

Last lecture

- (Theorem 25.2) If $F(\alpha):F$ and $K(\beta):K$ are simple (algebraic) extensions and that $\theta: F \rightarrow K$ is an isomorphism such that $\theta(m_\alpha(x)) = m_\beta(y) \in K[y]$ then $F(\alpha) \cong K(\beta)$
- (Theorem 25.3) If $E:F$ and $D:E$ are extensions then $D:FE$ is an extension and $[D:F] = [D:E][E:F]$.
- An extension $E:FF$ is **algebraic** if every element of E is algebraic over F .
- (Corollary 25.5) An extension $E:F$ is finite if and only if it is algebraic and $E = F(\alpha_1, \dots, \alpha_n)$, for some $\alpha_i \in K$.

This lecture

Ruler and compass constructions and constructible numbers.

Ruler and compass constructions

Question Asked by the ancient Greeks – but answered by Galois!

Suppose that you have an unmarked ruler and a compass. Can you:

- 1 Trisect any angle using just the ruler and compass?
- 2 Draw a regular n -sided polygon?
- 3 Construct a square with the same area as a given circle?

It turns out that these are mostly impossible – the exception being that one can construct a regular n -gon when n is prime.

Nonetheless, the ancient Greeks, and many others since them, tried valiantly to answer these questions, failing miserably, but sometimes managing to prove important theorems from the ashes.

At first sight, these questions appear to have nothing to do with field extensions, but of course they do!

Definition 26.1

A number r is **constructible** if the coordinate $(r, 0)$ can be constructed using ruler and compass. Let \mathbb{K} be the set of all constructible numbers.

Ruler and compass constructions

Suppose that we have an unmarked ruler and a compass.

Starting from two points A and B we can:

- 1 Draw a straight line through any two points that we already have.
- 2 Draw a circle with centre one of the points that we have already constructed and with radius the distance between any two of these points.
- 3 Mark any points in the intersections of these curves.

Let $\mathbb{K}^2 = \mathbb{K}_{AB}^2 \subseteq \mathbb{R}^2$ be the set of all points constructible this way.

By rescaling we can assume that $A = (0, 0)$ and $B = (1, 0)$.

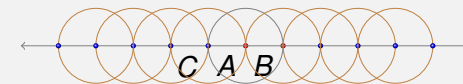
Our first exercise is to show that $\mathbb{Q} \times \mathbb{Q} \subseteq \mathbb{K}^2$.

We start slowly and show that $\mathbb{Z} \times \{0\}$ and $\mathbb{Z} \times \mathbb{Z}$ are contained in \mathbb{K}^2 .

The point of this exercise is two-fold: first, we apply the theory that we have developed to solve some seemingly unrelated and famous old problems. Secondly, through this *extended example* we will improve our understanding of field extensions and irreducible polynomials.

Constructing the integers

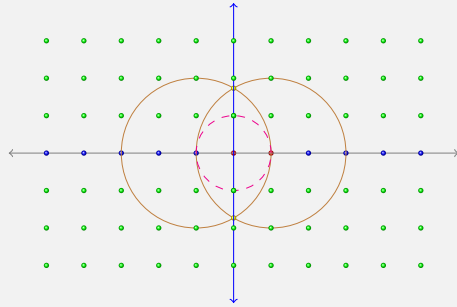
Step 1. $\{(m, 0) : m \in \mathbb{Z}\} \subseteq \mathbb{K}^2$



- 1 Draw a line through $A = (0, 0)$ and $B = (1, 0)$
- 2 Draw a circle through $B = (1, 0)$ with centre $A = (0, 0)$
- 3 Mark the point $C = (-1, 0)$
- 4 Repeat!

