Chapter 12: Ruler and compass constructions

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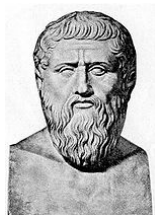
Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Summer I 2014

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 BC, 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.
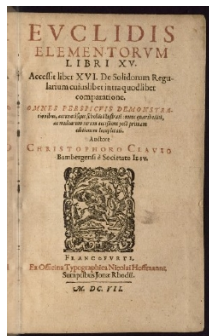
Euclid's first three postulates

1. A straight line segment can be drawn joining any two points.
2. Any straight line segment can be extended indefinitely in a straight line.
3. Given any straight line segment, a circle can be drawn having the segment as radius and one endpoint as center.

Using only these tools, lines can be divided into equal segments, angles can be bisected, parallel lines can be drawn, *n*-gons can be "squared," and so on.

Overview and some history

One of the chief purposes of Greek mathematics was to find exact constructions for various lengths, using only the basic tools of a ruler and compass.

The ancient Greeks were unable to find constructions for the following problems:

Problem 1: Squaring the circle

Draw a square with the same area as a given circle.

Problem 2: Doubling the cube

Draw a cube with twice the volume of a given cube.

Problem 3: Trisecting an angle

Divide an angle into three smaller angles all of the same size.

For over 2000 years, these problems remained unsolved.

Alas, in 1837, Pierre Wantzel used field theory to prove that these constructions were impossible.

What does it mean to be "constructible"?

Assume P_0 is a set of points in $\mathbb{R}^2$ (or equivalently, in the complex plane $\mathbb{C}$).

Definition

The points of intersection of any two distinct lines or circles are constructible in one step.

A point $r \in \mathbb{R}^2$ is constructible from P_0 if there is a finite sequence $r_1, \ldots, r_n = r$ of points in $\mathbb{R}^2$ such that for each $i = 1, \ldots, n$, the point r_i is constructible in one step from $P_0 \cup \{r_1, \ldots, r_{i-1}\}$.

Example: bisecting a line

1. Start with a line $p_1 p_2$;
2. Draw the circle of center p_1 of radius $p_1 p_2$;
3. Draw the circle of center p_2 of radius $p_1 p_2$;
4. Let r_1 and r_2 be the points of intersection;
5. Draw the line $r_1 r_2$;
6. Let r_3 be the intersection of $p_1 p_2$ and $r_1 r_2$.
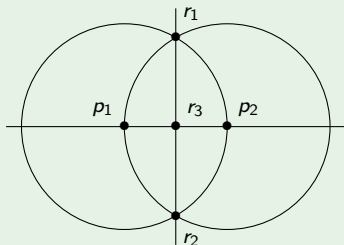
Bisecting an angle

Example: bisecting an angle

1. Start with an angle at A;
2. Draw a circle centered at A;
3. Let B and C be the points of intersection;
4. Draw a circle of radius BC centered at B;
5. Draw a circle of radius BC centered at C;
6. Let D and E be the intersections of these 2 circles;
7. Draw a line through DE.
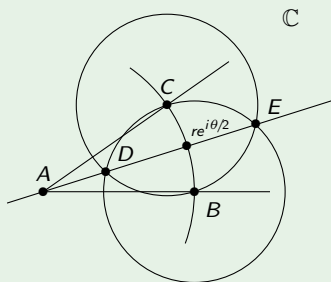
Suppose A is at the origin in the complex plane. Then $B = r$ and $C = re^{i\theta}$.

Bisecting an angle means that we can construct $re^{i\theta/2}$ from $re^{i\theta}$.

Constructible numbers: Real vs. complex

Henceforth, we will say that a point is constructible if it is constructible from the set

$$P_0 = \{(0,0),\ (1,0)\} \subset \mathbb{R}^2\,.$$

Say that $z = x + yi \in \mathbb{C}$ is constructible if $(x, y) \in \mathbb{R}^2$ is constructible. Let $K \subseteq \mathbb{C}$ denote the constructible numbers.

Lemma

A complex number $z = x + yi$ is constructible if x and y are constructible.

By the following lemma, we can restrict our focus on real constructible numbers.

Lemma

1. $K \cap \mathbb{R}$ is a subfield of $\mathbb{R}$ if and only if K is a subfield of $\mathbb{C}$.
2. Moreover, $K \cap \mathbb{R}$ is closed under (nonnegative) square roots if and only if K is closed under (all) square roots.

$K \cap \mathbb{R}$ closed under square roots means that $a \in K \cap \mathbb{R}^+$ implies $\sqrt{a} \in K \cap \mathbb{R}$.

K closed under square roots means that $z = re^{i\theta} \in K$ implies $\sqrt{z} = \sqrt{r}e^{i\theta/2} \in K$.

The field of constructible numbers

Theorem

The set of constructible numbers K is a subfield of $\mathbb{C}$ that is closed under taking square roots and complex conjugation.

Proof (sketch)

Let a and b be constructible real numbers, with $a > 0$. It is elementary to check that each of the following hold:

1. $-a$ is constructible;
2. $a + b$ is constructible;
3. ab is constructible;
4. a^{-1} is constructible;
5. $\sqrt{a}$ is constructible;
6. $a - bi$ is constructible provided that $a + bi$ is.

Corollary

If $a, b, c \in \mathbb{C}$ are constructible, then so are the roots of $ax^2 + bx + c$.

Constructions as field extensions

Let $F \subset K$ be a field generated by ruler and compass constructions.

Suppose α is constructible from F in one step. We wish to determine $[F(\alpha) : F]$.

The three ways to construct new points from F

1. **Intersect two lines**. The solution to $ax + by = c$ and $dx + ey = f$ lies in F.

2. **Intersect a circle and a line**. The solution to

$$\begin{cases} ax + by = c \\ (x - d)^2 + (y - e)^2 = r^2 \end{cases}$$

   lies in (at most) a quadratic extension of F.

3. **Intersect two circles**. We need to solve the system

$$\begin{cases} (x - a)^2 + (y - b)^2 = s^2 \\ (x - d)^2 + (y - e)^2 = r^2 \end{cases}$$

   Multiply this out and subtract. The x^2 and y^2 terms cancel, leaving the equation of a line. Intersecting this line with one of the circles puts us back in Case 2.

In all of these cases, $[F(\alpha) : F] \leq 2$.

Constructions as field extensions

In others words, constructing a number $\alpha \notin F$ in one step amounts to taking a degree-2 extension of F.

Theorem

A complex number α is constructible if and only if there is a tower of field extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subseteq \mathbb{C}$$

where $\alpha \in K_n$ and $[K_{i+1} : K_i] \leq 2$ for each i.

Corollary

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

We will show that the ancient Greeks' classical construction problems are impossible by demonstrating that each would yield a number $\alpha \in \mathbb{R}$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is not a power of two.

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 $\sqrt{\pi} \in K$. 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 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 $\theta = 60°$ cannot be trisected. In other words, that $\alpha = \cos(20°)$ cannot be constructed from $\cos(60°)$.

The triple angle formula yields

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

Set $\theta = 60°$. Plugging in $\cos(\theta) = 1/2$ and $\alpha = \cos(20°)$ 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, $u = 2\cos(20°)$ is not constructible, so neither is $\alpha = \cos(20°)$.

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 $\cos(20°)$ 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 came up with 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 nth 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)