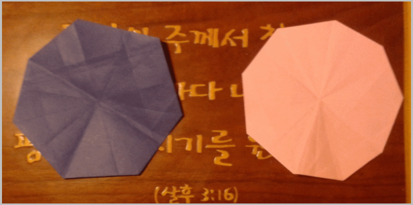
Constructibility, Solvability, and Origami

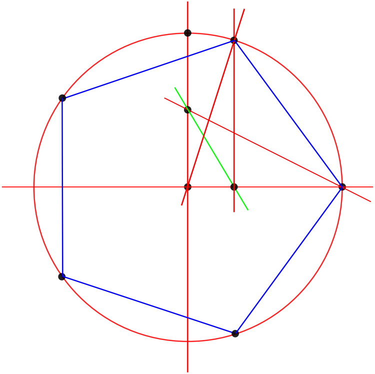


Alan Haynes

Overview

- We will look at several representative problems which explore the question: What objects can you construct using a particular collection of tools?
- This arises from very practical considerations, as well as being a fun and interesting question in its own right. As we will see, the answer, in some cases, turns out to rely fundamentally on abstract ideas from higher mathematics.

§1 Constructibility using straightedge and compass



Straightedge and compass

- Straightedge: an unmarked ruler, allowing us to draw the line passing through two points.
- Compass: a tool which allows us to draw a circle with one point at the center and another point on the circumference.

Question: Starting with two points in the plane, what lengths, angles, and shapes can we construct?

This question was studied extensively by the Greeks, as early as 400-500 B.C.

Description of rules

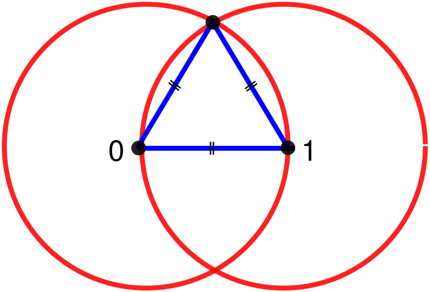
Identify the plane with $\mathbb{C}$. The subset $\mathcal{C} \subseteq \mathbb{C}$ of *constructible numbers* is the collection of numbers which can be realized, starting from 0 and 1, and applying a finite sequence of the following operations:

(A1) Draw a line through two points which have already been constructed.

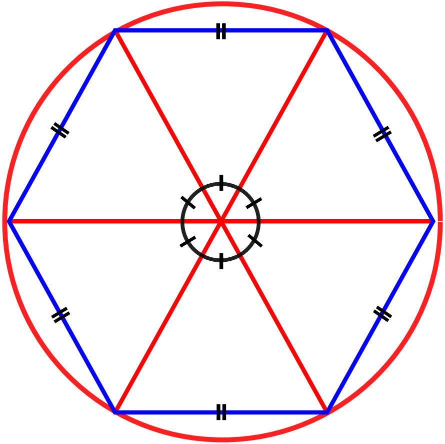
(A2) Draw a circle with the center at a point that has already been constructed, and the circumference passing through another point that has been constructed.

(A3) Add to the collection of constructed points an intersection point of two non-parallel lines, two circles, or a line and a circle.

