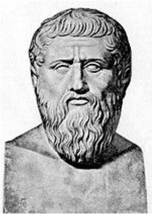
Lecture 6.7: Ruler and compass constructions

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 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 Greek's "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 $\mathbb{C}$).

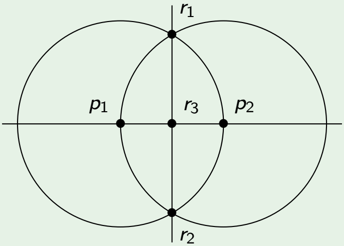
Definition

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

Example: bisecting a line

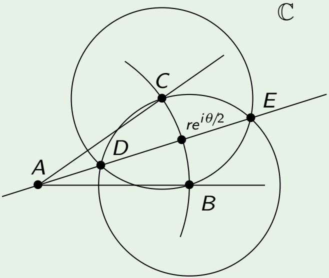
1. Start with a line $p_1 p_2$;
2. Draw the circle of center p_1 of radius $p_1 p_2$;
3. Draw the circle of center p_2 of radius $p_1 p_2$;
4. Let r_1 and r_2 be the points of intersection;
5. Draw the line $r_1 r_2$;
6. Let r_3 be the intersection of $p_1 p_2$ and $r_1 r_2$.



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

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

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 $n \in \mathbb{N}$.

In the next lecture, 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.