

# GALOIS THEORY

ADAM KELLY – MATHEMATICAL TRIPOS PART II

## 1. FIELDS

**1.1. Field extensions.** We introduce our fundamental object of study.

### Definition 1.1 (Field Extension)

Let  $K \subset L$  be fields<sup>a</sup>. We say  $K$  is a subfield of  $L$ , and  $L$  is a **field extension** of  $K$ , denoted  $L/K$  (read ‘ $L$  over  $K$ ’).

<sup>a</sup>Implicitly assuming that the field operations and identity elements on  $K$  and  $L$  are the same.

### Definition 1.2 (Adjoining Elements)

Let  $K \subset L$ , and  $x \in L$ . We define

$$K[x] = \{p(x) \mid p \in K[T]\}$$

to be the ring where we **adjoin**  $x$  to  $K$ .

We further define

$$K(x) = \left\{ \frac{p(x)}{q(x)} \mid p, q \in K[T], q(x) \neq 0 \right\}$$

to be the field of fractions of  $K[x]$ .

**1.2. Field Extensions as Vector Spaces.** A field extension  $L/K$  turns  $L$  into a  $K$ -vector space by forgetting the multiplication between elements of  $L$ .

### Definition 1.3 (Finite/Infinite Extensions)

A field extension  $L/K$  is called a **finite extension** if  $L$  is a finite-dimensional  $K$ -vector space. We write  $[L : K] = \dim_K L$  for the **degree** of the extension.

Otherwise, we say  $L/K$  is an **infinite extension**, and write  $[L : K] = \infty$ .

We particularly care about finite field extensions.

### Definition 1.4 (Quadratic/Cubic/... Extensions)

An extension is **quadratic**, **cubic**, etc. if its degree is 2, 3, etc.

### Proposition 1.5 (Sizes of Finite Fields)

Suppose  $K$  is a finite field (necessarily of prime characteristic  $p$ ). Then  $|K|$  is a power of  $p$ .

*Proof.* Note that  $K/\mathbb{F}_p$  is a finite extension, and so  $K \cong \mathbb{F}_p^n$ , giving  $|K| = p^n$ .  $\square$

We will later show that for all prime powers  $q = p^n$ , there exists a finite field  $\mathbb{F}_q$  with  $q$  elements.

### Lemma 1.6

Let  $L/K$  and  $V$  is an  $L$ -vector space. Then  $V$  is a  $K$ -vector space, and<sup>a</sup>  $\dim_K V = [L : K] \dim_L V$ .

<sup>a</sup>Take the obvious meaning if any of these expressions are infinite.

*Proof.* Let  $\dim_L V = d < \infty$ . Then  $V \cong L \oplus \cdots \oplus L = L^d$  as an  $L$ -vector space, so this also holds as a  $K$ -vector space. But since  $L \cong K^{[L:K]}$  as a  $K$ -vector space, we have  $V \cong (K^{[L:K]})^d \cong K^{d[L:K]}$  as a  $K$ -vector space.

If  $V$  is finite-dimensional over  $K$ , then a  $K$ -basis for  $V$  will span  $V$  over  $L$ , so  $V$  is finite-dimensional over  $L$ . Thus if  $V$  is infinite-dimensional over  $L$ , it is infinite-dimensional over  $K$ .

Likewise, if  $[L : K] = \infty$  and  $V \neq 0$ , then  $V$  has an infinite set of linearly independent vectors as a  $K$ -vector space, so  $\dim_K V = \infty$ .  $\square$

### Theorem 1.7 (Tower Law)

Let  $M/L, L/K$  be a pair of field extensions. Then  $M/K$  is a finite extension if and only if  $M/L$  and  $L/K$  are finite. If so, we have  $[M : K] = [M : L][L : K]$ .

*Proof.* Take  $V = M$  in the previous lemma.  $\square$

### Proposition 1.8 (Multiplicative Group Structure)

Let  $K$  be a field, and  $G \subset K^\times$  be a finite subgroup of the multiplicative group. Then  $G$  is cyclic. In particular, if  $K$  is finite,  $K^\times$  is cyclic.

*Proof.* We can find  $m_i$  such that

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

where  $1 < m_1 \mid m_2 \mid \cdots \mid m_k = m$  by the structure theorem for abelian groups. Then, every element of  $G$  satisfies  $x^m = 1$ . Since  $K$  is a field, the polynomial  $T^m - 1$  has at most  $m$  roots. Every element of  $G$  is a root of this polynomial, so  $|G| \leq m$ . This can only happen when  $k = 1$ , so  $G \cong \mathbb{Z}/m\mathbb{Z}$ .  $\square$

### Proposition 1.9 (Frobenius Endomorphism)

Let  $R$  be a ring, with finite prime characteristic  $p$ . Then, the map  $\varphi_p : R \rightarrow R$  given by  $\varphi_p(x) =$

$x^p$  is a homomorphism, known as the **Frobenius endomorphism**.

*Proof.* First,  $\varphi_p(1) = 1^p = 1$  and  $\varphi_p(x)\varphi_p(y) = x^p y^p = (xy)^p = \varphi_p(xy)$ . For  $x, y \in R$ ,

$$\begin{aligned}\varphi_p(x+y) &= \sum_{k=0}^p \binom{p}{k} x^{p-k} y^k = x^p + y^p \\ &= \varphi_p(x) + \varphi_p(y)\end{aligned}$$

since  $p \mid \binom{p}{k}$  for  $k = 1, \dots, p-1$  as  $p$  is prime.  $\square$

**1.3. Algebraic Elements and Minimal Polynomials.** We now want to consider field elements that satisfy some polynomial over the field.

**Definition 1.10 (Algebraic and Transcendental)**

Let  $L/K$  be an extension and  $x \in L$ .  $x$  is **algebraic** over  $K$  if there exists a nonzero polynomial  $f \in K[T]$  such that  $f(x) = 0$ . Otherwise, we say  $x$  is **transcendental** over  $K$ .

For  $f \in K[T]$ , we have  $f(x) \in L$ . Varying  $f$ , this gives a map  $\text{ev}_x: K[T] \rightarrow L$  defined by  $f \mapsto f(x)$ . This is a ring homomorphism.

The kernel  $I = \ker(\text{ev}_x) \subset K[T]$  is an ideal, the set of polynomials which vanish at  $x$ . As  $\text{Im}(\text{ev}_x)$  is a subring of  $L$  which is a field, it is an integral domain. In particular,  $I$  is a prime ideal, so either  $I = 0$ , in which case  $x$  is transcendental over  $K$ , or there exists a unique monic irreducible polynomial  $0 \neq g \in K[T]$  such that  $I = (g)$ , in which case  $x$  is algebraic and we say  $g$  is the *minimal polynomial* of  $x$  over  $K$ . In this case,  $f(x) = 0$  if and only if  $g \mid f$ . We write  $m_{x,K}$  for the minimal polynomial of  $x$  over  $K$ . Note that  $m_{x,K}$  is the monic polynomial in  $K$  of least degree with  $x$  as a root.

**Example 1.11**

If  $x \in K$ ,  $m_{x,K} = T - x$ . If  $p$  is prime and  $d \geq 1$ ,  $T^d - p \in \mathbb{Q}[T]$  is irreducible by Eisenstein's criterion, so it is the minimal polynomial of  $\sqrt[p]{p} \in \mathbb{R}$  over  $\mathbb{Q}$ . If  $p$  is prime,  $z = e^{\frac{2\pi i}{p}}$  is a root of  $T^p - 1 = (T-1)(T^{p-1} + T^{p-2} + \dots + 1) = (T-1)g(T)$ , which is a product of irreducibles as

$$g(T+1) = \binom{p}{p}T^{p-1} + \binom{p}{p-1}T^{p-2} + \dots + \binom{p}{2}T + \binom{p}{1}$$

This is irreducible by Eisenstein's criterion, so  $g$  is minimal for  $z$  over  $\mathbb{Q}$ .

We say the degree of an algebraic element  $x$  over  $K$  is the degree of its minimal polynomial, written  $\deg_K x = \deg(x/K)$ .

**Proposition 1.12**

Let  $L/K$  and  $x \in L$ . Then, the following are equivalent.

- (1)  $x$  is algebraic over  $K$ .
- (2)  $[K(x) : K]$  is finite.
- (3)  $K[x]$  is finite-dimensional as a  $K$ -vector space.
- (4)  $K[x] = K(x)$ .
- (5)  $K[x]$  is a field.

If these hold,  $\deg x = [K(x) : K]$ .

*Proof.* (ii) implies (iii). This follows since  $K[x] \subseteq K(x)$ .

(iv) is equivalent to (v) is trivial.

(iii) implies (v) and (ii). Let  $0 \neq y = g(x) \in K[x]$ . Consider the map  $K[x] \rightarrow K[x]$  given by  $z \mapsto yz$ . This is a  $K$ -linear transformation, and since  $y \neq 0$  this is injective. Because  $\dim K[x]$  is finite, this injective map must be a bijection. Therefore there exists  $z$  such that  $yz = 1$ , so  $y$  is invertible. Hence (v) holds. Since (v) implies (iv),  $[K(x) : K] = \dim_K K[x] < \infty$  as required for (ii).

(v) implies (i). If  $x = 0$ , the proof is complete, so assume  $x \neq 0$ . Then  $x^{-1} = a_0 + a_1x + \dots + a_nx^n \in K[x]$ . Therefore,  $a_nx^{n+1} + \dots + a_0x - 1 = 0$ , so  $x$  is algebraic over  $K$ .

(i) implies (v), (iii), and the degree formula. The image of  $\text{ev}_x: K[T] \rightarrow L$  is the subring  $K[x] \subset L$ . If  $x$  is algebraic over  $K$ ,  $\ker(\text{ev}_x) = (m_{x,K})$  is a maximal ideal by irreducibility of  $m_{x,K}$ . By the first isomorphism theorem,  $K[T]/(m_{x,K}) \cong K[x]$ . But quotients by maximal ideals are fields, so  $K[x]$  is a field, proving (v). This polynomial is monic of degree  $d = \deg_K x$ . Hence  $K[T]/(m_{x,K})$  has a  $K$ -basis  $1, T, \dots, T^{d-1}$ . Thus,  $\dim_K K[x] = d = [K(x) : K] < \infty$ , proving (iii) and the degree formula.  $\square$

**Corollary 1.13**

$x_1, \dots, x_n$  are algebraic over  $K$  if and only if  $L = K(x_1, \dots, x_n)$  is finite over  $K$ . If so, every element of  $K(x_1, \dots, x_n)$  is algebraic over  $K$ .

If  $x, y$  are algebraic over  $K$ , then so are  $x \pm y$ ,  $xy$ , and  $x^{-1}$  if  $x$  is nonzero. If  $L/K$  is a field extension, the set of algebraic elements of  $L$  forms a subfield of  $L$ .

*Proof.* If  $x_n$  is algebraic over  $K$ , then it is also algebraic over  $K(x_1, \dots, x_{n-1})$ . Hence  $L/K(x_1, \dots, x_{n-1})$  is finite. By induction on  $n$ , the tower law gives the required result. Conversely, if  $L$  is finite over  $K$ , the subfield  $K(y)$  is finite over  $K$  for all  $y \in L$ , so  $y$  is algebraic over  $K$ .

Suppose  $x, y$  are algebraic over  $K$ . Then  $x \pm y, xy, x^{-1} \in K(x, y)$ , which is finite over  $K$  as required.  $\square$

### Example 1.14

Consider  $z = e^{2\pi i/p} \in \mathbb{C}$  where  $p$  is an odd prime. This has degree  $p - 1$  as discussed above. Now consider  $x = 2 \cos \frac{2\pi}{p}$ , so  $x = z + \frac{1}{z} \in \mathbb{Q}(z)$ . This is algebraic over  $\mathbb{Q}$  because it belongs to this finite extension. Note that  $\mathbb{Q}(z) \supset \mathbb{Q}(x) \supset \mathbb{Q}$ , and  $z^2 - xz + 1 = 0$ . Hence the degree of  $z$  over  $\mathbb{Q}(x)$  is at most 2. But  $[\mathbb{Q}(z) : \mathbb{Q}(x)] \neq 1$  because  $z \in \mathbb{C} \setminus \mathbb{R}$ . By the tower law, we must have  $[\mathbb{Q}(z) : \mathbb{Q}] = \frac{p-1}{2}$ .

We can now derive the minimal polynomial by considering  $z^{\frac{p-1}{2}} + z^{\frac{p-3}{2}} + \cdots + z^{-\frac{p-1}{2}} = 0$ . Since  $z + z^{-1} = x$ , we can express this as a polynomial in  $x$  of degree  $\frac{p-1}{2}$ .

### Example 1.15

Let  $x = \sqrt{m} + \sqrt{n}$  where  $m, n$  are integers, and  $m, n, mn$  are not squares. We know that  $n = (x - \sqrt{m})^2 = x^2 - 2x\sqrt{m} + m$ , so  $[\mathbb{Q}(x) : \mathbb{Q}(\sqrt{m})] \leq 2$ . By symmetry,  $[\mathbb{Q}(x) : \mathbb{Q}(\sqrt{n})] \leq 2$ . Note that  $\sqrt{m} \in \mathbb{Q}(x)$  because  $\frac{x^2 + m - n}{2x} = \sqrt{m}$ .

$m, n$  are not squares, so  $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$ . By the tower law we have  $[\mathbb{Q}(x) : \mathbb{Q}] \in 2, 4$ . If  $[\mathbb{Q}(x) : \mathbb{Q}] = 2$ , we have  $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$ . In this case,  $\sqrt{m} = a + b\sqrt{n} \implies m = a^2 + b^2n + 2ab\sqrt{n}$ , but  $n$  is not a square, so by rationality,  $ab = 0$ . But if  $b = 0$ ,  $m$  is a square, and if  $a = 0$ ,  $mn = b^2n^2$  is a square. Hence the degree of the field extension is 4.

### Definition 1.16

An extension  $L/K$  is *algebraic* if all elements of  $L$  are algebraic over  $K$ .

### Lemma 1.17

Let  $M/L/K$ , where  $L/K$  is algebraic. Suppose  $x$  is algebraic over  $L$ . Then  $x$  is algebraic over  $K$ .