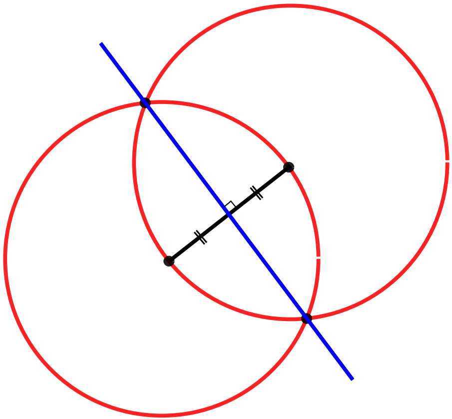
Ex. 1: Equilateral triangle



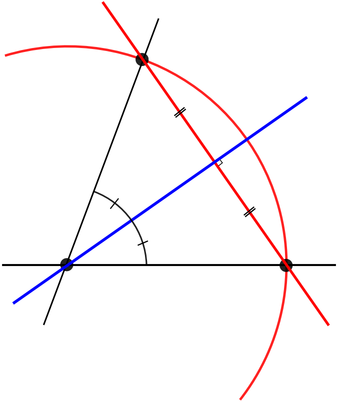
Ex. 2: Regular hexagon



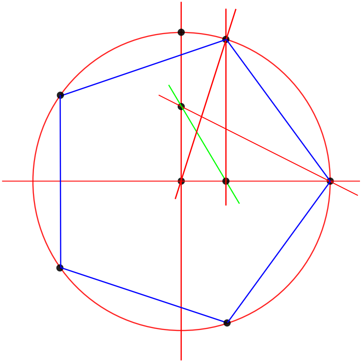
Ex. 3: Perpendicular bisector

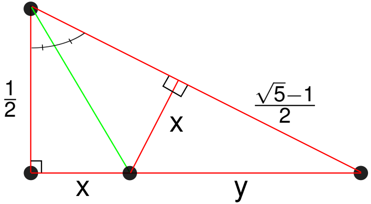


Ex. 4: Angle bisector



Ex. 5: Regular pentagon





$$x + y = 1,$$

$$x^2 + \left(\frac{\sqrt{5}-1}{2}\right)^2 = y^2$$

$$\Rightarrow x = \mathrm{Re}(e^{2\pi i/5})$$

Questions the Greeks could not answer

Using only the rules above, is it possible to:

- Trisect an arbitrary angle?
- Double the cube?
- Square the circle?
- Construct a regular septagon or nonagon?

All of these problems were eventually proved to be impossible, but not until the 1800's (Wantzel, 1837 + Lindemann, 1882).

§2 Solvability of polynomial equations by radicals

$$x = \sqrt[3]{\left(\frac{-a_2^3}{27a_3^3} + \frac{a_2 a_1}{6a_3^2} - \frac{a_0}{2a_3}\right) + \sqrt{\left(\frac{-a_2^3}{27a_3^3} + \frac{a_2 a_1}{6a_3^2} - \frac{a_0}{2a_3}\right)^2 + \left(\frac{a_1}{3a_3} - \frac{a_2^2}{9a_3^2}\right)^3}}$$
$$+ \sqrt[3]{\left(\frac{-a_2^3}{27a_3^3} + \frac{a_2 a_1}{6a_3^2} - \frac{a_0}{2a_3}\right) - \sqrt{\left(\frac{-a_2^3}{27a_3^3} + \frac{a_2 a_1}{6a_3^2} - \frac{a_0}{2a_3}\right)^2 + \left(\frac{a_1}{3a_3} - \frac{a_2^2}{9a_3^2}\right)^3}}$$
$$- \frac{a_2}{3a_3}.$$

Roots of polynomials

- Suppose that

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

is a polynomial with rational coefficients, i.e. $a_i \in \mathbb{Q}$ for each $0 \leq i \leq n$.

- The roots of f are the numbers $x \in \mathbb{C}$ which satisfy the equation $f(x) = 0$.

Question: Is there a formula for the roots of f, which involves only its coefficients and a finite sequence of operations from the list:

$$+, -, \times, \div, \sqrt[m]{}.$$

If so, we say that f is *solvable by radicals.*

Linear and quadratic polynomials

- If $f(x) = a_1 x + a_0$, with $a_1 \neq 0$, then there is one root, the number $x = -a_0/a_1$.
- If $f(x) = a_2 x^2 + a_1 x + a_0$, with $a_2 \neq 0$, then the roots are given by the quadratic equation,

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}.$$

- These formulas have been known for over 4000 years.

Cubic and quartic polynomials

- Let $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, with $a_3 \neq 0$. There is a formula for the roots of f, analogous to the quadratic equation. For example, one such root is:

$$x = \sqrt[3]{\left(\frac{-a_2^3}{27a_3^3} + \frac{a_2a_1}{6a_3^2} - \frac{a_0}{2a_3}\right) + \sqrt{\left(\frac{-a_2^3}{27a_3^3} + \frac{a_2a_1}{6a_3^2} - \frac{a_0}{2a_3}\right)^2 + \left(\frac{a_1}{3a_3} - \frac{a_2^2}{9a_3^2}\right)^3}}$$
$$+ \sqrt[3]{\left(\frac{-a_2^3}{27a_3^3} + \frac{a_2a_1}{6a_3^2} - \frac{a_0}{2a_3}\right) - \sqrt{\left(\frac{-a_2^3}{27a_3^3} + \frac{a_2a_1}{6a_3^2} - \frac{a_0}{2a_3}\right)^2 + \left(\frac{a_1}{3a_3} - \frac{a_2^2}{9a_3^2}\right)^3}}$$
$$- \frac{a_2}{3a_3}.$$

- The general cubic equation was solved in the 1500's AD by del Fiorro and Tartaglia, and published by Cardano.
- The solution of the cubic equation also led to a solution to the general quartic (Ferrari, 1540).

