GALOIS THEORY : LECTURE 11

LEO GOLDMAKHER

1. ALGEBRAIC FIELD EXTENSIONS

Given $\alpha \in L/K$, the *degree of* α *over* K is defined to be $\deg m_\alpha$, where m_α is the minimal polynomial of α over K; recall that this, in turn, is equal to $[K(\alpha) : K]$. The notion of degree holds even when α is transcendental over K, since in this case we say the degree of α is infinite.

Remark. Note that α is algebraic over K if and only if α has finite degree over K.

Question 1. *Does the above remark hold for field extensions? I.e. is a field extension algebraic if and only if it has finite degree?*

In order to answer this question, we first need to define what we mean by an algebraic field extension.

Definition. A field extension L/K is *algebraic* if and only if every $\alpha \in L$ is algebraic over K.

Now we want to know whether a field extension is finite if and only it is algebraic. This turns out to be false:

Example 1 (Michael)**.** Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)$. Then $[L : \mathbb{Q}] = \infty$, but every $\alpha \in L$ is algebraic over $\mathbb{Q}$.

By our example, we see that an algebraic field extension is not always finite. Eli conjectured that the other direction is true, i.e. that a finite field extension must always be algebraic. His intuition for this was that any transcendental number would require an infinite basis to be expressed. This idea leads us to the following proposition.

Proposition 1. *If L/K is finite, then it is algebraic.*

Remark. Whenever we refer to an extension as finite, we implicitly mean finite *degree*.

Proof. Let $[L : K] = n$ and $\alpha \in L$. We want to show that α is algebraic over K. Notice that since the degree of L/K is n, any collection of $n+1$ elements is linearly dependent. Thus the set $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is linearly dependent and so there exist c_i's from K, not all zero, such that

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0.$$

It follows that α satisfies some polynomial over K, and is therefore algebraic. Since this is true for an arbitrary element of L, we conclude that L/K is algebraic. □

Remark. We've actually proved slightly more than we claimed: that $\deg \alpha \leq [L : K]$ for any $\alpha \in L/K$.

From the proposition we deduce the following corollary.

Corollary 2. *If α is algebraic over K, then $K(\alpha)/K$ is algebraic.*

Proof. If α is algebraic over K, then it must have finite degree, whence $[K(\alpha) : K] = \deg m_\alpha$ is finite. The proposition implies $K(\alpha)/K$ is algebraic. □

This means that every element generated by some algebraic α and the field K is also algebraic over K. We can iterate this idea:

Corollary 3. *If α, β are algebraic over K, then $K(\alpha, \beta)/K$ is algebraic.*

Date: March 8, 2018.
Based on notes by Anya Michaelsen.

Proof. If we can show that $[K(\alpha,\beta):K]$ is finite, then we are done. Consider the following tower of fields.

$$\begin{array}{c} K(\alpha,\beta) \\ \big|\,? \\ K(\alpha) \\ \big|\,\text{finite} \\ K \end{array}$$

We know that $[K(\alpha):K]$ is finite, so by the Tower Law it suffices to show that $[K(\alpha,\beta):K(\alpha)]$ is also finite. Note that β is algebraic over K, hence must also be algebraic over $K(\alpha)$. But this means β has finite degree over $K(\alpha)$, whence $[K(\alpha,\beta):K(\alpha)]$ is finite. This concludes the proof. ☐

In particular, we immediately deduce

Corollary 4. *If α, β algebraic over K, then $\alpha+\beta$ and $\alpha\beta$ are algebraic over K.*

For example, this allows us to assert that $\sqrt{2}+\sqrt{-5}$ is algebraic without finding a polynomial that it satisfies.

2. (Old) Geometry

A long time ago the Greeks did a whole lot of geometry. They even developed integral calculus, even though it was phrased in rather different terms (since algebra hadn't been invented yet). For example, Archimedes determined a formula for the area between a parabola and an intersecting line.