*Proof.* There exists  $f = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in L[T]$  where  $f \neq 0$  and  $f(x) = 0$ . Let  $L_0 = K(a_0, \dots, a_{n-1})$ . As each  $a_i \in L$  is algebraic over  $K$ , we must have that  $[L_0 : K]$  is finite. As  $f \in L_0[T]$ ,  $x$  is algebraic over  $L_0$ . So  $[L_0(x) : L_0] < \infty \implies [L_0(x) : K] < \infty$ . Hence  $[K(x) : K] < \infty$ , so  $x$  is algebraic over  $K$ .  $\square$

**Proposition 1.18** (1) Finite extensions are algebraic.

(2)  $K(x)$  is algebraic over  $K$  if and only if  $x$  is algebraic over  $K$ .

(3) If  $M/L/K$ , we have  $M/K$  is algebraic if and only if  $M/L$  and  $L/K$  are algebraic.

*Proof.* (1)  $[L : K] < \infty$ , so for all  $x \in L$ ,  $[K(x) : K] < \infty$ , so  $x$  is algebraic.

(2) Certainly if  $K(x)$  is algebraic over  $K$ , we have that  $x$  is algebraic over  $K$ . Conversely, if  $x$  is algebraic over  $K$ ,  $[K(x) : K]$  is finite, so it is algebraic by part (i).

(3) Suppose  $M/K$  is algebraic. Then for all  $x \in M$ , we have that  $x$  is algebraic over  $K$ , so it satisfies a polynomial  $f \in K[T]$ . Hence  $f \in L[T]$  is another polynomial that  $x$  satisfies, so  $M/L$  is algebraic.  $L/K$  is clearly algebraic because it is contained within  $M$ .

Conversely, suppose  $M/L$  and  $L/K$  are algebraic. Let  $x \in M$ . Then by the previous lemma,  $x$  is algebraic over  $K$  as required.  $\square$

### Example 1.19

Let  $K = \mathbb{Q}$  and  $L = \{x \in \mathbb{C} \mid x \text{ is algebraic over } \mathbb{Q} = \overline{\mathbb{Q}}\}$ . This extension  $\overline{\mathbb{Q}}/\mathbb{Q}$  is algebraic, but not finite. Indeed, for every  $n \geq 1$ ,  $\sqrt[n]{2} \in L$ , and  $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$  by irreducibility of  $T^n - 2$ . In particular,  $L$  contains subfields of arbitrarily large degree, so cannot be a finite extension.

**1.4. Algebraic numbers in the real line and complex plane.** Traditionally, we call  $x \in \mathbb{C}$  algebraic if it is algebraic over  $\mathbb{Q}$ , otherwise it is transcendental.  $\overline{\mathbb{Q}} = \{x \mid x \text{ algebraic}\}$  is a proper subfield of  $\mathbb{C}$ . Indeed,  $\overline{\mathbb{Q}}[T]$  is a countable set, and  $\mathbb{C}$  is uncountable. However, it is difficult to explicitly find an element of  $\mathbb{C} \setminus \overline{\mathbb{Q}}$ , or to show that a given number is transcendental.

### Example 1.20

Liouville's constant  $c = \sum_{n \geq 1} 10^{-n!}$  is transcendental, as proven in IA Numbers and Sets. This can be proven by showing that algebraic numbers cannot be 'well approximated' by rationals.

### Example 1.21

Hermite and Lindemann showed that  $e$  and  $\pi$  are transcendental.

### Example 1.22

Let  $x, y$  be algebraic, and  $x \neq 0, 1$ . Gelfond and Schneider showed that  $x^y$  is algebraic if and only if  $y$  is rational. In particular,  $e^\pi = (-1)^{-i}$  is transcendental.

## 1.5. Ruler and compass constructions.

### Definition 1.23

A *ruler and compass construction* in plane geometry is a drawing constructed with the following methods.

- (1) Given  $P_1, P_2, Q_1, Q_2$  in the plane and  $P_i \neq Q_i$ , we can construct the point of intersection of the lines  $P_1Q_1$  and  $P_2Q_2$ , if indeed they do intersect.
- (2) Given  $P_1, P_2, Q_1, Q_2$  in the plane and  $P_i \neq Q_i$ , we can construct the points of intersection of the circles with centres  $P_i$  that pass through the  $Q_i$ , if they intersect.
- (3) Similarly we can construct the points of intersection of a line and a circle.

A point  $(x, y) \in \mathbb{R}^2$  is *constructible* from a set  $(x_1, y_1), \dots, (x_n, y_n)$  if it can be obtained by finitely many expansions of the set under applications of the above operations. A real number  $x \in \mathbb{R}$  is *constructible* if  $(x, 0)$  is constructible from  $(0, 0), (1, 0)$ .

**Remark.** Every rational is constructible. Square roots of constructible numbers are constructible.

#### Definition 1.24

Let  $K \subseteq \mathbb{R}$  be a subfield of the reals. We say  $K$  is *constructible* if there exists  $n \in \mathbb{N}$  and fields  $\mathbb{Q} = F_0 \subset F_1 \subset \dots \subset F_n \subseteq \mathbb{R}$  and  $a_i \in F_i$  for  $1 \leq i \leq n$  such that

- (1)  $K \subseteq F_n$ ;
- (2)  $F_i = F_{i-1}(a_i)$ ;
- (3)  $a_i^2 \in F_{i-1}$ .

**Remark.** By conditions (ii) and (iii),  $F_i/F_{i-1}$  is at most a quadratic extension. Then, by the tower law,  $F_n/\mathbb{Q}$  has degree a power of two, so  $K/\mathbb{Q}$  is a finite extension with degree a power of two.

#### Theorem 1.25

If  $x$  is constructible,  $\mathbb{Q}(x)$  is constructible.

*Proof.* Let  $K = \mathbb{Q}(x)$ . We show that if  $(x, y)$  can be constructed with  $k$  steps,  $\mathbb{Q}(x, y)$  is a constructible extension of  $\mathbb{Q}$ . By induction, suppose  $\mathbb{Q} = F_0 \subset \dots \subset F_n$  satisfy conditions (ii) and (iii) such that the coordinates of the points obtained after  $k-1$  constructions lie in  $F_n$ .

The intersection point of two lines has coordinates given by rational functions of the coordinates of the points  $P_i, Q_i$  with rational coefficients. In particular, if the  $k$ th construction is of this type, the intersection point has coordinates in  $F_n$ . We can similarly see that the intersection points of two circles and the intersection points of a line and a

circle have coordinates given by quadratic equations  $a \pm b\sqrt{e}, c \pm d\sqrt{e}$ , where  $a, b, c, d, e$  are rational functions of the coordinates  $P_i, Q_i$ . Thus the new points have coordinates which lie in  $F_n(\sqrt{e})$ , a constructible extension of  $\mathbb{Q}$  as required.  $\square$

#### Corollary 1.26

If  $x$  is constructible,  $x$  is algebraic over  $\mathbb{Q}$  and the degree of the minimal polynomial is a power of two.

**Remark.** One can show that if  $\mathbb{Q}(x)$  is constructible, we also have  $x$  is constructible, so the above theorem is a bi-implication. However, this will not be required for our purposes in this course.

### 1.6. Classical problems.

#### Theorem 1.27

It is impossible to square the circle.

*Proof.* The statement is to construct a square with area equal to that of a given circle. In particular, we must construct  $\sqrt{\pi}$ . Suppose such a construction can occur. Then  $\pi$  is also constructible. But  $\pi$  is transcendental and hence inconstructible.  $\square$

#### Theorem 1.28

It is impossible to duplicate the cube.

*Proof.* To duplicate the cube, one must be able to construct  $\sqrt[3]{2}$ . The minimal polynomial of  $\sqrt[3]{2}$  is  $X^3 - 2$ . This can be easily checked with Eisenstein's criterion. Since the minimal polynomial is of degree not a power of two,  $\sqrt[3]{2}$  is inconstructible.  $\square$

#### Theorem 1.29

It is impossible to trisect a given angle.

*Proof.* If we can trisect any constructible angle, we can in particular trisect the (constructible) angle  $\frac{2\pi}{3}$ , for example to construct a regular nonagon. Then the angle  $\frac{2\pi}{9}$  would be constructible, so its sine and cosine would be constructible. By the triple angle formula for cosine,

$$\cos 3\theta = 4 \cos^3 \theta - 3 \cos \theta \implies 4 \cos^3 \left( \frac{2\pi}{9} \right) - 3 \cos \left( \frac{2\pi}{9} \right) = \cos \left( \frac{2\pi}{3} \right) = -\frac{1}{2}$$

Hence  $\cos \left( \frac{2\pi}{9} \right)$  is a root of  $8X^3 - 6X + 1$ . In particular,  $2 \cos \left( \frac{2\pi}{9} \right) - 2$  is a root of  $X^3 + 6X^2 + 9X + 3$ , which can be shown to be irreducible by Eisenstein's criterion. But this has degree 3, so  $\deg_{\mathbb{Q}} \cos \left( \frac{2\pi}{9} \right) = 3$ , so this is inconstructible. In particular, the regular nonagon is inconstructible.  $\square$

We will later prove the following theorem.

**Theorem 1.30 (Gauss)**

A regular  $n$ -gon is constructible if and only if  $n$  is the product of a power of two and distinct *Fermat primes*, which are the primes of the form  $2^{2^k} + 1$ .

2. TYPES OF FIELD EXTENSIONS

**2.1. Fields from polynomials.** Suppose  $K$  is a field and  $f \in K[T]$ . We wish to find an extension  $L/K$  of degree as small as possible such that  $f$  is expressible as a product of linear factors in  $L[T]$ .

**Example 2.1**

Let  $K = \mathbb{Q}$ . Then by the fundamental theorem of algebra, a monic polynomial  $f \in \mathbb{Q}[T]$  is expressible as a product of  $n$  linear factors  $(T - x_i)$  in  $\mathbb{C}[T]$ . One example of such a field extension is  $L = \mathbb{Q}(x_1, \dots, x_n)$ , which is a finite extension of  $\mathbb{Q}$ .

We will later give another proof of the fundamental theorem of algebra using techniques from Galois theory.

**Example 2.2**

Let  $K = \mathbb{F}_p$ , and  $f$  is irreducible and has degree  $d > 1$ . Since there is no ambient field structure, explicitly finding  $L$  is more challenging. We will first find an extension in which  $f$  has at least one root, and then use induction.

**Theorem 2.3**

Let  $f$  be a monic irreducible polynomial. Let  $L_f = K[T]_{(f)}$ . Since  $f$  is irreducible,  $(f)$  is maximal, hence  $L_f$  is a field. Let  $t \in L_f$  be the residue class  $T$  modulo  $(f)$ . Then  $L_f/K$  is a finite field extension of degree  $\deg f$ , and  $f$  is the minimal polynomial for  $t$ .

We have thus constructed a field extension of  $K$  for which  $f$  has at least a single root. Recall that if  $x$  is algebraic over  $K$ , then  $K(x) \cong K[T]_{(f)}$  where  $f$  is minimal for  $x$ .

**Definition 2.4**

Let  $K$  be a field, and  $L/K, M/K$  are field extensions. A *K-homomorphism* or *K-embedding* from  $L$  to  $M$  is a field homomorphism  $\sigma: L \rightarrow M$  such that  $\sigma|_K = \text{id}_K$ .

The naming ‘ $K$ -embedding’ is justified because any field homomorphism is injective.

**Theorem 2.5**

Let  $f \in K[T]$  be irreducible, and  $L/K$  a field extension. Then:

- (1) If  $x \in L$  is a root of  $f$ , there exists a unique  $K$ -homomorphism  $\sigma: L_f = K[T]_{(f)} \rightarrow L$  such that  $t = T + (f) \mapsto x$ .
- (2) Every  $K$ -homomorphism  $\sigma: L_f \rightarrow L$  arises in this way.

Hence, we have a bijection between  $K$ -homomorphisms  $\sigma: L_f \rightarrow L$  and the set of roots of  $f$  in  $L$ . In particular, there are at most  $\deg f$ -many  $K$ -homomorphisms.

*Proof.* Let  $x \in L$  be a root of  $f$ . We define the  $K$ -homomorphism  $\sigma: K[T]_{(f)} \rightarrow L$  by  $\sigma(T) = x$ . Conversely, suppose  $\sigma: K[T]_{(f)} \rightarrow L$  is a  $K$ -homomorphism. Then  $\sigma(T)$  is a root of  $f$ , because  $f(\sigma(T)) = \sigma(f(T)) = \sigma(0) = 0$ . So the two definitions are inverses, so we have a one-to-one correspondence as required.  $\square$

**Corollary 2.6**

Let  $L = K(x)$  for some  $x$  algebraic over  $K$ . Then there exists a unique isomorphism  $\sigma: L_f \rightarrow K(x)$  such that  $\sigma(t) = x$ , where  $f$  is minimal for  $x$  over  $K$ .

**Definition 2.7**

Let  $x, y$  be algebraic over  $K$ . We say  $x, y$  are *K-conjugate* if they have the same minimal polynomial over  $K$ .

By the corollary above,  $K(x)$  and  $K(y)$  are isomorphic to  $L_f$  where  $f$  is minimal for  $x$  and  $y$  over  $K$ .

**Corollary 2.8**

Algebraic elements  $x, y$  are  $K$ -conjugate if and only if there exists a  $K$ -isomorphism  $\sigma: K(x) \rightarrow K(y)$  such that  $\sigma(x) = y$ .

*Proof.* The above corollary shows the forward direction. Conversely, for all  $g \in K[T]$ , we have  $\sigma(g(x)) = g(\sigma(x))$  so they have the same minimal polynomial.  $\square$

Informally, the roots of an irreducible polynomial are algebraically indistinguishable.

It can be useful for inductive arguments to have a generalisation of the above theorem.

**Definition 2.9**

Let  $L/K, L'/K'$  be field extensions, and let  $\sigma: K \rightarrow K'$  be a field homomorphism. Let  $\tau: L \rightarrow L'$  be a field homomorphism such that  $\tau(x) = \sigma(x)$  for all



$x \in K$ . Then we say  $\tau$  is a  $\sigma$ -homomorphism from  $L$  to  $L'$ . We also say  $\tau$  extends  $\sigma$ , or that  $\sigma$  is the restriction of  $\tau$  to  $K$ .

We can now define the following variant of the previous theorem.

### Theorem 2.10

Let  $f \in K[T]$  be irreducible, and  $\sigma: K \rightarrow L$  be a field homomorphism. Let  $\sigma f$  be the polynomial obtained by applying  $\sigma$  to the coefficients of  $f$ .