Quintic and higher degree

- Some polynomials of higher degree are solvable by radicals, for example

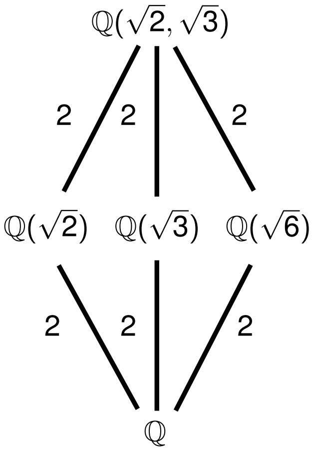
$$f(x) = x^5 - 2$$

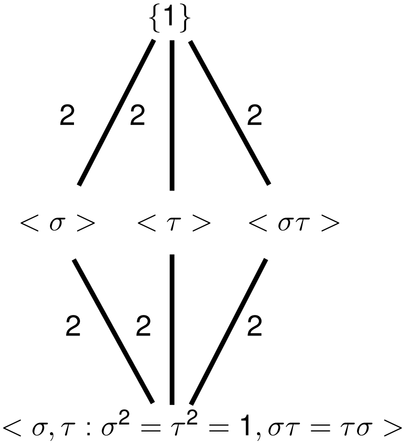
and

$$f(x) = x^9 + 3x^6 + 4x^3 + 1.$$

- By the Fundamental Theorem of Algebra, all polynomials f with complex coefficients have a root in $\mathbb{C}$.
- However, for every $n \geq 5$, there are polynomials of degree n which are not solvable by radicals (Abel, 1823).

§3 Algebraic framework: Fields and Galois theory





Constructible numbers form a field

Returning to $\mathcal{C}$, the collection of complex numbers constructible using straightedge and compass, it is not difficult to show that:

- If $z \in \mathcal{C},\ z \neq 0$, then $-z$ and z^{-1} are also in $\mathcal{C}$.
- If $z, w \in \mathcal{C},\ z \neq 0$, then $z + w$ and zw are in $\mathcal{C}$.

This implies that $\mathcal{C}$ is a *field*, an algebraic object where we can perform arithmetic (multiplication and addition) in a way analogous to $\mathbb{Q}$.

Examples of fields that you may have encountered:

$$\mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \text{and } \mathbb{Z}/p\mathbb{Z} \text{ for } p \text{ prime.}$$

Examples of algebraic objects which are **not** fields:

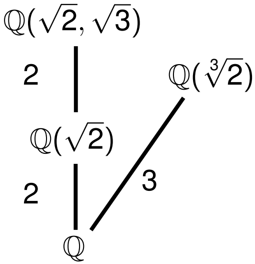
$$\mathbb{Z} \quad \text{and} \quad \mathbb{Z}/n\mathbb{Z} \text{ for } n \text{ composite.}$$

More examples of fields

$$\mathbb{Q}(\sqrt{2}) = \{a_0 + a_1\sqrt{2} : a_0, a_1 \in \mathbb{Q}\}$$

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} : a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$$

$$\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1 2^{1/3} + a_2 2^{2/3} : a_0, a_1, a_2 \in \mathbb{Q}\}$$



Field extensions as vector spaces

- If F and K are fields with $F \subseteq K$, then K has a natural structure as a vector space over F.
- If $F \subseteq K \subseteq L$ are all fields, then it is not difficult to show that

$$\dim_F(L) = \dim_K(L) \cdot \dim_F(K).$$

- This implies, for example, that any field L which is a finite dimensional vector space over $\mathbb{Q}$ and which contains the field $\mathbb{Q}(\sqrt[3]{2})$ must satisfy

$$3 \mid \dim_{\mathbb{Q}}(L).$$

Structure of the field $\mathcal{C}$

- Every number $\alpha \in \mathcal{C}$ is constructed by a finite sequence of steps that involves intersecting only circles and lines (i.e. with other circles or lines).
- Finding the intersection point of two circles, lines, or a circle and a line requires us, at most, to perform addition, subtraction, multiplication, and division, and possibly to take a square root, using a collection of numbers that we already know how to construct.
- It follows that if $\alpha \in \mathcal{C}$, then the smallest field K containing both $\mathbb{Q}$ and α is a vector space over $\mathbb{Q}$ of dimension 2^n, for some integer $n \geq 0$.