Constructing \mathbb{Z}^2

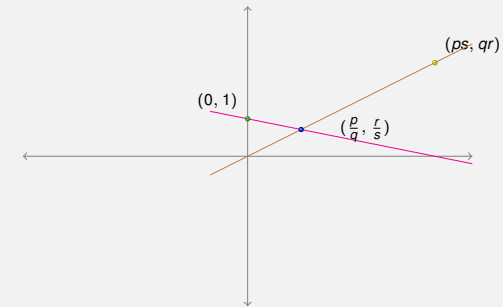
Step 2. $\{(m, n) : m, n \in \mathbb{Z}\} \subseteq \mathbb{K}^2$



- 1 Draw circles of radius 2 with centers at $(1, 0)$ and $(-1, 0)$.
- 2 Draw a line through the intersection points $(0, \sqrt{3})$ and $(0, -\sqrt{3})$
- 3 Draw a circle of radius 1 with centre $(0, 0)$ and mark $(0, \pm 1)$.
- 4 Now construct $\mathbb{Z} \times \mathbb{Z}$ using Step 1 and Step 2.

The rational numbers are constructible

Step 3. $\mathbb{Q}^2 = \{(\frac{p}{q}, \frac{r}{s}) : p, q, r, s \in \mathbb{Z}\} \subseteq \mathbb{K}^2$



- 1 Draw the line connecting $(0, 0)$ and (ps, qr)
- 2 Draw the line connecting $(1, 0)$ and $(ps, qr - sq + 1)$
- 3 The intersection of these two lines is the point $(\frac{p}{q}, \frac{r}{s})$

Constructible numbers

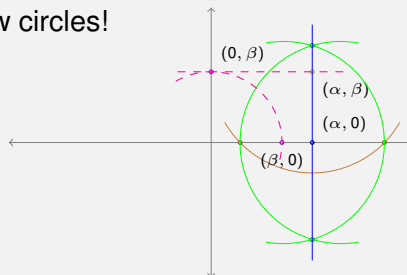
Definition 26.2

Let $\mathbb{K} = \{r \in \mathbb{R} : (r, 0) \in \mathbb{K}^2 \text{ is constructible}\}$.
A real number $r \in \mathbb{R}$ is **constructible** if $r \in \mathbb{K}$.

Lemma 26.3

Suppose that $\alpha, \beta \in \mathbb{R}$. Then $\alpha, \beta \in \mathbb{K}$ if and only if $(\alpha, \beta) \in \mathbb{K}^2$.

Proof Draw a few circles!



□

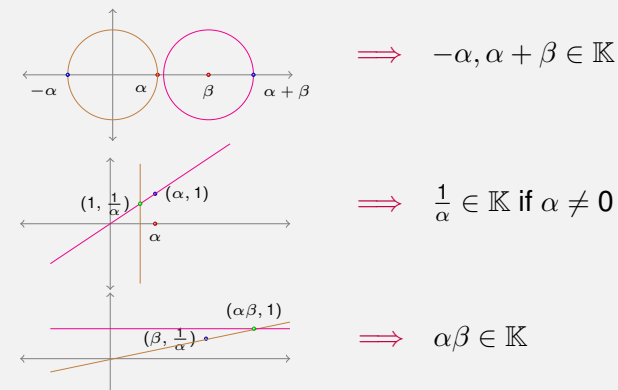
Hence, $\mathbb{Q} \subseteq \mathbb{K}$ by the last three slides.

The constructible numbers form a field

Proposition 26.4

The set of constructible numbers \mathbb{K} is a subfield of \mathbb{R} .

Proof Suppose that $\alpha, \beta \in \mathbb{K} \iff (\alpha, 0), (\beta, 0) \in \mathbb{K}^2$.



$\implies -\alpha, \alpha + \beta \in \mathbb{K}$

$\implies \frac{1}{\alpha} \in \mathbb{K}$ if $\alpha \neq 0$

$\implies \alpha\beta \in \mathbb{K}$

Hence, \mathbb{K} is a subfield of \mathbb{R} .

□

The constructible numbers are an extension of \mathbb{Q}

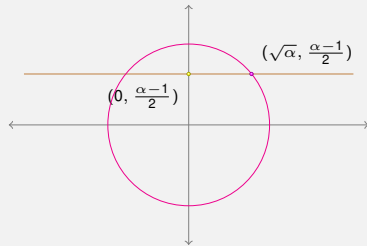
As $\mathbb{Q} \subseteq \mathbb{K}$ we have that $\mathbb{K}:\mathbb{Q}$ is a field extension.

