Lecture 7.2

Last time:

- A simple extension of $\mathbb{Q}$ is of the form

$$\mathbb{Q}(\alpha) = \bigcap_{\substack{\mathbb{Q} \subseteq K \subseteq \mathbb{C} \\ \alpha \in K}} K$$

- $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ with $\mathbb{Q}$-basis

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}.$$

Ex 1 Picking up where we left off, we wanted to show $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ was a simple extension of $\mathbb{Q}$.

Claim 2: $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

Claim 2: $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Pf: On one hand, $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq K$

since $\sqrt{2}+\sqrt{3} \in K$.

On the other hand,

$$(\sqrt{2}+\sqrt{3})^2 = 5 + 2\sqrt{6} \qquad (i)$$

$$(\sqrt{2}+\sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3} \qquad (ii)$$

$$(\sqrt{2}+\sqrt{3})^4 = 49 + 20\sqrt{6} \qquad (iii)$$

Set $\alpha = \sqrt{2}+\sqrt{3}$. Then

$$\sqrt{6} = \frac{\alpha - 5}{2} \quad \text{by (i)}$$

$$\sqrt{2} = \frac{\alpha^3 - 9\alpha}{2} \quad \text{by (ii)}$$

$$\sqrt{3} = \frac{\alpha^3 - 9\alpha}{2} \quad \text{by (ii)}$$

$\frac{\alpha}{2} = \frac{11\alpha - \alpha}{2}$ also by (ii).

So $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$, showing they are equal. □

Claim 3: The minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is

$$p_\alpha(x) = x^4 - 10x + 1.$$

Pf: (i) and (iii) imply α is a root of $p_\alpha(x)$.

On the other hand, $p_\alpha(x)$ is irreducible since, for example, it is irreducible over $\mathbb{F}_5$. (Check it!)

Since it is also monic, it must be the minimal polynomial of α. $\square$

Either Claim 1 or Claim 3 implies

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4.$$

More generally:

Theorem (Tower Law) If $L/K/F$ is a "tower" of field extensions, meaning L/K and K/F are each field extensions,

$$[L : F] = [L : K][K : F].$$

Pf: Assume for simplicity that both

extensions are finite — the infinite degree case is basically the same.

Let $\{x_1, \ldots, x_n\} \subseteq K$ be an F-basis of K and let $\{y_1, \ldots, y_m\}$ be a K-basis of L.

We want to show that $\{x_1y_1, \ldots, x_ny_m\}$ is an F-basis of L, so that

$$[L : F] = mn = [L : K][K : F].$$

First, since the y_j span L/K, any element of L is of the form

$$\alpha = a_1y_1 + \ldots + a_my_m$$

for some $a_j \in K$.

But K/F is spanned by the x_i, so each

$$a_j = b_{1j} x_1 + \ldots + b_{nj} x_n$$

for some $b_{ii} \in F$.

Putting them together,

$$\alpha = (b_{11} x_1 + \ldots + b_{n1} x_n) y_1 + \ldots + (b_{1m} x_1 + \ldots + b_{nm} x_n) y_m$$

so L/F is spanned by the $a_i b_j$.

On the other hand, suppose

$$b_{11} x_1 y_1 + \ldots + b_{nm} x_n y_m = 0.$$

Grouping terms, we get

$$(b_{11}x_1 + \dots + b_{n1}x_n)y_1 + \dots + (b_{1m}x_1 + \dots + b_{nm}x_n)y_m = 0$$

but since the y_j are a basis for L/K, each coefficient is 0:

$$b_{1j}x_1 + \dots + b_{nj}x_n = 0.$$

Now $x_1, \dots, x_n$ are a basis for K/F, so $b_{1j} = \dots = b_{nj} = 0$ and this holds for all j. □

Ex 1, cont'd. This gives us a fast way to check that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$

by showing that

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

$$= 2 \cdot 2.$$

In the tower $\mathbb{Q}(\sqrt{2},\sqrt{3}) / \mathbb{Q}(\sqrt{2}) / \mathbb{Q}$, we know $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has degree 2.

But part of our previous work showed that

$\sqrt{3} \notin \text{Span}_{\mathbb{Q}}\{1, \sqrt{2}\} = \mathbb{Q}(\sqrt{2})$, so

$x^2 - 3$ remains irreducible over $\mathbb{Q}(\sqrt{2})$

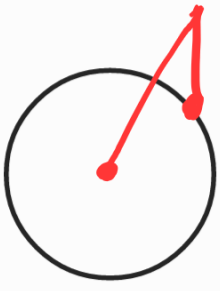
and hence $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

In ancient times, mathematicians (e.g. the Greeks) were stumped by certain geometric questions, which we will explore next.

To get started, let's assume we only have two tools at our disposal:

a ruler

and



a compass

In the xy-plane, we can "construct" geometric shapes using these tools, according to the following rules:

(1) The ruler may be used to draw a

straight line between any two points.

(2) The compass may be placed at two existing points and used to draw a circle centered at one or the other point.

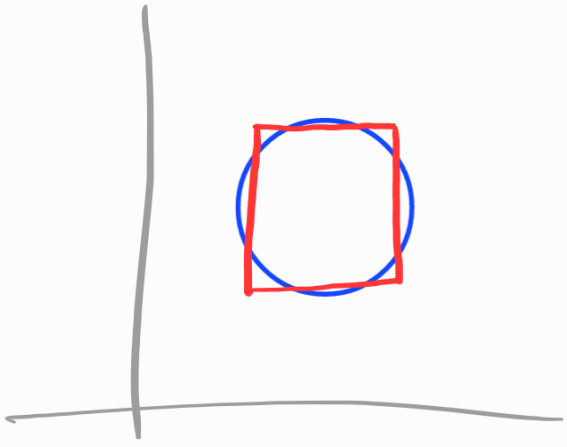
(3) Any intersection is marked as a new point, called a constructible point.

Q: Starting from (0,0) and with a ruler of unit length, which points in the plane are constructible?

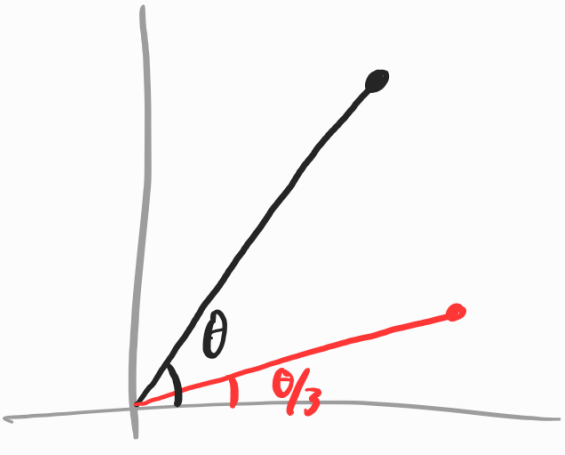
Here are some questions that stumped the

Greeks, that we will study in more detail.

Q1: Given a circle, is it possible to "square the circle", i.e. construct a square with the same area as the circle?



Q2: Is it possible to trisect an angle?



Q3: In three dimensions, is it possible to find a cube with double the volume of a given cube?

Next time: how this relates to field extensions.