Consequences of this structure

- It is impossible to double the cube, i.e. to construct the number $\sqrt[3]{2}$, since $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = 3$.
- It is impossible to trisect an angle of 60°. If we could, then we could construct the number $\alpha = \cos 20^\circ$, but this number is a root of the degree 3 irreducible polynomial

$$f(x) = 8x^3 - 6x - 1.$$

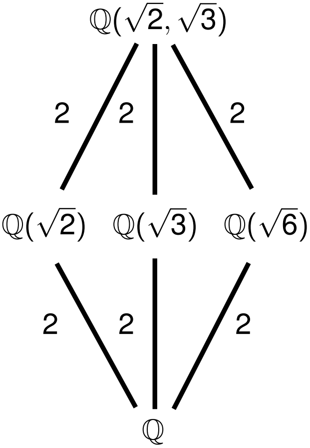
- It is impossible to construct a regular nonagon, or septagon, for similar reasons.
- It is impossible to square the circle, i.e. to construct the number $\sqrt{\pi}$, because then we could construct the number π. However, π is transcendental (Lindemann, 1882).

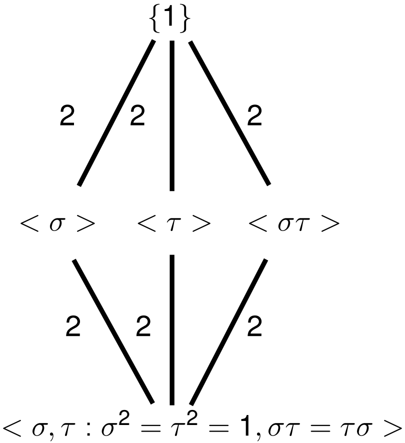
The field of solvable numbers

The collection of roots of polynomials which are solvable by radicals also forms a field, with a particular, but more complicated, structure.

- A root of a polynomial is solvable by radicals if and only if we can build it up, starting from $\mathbb{Q}$ and performing a sequence of operations from the list $+, -, \times, \div$, and $\sqrt[m]{}$.
- The first four of these operations take place in whatever field we are in, while the operation $\sqrt[m]{}$ may require us to move to a field extension of a particular form.
- Therefore we can translate the problem of determining whether or not a number α is solvable by radicals into one about understanding the *intermediate fields* between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$.

Intermediate fields and groups of symmetries

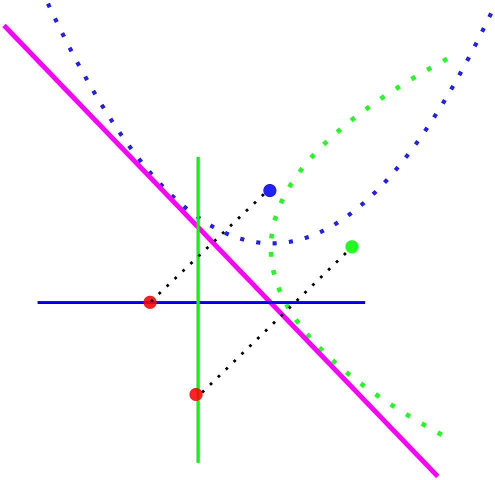




Fundamental Theorem of Galois Theory

- The Fundamental Theorem of Galois Theory allows us to understand the collection of intermediate fields of special kinds of field extensions, by understanding the groups of symmetries (field automorphisms) of the extensions.
- The subgroups of the group of symmetries are in explicit one to one correspondence with intermediate fields of the extension.
- If a certain subgroup structure is not present (i.e. the group of symmetries is not a *solvable group*) then numbers in the corresponding field extension are not solvable.
- Polynomials of degree n 'typically' correspond to field extensions with groups S_n. For $n \geq 5$ these groups are not solvable.

§4 Origami



Paper folding

Finally, instead of using our straightedge and compass to draw lines and circles on an infinite sheet of paper, let us consider what numbers we could construct if we were only allowed to fold the paper, according to standard 'rules of origami'. It turns out that we can still:

- Construct the line through any two points (easy).
- Construct the perpendicular bisector of a line segment and the angle bisector of an angle.
- Construct regular triangles, quadrilaterals, pentagons, hexagons, and octagons.

