

## Last lecture

- 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.
- The set of constructible numbers  $\mathbb{K}$  is a subfield of  $\mathbb{R}$  which contains  $\mathbb{Q}$ . Moreover, if  $\alpha \in \mathbb{K}$  then  $\sqrt{\alpha} \in \mathbb{K}$ .
- (Proposition 26.7) If  $\alpha \in \mathbb{R}$  is constructible then  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ , for some  $n \geq 0$ .

### This lecture

Proving the impossible (for certain ruler and compass constructions), field extensions and the Galois group.

## Trisecting angles

### Theorem 27.1

*In general, it is not possible to trisect an angle using a ruler and compass.*

**Proof** Trisecting an angle  $3\theta$  is equivalent to constructing  $\cos \theta$ , so it is enough to produce one number in  $[-1, 1]$  which is not constructible.

**Claim** Let  $\theta = \frac{2\pi}{18}$ . Then  $\cos \theta$  is not constructible.

Observe that  $\frac{1}{2} = \cos \frac{\pi}{3} = \cos(3\theta) = 4 \cos^3 \theta - 3 \cos \theta$ .

$\implies \cos \theta$  is a root of the polynomial  $f(x) = 8x^3 - 6x - 1$ .

By the rational roots theorem (Theorem 23.1), the only possible rational roots of  $f(x)$  are  $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}$  and  $\pm \frac{1}{8}$

Hence,  $f(x)$  is irreducible over  $\mathbb{Q}$  since none of these are roots of  $f(x)$

$\implies [\mathbb{Q}(\cos \theta) : \mathbb{Q}] = 3$  by Proposition 24.4

$\implies \cos \theta$  is not constructible by Proposition 26.7/Theorem 26.6.

□

### Corollary 27.2

*It is not possible to construct a regular 18-gon by ruler and compass.*

## Duplicating the cube

### Theorem 27.3

*It is not possible to construct a cube with twice the volume of a cube using only a ruler and a compass (i.e. we cannot duplicate the cube).*

**Proof** Without loss of generality we can assume that the cube is the unit cube in  $\mathbb{R}^3$ .

As the unit cube has volume  $1m^3$  we need to construct a cube with volume  $2m^3$ .

$\implies$  We must construct a cube with sides of length  $\sqrt[3]{2}$ .

The minimum polynomial of  $\sqrt[3]{2}$  over  $\mathbb{Q}$  is  $x^3 - 2$  — which is irreducible by applying Eisenstein's criterion (Theorem 23.3) with  $p = 2$ .

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

$\implies \sqrt[3]{2}$  is not constructible by Proposition 26.7 (alternatively, apply Theorem 26.6)

□

## Squaring the circle

### Theorem 27.4

*It is not possible to construct a square with the same area as a given circle using only a ruler and compass.*

**Proof** We may assume that the circle is the unit circle

$\implies$  the circle has area  $\pi$

$\implies$  the required square has sides of length  $\sqrt{\pi}$

$\implies$  we can 'square the circle' if and only if  $\sqrt{\pi} \in \mathbb{K}$ .

Assume, by way of contradiction, that we can square the circle.

$\implies \pi = (\sqrt{\pi})^2 \in \mathbb{K}$  since  $\mathbb{K}$  is closed under multiplication

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

However, this contradicts Slide 25.3 where we saw that  $\pi$  is transcendental over  $\mathbb{Q} \implies \pi \notin \mathbb{K}$ .

Thus, we cannot square a circle with ruler and compass.

□

## Automorphisms of field extensions

### Definition 27.5

Suppose that  $E$  a field and that  $F$  is a subfield of  $E$ .  
An  $F$ -automorphism of  $E$  is a ring isomorphism  $\theta: E \rightarrow E$  such that  $\theta(f) = f$  for all  $f \in F$ .

### Remarks

- 1 Taking  $E = F$  an automorphism of  $F$  is an isomorphism  $\theta: F \rightarrow F$  which fixes  $F \implies \theta = \text{id}_F$ , the identity map on  $F$ .
- 2 Let  $F$  be the smallest subfield of  $E$  which contains  $1_E (\implies F \cong \mathbb{Q}$  or  $F \cong \mathbb{Z}/p\mathbb{Z}$  for some prime  $p$ ). Then every automorphism of  $E$  is an  $F$ -automorphism of  $E$  as every automorphism of  $E$  fixes  $F$ .
- 3 An  $F$ -automorphism is an 'automorphism of the extension  $E:F$ '.

### Examples

- 1 The identity map  $\text{id}_E: E \rightarrow E; e \mapsto e$  is an  $F$ -automorphism for every subfield  $F$ .
- 2 If  $F = \mathbb{Q}$  and  $E = \mathbb{Q}(\sqrt{2})$  then the map  $\theta(a + b\sqrt{2}) = a - b\sqrt{2}$  is a  $\mathbb{Q}$ -automorphism of  $\mathbb{Q}(\sqrt{2})$ .