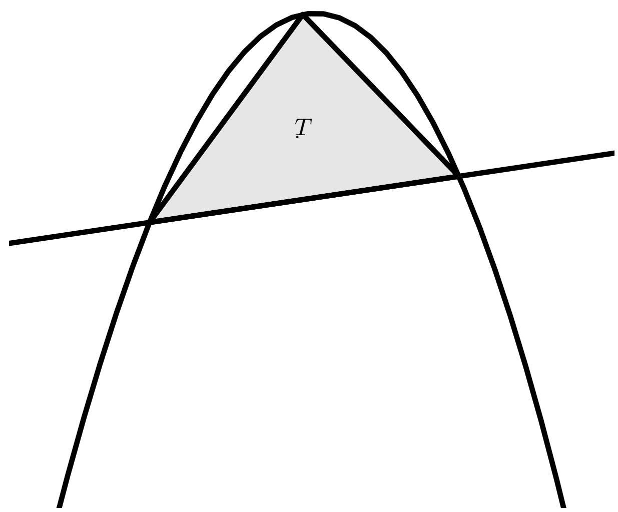
To do this, he first constructed the largest triangle enclosed by the two intersecting points and the parabola. If this triangle is T, then the regions to the right and left of T are also parabolas intersected by lines, and so we can insert the largest triangles into these regions, T' and T''. Archimedes then noted that

$$\text{Area } T = 4(\text{Area } T' + \text{Area } T'').$$

Iterating this process, the area of the enclosed region is given by

$$\text{Area } T\left(1+\tfrac{1}{4}+\tfrac{1}{16}+\tfrac{1}{64}+\cdots\right).$$

By finding a way of determining the area of the largest inscribed triangle, Archimedes was thus able to find the area of the enclosed region, in effect integrating a quadratic long before Newton and Leibniz.

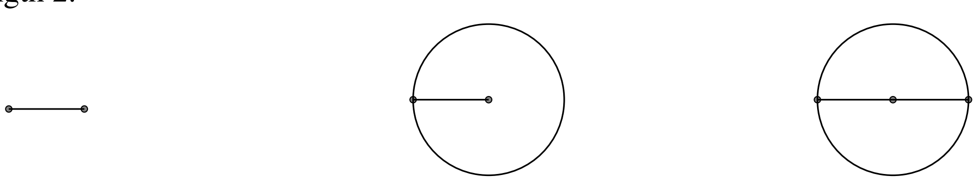


In fact, both differentiation and integration we used in mathematics long before Newton and Leibniz. However, these existed as totally separate techniques; Newton and Leibniz's key insight was the Fundamental Theorem of Calculus which provided the relationship between differentiation and integration.

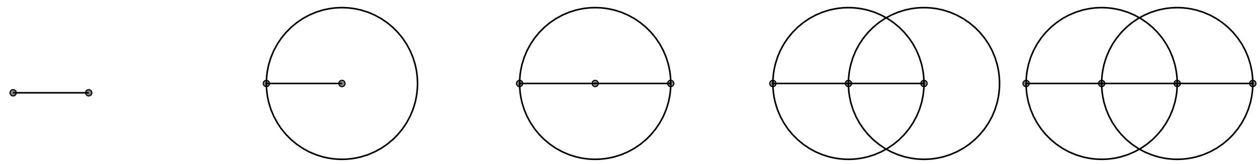
A lot of Greek geometry was based on geometric constructions using compass and straightedge. Here's how these two tools work. Given any two points x and y, a compass allows us to draw a circle centered at x that passes through y; a straightedge allows us to draw a straight line through both points (and extending arbitrarily far). We will work through some basic examples of constructions using these tools to get a sense for what they can accomplish.

1) Lengths

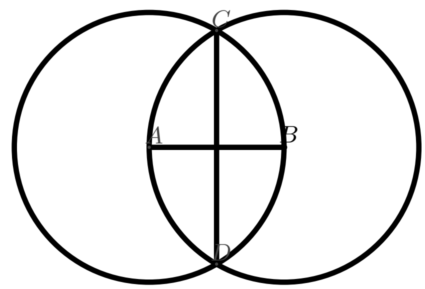
Given a unit length, we can construct a segment of length 2. We do this by taking our segment and using the compass to draw a circle from one point with radius 1. Then using a straightedge we extend this to create a segment of length 2.