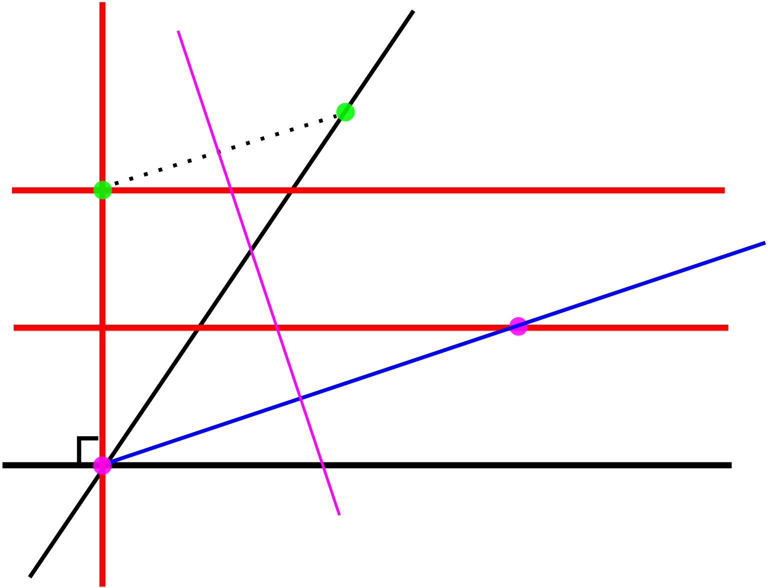
In fact, with an intuitive and reasonable set of rules, we can construct all numbers that are constructible using straightedge and compass. In addition, we have...

Solutions to some of the previously impossible problems

Origami allows us to:

- Trisect an arbitrary angle.
- Construct $\sqrt[3]{2}$.
- Construct regular septagons and nonagons.

Trisecting an arbitrary angle

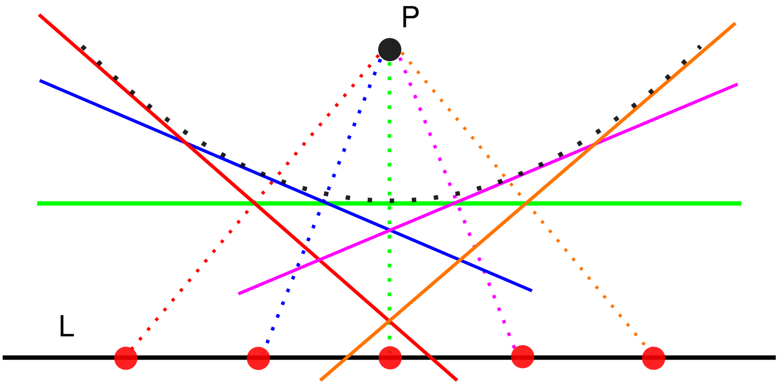


The neusis construction and the power to rule

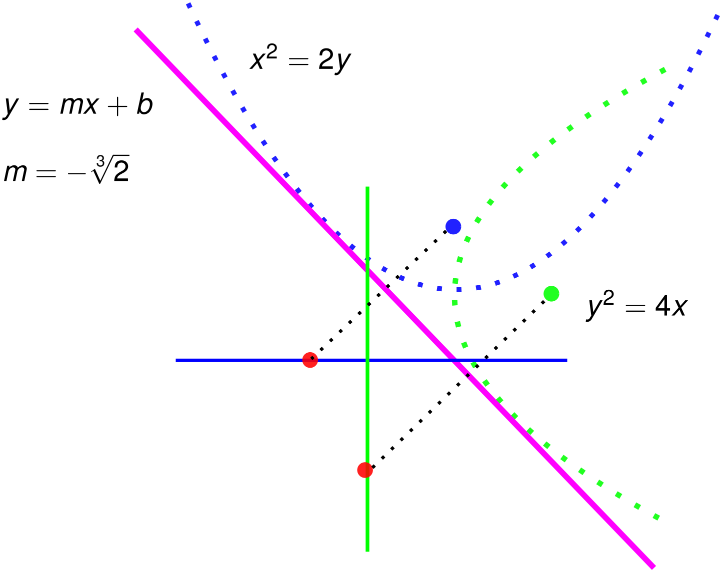
The extra power in origami comes from the ability to take points that we have already constructed and match them up with other objects that we have constructed, before folding the crease. This is similar to the power of having a ruler, as opposed to just a straightedge.

This extra technique allows us to perform the *neusis construction*, a construction known to the ancient Greeks, which can be used to find a common tangent line of two parabolas.

Constructing tangents to a parabola



A tangent to two parabolas



References

- Dummit, Foote: Abstract algebra.
- Geretschläger: Euclidean constructions and the geometry of origami. Math. Mag. 68 (1995), no. 5, 357–371
- Geretschläger: Folding the regular heptagon. (Google)

Thank you!