## The group of automorphisms

### Theorem 27.6

Suppose that  $E:F$  is a field extension. Then the set  $\text{Gal}(E:F)$  of all  $F$ -automorphisms of  $E$  forms a group under composition of maps.

**Proof** Now, the identity map  $\text{id}_E$  on  $E$  is an  $F$ -automorphism and  $\alpha \text{id}_E = \alpha = \text{id}_E \alpha$ , for all automorphisms of  $E$ .

Now, suppose that  $\alpha$  and  $\beta$  are  $F$ -automorphisms of  $E$   
 $\implies \alpha\beta: E \rightarrow E; e \mapsto \alpha(\beta(e))$  is an automorphism of  $E$   
 Further, if  $f \in F$  then  $(\alpha\beta)(f) = \alpha(\beta(f)) = \alpha(f) = f$   
 $\implies \alpha\beta \in \text{Gal}(E:F)$

Finally, any automorphism  $\alpha$  is a bijection, so the inverse map  $\alpha^{-1}: E \rightarrow E$  exists. The map  $\alpha^{-1}$  is a bijective ring homomorphism and  $\alpha^{-1}(f) = f$  since  $f = \alpha(f)$ , for all  $f \in F$ . Therefore,  $\alpha^{-1} \in \text{Gal}(E:F)$  is an  $F$ -automorphism.

As  $\alpha\alpha^{-1} = \text{id}_E = \alpha^{-1}\alpha$  this shows that every  $F$ -automorphism in  $\text{Gal}(E:F)$  has an inverse.  
Hence,  $\text{Gal}(E:F)$  is a group. □

## The Galois group

### Definition 27.7

Suppose that  $E:F$  is a field extension. Then the **Galois group** of  $E:F$  is the group  $\text{Gal}(E:F)$  of  $F$ -automorphisms of  $E$ .

**Example** Consider the field extension  $\mathbb{R}(i):\mathbb{R}$ .

**Claim**  $\text{Gal}(\mathbb{C}:\mathbb{R}) \cong C_2$ , the cyclic group of order 2.

Let  $\theta: \mathbb{C} \rightarrow \mathbb{C}$  be an  $\mathbb{R}$ -automorphism of  $\mathbb{C}$ .

Let  $j = \theta(i) \implies -1 = \theta(-1) = \theta(i^2) = (\theta(i))^2 = j^2$

$\implies j = \pm i$ . Hence, for any  $a + bi \in \mathbb{C}$  we have

$\theta(a + bi) = \theta(a) + \theta(b)\theta(i) = a + bj = a \pm bi$ .

$\implies$  If  $\theta \neq \text{id}_{\mathbb{C}}$  then  $\theta(a + bi) = a - bi$ , for  $a, b \in \mathbb{R}$ .

$\implies \theta^2(a + bi) = a + bi = \text{id}_{\mathbb{C}}$

$\implies \text{Gal}(\mathbb{C}:\mathbb{R}) = \{\text{id}_{\mathbb{C}}, \theta | \theta^2 = \text{id}_{\mathbb{C}}\} \cong C_2$ .

## The Galois group of $\mathbb{Q}(\omega):\mathbb{Q}$

**Example** Let  $\omega = \frac{1}{2}(-1 + \sqrt{-3}) \in \mathbb{C}$ .

Then  $\omega = \exp(\frac{2\pi i}{3})$  so that  $\omega^2 + \omega + 1 = 0$ .

$\implies$  the minimum polynomial of  $\omega$  over  $\mathbb{Q}$  is  $x^2 + x + 1$

$\implies [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg x^2 + x + 1 = 2$ .

As a  $\mathbb{Q}$ -vector space  $\mathbb{Q}(\omega)$  has basis  $\{1, \omega, \omega^2\}$ .

If  $\theta \in \text{Gal}(\mathbb{Q}(\omega):\mathbb{Q})$  then

$$\begin{aligned} \theta(a + b\omega + c\omega^2) &= \theta(a) + \theta(b\omega) + \theta(c\omega^2) \\ &= a + b\theta(\omega) + c\theta(\omega^2) \end{aligned}$$

Hence,  $\theta$  is completely determined by its value at  $\omega$ .

Now,  $1 = \omega^3 = \theta(\omega^3) = \theta(\omega)^3 \implies \theta(\omega) \in \{\omega, \omega^2\}$

Thus,  $\text{Gal}(\mathbb{Q}(\omega):\mathbb{Q}) = \{\text{id}_{\mathbb{Q}(\omega)}, \theta\}$ , where

$$\theta(a + b\omega + c\omega^2) = a + c\omega + b\omega^2$$

$\implies \theta^2 = \text{id}_{\mathbb{C}}$

$\implies \text{Gal}(\mathbb{Q}(\omega):\mathbb{Q}) \cong C_2$ .