Given a unit length, we can also construct a segment of length 3. Using the same technique as before, we can add another segment of unit length to the end:



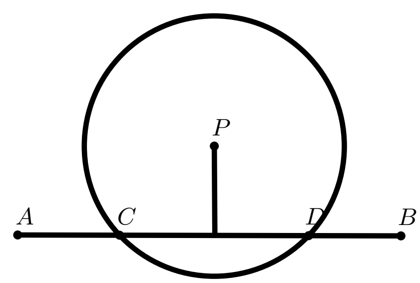
In this way we can construct all positive integer lengths. What about fractional lengths? For example, can we construct a segment of length $\frac{1}{2}$? Using the compass to make two unit circles centered at A and B, we can connect their intersecting points via straightedge to bisect the original line, thus producing a line segment with length $\frac{1}{2}$ (right).



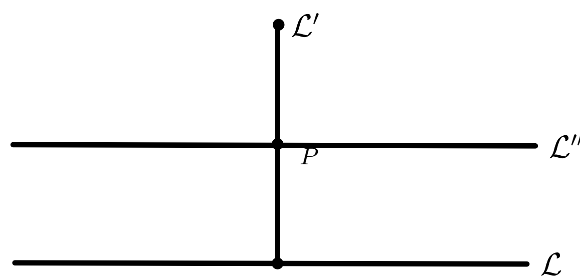
Note that by this construction we also created a perpendicular line to our original segment.

2) Perpendicular & Parallel Lines

Given a line $\mathcal{L}$ and point P, we can construct a line perpendicular to $\mathcal{L}$ passing through P. Starting with the line segment $\mathcal{L}$ with endpoints A and B, we can construct a circle centered at P that passes through $\mathcal{L}$ twice. Using the same construction as before, we can use the intersecting points, C and D, to construct a perpendicular bisector. This line segment will pass through P and thus be a line perpendicular to $\mathcal{L}$ passing through P. Note that this construction works whether or not P lies on $\mathcal{L}$.

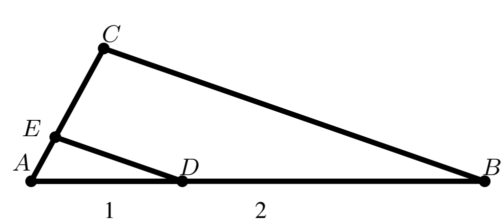


Next, given a line $\mathcal{L}$ and a point $P \notin \mathcal{L}$, we can construct a line parallel to $\mathcal{L}$ passing through P. To do this, we start by constructing a line $\mathcal{L}'$, perpendicular to $\mathcal{L}$, such that $\mathcal{L}'$ passes through P. Next we construct a perpendicular line $\mathcal{L}''$ to $\mathcal{L}'$ that passes through P. Thus $\mathcal{L}''$ is parallel to $\mathcal{L}$ and passes through P.



3) More complicated lengths

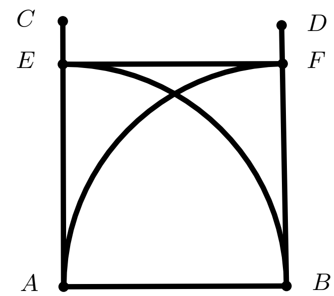
Given a unit length we can construct a segment of length $\frac{1}{3}$. To do this, we first construct a segment of length 3, and another segment of length 1 coming from point A. Then we connect these to form a triangle. From point D, which is a unit from A, we construct a line parallel to the line $\overline{BC}$, which then passes through AC at point E. By similar triangles, AE has length $\frac{1}{3}$.



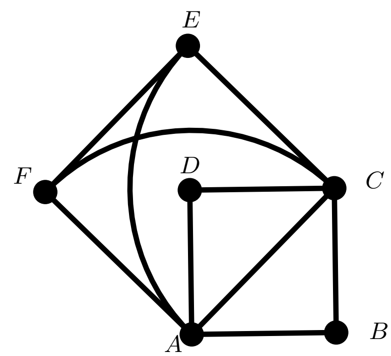
This idea can be used to construct any fractional length $\frac{a}{b}$.

4) Squares

Given a unit length, we can construct a unit square. First we extend rays on either side of $\overline{AB}$ perpendicular to $\overline{AB}$. Then we can use an arc centered at A starting at B to get line segment $\overline{AE}$, of length 1. Repeat this from point B to get segment $\overline{BF}$ of length 1. Finally we can connect points E and F to get a unit square.



Next, given a square, we can construct a square with twice the area of the original. To do this, we draw a line segment through the diagonal of the original square. Then by the method above, we construct a square whose sides are all this length. If the original square had side lengths a, this one has side lengths $a\sqrt{2}$, so it has twice the area.