- (1) If  $x \in L$  is a root of  $f$ , there exists a unique  $\sigma$ -homomorphism  $\tau: L_f \rightarrow L$  such that  $\tau(t) = x$ .
- (2) Every  $\sigma$ -homomorphism  $L_f \rightarrow L$  is of this form.

Therefore there is a bijection between the  $\sigma$ -homomorphisms  $L_f \rightarrow L$  and the roots of  $f$  in  $L$ .

### Example 2.11

Let  $K = \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ , and  $L = \mathbb{C}$ . Let  $\sigma: K \rightarrow L$  be the homomorphism such that  $\sigma(x + y\sqrt{2}) = x - y\sqrt{2}$ . Then let  $f = T^2 - (1 + \sqrt{2})$ . Then the map  $\tau: L_f \rightarrow \mathbb{C}$  must satisfy  $\tau(t) = \pm\sqrt{1 - \sqrt{2}} = \pm i\sqrt{\sqrt{2} - 1} \in \mathbb{C}$ . If instead we let  $\sigma(x + y\sqrt{2}) = x + y\sqrt{2}$ , we have  $\tau(t) = \pm\sqrt{\sqrt{2} + 1}$ , which are both real.

## 2.2. Splitting fields.

### Definition 2.12

Let  $f \in K[T]$  be a nonzero polynomial that is not necessarily irreducible. We say that an extension  $L/K$  is a *splitting field* for  $f$  over  $K$  if

- (1)  $f$  splits into linear factors in  $L[T]$ ;
- (2)  $L = K(x_1, \dots, x_n)$ , where the  $x_i$  are the roots of  $f$  in  $L$ .

**Remark.** The second criterion ensures that  $f$  does not split into linear factors in any proper subfield of  $L$ . Note that any splitting field is finite, because the adjoined elements are algebraic.

### Theorem 2.13

Every nonzero polynomial has a splitting field.

*Proof.* Let  $f \in K[T]$ . We prove this by induction on the degree of  $f$ , but allow  $K$  to vary. If  $f$  is constant, there is nothing to prove, since  $K$  is already a splitting field. Suppose that for all fields  $K'$  and all polynomials in  $K'[T]$  of degree less than  $f$ , there is a splitting field. Consider an irreducible factor  $g$  of  $f$ , and consider  $K' = L_g = K[T]_{(g)}$ .

Let  $x_1 = T + (g)$ . Then  $g(x_1) = 0$ , so  $f(x_1) = 0$ , hence  $f = (T - x_1)f_1$ , where  $f_1 \in K'[T]$ . By induction, there exists a splitting field  $L$  for  $f_1$  over  $K'$  since  $\deg f_1 < \deg f$ . Let  $x_2, \dots, x_n \in L$  be the roots of  $f_1$  in  $L$ . Then  $f$  splits into linear factors in  $L$  with roots  $x_1, x_2, \dots, x_n$ . Because  $L$  is a splitting field for  $f_1$  over  $K'$ , we have  $L = K'(x_2, \dots, x_n) = K(x_1)(x_2, \dots, x_n) = K(x_1, \dots, x_n)$ , so  $L$  is a splitting field for  $f$ .  $\square$

**Remark.** If  $K \subseteq \mathbb{C}$ , we already know by the fundamental theorem of algebra that any polynomial over  $K$  has a subfield of  $\mathbb{C}$  as its splitting field.

### Theorem 2.14

Let  $f \in K[T]$  be a polynomial and  $L/K$  be a splitting field for  $f$ . Then let  $\sigma: K \rightarrow M$  be a field homomorphism such that  $\sigma f$  splits in  $M[T]$ . Then

- (1)  $\sigma$  can be extended to a homomorphism  $\tau: L \rightarrow M$ ;
- (2) if  $M$  is a splitting field for  $\sigma f$  over  $\sigma K$ , then any  $\tau: L \rightarrow M$  is an isomorphism.

In particular, any two splitting fields are  $K$ -isomorphic.

**Remark.** When constructing the splitting field for a polynomial, we had choice in which irreducible factors to consider first. It is not clear, without this theorem, that two splitting fields have the same degree.

Note that we can have different  $\tau_1, \tau_2: L \rightarrow M$  for splitting fields  $L, M$  of  $f$  over  $K$ .

*Proof.* We will prove (i) by induction on  $[L : K]$ . If  $n = 1$ , we have  $L = K$  and there is nothing to prove. Suppose  $x \in L \setminus K$  is a root of an irreducible factor  $g$  of  $f$  in  $K$ , so  $\deg g > 1$ . Let  $y \in M$  be a root of  $\sigma g \in M[T]$ , which exists because  $\sigma f$  splits in  $M$ . Then, there exists  $\sigma_1: K(x) \rightarrow M$  such that  $\sigma_1(x) = y$ , and  $\sigma_1$  extends  $\sigma$ . Then,  $[L : K(x)] < [L : K]$ , so by induction,  $\sigma_1: K(x) \rightarrow M$  can be extended to  $\tau: L \rightarrow M$ , because  $L$  is a splitting field for  $f$  over  $K(x)$ . This  $\tau$  therefore extends  $\sigma$  as required.

To prove (ii), suppose  $M$  is a splitting field for  $\sigma f$  over  $\sigma K$ . Let  $\tau$  be as in (i), and  $x_i$  be the roots of  $f$  in  $L$ . Then the roots of  $\sigma f$  in  $M$  are  $\tau(x_i)$ . Since  $M$  is a splitting field,  $M = \sigma K(\tau(x_i)) = \tau L$  as  $L = K(x_i)$ . So  $\tau$  is an isomorphism.

If  $K \subseteq M$  and  $\sigma$  is the inclusion homomorphism,  $\tau$  is a  $K$ -isomorphism.  $\square$

### Example 2.15

Let  $f = T^3 - 2 \in \mathbb{Q}[T]$ . This has splitting field  $L = \mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq \mathbb{C}$  where  $\omega = e^{\frac{2\pi i}{3}}$ . We know  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ , but  $\omega \notin \mathbb{R}$  and  $\omega^2 + \omega + 1 = 0$ ,

so  $[L : \mathbb{Q}(\sqrt[3]{3})] = 2$  giving  $[L : \mathbb{Q}] = 6$  by the tower law. In particular, adjoining a single root to  $\mathbb{Q}$  is not enough to generate  $L$ .

### Example 2.16

Let  $f = \frac{T^5-1}{T-1} = T^4 + \cdots + T + 1 \in \mathbb{Q}[T]$ . Let  $z = e^{\frac{2\pi i}{5}}$ , then this is the minimal polynomial of  $z$ . We find  $f = \prod_{1 \leq a \leq 4} (T - z^a)$ , so  $\mathbb{Q}(z)$  is already a splitting field for  $f$  over  $\mathbb{Q}$ , and  $[\mathbb{Q}(z) : \mathbb{Q}] = 4$ .

### Example 2.17

Let  $f = T^3 - 2 \in \mathbb{F}_7[T]$ . This is irreducible because 2 is not a cube in  $\mathbb{F}_7$ . Consider  $L = \mathbb{F}_7[X]/X^3 - 2 = \mathbb{F}_7(x)$ , so  $x^3 = 2$ . Since  $2^3 = 4^3 = 1$  in  $\mathbb{F}_7$ , we have  $(2x)^3 = (4x)^3 = 2$ , so  $x, 2x, 4x$  are roots of  $f$  in  $L$ . In particular,  $L$  is a splitting field for  $f$ , since  $f = (T - x)(T - 2x)(T - 4x)$ ; here, adjoining one root is enough to make  $f$  split.

## 2.3. Normal extensions.

### Definition 2.18

An extension  $L/K$  is a *normal extension* if it is algebraic and for all  $x \in L$ , the minimal polynomial splits in  $L$ .

**Remark.** This condition is equivalent to the statement that for every  $x \in L$ ,  $L$  contains a splitting field for  $x$ . In other words, if an irreducible polynomial  $f \in K[T]$  has a single root in  $L$ , it splits and has all roots in  $L$ .

### Theorem 2.19

Let  $L/K$  be a finite extension. Then  $L$  is normal over  $K$  if and only if  $L$  is a splitting field for some (not necessarily irreducible) polynomial  $f \in K[T]$ .

*Proof.* Suppose  $L$  is normal. Then  $L = K(x_1, \dots, x_n)$  since  $L$  is algebraic. Then the minimal polynomial  $m_{x_i, K}$  of each  $x_i$  over  $K$  splits in  $L$ .  $L$  is generated by the roots of  $\prod_i m_{x_i, K}$ , so  $L$  is a splitting field for  $f$ .

For the converse, suppose  $L$  is a splitting field for  $f \in K[T]$ . Let  $x \in L$ , and let  $g = m_{x, K}$  be its minimal polynomial. We want to show that  $g$  splits in  $L$ . Let  $M$  be a splitting field for  $g$  over  $L$ , and let  $y \in M$  be a root of  $g$ . We want to show  $y \in L$ .

Since  $L$  is a splitting field for  $f$  over  $K$ ,  $L$  is a splitting field for  $f$  over  $K(x)$ , and  $L(y)$  is a splitting field for  $f$  over  $K(y)$ . Now, there exists a  $K$ -isomorphism between  $K(x)$  and  $K(y)$ , because  $x, y$  are roots of the same irreducible polynomial  $g$ . By the uniqueness of splitting fields,  $[L : K(x)] = [L(y) : K(y)]$ . Multiplying by  $[K(x) : K]$ , we find  $[L : K] = [L(y) : K]$  because  $[K(y) : K] = [K(x) :$

$K]$  as they are roots of the same irreducible polynomial. Hence  $[L(y) : L] = 1$ , so  $y \in L$  as required.  $\square$

### Corollary 2.20 (normal closure)

Let  $L/K$  be a finite extension. Then there exists a finite extension  $M/L$  such that  $M/K$  is normal, and if  $L \subseteq M' \subseteq M$  and  $M'/K$  is normal,  $M = M'$ . Moreover, any two such extensions  $M$  are  $L$ -isomorphic.

Such an  $M$  is said to be a *normal closure* of  $L/K$ .

*Proof.* Let  $L = K(x_1, \dots, x_k)$ , and  $f = \prod_{i=1}^k m_{x_i, K} \in K[T]$ . Then let  $M$  be a splitting field of  $f$  over  $L$ . Then, since the  $x_i$  are roots of  $f$ ,  $M$  is also a splitting field for  $f$  over  $K$ . So  $M/K$  is normal.

Let  $M'$  be such that  $L \subseteq M' \subseteq M$  and  $M'/K$  be normal. Then as  $x_i \in M'$ , the minimal polynomial  $m_{x_i, K}$  splits in  $M'$ . So  $M' = M$ .

Any normal extension  $M/K$  must contain a splitting field for  $f$ , and by the minimality condition,  $M$  must be a splitting field. By uniqueness of splitting fields, any two such extensions are  $L$ -isomorphic as required.  $\square$

**2.4. Separable polynomials.** Recall that over  $\mathbb{C}$ , a root  $x$  of a polynomial is said to be a multiple zero when its derivative vanishes at  $x$ . Over arbitrary fields, the same is true, but the analytic concept of derivative must be replaced with an algebraic process.

### Definition 2.21

The *formal derivative* of a polynomial  $f(T) = \sum_{i=0}^d a_i T^i$  is

$$f'(T) = \sum_{i=1}^d i a_i T^{i-1}$$

**Remark.** One can check from the definition that the familiar rules  $(f + g)' = f' + g'$ ,  $(fg)' = f'g + fg'$ , and  $(f^n)' = n f' f^{n-1}$  hold.

### Example 2.22

Consider a field  $K$  of characteristic  $p > 0$ , and let  $f = T^p + a_0$ . Then  $f' = 0$ , so a non-constant polynomial can have a zero derivative.

### Proposition 2.23

Let  $f \in K[T]$ ,  $L/K$  be a field extension, and  $x \in L$  a root of  $f$ . Then  $x$  is a simple root if and only if  $f'(x) \neq 0$ .

*Proof.* We can write  $f = (T - x)g \in L[T]$ . Then  $f' = g + (T - x)g'$ , so  $f'(x) = g(x)$ . In particular,  $f'(x) \neq 0$  if and only if  $(T - x)$  does not divide  $g$ , which is the criterion that  $x$  is a simple root of  $f$ .  $\square$

### Definition 2.24

A polynomial  $f \in K[T]$  is *separable* if it splits into distinct linear factors in a splitting field. Equivalently, it has  $\deg f$  distinct roots.

### Corollary 2.25

$f$  is separable if and only if the greatest common divisor of  $f$  and  $f'$  is 1.

For convenience, we will take  $\gcd(f, g)$  to be the unique monic polynomial  $h$  such that  $(h) = (f, g)$ . Then since  $K[T]$  is a Euclidean domain, we can compute a representation  $h = af + bg$  for polynomials  $a, b$ . Note that  $\gcd(f, g)$  is invariant under a field extension, because Euclid's algorithm does not depend on the ambient field structure.

*Proof.* We can replace  $K$  by a splitting field of  $f$ , so we can factorise  $f$  into a product of linear factors in  $K$ . The two are separable if  $f, f'$  have no common root, which is true if and only if  $\gcd(f, f') = 1$ .  $\square$

### Example 2.26

Let  $K$  have characteristic  $p > 0$ , and let  $f = T^p - b$  for  $b \in K$ . Then  $f' = 0$ , so  $\gcd(f, f') = f \neq 1$ . Hence  $f$  is inseparable. Let  $L$  be an extension of  $K$  containing a  $p$ th root  $a \in L$  of  $b$ , so  $a^p = b$ . Then  $f = (T - a)^p = T^p + (-a)^p = T^p - b$ . In particular,  $f$  has only one root in a splitting field.

If  $b$  is not a  $p$ th power in  $K$ , then  $f$  is irreducible. This is seen on the example sheets.

### Theorem 2.27

Let  $f \in K[T]$  be an irreducible polynomial. Then  $f$  is separable if and only if  $f' \neq 0$ .

In addition, if  $K$  has characteristic zero, every irreducible polynomial  $f \in K[T]$  is separable. If  $K$  has positive characteristic  $p > 0$ , an irreducible polynomial  $f \in K[T]$  is inseparable if and only if  $f(T) = g(T^p)$  for some  $g \in K[T]$ .

*Proof.* Without loss of generality, we can assume  $f$  is monic. Then, since  $f$  is irreducible, the greatest common divisor  $\gcd(f, f')$  is either  $f$  or 1. If  $\gcd(f, f') = f$ , then  $f' = 0$  by considering the degree.

