Constructibility by Straightedge and Compass

Liam Moore

Euler Circle

July 13, 2026

Outline

The Classical Problem

The ancient Greeks asked a simple question:

Which geometric figures can be constructed using only a straightedge and a compass?

This question eventually led to one of the earliest connections between

- Euclidean geometry,
- abstract algebra,
- field theory,
- and ultimately Galois theory.

Historical Motivation

Three famous problems remained unsolved for approximately two thousand years.

- Doubling the cube: (constructing a cube exactly twice the volume of a given cube)
- Trisecting an arbitrary angle: (dividing an arbitrary angle into three equal parts)
- Squaring the circle: (constructing a perfect square with the same area as a given circle)

The proofs of impossibility eventually came from Algebra, not geometry.

What is a Straightedge and Compass Construction?

An idealized construction allows only two tools.

Straightedge

- Draw the unique line through two known points.

Compass

- Draw a circle with known center and radius.

Every new point is obtained only as an intersection of

- two lines,
- a line and a circle,
- or two circles.

Constructible Numbers

Starting from the unit segment, every constructible point corresponds to a real number.

Examples include

$$0,\ 1,\ 2,\ \frac{3}{2},\ \sqrt{2},\ \sqrt{3},\ \sqrt{2+\sqrt{2}}.$$

Nonconstructible numbers include

$$\sqrt[3]{2}, \qquad \pi, \qquad \cos\left(\frac{\pi}{9}\right).$$

The goal is to determine which real numbers can arise from a finite sequence of constructions.

Definition: Constructible Number

Definition

A real number is called *constructible* if it can be obtained as the coordinate of a point constructed from the unit segment using only a straightedge and compass.

The remainder of this presentation develops an algebraic criterion for determining exactly which numbers satisfy this definition.

The Key

Rather than researching

which geometries can be drawn,

we instead research

the algebraic operations a straightedge and compass are capable of performing.

Answering this question transforms a geometric problem into one about field extensions.

The Fundamental Observation

Every straightedge and compass construction solves only one of two types of equations.

- Linear equations

$$ax + b = 0$$

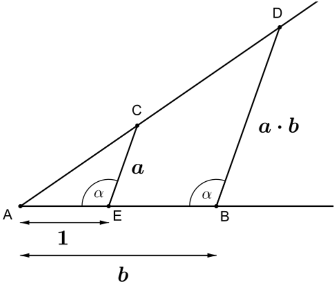
- Quadratic equations

$$ax^2 + bx + c = 0.$$

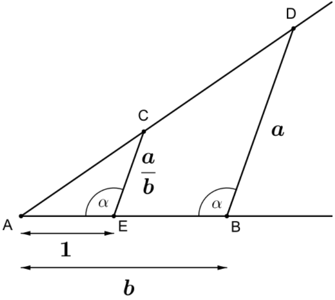
Therefore every new constructible number is obtained using

$$+, \quad -, \quad \times, \quad \div, \quad \sqrt{\ }.$$

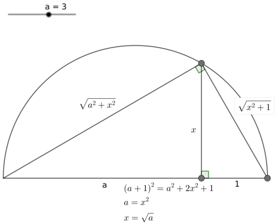
Constructions



(a) Multiplication



(b) Division



(c) Square Root

Figure: Straightedge and compass constructions for arithmetic operations: (a) multiplication, (b) division, and (c) square root.

From Geometry to Field Extensions

The arithmetic operations from the previous section generate larger and larger fields.

Starting with the rational numbers,

$$\mathbb{Q},$$

each square root construction enlarges the field by at most a quadratic extension.

A sequence of constructions therefore produces a tower

$$\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n,$$

where

$$[F_{i+1} : F_i] \leq 2.$$

Constructibility is therefore equivalent to building numbers through repeated linear or quadratic extensions.

Tower of Quadratic Extensions

$$\begin{array}{c} F_n \\ \uparrow \\ \vdots \\ \uparrow \\ F_3 = F_2(\sqrt{a_3}) \\ \uparrow \\ F_2 = F_1(\sqrt{a_2}) \\ \uparrow \\ F_1 = \mathbb{Q}(\sqrt{a_1}) \\ \uparrow \\ \mathbb{Q} \end{array}$$

Each step introduces at most one square root.
Consequently,

$$[F_n : \mathbb{Q}] = 2^k$$

for some integer k.

The Degree Condition

Theorem

If a real number is constructible, then its field extension over $\mathbb{Q}$ has degree

$$2^k$$

for some integer $k \geq 0$.

Examples

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$$

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8.$$

Every construction doubles the degree at most once.

Minimal Polynomials

The degree of a field extension is determined by the minimal polynomial of the constructed number.

Examples

$$\sqrt{2}$$

has minimal polynomial

$$x^2 - 2,$$

so

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

Minimal Polynomials

Similarly,

$$\sqrt[3]{2}$$

has minimal polynomial

$$x^3 - 2,$$

giving

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

Since

$$3 \neq 2^k,$$

the cube root of two cannot be constructed.

Constructible and Nonconstructible Numbers

Constructible

$$\sqrt{2}$$

$$\sqrt{3}$$

$$\sqrt{2+\sqrt{2}}$$

$$\cos\frac{\pi}{5}$$

$$\frac{1+\sqrt{5}}{2}$$

Not Constructible

$$\sqrt[3]{2}$$

$$\pi$$

$$\cos\frac{\pi}{9}$$

$$\sqrt[5]{3}$$

$$e$$

Why the Cube Cannot Be Doubled

Suppose a cube has side length

$$1.$$

Doubling its volume requires a new side length

$$x,$$

where

$$x^3 = 2.$$

Thus

$$x = \sqrt[3]{2}.$$

Its minimal polynomial is

$$x^3 - 2,$$

which has degree

$$3.$$

Since 3 is not a power of two, no straightedge and compass construction can produce this length.

