m(\alpha_{k+i})$ with $[F_m(\alpha_{k+i}) : F_m] \leq 2$.

The constructible number theorem

A number $\alpha \in \mathbb{C}$ is constructible *if and only if* α lies in an *iterated quadratic extension* of $\mathbb{Q}$, i.e. there exists a tower of fields

$$\mathbb{Q} = F_0 \hookrightarrow F_1 \hookrightarrow \cdots \hookrightarrow F_{n-1} \hookrightarrow F_n$$

with each $[F_j : F_{j-1}] = 2$ and $\alpha \in F_n$.

Proof of converse

Suppose that every number from F_{j-1} is constructible. If $[F_j : F_{j-1}] = 2$, then F_j/F_{j-1} has a basis of the form $\{1, \beta\}$, where

$$\beta^2 - 2\xi\beta + \zeta = 0 \iff \beta = \xi \pm \sqrt{\xi^2 - \zeta}$$

for some $\xi, \zeta \in F_{j-1}$. This means that β is constructible, since $\mathscr{C}$ is quadratically closed.

Consequently, every $\alpha \in F_j$ is constructible, since it can be written in the form $\alpha = \gamma + \delta\beta$ for $\gamma, \delta \in F_{j-1}$.

Bending the Rules

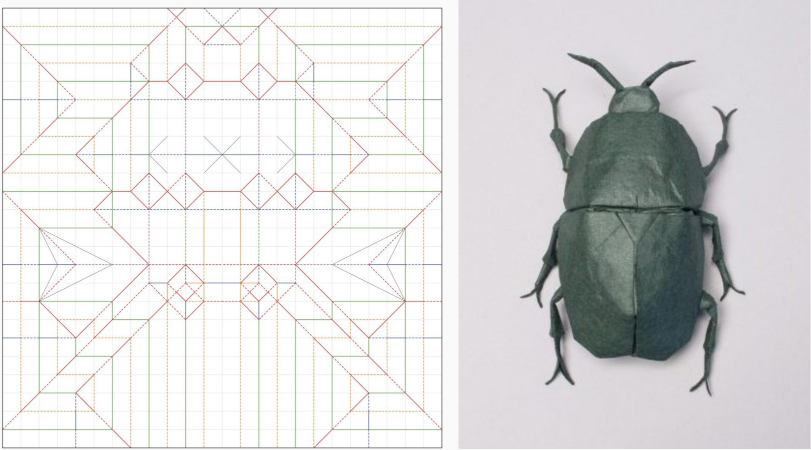

Figure 6: Scarab with Elytra, *Opus 594*, Robert J. Lang.

Origami constructions: Huzita-Hatori

1. A line can be drawn through any two constructed points.
2. The perpendicular bisector of any two constructed points can be drawn.
3. The angle bisector of any constructed angle can be drawn.
4. The perpendicular to any constructed line through any constructed point can be drawn.
5. Given a constructed line L and constructed points α, β, a line through β that reflects α onto L can be drawn.
6. Given constructed lines L, M and constructed points α, β, a line that simultaneously reflects α onto L and β onto M can be drawn.

A number $\alpha \in \mathbb{C}$ is origami constructible *if and only if* there exists a tower of fields

$$\mathbb{Q} = F_0 \hookrightarrow F_1 \hookrightarrow \cdots \hookrightarrow F_{n-1} \hookrightarrow F_n$$

with each $[F_j : F_{j-1}] = 2$ or 3, and $\alpha \in F_n$.

Remark

This means that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n 3^m$ for some integers n, m.

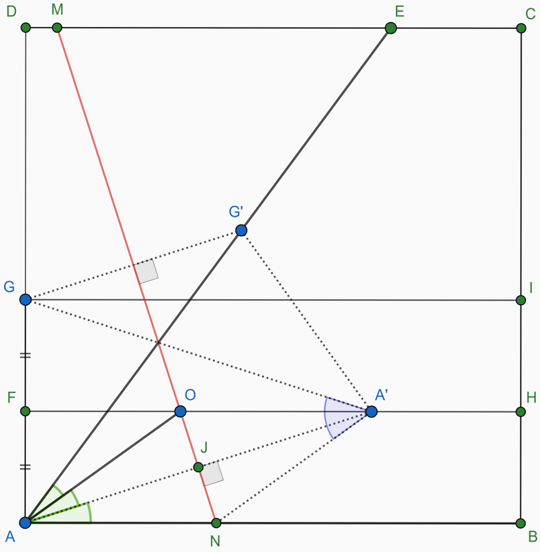

Figure 7: Using Origami to trisect the angle $\angle EAB$

David S. Dummit and Richard M. Foote.
Abstract Algebra.

James King.
Origami-constructible numbers.
2004.