For a polynomial  $f$ , we can write  $f = \sum_{i=0}^d a_i T^i$  and  $f' = \sum_{i=1}^d i a_i T^{i-1}$ , so  $f' = 0$  if and only if  $i a_i = 0$  for all  $1 \leq i \leq d$ . In particular, if  $K$  has characteristic zero, this is true if and only if  $a_i = 0$  for all  $1 \leq i \leq d$ , so  $f = a_0$  is a constant so not irreducible. If  $K$  has characteristic  $p > 0$ , the requirement is that  $a_i = 0$  for all  $i$  not divisible by  $p$ , or equivalently,  $f(T) = g(T^p)$ .  $\square$

## 2.5. Separable extensions.

### Definition 2.28

Let  $L/K$  be a field extension. We say  $x \in L$  is *separable* over  $K$  if  $x$  is algebraic and its minimal polynomial  $f$  is separable over  $K$ .  $L$  is *separable* over  $K$  if all elements  $x$  are separable over  $K$ .

### Theorem 2.29

Let  $x$  be algebraic over  $K$ , and  $L/K$  be an extension in which the minimal polynomial  $m_{x,K}$  splits. Then  $x$  is separable over  $K$  if and only if there are exactly  $\deg x$   $K$ -homomorphisms from  $K(x)$  to  $L$ .

*Proof.* The number of  $K$ -homomorphisms from  $K(x)$  to  $L$  is the number of roots of  $m_{x,K}$  in  $L$ . This is equal to the degree of  $x$  if and only if  $x$  is separable.  $\square$

Let  $\text{Hom}_K(L, M)$  be the set of  $K$ -homomorphisms from  $L$  to  $M$ . Note that not all  $K$ -linear maps from  $L$  to  $M$  are  $K$ -homomorphisms.

### Theorem 2.30 (counting embeddings)

Let  $L = K(x_1, \dots, x_k)$  be a finite extension of  $K$ , so the  $x_i$  are algebraic. Let  $M/K$  be any field extension. Then  $|\text{Hom}_K(L, M)| \leq [L : K]$ , with equality if and only if

- (1) for all  $i$ , the minimal polynomial  $m_{x_i, K}$  splits into linear factors in  $M$ ; and
- (2) all the  $x_i$  are separable over  $K$ .

**Remark.** The conditions (i) and (ii) are equivalent to the statement that  $m_{x_i, K}$  split into distinct linear factors over  $M$ . There is a variant of this theorem: let  $\sigma : K \rightarrow M$  be a field homomorphism, then  $|\text{Hom}_\sigma(L, M)| \leq [L : K]$ , and equality holds if and only if the  $\sigma m_{x_i, K}$  split into distinct linear factors over  $M$ .

*Proof.* We prove this by induction on  $k$ . The case  $k = 0$  is trivial. Let  $K_1 = K(x_1)$  and write  $d = \deg_K x_1 = [K_1 : K]$ . Then the number of  $K$ -homomorphisms from  $K_1$  to  $M$ , denoted  $e = |\text{Hom}_K(K_1, M)|$ , is the number of roots of  $m_{x_1, K}$  in  $M$ . Let  $\sigma : K_1 \rightarrow M$  be a  $K$ -homomorphism. By the inductive hypothesis, there exist at most  $[L : K_1]$  extensions of  $\sigma$  to a  $K$ -homomorphism



$L \rightarrow M$ . Hence the number of  $K$ -homomorphisms from  $L$  to  $M$  is at most  $e[L : K_1] \leq d[L : K_1] = [L : K]$ .

If equality holds, then  $e = d$ , and so  $m_{x_1, K}$  splits into  $d$  distinct linear factors in  $M$ , so (i) and (ii) hold for  $x_1$ . Replacing  $x_1$  with an arbitrary  $x_i$ , one implication follows. Conversely, suppose conditions (i) and (ii) hold. Then, by the previous theorem, there are  $d$  distinct homomorphisms from  $K_1$  to  $M$ . Conditions (i) and (ii) still hold over  $K_1$ , then by induction, each  $\sigma : K_1 \rightarrow M$  has  $[L : K_1]$  extensions to a homomorphism  $L \rightarrow M$ . Hence  $|\text{Hom}_K(L, M)| = [L : K]$  as required.  $\square$

### Theorem 2.31 (separably generated implies separable)

Let  $L = K(x_1, \dots, x_k)$  be a finite extension of  $K$ . Then  $L/K$  is a separable extension if and only if each  $x_i$  is separable over  $K$ .

*Proof.* If  $L/K$  is separable, the  $x_i$  are separable by definition. Suppose the  $x_i$  are separable. Let  $M$  be a normal closure of  $L/K$ , so the splitting field of the product of the  $m_{x_i, K}$  over  $L$ . By the counting embeddings theorem, conditions (i) and (ii) are satisfied so  $|\text{Hom}_K(L, M)| = [L : K]$ . But if  $x \in L$ ,  $L = K(x, x_1, \dots, x_k)$ , so  $x$  is separable.  $\square$

### Corollary 2.32

Let  $x, y \in L$ , and  $L/K$  a field extension. If  $x, y$  are separable over  $K$ , so are  $x + y, xy, x^{-1}$  for  $x \neq 0$ .

*Proof.* Consider the fields  $K(x, y)$  and  $K(x)$ . These are separable extensions of  $K$ . In particular,  $x \in L \mid x$  separable over  $K$  is a subfield of  $L$ .  $\square$

### Theorem 2.33 (primitive element theorem for separable extensions)

Let  $K$  be an infinite field and  $L = K(x_1, \dots, x_k)$  be a finite separable extension. Then there exists  $x \in L$  such that  $L = K(x)$ . In particular,  $x$  is separable over  $K$ .

*Proof.* It suffices to consider the case when  $k = 2$ , because if we can turn  $K(x, y)$  into  $K(z)$  for  $z \in K(x, y)$ , we can perform this inductively. Let  $L = K(x, y)$  with  $x, y$  separable over  $K$ . Let  $n = [L : K]$ , and let  $M$  be a normal closure for  $L/K$ . Then there exist  $n$  distinct  $K$ -homomorphisms  $\sigma_i : L \rightarrow M$ . Let  $a \in K$ , and consider  $z = x + ay$ . We will choose  $a$  such that  $L = K(z)$ .

Since  $L = K(x, y)$ , we have  $\sigma_i(x) = \sigma_j(x)$  and  $\sigma_i(y) = \sigma_j(y)$  implies  $i = j$ . Consider  $\sigma_i(z) =$

$\sigma_i(x) + a\sigma_i(y)$ . If  $\sigma_i(z) = \sigma_j(z)$ , we must have  $(\sigma_i(x) - \sigma_j(x)) + a(\sigma_i(y) - \sigma_j(y)) = 0$ . If  $i \neq j$ , at least one of the parenthesised terms is nonzero. Therefore there is at most one  $a \in K$  such that  $\sigma_i(z) = \sigma_j(z)$ . Since  $K$  is infinite, there exists  $a \in K$  such that all of the  $\sigma_i(z)$  are distinct. But then  $\deg_K z = n$ , so  $L = K(z)$ .  $\square$

### Theorem 2.34

Let  $L/K$  be an extension of finite fields. Then  $L = K(x)$  for some  $x \in L$ .

*Proof.* The multiplicative group  $L^\times$  is cyclic. Let  $x$  be a generator of this group. Then  $L = K(x)$ , since every nonzero element is a power of  $x$ .  $\square$

## 3. GALOIS THEORY

### 3.1. Field automorphisms.

#### Definition 3.1

A bijective homomorphism from a field to itself is called an *automorphism*. The set of automorphisms of a field  $L$  forms a group  $\text{Aut}(L)$  under composition:  $(\sigma\tau)(x) = \sigma(\tau(x))$ . This is called the *automorphism group of  $L$* . Let  $S \subseteq \text{Aut}(L)$ . Then, we define

$$L^S = \{x \in L \mid \forall \sigma \in S, \sigma(x) = x\}$$

This is a subfield of  $L$ , known as the *fixed field of  $S$* , since each  $\sigma$  is a homomorphism.

#### Example 3.2

Let  $L = \mathbb{C}$  and  $\sigma$  be the complex conjugation automorphism. Then the fixed field of  $\sigma$  is  $\mathbb{C}^\sigma = \mathbb{R}$ .

#### Definition 3.3

Let  $L/K$  be a field extension. We define  $\text{Aut}(L/K)$  to be the set of  $K$ -automorphisms of  $L$ , so  $\text{Aut}(L/K) = \{\sigma \in \text{Aut}(L) \mid \forall x \in K, \sigma(x) = x\}$ . Equivalently,  $\sigma \in \text{Aut}(L)$  is an element of  $\text{Aut}(L/K)$  if  $K \subseteq L^\sigma$ .  $\text{Aut}(L/K)$  is a subgroup of  $\text{Aut}(L)$ .

### Theorem 3.4

Let  $L/K$  be a finite extension. Then  $|\text{Aut}(L/K)| \leq [L : K]$ .

*Proof.* Let  $M = L$ , then  $\text{Hom}_K(L, M) = \text{Aut}(L/K)$ , which has at most  $[L : K]$  elements.  $\square$

### Proposition 3.5

If  $K = \mathbb{Q}$  or  $K = \mathbb{F}_q$ ,  $\text{Aut}(K) = 1$ .

*Proof.*  $\sigma(1_K) = 1_K$  hence  $\sigma(n_K) = n_K$ .  $\square$

In particular,  $\text{Aut}(L) = \text{Aut}(L/K)$  where  $K$  is the prime subfield of  $L$ .

**3.2. Galois extensions.** We need to define a notion of when an extension  $L/K$  has ‘many symmetries’.

### Definition 3.6

An extension  $L/K$  is a *Galois extension* if it is algebraic, and  $L^{\text{Aut}(L/K)} = K$ .

**Remark.** If  $x \in L \setminus K$ , there is a  $K$ -automorphism  $\sigma : L \rightarrow L$  such that  $x \neq \sigma(x)$ .

### Example 3.7

$\mathbb{C}/\mathbb{R}$  is a Galois extension, since the fixed field of complex conjugation is  $\mathbb{R}$ . Similarly,  $\mathbb{Q}(i)/\mathbb{Q}$  is a Galois extension.

### Example 3.8

Let  $K/\mathbb{F}_p$  be a finite extension, so  $K$  is a finite field. The Frobenius automorphism of  $K$ , given by  $\varphi_p(x) = x^p$ , has fixed field

$$K^{\varphi_p} = \{x \in K \mid x \text{ a root of } T^p - T\}$$

But since this has at most  $p$  roots, and each element of  $\mathbb{F}_p$  is a root, the fixed field is exactly  $\mathbb{F}_p$ . So  $K^{\text{Aut}(K/\mathbb{F}_p)} = \mathbb{F}_p$ , so this is a Galois extension.

### Definition 3.9

Let  $L/K$  be a Galois extension. We write  $\text{Gal}(L/K)$  for the automorphism group  $\text{Aut}(L/K)$ , called the *Galois group* of  $L/K$ .

### Theorem 3.10 (classification of finite Galois extensions)

Let  $L/K$  be a finite extension, and let  $G = \text{Aut}(L/K)$ , then the following are equivalent.

- (i)  $L/K$  is a Galois extension, so  $K = L^G$ .
- (ii)  $L/K$  is normal and separable.
- (iii)  $L$  is a splitting field of a separable polynomial in  $K$ .
- (iv)  $|\text{Aut}(L/K)| = [L : K]$ .

If this holds, the minimal polynomial of any  $x \in L$  over  $K$  is  $m_{x,K} = \prod_{i=1}^r (T - x_i)$ , where  $x_1, \dots, x_r$  is the orbit of  $G$  on  $x$ .

*Proof.* (i) implies (ii) and the minimal polynomial result. Let  $x \in L$ , and  $x_1, \dots, x_r$  be the orbit of  $G$  on  $x$ . Let  $f = \prod_{i=1}^r (T - x_i)$ . Then  $f(x) = 0$ . Since  $G$  permutes the  $x_i$ , the coefficients of  $f$  are

fixed by  $G$ . By assumption, the coefficients of  $f$  lie in  $K$ , so the minimal polynomial of  $x$  must divide  $f$ . Since  $m_{x,K}(\sigma(x)) = \sigma(m_{x,K}(x)) = 0$ , so every  $x_i$  is a root of the minimal polynomial of  $m_{x,K}$ . So  $f$  is exactly the minimal polynomial as required.  $m_{x,K}$  is a separable polynomial and splits in  $L$ . So  $L/K$  is normal and separable.

(ii) implies (iii). Since splitting fields are normal extensions,  $L$  is a splitting field for some polynomial  $f \in K[T]$ . Write  $f = \prod_{i=1}^r q_i^{e_i}$  where the  $q_i$  are distinct irreducible polynomials, and  $e_i \geq 1$ . Since  $L$  and  $K$  are separable, the  $q_i$  are separable as they are irreducible, so  $g = \prod_{i=1}^r q_i$  is separable and  $L$  is also a splitting field for  $g$ .

(iii) implies (iv). Let  $L = K(x_1, \dots, x_k)$  be the splitting field of a separable polynomial  $f \in K[T]$  with roots  $x_i$ . By the theorem on counting embeddings with  $M = L$ , since  $m_{x_i,K} \mid f$ , conditions (i) and (ii) in the theorem are satisfied, and we find  $|\text{Aut}(L/K)| = |\text{Hom}_K(L, M)| = [L : K]$ .

(iv) implies (i). Suppose  $|\text{Aut}(L/K)| = |G| = [L : K]$ . Note that  $G \subseteq \text{Aut}(L/L^G) \subseteq \text{Aut}(L/K)$ , so these inclusions are both equalities. So  $G = \text{Aut}(L/L^G)$ , so  $[L : K] = |G| \leq [L : L^G]$ . But since  $L^G \supseteq K$ , we must have equality by the tower law.  $\square$

### Corollary 3.11

Let  $L/K$  be a finite Galois extension. Then  $L = K(x)$  for some  $x \in L$  which is separable over  $K$ , and has degree  $[L : K]$ .

*Proof.* By (ii) above,  $L/K$  is separable. Then the primitive element theorem implies that  $L = K(x)$  for some  $x$ .  $\square$

### 3.3. Galois correspondence.

#### Theorem 3.12 (Galois correspondence: part (a))

Let  $L/K$  be a finite Galois extension with  $G = \text{Gal}(L/K)$ . Suppose  $F$  is another field, and  $K \subseteq F \subseteq L$ . Then  $L/F$  is also a Galois extension where  $\text{Gal}(L/F) \leq \text{Gal}(L/K)$ . The map  $F \mapsto \text{Gal}(L/F)$  is a bijection between the set of intermediate fields  $F$  and the set of subgroups of  $G \leq \text{Gal}(L/K)$ . The inverse of this map is  $H \mapsto L^H$ . This bijection reverses inclusions, and if  $F = L^H$ , we have  $[F : K] = (G : H)$ .