Current Chain of Logic

Geometry

$$\Downarrow$$

Arithmetic Operations

$$\Downarrow$$

Field Extensions

$$\Downarrow$$

$$\boxed{[F : \mathbb{Q}] = 2^k}$$

The remaining question is whether every extension of degree 2^k is in fact constructible.

1. Galois Theory

Splitting Fields

To fully understand constructibility, we must study all of its roots simultaneously via Galois Theory.

Definition

The *splitting field* of a polynomial is the smallest field containing every root of that polynomial.

Example:

$$x^2 - 2$$

has roots

$$\pm\sqrt{2},$$

so its splitting field is

$$\mathbb{Q}(\sqrt{2}).$$

Why Splitting Fields Matter

A splitting field contains every algebraic relationship among the roots of a polynomial.

Instead of studying a single constructible number, we study the entire algebraic structure generated by all of its conjugates.

This perspective allows us to describe geometric constructions using symmetry rather than individual calculations.

Galois Groups

The symmetries of a splitting field form a mathematical object called the *Galois group*.

Definition

The Galois group consists of every field automorphism that fixes the rational numbers.

$$\mathrm{Gal}(L/\mathbb{Q})$$

These automorphisms may permute the roots of a polynomial while preserving every algebraic relation between them.

Example: $x^2 - 2$

The roots are

$$\sqrt{2} \qquad \text{and} \qquad -\sqrt{2}.$$

There are only two automorphisms.

$$\sigma(\sqrt{2}) = \sqrt{2}$$

and

$$\sigma(\sqrt{2}) = -\sqrt{2}.$$

Thus,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2,$$

the cyclic group of order two.

The Fundamental Theorem of Galois Theory

The Fundamental Theorem establishes a bijective correspondence between

- intermediate fields, and
- subgroups of the Galois group.

Every field extension corresponds to exactly one subgroup, and every subgroup determines exactly one intermediate field.

Field–Group Correspondence

$$
\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \{1\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle f \rangle \arrow[dr, dash] & \langle fg \rangle \arrow[d, dash] & \langle g \rangle \arrow[dl, dash] \\
 & \mathrm{Gal}(K/\mathbb{Q}) &
\end{tikzcd}
$$

Figure: Lattice of subfields of $K/\mathbb{Q}$ (left) and the inverted lattice of subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ (right). Source: Wikipedia, *Fundamental theorem of Galois theory*.

Why Degree Alone Is Not Enough

The degree condition is necessary,

$$[F : \mathbb{Q}] = 2^k,$$

but it is **not** sufficient.

There exist field extensions whose degree is a power of two that still cannot be obtained through repeated quadratic extensions.

The associated Galois group itself must contain the appropriate chain of subgroups (quadratic or linear).

A Counterexample

Consider the polynomial

$$x^4 - x - 1.$$

Its splitting field has degree

$$8 = 2^3,$$

yet its Galois group is

$$S_4,$$

the symmetric group on four letters.

Since S_4 is not built solely from successive quadratic extensions, the roots are not constructible despite the extension degree being a power of two.

The degree condition alone therefore cannot characterize constructibility.

The Main Result

Constructibility Criterion

A real algebraic number is constructible by straightedge and compass if and only if

1. its splitting field has degree 2^k, and
2. its Galois group is a finite 2-group, meaning, there exists a chain of quadratic field extensions leading from $\mathbb{Q}$ to the desired field.

Applications of the Criterion

At last, the criterion resolves the Geometric Problems of Antiquity

Problem	Constructible?	Reason
Doubling the cube	No	Degree 3
Angle trisection	No	Cubic extension
Squaring the circle	No	π is transcendental

Summary

Chain of ideas:

1. Geometry
2. Arithmetic
3. Field Theory
4. Galois Theory

Conclusion

Although the classical constructibility with straightedge and compass problems have been solved, the field remains very active and open.

Other Geometric Methods of Constructibility

- Origami
- Paper Strips
- Compass and Straightedge

Open Problems in Geometric Constructibility

- Which polygons can be formed through a sequence of specific folds?
- Classify and limit the maximum number of edges a polygon can possibly have when constructed from a single continuous flat-folded paper strip.
- Infinitely many Fermat primes?
  - The list of constructible polygons remains open

Real World Applications

- NASA and JAXA use the Miura-ori fold to pack massive solar panels into 1/25th of their original size.
- Origami Heart Stents
- Aerospace machinists
- Construction

Thank You

References I

Sheldon Axler.
Linear Algebra Done Right.
Springer, 4th edition, 2024.
Open Access.

James Belk.
Number theory for polynomials.
Cornell University Lecture Notes, 2026.
Accessed: July 3, 2026.

Euclid.
The Thirteen Books of Euclid's Elements.
Dover Publications, New York, 1956.
Translated with introduction and commentary.

James S. Milne.
Fields and galois theory (v5.10), 2022.
Available at www.jmilne.org/math/.

Fiona Murnaghan.
MAT 240 - Algebra I: Fields.
https://www.math.toronto.edu/fiona/courses/mat240/field.pdf.
Course lecture notes, Department of Mathematics, University of Toronto.

Joseph J. Rotman.
Galois Theory.
Universitext. Springer-Verlag, New York, NY, 1998.

Paul Russell.
Eisenstein's irreducibility criterion.
University of Cambridge, DPMMS Lecture Notes, 2009.
Based on lectures by J. M. E. Hyland; Accessed: July 3, 2026.

Ferdinand von Lindemann.
Über die zahl π.
Mathematische Annalen, 20(2):213–225, 1882.