In fact, \mathbb{K} is a proper extension of \mathbb{Q} . i.e. $\mathbb{Q} \subsetneq \mathbb{K}$.

Lemma 26.5

Suppose that $\alpha \in \mathbb{K}$. Then $\sqrt{\alpha} \in \mathbb{K}$.

Proof The line $y = \frac{\alpha-1}{2}$ meets the circle $x^2 + y^2 = (\frac{\alpha+1}{2})^2$ at $(\sqrt{\alpha}, \frac{\alpha-1}{2})$.



□

Question Can we describe the set \mathbb{K} of constructible numbers?

A description of the constructible numbers

Theorem 26.6

Let \mathbb{K}' be the set of all real numbers which can be constructed from a sequence $t_0 = 0, t_1 = 1, t_2, \dots, t_n$ where, for $i = 2, \dots, n$, we have $t_i \in \{t_j \pm t_k, t_j t_k, \frac{1}{t_j}, \sqrt{t_j} : 0 \leq j, k < i\}$. Then $\mathbb{K} = \mathbb{K}'$.

Proof By Lemma 26.5 we have that $\mathbb{K}' \subseteq \mathbb{K}$.

To prove the converse first observe that \mathbb{K}' is a subfield of \mathbb{R} which is closed under taking square roots. (so $k \in \mathbb{K}' \implies \sqrt{k} \in \mathbb{K}'$).

Any two points in \mathbb{K} are constructed using a sequence of ruler and compass operations starting from the points $A = (0, 0)$ and $B = (1, 0)$. New points are constructed by intersecting two lines, a circle and a line or two circles which are defined using previously constructed points.

Thus, we are intersecting curves of the form $ax + by = c$ and $x^2 + y^2 + dx + ey = f$, where $a, b, c, d, e, f \in \mathbb{K}$.

\implies the new points have the form $p \pm \sqrt{q}$, where p and q are obtained by adding, multiplying and taking inverses of coefficients.

$\implies \mathbb{K} \subseteq \mathbb{K}'$ as we wanted to prove. □

Degrees of constructibility

Proposition 26.7

Suppose that $\alpha \in \mathbb{K}$ is a constructible number.

Then $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^n$, for some $n \geq 0$.

Proof By Theorem 26.6 we can find a sequence

$t_0 = 0, t_1 = 1, \dots, t_n = \alpha$ with $t_i \in \{t_j \pm t_k, t_j t_k, \frac{1}{t_j}, \sqrt{t_j} : 0 \leq j, k < i\}$.

Hence, $\mathbb{Q} = \mathbb{Q}(t_0) = \mathbb{Q}(t_1) \subseteq \mathbb{Q}(t_2) \subseteq \dots \subseteq \mathbb{Q}(t_{n-1}) \subseteq \mathbb{Q}(\alpha)$ is a sequence of field extensions.

Therefore, by Theorem 25.3, we have

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(t_{n-1})] \dots [\mathbb{Q}(t_3):\mathbb{Q}(t_2)] [\mathbb{Q}(t_2):\mathbb{Q}].$$

If $t_i \in \mathbb{Q}(t_{i-1})$ then $\mathbb{Q}(t_i) = \mathbb{Q}(t_{i-1}) \implies [\mathbb{Q}(t_i):\mathbb{Q}(t_{i-1})] = 1$.

If $t_i \notin \mathbb{Q}(t_{i-1})$ then $t_i = \sqrt{t_j} \notin \mathbb{Q}(t_{i-1})$, for some $j < i$

\implies The minimum polynomial of t_i over $\mathbb{Q}(t_{i-1})$ is $x^2 - t_j$

$\implies [\mathbb{Q}(t_i):\mathbb{Q}(t_{i-1})] = 2$.

The Proposition follows. □