*Proof.* Let  $x \in L$ . Then  $m_{x,F} \mid m_{x,K}$  in  $F[T]$ . As  $m_{x,K}$  splits into distinct linear factors in  $L$  so does  $m_{x,F}$ . So  $L/F$  is normal and separable, and hence a Galois extension as required. By definition,  $\text{Gal}(L/F) \leq \text{Gal}(L/K)$ .

To check the map  $F \mapsto \text{Gal}(L/F)$  is a bijection with the given inverse, we first consider a field  $F$ ,

and its image  $L^{\text{Gal}(L/F)}$  under both maps. We have  $L^{\text{Gal}(L/F)} = F$ , since  $L/F$  is Galois as required. Conversely, suppose  $H \leq \text{Gal}(L/F)$ , and consider its image  $\text{Gal}(L/L^H)$ . To show  $\text{Gal}(L/L^H) = H$ , it suffices to show that  $[L : L^H] \leq |H|$ , because certainly  $H \leq \text{Gal}(L/L^H)$  and  $|\text{Gal}(L/L^H)| \leq [L : L^H]$ . By the previous corollary,  $L = L^H(x)$  for some  $x$ , and  $f = \prod_{\sigma \in H} (T - \sigma(x)) \in L^H[T]$  is a polynomial with  $x$  as a root. In particular,  $[L : L^H] = \deg_{L^H}(x) \leq \deg f = |H|$ . So we have a bijection as claimed.

Suppose  $F \subseteq F'$  are fields between  $K$  and  $L$ . Then  $\text{Gal}(L/F') \subseteq \text{Gal}(L/F)$ , so the bijection reverses inclusions. Finally, if  $F = L^H$ , we have  $[F : K] = \frac{[L : K]}{[L : F]} = \frac{|\text{Gal}(L/K)|}{|\text{Gal}(L/F)|} = \frac{|G|}{|H|} = (G : H)$ .  $\square$

### Theorem 3.13 (Galois correspondence: part (b))

Let  $H \leq G$  be a subgroup of a Galois group  $G = \text{Gal}(L/K)$ . Then  $\sigma H \sigma^{-1}$  corresponds to the field  $\sigma L^H$ .

*Proof.* Under the Galois correspondence,  $\sigma H \sigma^{-1}$  corresponds to its fixed field

$$L^{\sigma H \sigma^{-1}} = \{x \in L \mid \sigma \tau \sigma^{-1}(x) = x \text{ for all } \tau \in H\}$$

Note that  $\sigma \tau \sigma^{-1}(x) = x$  if and only if  $\tau \sigma^{-1}(x) = \sigma^{-1}(x)$ , so  $\tau(y) = y$  for  $x = \sigma(y)$ . Hence  $x \in L^{\sigma H \sigma^{-1}}$  if and only if there exists  $y \in L^H$ ,  $x = \sigma(y)$ . Therefore  $L^{\sigma H \sigma^{-1}} = \sigma L^H$  as required.  $\square$

### Theorem 3.14 (Galois correspondence: part (c))

Let  $H \leq G = \text{Gal}(L/K)$ . Then the following are equivalent.

- (1)  $L^H/K$  is Galois;
- (2)  $L^H/K$  is normal;
- (3) for all  $\sigma \in G$ ,  $\sigma L^H = L^H$ ;
- (4)  $H$  is a normal subgroup of  $G$ .

If so,  $\text{Gal}(L^H/K) = \text{Gal}(L/K)_H = G/H$ .

*Proof.* (i) and (ii) are equivalent.  $L/K$  is separable since it is Galois. So  $L^H/K$  is also separable.

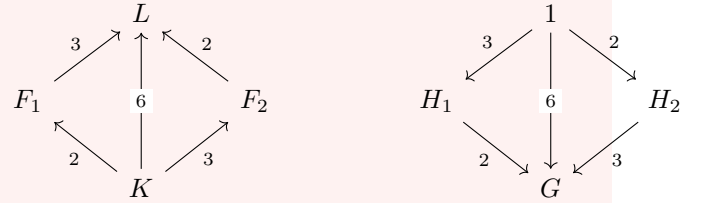
(iii) and (iv) are equivalent. Let  $F = L^H$ , and let  $x \in F$ . Then the set of roots of  $m_{x,K}$  is the orbit of  $x$  under  $G$ , so the minimal polynomial splits in  $F$  if and only if for all  $\sigma \in G$ ,  $\sigma(x) \in F$ . As this holds for all  $x \in F$ ,  $F$  is normal if and only if  $\sigma F \subseteq F$ . Since  $[\sigma F : K] = [F : K]$ , as  $F$  and  $\sigma F$  are  $K$ -isomorphic, this holds if and only if  $\sigma F = F$ . By part (b) of the Galois correspondence, this is equivalent to the statement that  $\sigma H \sigma^{-1} = H$  for all  $\sigma$ , so  $H$  is normal.

If any of the above hold, for all  $\sigma \in G$ , we have  $\sigma F = F$ , so we have homomorphisms  $G \rightarrow \text{Gal}(F/K)$  given by the restriction of  $\sigma \in G$  to  $F$ . Its kernel is  $H$ . Then from the isomorphism theorem,  $G/H$  is isomorphic to a subgroup of  $\text{Gal}(F/K)$ . This must be an isomorphism because  $[F : K] = (G : H)$ .  $\square$

### Example 3.15

Let  $K = \mathbb{Q}$  and  $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$  where  $\omega = e^{\frac{2\pi i}{3}}$ .  $L$  is a splitting field for  $T^3 - 2$  with  $[L : \mathbb{Q}] = 6$ . Since  $T^3 - 2$  is a separable polynomial,  $L$  is the splitting field of a separable polynomial and hence Galois. Therefore  $G = \text{Gal}(L/\mathbb{Q})$  has order 6.

We have the subfields  $F_1 = \mathbb{Q}(\omega)$ ,  $F_2 = \mathbb{Q}(\sqrt[3]{2})$ , where  $[F_1 : \mathbb{Q}] = 2$  and  $[F_2 : \mathbb{Q}] = 3$ . In the following diagram, the arrows on the left hand side are annotated with the degrees of an extensions, and the arrows on the right hand side are labelled with the index of the relevant subgroup.



By the classification of finite groups of order 6,  $G$  is isomorphic either to  $C_6$  or  $S_3$ .  $F_2 = \mathbb{Q}(\sqrt[3]{2})$  is not a normal extension of  $\mathbb{Q}$ , because  $\omega \sqrt[3]{2} \notin F_2$ . So  $H_2$  is not a normal subgroup of  $G$ . Since all subgroups of abelian groups are normal,  $G$  is not abelian. So  $G \cong S_3$ . Hence  $H_1 \cong A_3$ , and  $H_2$  is a transposition, but since all subgroups generated by transpositions are conjugate, we can set  $H_2 = \langle (1\ 2) \rangle$ .

The other two subgroups are conjugate to  $H_2$ , corresponding to the subfields  $\sigma F_2$  where  $\sigma \in G$ . Hence, these subfields are exactly  $\mathbb{Q}(\omega \sqrt[3]{2})$  and  $\mathbb{Q}(\omega^2 \sqrt[3]{2})$ , since the conjugates of  $\sqrt[3]{2}$  are exactly the roots of the minimal polynomial. Note that since these are the only subgroups, we have found all intermediate fields between  $\mathbb{Q}$  and  $\mathbb{Q}(\sqrt[3]{2}, \omega)$ .

There is an easier way to prove  $G \cong S_3$ . Consider a separable polynomial  $f \in K[T]$ , and its roots  $x_1, \dots, x_n$  in a splitting field  $L$ . Then  $G = \text{Gal}(L/K)$  permutes the  $x_i$ , because  $f(\sigma x_i) = \sigma f(x_i) = 0$ . If  $\sigma(x_i) = x_i$  for all  $i$ , since  $L = K(x_1, \dots, x_n)$ ,  $\sigma$  must be the identity map. This gives an injective homomorphism from  $G$  into  $S_n$ . So  $G$  is isomorphic to a subgroup of  $S_n$ . In our example above,  $|G| = 6$  and  $G$  is isomorphic to a subgroup of  $S_3$ , so  $G \cong S_3$ .

### 3.4. Galois groups of polynomials.

**Definition 3.16**

Let  $f \in K[T]$ , and let  $L$  be a splitting field for  $f$ .

There is an action of  $\text{Gal}(L/K)$  on the set of roots of  $f$  in  $L$ . If  $f$  has  $n$  roots, this action induces a subgroup of permutations of roots  $\text{Gal}(f/K) \leq S_n$ , called the *Galois group of  $f$  over  $K$* .

**Remark.** Note that  $[L : K] = |\text{Gal}(L/K)| = |\text{Gal}(f/K)| \mid n!$ .

There exist several methods for finding the Galois group for a particular polynomial.

**Proposition 3.17**

$f \in K[T]$  is irreducible if and only if  $\text{Gal}(f/K)$  is *transitive*, so for all  $i, j \in 1, \dots, n$ , there exists  $\sigma \in \text{Gal}(f/K)$  such that  $\sigma(i) = j$ .

**Remark.** A subgroup of  $S_n$  is transitive if and only if there is exactly one orbit.

*Proof.* Let  $x$  be a root of  $f$  in a splitting field  $L$ . Then its orbit under  $G = \text{Gal}(f/K)$  is exactly the set of roots of  $m_{x,K}$ . Since  $m_{x,K}$  is an irreducible factor of  $f$ ,  $m_{x,K} = f$  if and only if  $f$  is irreducible. Conversely,  $m_{x,K} = f$  if and only if each root of  $f$  is in the orbit of  $x$ , which is exactly the statement that  $G$  acts transitively on the roots of  $f$ .  $\square$

**Remark.** If  $G \subseteq S_n$  is transitive, by the orbit-stabiliser theorem,  $n \mid |G|$ .

Recall that for a monic polynomial  $f = \prod_{i=1}^n (T - x_i)$ , the *discriminant* of  $f$  is  $\text{Disc}(f) = \Delta^2 \in K$ , where  $\Delta = \prod_{i < j} (x_i - x_j)$ . The discriminant is nonzero if and only if  $f$  is separable.

**Proposition 3.18**

Let  $\text{char } K \neq 2$ , and let  $f \in K[T]$  be a monic polynomial with splitting field  $L$ . Let  $G = \text{Gal}(f/K)$ . Then the fixed field of  $G \cap A_n$  is  $K(\Delta)$ , where  $\Delta^2$  is the discriminant. In particular,  $\text{Gal}(f/K) \subseteq A_n$  if and only if the discriminant  $\text{Disc}(f)$  is a square.

*Proof.* Let  $\pi \in S_n$ . The sign of the permutation is given by  $\prod_{i < j} (T_{\pi(i)} - T_{\pi(j)}) = \text{sgn } \pi \prod_{i < j} (T_i - T_j)$ . Hence, if  $\sigma \in G$ , we have  $\sigma(\Delta) = \text{sgn } \sigma \cdot \Delta$ . Because the characteristic is not 2,  $-1 \neq 1$ . Since  $\Delta \neq 0$ , this implies  $\Delta \in K$  if and only if  $G \subseteq A_n$ , and  $\Delta$  lies in the fixed field  $F$  of  $G \cap A_n$ . Because  $[F : K] = (G : G \cap A_n) \in 1, 2$ ,  $F = K(\Delta)$  exactly.  $\square$

**Example 3.19**

Let  $n = 3$ ,  $f = T^3 + aT + b = \prod_{i=1}^3 (T - x_i)$  where  $x_i$  lie in a splitting field for  $f$ . Since there is no  $T^2$  term,  $x_3 = -x_1 - x_2$ . Hence,  $a = x_1x_2 - (x_1 + x_2)^2$ , and  $b = x_1x_2(x_1 + x_2)$ . Therefore,

$$\text{Disc}(f) = [(x_1 - x_2)(2x_1 + x_2)(x_1 + 2x_2)]^2 = -4a^3 - 27b^2$$

In particular,  $\text{Gal}(f/K) \subseteq A_3$  if and only if  $-4a^3 - 27b^2$  is a square in  $K$ .

For example, consider  $f = T^3 - 21T - 7 \in \mathbb{Q}[T]$ . This is irreducible by Eisenstein's criterion. Its discriminant is  $4 \cdot 21^3 - 27 \cdot 7^2 = (27 \cdot 7)^2$ , which is a square. So  $\text{Gal}(f/K) \subseteq A_3$ . Since  $f$  is irreducible,  $\text{Gal}(f/K)$  is transitive, so its order is divisible by 3. So  $\text{Gal}(f/K)$  must be exactly  $A_3$ .

**Remark.** This technique can be used to calculate the Galois group of any cubic polynomial for characteristic not 2, 3, for example.

#### 4. FINITE FIELDS

**4.1. Construction of finite fields.** Every finite field has characteristic  $p > 0$ , and so it can be regarded as a field extension of  $\mathbb{F}_p$ . We will classify every finite field and study their Galois theory. Recall that, for a finite field  $F$  of characteristic  $p$ ,

- (1)  $|F| = p^n$ , where  $[F : \mathbb{F}_p] = n$ ;
- (2)  $F^\times$  is cyclic, of order  $p^n - 1$ ;
- (3) The Frobenius automorphism  $\varphi_p: F \rightarrow F$  given by  $x \mapsto x^p$  is an automorphism of  $F$ .

##### Theorem 4.1

Let  $p$  be a prime, and  $n \geq 1$ . Then there is a finite field with  $q = p^n$  elements. Any such field is a splitting field of the polynomial  $f = T^q - T$  over  $\mathbb{F}_p$ . Since splitting fields are unique up to  $\mathbb{F}_p$ -isomorphism, any two finite fields of the same order are isomorphic.

*Proof.* Let  $F$  be a field with  $q = p^n$  elements. Then if  $x \in F^\times$ ,  $x^{q-1} = 1$ . Hence, for all  $x \in F$ ,  $x^q = x$ . In particular,  $f$  has  $q$  distinct roots in  $F$ , which are all of the elements of  $F$ . So  $f$  splits into linear factors in  $F$ , and not in any proper subfield, so  $F$  is indeed a splitting field for  $f$  as required.