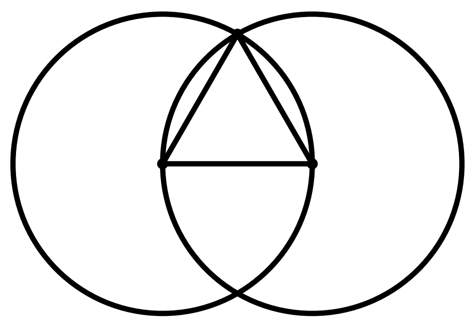


Exercise 1. Given a square, construct a square with area three times that of the original.

5) Angles

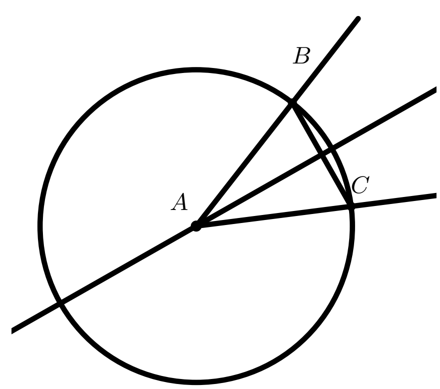
We saw before how to construct a 90° angle. We can construct other angles, too!

For example, we can construct a 60° angle. We can proceed as though we were constructing a perpendicular bisector. However instead of taking the intersecting points of the circle and connecting them, we take one point and connect it to both centers of the circles. This yields an equilateral triangle, and so every interior angle has 60°.

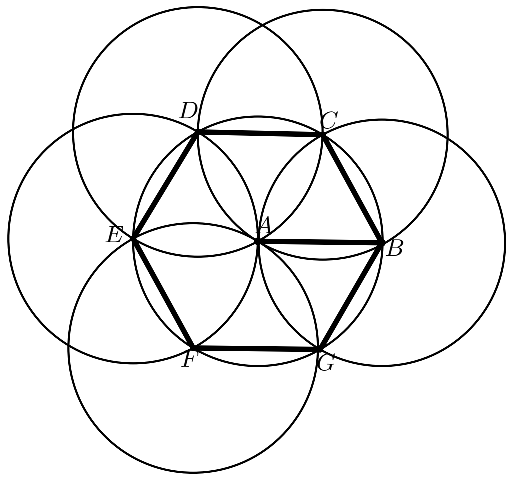


Observe that this allows us to construct 30° angles as well, simply by drawing in the perpendicular bisector.

More generally, it turns out that it's possible to bisect any given angle. To do this, we draw a circle centered at the point A. Using the intersecting points B and C we then construct a perpendicular bisector to the line $\overline{BC}$; this bisects the original angle.

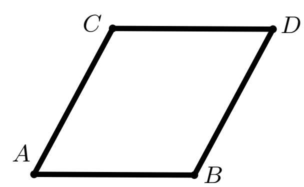


6) Regular polygons
Given a line segment, we can construct a regular hexagon (i.e. hexagon with equal angles and side lengths). Using a series of intersecting circles we can construct a regular hexagon from the intersection points as shown below.



The Greeks also constructed regular n-gons for $n = 3, 4, 5, 6, 8, 10$, and 12. Gauss was the first to give an explicit construction of the regular 17-gon.

7) Duplicating a Parallel Line
One potential issue with a compass is that it might not hold its shape. In other words, it might not be possible to use it to measure length, since as soon as you pick it up off the page the compass might collapse. It turns out that this isn't an issue: given a line segment, AB, we can construct a parallel line segment starting at an arbitrary given point, C. We do this by constructing a parallelogram with one side as our line segment including the point C.



3. Impossible Constructions

While the Greeks accomplished many geometric constructions, there were a number of difficult problems they were never able to solve. Here are four of these:

(1) *Double a cube.* Given a cube, construct a cube with twice the volume of the original.
(2) *Trisect a given angle.* Given an angle, divide it into three equal angles.
(3) *Square the circle.* Given a circle, construct a square with the same area.
(4) *Construct a regular heptagon.* Construct a 7-gon with equal angles and side lengths.

Next class we will show that (1), (2), and (4) are impossible using only a compass and straightedge. If we take on faith that π is transcendental over $\mathbb{Q}$, then we will also be able to show that (3) is impossible.