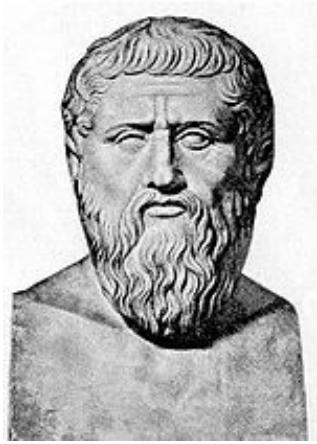
Lecture 6.8: Impossibility proofs

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Overview and some history



Plato (5th century B.C.) believed that the only "perfect" geometric figures were the straight line and the circle.

In Ancient Greek geometry, this philosophy meant that there were only two instruments available to perform geometric constructions:

1. the ruler: a single unmarked straight edge.
2. the compass: collapses when lifted from the page

Formally, this means that the only permissible constructions are those granted by Euclid's first three postulates.

Overview and some history

Around 300 B.C., ancient Greek mathematician Euclid wrote a series of thirteen books that he called The Elements.

It is a collection of definitions, postulates (axioms), and theorems & proofs, covering geometry, elementary number theory, and the Greeks' "geometric algebra."

Book 1 contained Euclid's famous *10 postulates*, and other basic propositions of geometry.


EVCLIDIS
ELEMENTORVM
LIBRI XV.
Accessit liber XVI. De Solidorum Regularium cuiuslibet intra quodlibet comparatione.
OMNES PERSPICVIS DEMONSTRATIONIBVS, accuratisque Scholijs illustrati: nunc quarto editi, ac multorum rerum accessione post primam editionem locupletati.
Auctore
CHRISTOPHORO CLAVIO
Bambergensi è Societate Iesv.
FRANCOFVRTI,
Ex Officina Typographica Nicolai Hoffmanni,
Sumptibus Ionae Rhodij.
M. DC. VII.

Using only a ruler and compass, lines can be divided into equal segments, angles can be bisected, parallel lines can be drawn, n-gons can be "squared," and so on.

Theorem

The set $K \subset \mathbb{C}$ of constructible numbers is a field. Moreover, if $\alpha \in K$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ for some integer n.

Classical constructibility problems, rephrased

Problem 1: Squaring the circle

Given a circle of radius r (and hence of area πr^2), construct a square of area πr^2 (and hence of side-length $\sqrt{\pi} r$).

If one could square the circle, then $\sqrt{\pi} \in K \subset \mathbb{C}$, the field of constructible numbers.

However,

$$\mathbb{Q} \subset \mathbb{Q}(\pi) \subset \mathbb{Q}(\sqrt{\pi})$$

and so $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] \geq [\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. Hence $\sqrt{\pi}$ is not constructible.

Problem 2: Doubling the cube

Given a cube of length ℓ (and hence of volume ℓ^3), construct a cube of volume $2\ell^3$ (and hence of side-length $\sqrt[3]{2}\ell$).

If one could double the cube, then $\sqrt[3]{2} \in K$.

However, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ is not a power of two. Hence $\sqrt[3]{2}$ is not constructible.

Classical constructibility problems, rephrased

Problem 3: Trisecting an angle

Given $e^{i\theta}$, construct $e^{i\theta/3}$. Or equivalently, construct $\cos(\theta/3)$ from $\cos(\theta)$.

We will show that $\theta = 60^\circ$ cannot be trisected. In other words, that $\alpha = \cos(20^\circ)$ cannot be constructed from $\cos(60^\circ)$.

The triple angle formula yields

$$\cos(\theta) = 4\cos^3(\theta/3) - 3\cos(\theta/3)\,.$$

Set $\theta = 60^\circ$. Plugging in $\cos(\theta) = 1/2$ and $\alpha = \cos(20^\circ)$ gives

$$4\alpha^3 - 3\alpha - \frac{1}{2} = 0\,.$$

Changing variables by $u = 2\alpha$, and then multiplying through by 2:

$$u^3 - 3u - 1 = 0\,.$$

Thus, u is the root of the (irreducible!) polynomial $x^3 - 3x - 1$. Therefore, $[\mathbb{Q}(u) : \mathbb{Q}] = 3$, which is not a power of 2.

Hence, $u = 2\cos(20^\circ)$ is not constructible, so neither is $\alpha = \cos(20^\circ)$.

Summary

The three classical ruler-and-compass constructions that stumped the ancient Greeks, when translated in the language of field theory, are as follows:

Problem 1: Squaring the circle

Construct $\sqrt{\pi}$ from 1.

Problem 2: Doubling the cube

Construct $\sqrt[3]{2}$ from 1.

Problem 3: Trisecting an angle

Construct $\cos(\theta/3)$ from $\cos(\theta)$. [Or $\cos(20^\circ)$ from 1.]

Since none of these numbers these lie in an extension of $\mathbb{Q}$ of degree 2^n, they are not constructible.

If one is allowed a "marked ruler," then these constructions become possible, which the ancient Greeks were aware of.

Construction of regular polygons

The ancient Greeks were also interested in constructing regular polygons. They knew constructions for 3-, 5-, and 15-gons.

In 1796, nineteen-year-old Carl Friedrich Gauß, who was undecided about whether to study mathematics or languages, discovered how to construct a regular 17-gon.

Gauß was so pleased with his discovery that he dedicated his life to mathematics.

He also proved the following theorem about which n-gons are constructible.

Theorem (Gauß, Wantzel)

Let p be an odd prime. A regular p-gon is constructible if and only if $p = 2^{2^n} + 1$ for some $n \geq 0$.

The next question to ask is for which n is $2^{2^n} + 1$ prime?

Construction of regular polygons and Fermat primes

Definition

The n^{th} Fermat number is $F_n := 2^{2^n} + 1$. If F_n is prime, then it is a Fermat prime.

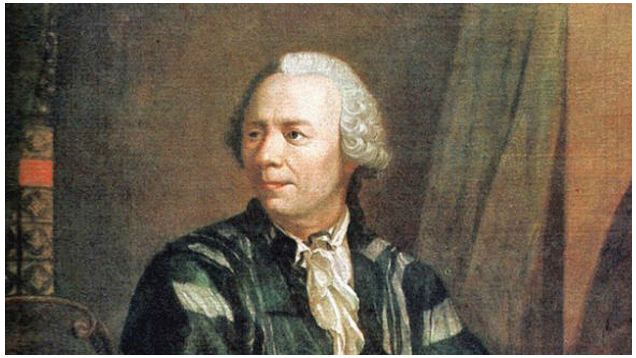
The first few Fermat primes are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$.

They are named after Pierre Fermat (1601–1665), who conjectured in the 1600s that all Fermat numbers $F_n = 2^{2^n} + 1$ are prime.

Construction of regular polygons and Fermat primes

In 1732, Leonhard Euler disproved Fermat's conjecture by demonstrating

$$F_5 = 2^{2^5}+1 = 2^{32}+1 = 4294967297 = 641 \cdot 6700417\,.$$



It is not known if any other Fermat primes exist!

So far, every F_n is known to be composite for $5 \leq n \leq 32$. In 2014, a computer showed that $193 \times 2^{3329782} + 1$ is a prime factor of

$$F_{3329780} = 2^{2^{3329780}} + 1 > 10^{10^{10^6}}\,.$$

Theorem (Gauß, Wantzel)

A regular n-gon is constructible if and only if $n = 2^k p_1 \cdots p_m$, where $p_1, \ldots, p_m$ are distinct Fermat primes.

If these type of problems interest you, take Math 4100! (Number theory)