Now, we wish to explicitly construct such a field. Let  $L$  be a splitting field for  $f = T^q - T$  over  $\mathbb{F}_p$ . Let  $F \subseteq L$  be the fixed field of  $\varphi_p^n$ , the map  $x \mapsto x^q$ . So  $F$  is the set of roots of  $f$  in  $L$ . So  $|F| = q$ . Therefore,  $L = F$  because  $F$  has  $q$  elements, using the above argument.  $\square$

Now that we have shown isomorphism, we simply write  $\mathbb{F}_q$  for any finite field of  $q$  elements. There is no canonical finite field of a given order in general.

#### 4.2. Galois theory of finite fields.

##### Theorem 4.2

The extension  $\mathbb{F}_{p^n}/\mathbb{F}_p$  is Galois, and the Galois group is cyclic of order  $n$ , generated by the Frobenius automorphism  $\varphi_p$ .

*Proof.* Since  $\mathbb{F}_{p^n}$  is the splitting field of the separable polynomial  $T^{p^n} - T$ , the extension is Galois. Let  $G \leq \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$  be the subgroup generated by  $\varphi_p$ . Then  $\mathbb{F}_{p^n}^G = \{x \mid x^p = x\} = \mathbb{F}_p$ , so by the Galois correspondence,  $G$  must be the entire group  $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ .  $\square$

##### Theorem 4.3

$\mathbb{F}_{p^n}$  has a unique subfield of order  $p^m$  for all  $m \mid n$ , and no others. If  $m \mid n$ , then  $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$  is the fixed field of  $\varphi_p^m$ .

*Proof.* By the Galois correspondence, it suffices to check the subgroups of  $\mathbb{Z}/n\mathbb{Z}$ . The subgroups of  $\mathbb{Z}/n\mathbb{Z}$  are  $m\mathbb{Z}/n\mathbb{Z}$  for  $m \mid n$ . Hence, the subfields of  $\mathbb{F}_{p^n}$  are the fixed fields of the subgroups  $\langle \varphi_p^m \rangle$ , which have degree equal to the indices  $(\mathbb{Z}/n\mathbb{Z} : m\mathbb{Z}/n\mathbb{Z}) = m$ .  $\square$

**Remark.** If  $m \mid n$ ,  $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \varphi_p^m \rangle$ , which has order  $\frac{n}{m}$ .

##### Theorem 4.4

Let  $f \in \mathbb{F}_p[T]$  be separable, and let  $n = \deg f$ . Suppose the irreducible factors of  $f$  have degrees  $n_1, \dots, n_r$ , so  $\sum_{i=1}^r n_i = n$ . Then  $\text{Gal}(f/\mathbb{F}_p) \subseteq S_n$  is cyclic and generated by an element of cycle type  $(n_1, \dots, n_r)$ . In particular,  $|\text{Gal}(f/\mathbb{F}_p)|$  is the least common multiple of the  $n_i$ .

Recall that  $\pi \in S_n$  has cycle type  $(n_1, \dots, n_r)$  if it is a product of  $r$  disjoint cycles  $\pi_i$ , each with length  $n_i$ .

*Proof.* Let  $L$  be a splitting field for  $f$  over  $\mathbb{F}_p$ . Consider  $x_1, \dots, x_n \in L$ . Then  $\text{Gal}(L/\mathbb{F}_p)$  is cyclic and generated by  $\varphi_p$ . As the irreducible factors  $g_i$  of  $f$  are the minimal polynomials of the  $x_i$ , and the roots of the minimal polynomial of  $x_i$  are precisely the orbit of  $\varphi_p$  on  $x_i$ , the cycle type must be as required. The order of any such permutation is the lowest common multiple of the lengths of the cycles.  $\square$

#### 4.3. Reduction modulo a prime.

##### Theorem 4.5

Let  $f \in \mathbb{Z}[T]$  be a monic separable polynomial with  $\deg f = n$ , and let  $p$  be a prime. Suppose that the reduction  $\bar{f} \in \mathbb{F}_p[T]$  of  $f$  is also separable. Then  $\text{Gal}(\bar{f}/\mathbb{F}_p) \leq \text{Gal}(f/\mathbb{Q})$  as subgroups of  $S_n$ .

**Remark.** The identification of  $\text{Gal}(f/\mathbb{Q})$  with a subgroup of  $S_n$  depends on the choice of ordering of the roots of  $f$ . Choosing a different ordering corresponds to conjugation of  $\text{Gal}(f/\mathbb{Q})$  in  $S_n$ . The meaning of the



statement  $\text{Gal}(\bar{f}/\mathbb{F}_p) \leq \text{Gal}(f/\mathbb{Q})$  therefore means that  $\text{Gal}(\bar{f}/\mathbb{F}_p)$  is conjugate to a subgroup of  $\text{Gal}(f/\mathbb{Q})$  in  $S_n$ , not that it is exactly a subgroup.

The following proof is based in algebraic number theory; alternatives are available. The proof is not examinable.

*Proof.* Let  $L = \mathbb{Q}(x_1, \dots, x_n)$  be a splitting field for  $f$ , where the  $x_i$  are the roots of  $f$ . Let  $N = [L : \mathbb{Q}]$ . Consider  $R = \mathbb{Z}[x_1, \dots, x_n]$ . Since  $f(x_i) = 0$  and  $f$  is monic, every element of  $R$  is a  $\mathbb{Z}$ -linear combination of  $x_1^{a_1}, \dots, x_n^{a_n}$  where the  $a_i < n$  by using  $f$  to reduce the degrees. So  $R$  is finitely-generated as a  $\mathbb{Z}$ -module, or equivalently, as an abelian group.  $R$  is contained inside  $L \simeq \mathbb{Q}^N$ .  $R$  is torsion-free, so  $R \simeq \mathbb{Z}^M$  with  $M \leq N$  (in fact,  $M = N$ ).

Then  $\bar{R} = R/pR$  has  $p^M$  elements. Let  $\bar{P}$  be a maximal ideal for  $\bar{R}$ , which corresponds to an ideal  $P$  of  $R$  that contains  $pR$ . Then  $F = R/P \simeq \bar{R}/\bar{P}$  (by the isomorphism theorem) is a finite field with  $p^d$  elements for some  $d$ . Since  $R$  is generated by  $x_1, \dots, x_n$ ,  $F$  is generated by  $\bar{x}_1, \dots, \bar{x}_n$ , where  $\bar{x}_i = x_i + P \in F$ . In particular,  $\bar{f} = \prod_{i=1}^n (T - \bar{x}_i)$ . Since  $\bar{f}$  is separable, the  $\bar{x}_i$  are distinct, and  $F$  is a splitting field for  $\bar{f}$ .

Let  $G = \text{Gal}(f/\mathbb{Q})$ . Then  $G$  maps  $R$  to  $R$  since it permutes the  $x_i$ . Let  $H \leq G$  be the stabiliser of  $P$ , so  $H = \sigma \in G \mid \sigma P = P$ . Since  $H$  fixes  $P$ ,  $H$  acts on the quotient  $R/P = F$ , and it permutes the  $\bar{x}_i$  in the same way as it permutes the  $x_i$ . In particular, there is an injective homomorphism from  $H$  into  $\text{Gal}(F/\mathbb{F}_p)$ . It now suffices to show that this homomorphism is an isomorphism.

Let  $P = P_1, P_2, \dots, P_r$  be the orbit of  $P$  under  $G$ , so  $P_i = \sigma P$  for some  $\sigma \in G$ . These are all maximal ideals since  $P$  is, and  $R/P_i \simeq R/P$  so each  $R/P_i$  have  $p^d$  elements. The  $P_i$  are maximal, so  $P_i + P_j = R$  if  $i \neq j$ . So by the Chinese remainder theorem for rings,

$$R/(P_1 \cap \dots \cap P_k) \simeq R/P_1 \times \dots \times R/P_r$$

As  $p \in P_1, pR \subseteq P_1 \cap \dots \cap P_r$ . So

$$p^N \geq p^M = |R/pR| \geq |R/(P_1 \cap \dots \cap P_r)| = \prod_{i=1}^r |R/P_i|$$

Now, by the orbit-stabiliser theorem,  $r = (G : H) = \frac{N}{|H|}$ . Since  $H$  injects into  $\text{Gal}(F/\mathbb{F}_p)$ , we have  $|H| \leq d$  with equality if and only if the injection is an isomorphism. So  $N \leq rd$ , but since  $N \geq rd$ , we must have  $N = rd$ , so the injection is an isomorphism, and  $H \simeq \text{Gal}(\bar{f}/\mathbb{F}_p)$ .  $\square$

#### Corollary 4.6

Let  $f \in \mathbb{Z}[T]$  be monic and separable with  $p$  a

prime such that  $\bar{f} \in \mathbb{F}_p[T]$  is separable. Consider the factorisation into irreducibles  $\bar{f} = g_1 \dots g_r \in \mathbb{F}_p[T]$ , where  $\deg g_i = n_i$ . Then  $\text{Gal}(f/\mathbb{Q})$  contains an element of cycle type  $(n_1, \dots, n_r)$ .

*Proof.* Combine the previous two theorems.  $\square$

#### Example 4.7

Let  $f = T^4 - 3T + 1$ . Consider  $p = 2$ . In  $\mathbb{F}_2$ ,  $f = T^4 + T + 1$ . This does not have a root, and not divisible by  $T^2 + T + 1$  which is the only irreducible quadratic, so it is irreducible.

Now, consider  $p = 5$ . In  $\mathbb{F}_5$ ,  $f = (T + 1)(T^3 - T^2 + T + 1)$ , which is a factorisation into irreducibles.

By the above corollary,  $\text{Gal}(f/\mathbb{Q})$  has a 4-cycle and a 3-cycle. In particular,  $12 \mid |\text{Gal}(f/\mathbb{Q})|$ , so the group is either all of  $S_4$  or it is  $A_4$ , as this is the unique index 2 subgroup of  $S_4$ . But 4-cycles are odd, so do not lie in  $A_4$ . So  $\text{Gal}(f/\mathbb{Q}) = S_4$ .

Note that if  $\bar{f}$  is separable,  $\text{Disc}(\bar{f}) \neq 0$ , so  $p \nmid \text{Disc}(\bar{f})$  so  $f$  is separable. If  $f$  is separable, then  $\bar{f}$  is separable for all primes but the finite set of primes dividing  $\text{Disc}(f)$ .

**Remark.** If  $\text{Gal}(f/\mathbb{Q})$  contains an element of cycle type  $(n_1, \dots, n_r)$ , it can in fact be shown that there exist infinitely many primes  $p$  such that  $\bar{f}$  factors into irreducibles of degrees  $n_1, \dots, n_r$  in  $\mathbb{F}_p$ . This is known as the Chebotarev density theorem, which is a generalisation of Dirichlet's theorem on primes in arithmetic progression. However, the proof is far outside the scope of this course.

### 5.1. CYCLOTOMIC AND KUMMER EXTENSIONS

#### Lemma 5.1

Let  $C$  be a cyclic group of order  $n > 1$ . Let  $a \in \mathbb{Z}$  be coprime with  $n$ , also written  $(a, n) = 1$ . Then the map  $[a]: C \rightarrow C$  given by  $[a](g) = g^a$  is an automorphism of  $C$ , and the map  $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(C)$  defined by  $a \mapsto [a]$  is an isomorphism.

*Proof.*  $[a]$  is clearly a homomorphism, and since  $a$  is coprime to  $n$ , it is an automorphism since there exists  $b$  such that  $ab$  is congruent to 1 modulo  $n$ . Hence, there is an injection  $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(C)$  given by  $a \mapsto [a]$ , and it is a homomorphism. If  $\varphi \in \text{Aut}(C)$  and  $g$  is a generator for  $C$ ,  $\varphi(g) = g^a$  for some  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ . So  $\varphi = [a]$ , and in particular, the map is an isomorphism.  $\square$

Let  $K$  be a field and  $n \geq 1$ . We define  $\mu_n(K) = \{x \in K \mid x^n = 1\}$  for the group (under multiplication) of  $n$ th roots of unity in  $K$ . This is a finite subgroup of  $K^\times$ ,

hence it is cyclic. The order of any element divides  $n$ , so it has order dividing  $n$ .

We say that  $\zeta \in \mu_n(K)$  is a *primitive*  $n$ th root of unity if its order is exactly  $n$ . Such a  $\zeta$  exists if and only if  $\mu_n(K)$  has  $n$  elements, and then  $\zeta$  is a generator for the group. In particular,  $f = T^n - 1$  has  $n$  distinct roots,  $\zeta^i$  for  $i \in 0, \dots, n-1$ , and hence it is separable. In general,  $f = T^n - 1$  is separable if and only if  $f$  is coprime with  $f' = nT^{n-1}$ , which holds if and only if  $n \neq 0$ . In this section, we assume that the characteristic of  $K$  is zero or is a positive number  $p$  that does not divide  $n$ , so  $f$  is separable.

Let  $L/K$  be a splitting field for  $T^n - 1$ . This is Galois since  $f$  is separable, so we can define  $G = \text{Gal}(L/K)$ . Then  $|\mu_n(L)| = n$ , and so there exists a primitive  $n$ th root of unity  $\zeta = \zeta_n \in L$ . Such an  $L$  is called a *cyclotomic extension*.

### Proposition 5.2

$L = K(\zeta)$ . There exists an injective homomorphism  $\chi = \chi_n: \text{Gal}(L/K) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$  such that  $\chi(\sigma) = a$  implies  $\sigma(\zeta) = \zeta^a$ . In particular,  $G$  is abelian.  $\chi$  is an isomorphism if and only if  $G$  acts transitively on the set of primitive roots of unity in  $L$ .

The homomorphism  $\chi$  is called the *cyclotomic character*.

*Proof.*  $\mu_n(L)$  is cyclic and generated by  $\zeta$ , so the roots of  $T^n - 1$  are the powers of  $\zeta$ , so  $L = K(1, \zeta, \zeta^2, \dots, K(\zeta))$ . Consider the action of  $G$  on  $L$ . This action permutes  $\mu_n(L)$ , and if  $\zeta, \zeta' \in \mu_n(L)$  and  $\sigma \in G$ , then  $\sigma(\zeta\zeta') = \sigma(\zeta)\sigma(\zeta')$ , so  $\sigma$  acts as an automorphism of  $\mu_n(L)$ .  $\sigma(\zeta) = \zeta$  if and only if  $\sigma$  is the identity because  $L = K(\zeta)$ . This gives an injective homomorphism  $G \hookrightarrow \text{Aut}(\mu_n(L)) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ .

$\zeta_n^a$  is primitive if and only if  $a$  is coprime to  $n$ . Therefore the set of primitive  $n$ th roots of unity is  $\zeta^a \mid a \in (\mathbb{Z}/n\mathbb{Z})^\times$ , which by the previous part, is the orbit of  $\zeta$  under  $G$ . The map is surjective if and only if there is one orbit, so the result follows.  $\square$

## 5.2. Cyclotomic polynomials.

### Definition 5.3

Let  $K$  have characteristic zero or a prime  $p$  that does not divide  $n$ . The  *$n$ th cyclotomic polynomial* is

$$\Phi_n(t) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (T - \zeta_n^a)$$

in a splitting field  $L$  of  $T^n - 1$ .

This is the polynomial where the roots are the primitive  $n$ th roots of unity. As  $G$  permutes the primitive  $n$ th roots of unity in  $L$ ,  $\Phi_n$  has coefficients in  $L^G = K$ . The last part of the above proposition shows that  $\chi$  is surjective if and only if  $\Phi_n \in K[T]$  is irreducible.

$x \in L$  satisfies  $x^n - 1 = 0$  if and only if  $x$  is a primitive  $d$ th root of unity for some unique  $d \mid n$ . Hence  $T^n - 1 = \prod_{d \mid n} \Phi_d$ , since the sets of roots are equal. In particular, we could have inductively defined the cyclotomic polynomials by  $\Phi_n = \frac{T^n - 1}{\prod_{d \mid n, d \neq n} \Phi_d}$ . This shows that the  $\Phi_n$  do not depend on the choice of field  $K$ , since  $\Phi_n$  is the image in  $K[T]$  of a polynomial in  $\mathbb{Z}[T]$ .

For example,  $\Phi_p = \frac{T^p - 1}{T - 1} = T^{p-1} + T^{p-2} + \dots + T + 1$ . We also have  $\Phi_1 = T - 1$  and  $\Phi_{p^n}(T) = \frac{T^{p^n} - 1}{T^{p^{n-1}} - 1} = \Phi_p(T^{p^{n-1}})$ . We have  $\deg \Phi_n = \left| (\mathbb{Z}/n\mathbb{Z})^\times \right| = \varphi(n)$  where  $\varphi$  is the Euler totient function.

### Theorem 5.4 (rationals)

Let  $K = \mathbb{Q}$ . Then  $\chi_n$  is an isomorphism for all  $n > 1$ . In particular,  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ , and  $\Phi_n$  is irreducible over  $\mathbb{Q}$ .

*Proof.* The statements in the theorem are all equivalent by the previous results, so it suffices to prove that  $\Phi_n$  is irreducible over  $\mathbb{Q}$ . If  $n$  is prime, we have already proven its irreducibility by Eisenstein's criterion and Gauss' lemma. We can easily extend this to the case where  $n$  is a prime power.

Note that  $\chi_n$  is an isomorphism if for all primes  $p \nmid n$ , the residue class of  $p \in (\mathbb{Z}/n\mathbb{Z})^\times$  is in the image of  $\chi$ , by factorising  $a$  as a product of primes if  $a$  is coprime to  $n$ . Let  $f$  be the minimal polynomial of  $\zeta$  over  $\mathbb{Q}$ , and let  $g$  be the minimal polynomial of  $\zeta^p$  over  $\mathbb{Q}$ . If  $f = g$ , then  $\zeta^p$  lies in the orbit of  $\text{Gal}(L/K)$  on  $\zeta$ , so  $p$  lies in the image of  $\chi$  as required. Otherwise,  $f$  and  $g$  are coprime, and they divide  $T^n - 1$  so  $fg \mid T^n - 1$ . As  $\zeta$  is a root of  $g(T^p)$ , we have  $f \mid g(T^p)$ . Reducing modulo  $p$ ,  $\bar{f} \in \mathbb{F}_p[T]$  divides  $\bar{g}(T^p) \in \mathbb{F}_p[T]$ . But since we are working over  $\mathbb{F}_p$ ,  $\bar{g}(T^p) = \bar{g}(T)^p$ . Now,  $\bar{f}$  and  $\bar{g}$  divide  $T^n - 1$  in  $\mathbb{F}_p[T]$ , which is separable because  $p \nmid n$ . So  $\bar{f} \mid \bar{g}^p$ , so  $\bar{f} \mid \bar{g}$ . But then  $\bar{f}^2 \mid \bar{f}\bar{g} \mid T^n - 1$ , contradicting separability of  $T^n - 1$ .  $\square$

Therefore, the minimal polynomial of  $e^{\frac{2\pi i}{n}}$  over  $\mathbb{Q}$  is  $\Phi_n$ .

### Theorem 5.5 (finite fields)

Let  $K = \mathbb{F}_p$ , and let  $n$  be coprime to  $p$ . Let  $L$  be a splitting field for  $T^n - 1$ . Then  $\chi_n$  is an isomorphism from  $\text{Gal}(L/K)$  to  $\langle p \rangle \leq (\mathbb{Z}/n\mathbb{Z})^\times$ , the subgroup generated by the residue class of  $p$ , and  $\chi_n(\varphi_p) = p \bmod n$  where  $\varphi_p$  is the Frobenius endomorphism  $x \mapsto x^p$ , which is a generator of  $\text{Gal}(L/K)$ . Further,  $[L : K] = r$ , where  $r$  is the order of  $p$  modulo  $n$ . Finally,  $\varphi_p$  has cycle type  $(r, \dots, r)$  acting as a permutation of the roots of the cyclotomic polynomial  $\Phi_n$ , which are the primitive  $n$ th roots of unity.

*Proof.* Since  $\varphi_p(\zeta) = \zeta^p$  and  $L = K(\zeta)$ , by definition of  $\chi_n$ , we have  $\chi_n(\varphi_p) = p$ , or more precisely,  $p \bmod n$ . In particular,  $\chi_n(G) = \langle p \rangle$ , and as this is a Galois extension,  $[L : K] = |G| = |\langle g \rangle| = r$ . For the last part, notice that if  $a$  and  $n$  are coprime,  $\varphi_p^k(\zeta^a) = \zeta^a$  holds if and only if  $\varphi_p^k(\zeta) = \zeta$ , or equivalently,  $r \mid k$ . So the orbits of  $\varphi_p$  on the set  $\zeta_n^a \mid (a, n) = 1$ , which is the set of roots of  $\Phi_n$ , all have length  $r$ .  $\square$

**Remark.** This almost gives another proof of the irreducibility of the cyclotomic polynomials  $\Phi_n$  over  $\mathbb{Q}$ . By reduction modulo  $p$ ,  $\text{Gal}(\Phi_n/\mathbb{Q})$  contains  $\text{Gal}(\Phi_n/\mathbb{F}_p)$  as a subgroup, up to conjugacy by elements of  $S_{\varphi(n)}$ . It is not difficult to show that in fact  $\chi_n(\text{Gal}(\Phi_n/\mathbb{Q})) \supseteq \chi_n(\text{Gal}(\Phi_n/\mathbb{F}_p)) = \langle p \rangle$ . As this holds for all primes  $p$  not dividing  $n$ ,  $\chi_n(\text{Gal}(\Phi_n/\mathbb{Q})) = (\mathbb{Z}/n\mathbb{Z})^\times$ .

**Remark.** The last part of the above theorem implies that over  $\mathbb{F}_p$ , the cyclotomic polynomial  $\Phi_n$  factors as a product of irreducibles of degree  $r$ . This depends only on the value of  $p$  modulo  $n$ . In general, for a polynomial with integer coefficients  $f \in \mathbb{Z}[T]$ , its factorisation modulo  $p$  does not follow an obvious pattern.

Answering this question is part of the Langlands programme, a large area of research in modern number theory. The case where there is such a congruence pattern turns out to be when  $\text{Gal}(f/\mathbb{Q})$  is abelian. This study is known as class field theory, which is studied in Part III.

**5.3. Quadratic reciprocity.** The following theorem is from Part II Number Theory. This theorem has several hundred proofs, and this particular one follows from the above theory on cyclotomic polynomials.

Let  $p$  be an odd prime and  $a$  an integer coprime to  $p$ . Then the *Legendre symbol*  $\left(\frac{a}{p}\right)$  is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{otherwise} \end{cases}$$

Euler's formula for the Legendre symbol is

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Let  $q$  be another odd prime, and consider the case  $n = q$  in the above discussion, so  $L = K(\zeta_q)$  is a splitting field for  $f = T^q - 1 = (T - 1)\Phi_q$ . On roots of  $f$  in  $L$ , the Frobenius map  $\varphi_p$  has cycle type  $(1, r, \dots, r)$ . There are  $\frac{q-1}{r}$ -many  $r$ -cycles. The sign of the permutation  $\varphi_p$  is  $(-1)^{(r-1)\frac{q-1}{r}} = (-1)^{\frac{q-1}{r}}$  since  $q$  is odd. Note that  $2 \mid \frac{q-1}{r}$  holds if and only if  $r \mid \frac{q-1}{2}$ , or equivalently,  $p^{\frac{q-1}{2}} \equiv 1 \pmod{2}$ . This is in the form of Euler's formula for the Legendre symbol. So the sign of  $\varphi_p$  is exactly  $\left(\frac{p}{q}\right)$ .

Since  $G = \langle \varphi_p \rangle$ , the sign of  $\varphi_p$  is  $+1$  if and only if  $G \subseteq A_q$  since  $q = \deg f$ . This holds if and only if  $\text{Disc}(f)$  is a square in  $\mathbb{F}_p$ .

### Lemma 5.6

Let  $f = \prod (T - x_i)$  over some field. Then  $\text{Disc}(f) = (-1)^{\frac{d(d-1)}{2}} \prod f'(x_i)$ , where  $d = \deg f$ .

This lemma can be shown directly from the definition of the discriminant. We use the above lemma with  $f = T^q - 1 = \prod_{a=0}^{q-1} (T - \zeta_q^a)$  and  $f' = qT^{q-1}$  to find

$$\text{Disc}(f) = (-1)^{\frac{q(q-1)}{2}} \prod_{a=0}^{q-1} q\zeta_q^{a(q-1)} = (-1)^{\frac{q-1}{2}} q^q \zeta_q^{(q-1)\frac{q(q-1)}{2}} = (-1)^{\frac{q-1}{2}}$$

since  $q$  is odd. Hence, by the fact that  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ ,

$$\left(\frac{p}{q}\right) = \left(\frac{\text{Disc}(f)}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) = \left(\frac{q}{p}\right) (-1)^{\frac{(p-1)(q-1)}{4}}$$

which is the quadratic reciprocity law.

### 5.4. Construction of regular polygons.

#### Lemma 5.7

If  $m$  is a positive integer such that  $2^m + 1$  is prime, then  $m$  is a power of two.

*Proof.* If  $q$  is odd,  $2^{qr} + 1 = (2^r + 1)(2^{qr-r} - 2^{qr-2r} + \dots + 1)$ , which is a nontrivial factorisation.  $\square$

Ruler and compass construction of a regular  $n$ -gon for  $n \geq 3$  is equivalent to constructing the real number  $\cos\left(\frac{2\pi}{n}\right)$ .

#### Theorem 5.8 (Gauss)

A regular  $n$ -gon is constructible if and only if  $n$  is a power of two multiplied by a product of distinct primes of the form  $2^{2^k} + 1$ .

**Remark.** Let  $F_k = 2^{2^k} + 1$  be the  $k$ th *Fermat number*.  $F_1 = 5$ ,  $F_2 = 17$ ,  $F_3 = 257$ , and  $F_4 = 65537$  are all prime. Fermat conjectured that all  $F_k$  are prime. This is false; Euler proved that  $F_5 = 641 \cdot 6700417$ . Many Fermat numbers are known to be composite, and no more have been found to be prime.

*Proof.* Recall that a real number  $x \in \mathbb{R}$  is constructible if and only if there is a sequence of fields  $\mathbb{Q} = K_0 \subset K_1 \subset \dots \subset K_n$  such that  $x \in K_n$  and  $[K_{i+1} : K_i] = 2$ . In particular, if  $x$  is constructible,  $[\mathbb{Q}(x) : \mathbb{Q}] = \deg_{\mathbb{Q}}(x)$  is a power of two. Note that

$$x = \cos\left(\frac{2\pi}{n}\right) = \frac{1}{2}(\zeta_n + \zeta_n^{-1}) \implies \zeta_n^2 - 2x\zeta_n + 1 = 0$$

Since  $x \in \mathbb{R}$  and  $\zeta_n \notin \mathbb{R}$  (for  $n \geq 3$ ),  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(x)] = 2$ . If  $x$  is constructible, then  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$  is a power of two. But  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ .

Let  $n = \prod_{i=1}^r p_i^{e_i}$  be the prime factorisation of  $n$ . Then  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \prod_{i=1}^r p_i^{e_i-1} (p_i - 1)$ . This is a power of two if and only if for all odd  $p_i$ , we have  $e_i = 1$  and  $p_i - 1$  is a power of two. By the previous

lemma,  $\varphi(n)$  is a power of two if and only if  $n$  is of the required form.

Now suppose  $n$  is of the required form, so  $\varphi(n) = 2^m$ .  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  is Galois, with Galois group  $G \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ , which has  $2^m$  elements. There exist subgroups  $G = H_0 \supset H_1 \supset \cdots \supset H_m = 1$  such that  $[H_i : H_{i+1}] = 2$ . Indeed, as  $2 \mid 2^m$ , by Cauchy's theorem there exists an element  $\sigma \in G$  of order 2, assuming  $G$  is not the trivial group. Take  $H_{m-1} = \langle \sigma \rangle$ , and then consider  $G/\langle \sigma \rangle$ , which contains a subgroup of order 2 by the same argument; we can proceed inductively. Then the tower of fixed fields  $K_i = \mathbb{Q}(\zeta_n)^{H_i}$  is a tower of quadratic extensions by the Galois correspondence.  $\square$

### 5.5. Kummer extensions.

#### Theorem 5.9 (linear independence of field embeddings)

Let  $K, L$  be fields, and let  $\sigma_1, \dots, \sigma_n: K \rightarrow L$  be distinct field homomorphisms. Let  $y_1, \dots, y_n \in L$  be such that for all  $x \in K^\times$ ,  $y_1\sigma_1(x) + \cdots + y_n\sigma_n(x) = 0$ . Then all  $y_i = 0$ . In other words,  $\sigma_1, \dots, \sigma_n$  are  $L$ -linearly independent elements of the set of functions  $K \rightarrow L$ , considered as an  $L$ -vector space.

This is a special case, using  $G = K^\times$ , of the following theorem.

#### Theorem 5.10 (linear independence of characters)

Let  $G$  be a group and  $L$  be a field. Let  $\sigma_1, \dots, \sigma_n: G \rightarrow L^\times$  be distinct group homomorphisms. Then  $\sigma_1, \dots, \sigma_n$  are  $L$ -linearly independent elements.

*Proof.* We use induction on  $n$ . If  $n = 1$ , the result is clear. Suppose  $n > 1$ . Let  $y_1, \dots, y_n \in L$  be such that for all  $g \in G$ ,  $y_1\sigma_1(g) + \cdots + y_n\sigma_n(g) = 0$ . Since the homomorphisms are distinct, there is an element  $h \in G$  such that  $\sigma_1(h) \neq \sigma_n(h)$ . The  $\sigma_i$  are homomorphisms, so

$$y_1\sigma_1(hg) + \cdots + y_n\sigma_n(hg) = y_1\sigma_1(h)\sigma_1(g) + \cdots + y_n\sigma_n(h)\sigma_n(g)$$

Multiplying the original expression in  $g$  by  $\sigma_n(h)$  and subtracting,

$$y'_1\sigma_1(g) + \cdots + y'_{n-1}\sigma_{n-1}(g) = 0; \quad y'_i = y_i(\sigma_i(h) - \sigma_n(h))$$

By induction, all  $y'_i = 0$ . But  $\sigma_1(h) \neq \sigma_n(h)$ , so  $y_1 = 0$ . So the original equation  $y_1\sigma_1(g) + \cdots + y_n\sigma_n(g) = 0$  can be simplified into  $y_2\sigma_2(g) + \cdots + y_n\sigma_n(g) = 0$ , so again by induction, all  $y_i$  are zero.  $\square$

We now consider extensions of the form  $L = K(x)$  for  $x^n = a \in K$ . The special case  $a = 1$  gives the cyclotomic extensions. These extensions are not necessarily Galois; for example,  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  is not Galois. In this section, let  $n > 1$ , and  $n \neq 0$  in  $K$ .

#### Theorem 5.11

Let  $K$  be a field that contains a primitive  $n$ th root of unity  $\zeta = \zeta_n$ . Let  $L/K$  be a field extension with  $L = K(x)$ , where  $x^n = a \in K^\times$ . Then  $L/K$  is a splitting field for  $f = T^n - a$ , and is Galois with cyclic Galois group.  $[L : K]$  is the least  $m \geq 1$  such that  $x^m \in K$ .

*Proof.* Note that  $\mu_n(K) = \{\zeta^i \mid 0 \leq i < n\}$  has  $n$  elements. Then  $f$  has  $n$  distinct roots  $\zeta^i x$  in  $L$ . So  $L$  is a splitting field for the separable polynomial  $f$ , and in particular,  $L$  is a Galois extension.

Let  $\sigma \in \text{Gal}(L/K) = G$ . Then  $f(\sigma(x)) = 0$ , so  $\sigma(x) = \zeta^i x$  for some  $i$ , which is unique modulo  $n$ . This induces a map  $\theta: G \rightarrow \mu_n(K) \simeq \mathbb{Z}/n\mathbb{Z}$ , given by  $\theta(\sigma) = \frac{\sigma(x)}{x}$  which is equal to  $\zeta^i$  for some  $i$ . We claim this is a homomorphism. Let  $\sigma, \tau \in G$ . Then since  $\zeta \in K$ ,  $\tau(\theta(\sigma)) = \theta(\sigma)$ . So

$$\theta(\tau\sigma) = \frac{\tau\sigma(x)}{x} = \tau\left(\frac{\sigma(x)}{x}\right) \cdot \frac{\tau(x)}{x} = \tau(\theta(\sigma)) \cdot \theta(\tau) = \theta(\sigma)\theta(\tau)$$

It is injective, because  $\theta(\sigma) = 1$  if and only if  $\sigma(x) = x$ , so  $\sigma = \text{id}$ . So  $G$  is isomorphic to a subgroup of a cyclic group. Hence it is cyclic.

If  $m \geq 1$ , since  $L/K$  is Galois,  $x^m \in K$  if and only if for all  $\sigma \in G$ ,  $\sigma(x^m) = x^m$ . By the definition of  $\theta$ , this holds if and only if for all  $\sigma \in G$ ,  $\theta(\sigma)^m = 1$ . So  $|G| = [L : K]$  divides  $m$ . So  $[L : K]$  must be the least  $m$  such that  $x^m \in K$ , as required.  $\square$

#### Corollary 5.12

Let  $K$  be a field that contains a primitive  $n$ th root of unity  $\zeta = \zeta_n$ . Let  $a \in K^\times$ . Then  $f = T^n - a$  is irreducible over  $K$  if and only if  $a$  is not a  $d$ th power in  $K$  for any  $1 \neq d \mid n$ .

*Proof.* Let  $L$  be a splitting field for  $f = T^n - a$ , so  $L = K(x)$  for  $x^n = a$ . Then the minimal polynomial of  $x$  divides  $f$ . So  $f$  is irreducible if and only if  $f = m_{x,K}$ , or equivalently,  $[L : K] = n$ .

Suppose  $n = md$  for  $d \neq 1$ . Then  $a$  is a  $d$ th power in  $K$  if and only if  $x^m \in K$  since  $\zeta_n \in K$ . By the above theorem, this holds if and only if  $|G| \mid m$ .  $\square$

**Remark.** This does not hold if we relax the assumption  $\zeta_n \in K$ . For example, consider  $K = \mathbb{Q}$  and  $T^4 + 4$ .

#### Definition 5.13

Extensions of the form  $L = K(x)$  where  $x^n = a \in K$  and  $\zeta_n \in K$  are called *Kummer extensions*.

#### Example 5.14

Let  $n = 2$  and  $\text{char } K \neq 2$ . Then  $\zeta_2 = -1 \in K$ .



Then  $K(\sqrt{a})/K$  is a quadratic Kummer extension if  $a \notin (K^\times)^2$ . Conversely, any quadratic extension must be of this form.

### Theorem 5.15

Let  $K$  be a field that contains a primitive  $n$ th root of unity  $\zeta = \zeta_n$  where  $n > 1$ . Let  $L/K$  be a Galois extension with cyclic Galois group of order  $n$ . Then  $L$  is a Kummer extension of  $K$ .

*Proof.* Let  $\text{Gal}(L/K) = \langle \sigma \rangle$ ,  $\sigma^n = 1$ . For  $y \in L$ , let

$$x = R(y) = y + \zeta^{-1}\sigma(y) + \zeta^{-2}\sigma^2(y) + \cdots + \zeta^{-(n-1)}\sigma^{n-1}(y)$$

This is known as a *Lagrange resolvent*. Then

$$\sigma(x) = \sum_{j=0}^{n-1} \zeta^{-j} \sigma^{j+1}(y) = \sum_{j=0}^{n-1} \zeta^{1-j} \sigma^j(y) = \zeta x$$

Hence  $\sigma(x^n) = \zeta^n x^n = x^n$ , so  $x^n \in K$ . By the linear independence of field embeddings with  $\sigma_i = 1, \sigma, \dots, \sigma^{n-1}$ , there exists  $y$  such that  $R(y) = x \neq 0$ . Now, since  $\sigma^i x = \zeta^i x$ , the  $\sigma^i(x)$  are distinct, and so  $\deg_K x = n$ . In particular,  $[K(x) : K] = n = [L : K]$ , so  $L = K(x)$ .  $\square$

### Example 5.16

Let  $L/\mathbb{Q}$  be a Galois extension of degree 3. Since  $\zeta_3 \notin \mathbb{Q}$ , this is not a Kummer extension.

## 6. TRACE AND NORM

**6.1. Trace and norm.** Let  $L/K$  be an extension of degree  $n$ , so  $L$  is a  $K$ -vector space of dimension  $n$ . Let  $x \in L$ . Then the map  $U_x : L \rightarrow L$  defined by  $U_x(y) = xy$  is  $K$ -linear, as it is  $L$ -linear. Since it is a linear map, it has a characteristic polynomial, a determinant, and a trace.

### Definition 6.1

The *trace* and *norm* of  $x \in L$  (relative to the extension  $L/K$ ) are  $\text{Tr}_{L/K}(x) = \text{tr } U_x \in K$  and  $N_{L/K}(x) = \det U_x \in K$  respectively. The *characteristic polynomial* of  $x \in L$  is  $f_{x,L/K} = \det(TI - U_x) \in K[T]$  where  $I$  is the identity linear transformation.

We sometimes write  $\text{tr}_K$ ,  $\det_K$ . Let  $e_1, \dots, e_n$  be a basis for  $L/K$ . Then  $U_x$  can be written as a unique  $K$ -valued matrix  $A = (a_{ij})$ , so  $xe_i = \sum_j a_{ji}e_j$ . Then  $\text{Tr}_{L/K}(x) = \text{tr}(A)$ , and so on.

### Example 6.2

Consider the quadratic extension  $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$  with the basis  $1, \sqrt{d}$ . Let  $x = a + b\sqrt{d}$ . Since  $x \cdot 1 =$

$$a + b\sqrt{d} \text{ and } x \cdot \sqrt{d} = bd + a\sqrt{d},$$

$$A = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

$$\text{Hence } \text{Tr}_{L/K}(x) = 2a \text{ and } N_{L/K}(x) = a^2 - b^2d.$$

### Example 6.3

Consider  $\mathbb{C}/\mathbb{R}$  with the basis  $1, i$ . Then the matrix of  $U_{x+iy}$  is

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

which is the usual encoding of complex numbers as  $2 \times 2$  real matrices. Note the similarity between this matrix and the Cauchy–Riemann equations

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}; \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$$

### Lemma 6.4

Let  $x, y \in L$  and  $a \in K$ , where  $n = [L : K]$ . Then,

- (1)  $\text{Tr}_{L/K}(x + y) = \text{Tr}_{L/K}(x) + \text{Tr}_{L/K}(y)$ ;
- (2)  $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$ ;
- (3)  $N_{L/K}(x) = 0$  if and only if  $x = 0$ ;
- (4)  $\text{Tr}_{L/K}(1) = n$  and  $N_{L/K}(1) = 1$ ;
- (5)  $\text{Tr}_{L/K}(ax) = a \text{Tr}_{L/K}(x)$  and  $N_{L/K}(ax) = a^n N_{L/K}(x)$ .

In particular,  $\text{Tr}_{L/K}$  is  $K$ -linear and  $N_{L/K} : L^\times \rightarrow K^\times$  is a homomorphism.

*Proof.* For part (iii),  $N_{L/K}(x) = \det(U_x) \neq 0$  if and only if  $U_x$  is invertible. But this holds if and only if  $x$  is nonzero because  $L$  is a field. The other results follow from the laws of linear transformations.  $\square$

## 6.2. Formulae and applications.

### Theorem 6.5

Let  $M/L/K$  be a tower of finite extensions. Then, for all  $x \in M$ ,

$$\text{Tr}_{L/K}(\text{Tr}_{M/L}(x)) = \text{Tr}_{M/K}(x); \quad N_{L/K}(N_{M/L}(x)) = N_{M/K}(x)$$

*Proof.* We prove the theorem for the trace; we will not need the result for the norm. Let  $x \in M$ . Let  $u_1, \dots, u_m$  be a basis for  $M/L$ , and let  $v_1, \dots, v_n$  be a basis for  $L/K$ . Let  $(a_{ij})$  be the matrix of  $U_{x,M/L}$ , so  $(a_{ij}) \in \text{Mat}_{m,m}(L)$ . Then  $\text{Tr}_{M/L}(x) = \sum_{i=1}^m a_{ii}$ . For each  $(i, j)$ , let the matrix of  $U_{a_{ij}}$  be  $A_{ij} \in \text{Mat}_{n,n}(K)$ . Then,  $\text{Tr}_{L/K}(\text{Tr}_{M/L}(x)) = \sum_{i=1}^m \text{Tr}_{L/K}(a_{ii}) = \sum_{i=1}^m \text{tr}(A_{ii})$ .

Consider the basis  $u_1v_1, \dots, u_1v_m, u_2v_1, \dots, u_nv_m$  for  $M$  over  $K$ . Then the matrix of  $U_{x,M/K}$  is the



block matrix

$$\begin{pmatrix} A_{11} & & & \\ & A_{22} & & \\ & & \ddots & \\ & & & A_{nn} \end{pmatrix}$$

which has trace  $\sum_{i=1}^n \text{tr}(A_{ii})$  as required.  $\square$

### Proposition 6.6

Let  $L = K(x)$ , and  $f = T^n + c_{n-1}T^{n-1} + \cdots + c_0 \in K[T]$  be the minimal polynomial for  $x$  over  $K$ . Then  $f_{x,L/K} = f$ . Further,  $\text{Tr}_{L/K}(x) = -c_{n-1}$  and  $N_{L/K}(x) = (-1)^n c_0$ .

*Proof.* It suffices to prove the first statement, since the second follows from the fact that the determinant and trace are the given coefficients of the characteristic polynomial for any linear transformation. Consider the basis  $1, x, \dots, x^{n-1}$  for  $L/K$ . Then, the matrix of  $U_x$  is

$$\begin{pmatrix} 0 & \cdots & & & -c_0 \\ 1 & 0 & \cdots & & -c_1 \\ 0 & 1 & 0 & \cdots & \\ \vdots & 0 & 1 & 0 & \cdots \\ & \vdots & 0 & 1 & \cdots \\ & & \vdots & \vdots & \ddots \\ & & & & -c_{n-1} \end{pmatrix}$$

which has characteristic polynomial  $f$  since it is in rational canonical form.  $\square$

### Corollary 6.7

Let  $\text{char } K = p > 0$ , and  $L = K(x)$  where  $x \notin K$  but  $x^p \in K$ . Then for all  $y \in L$ , we have  $\text{Tr}_{L/K}(y) = 0$  and  $N_{L/K}(y) = y^p$ .

*Proof.* Recall that the minimal polynomial of  $x$  is  $T^p - x^p$ , so  $[L : K] = p$ . Suppose that  $y \in K$ . By a previous lemma,  $\text{Tr}_{L/K}(y) = py = 0$  and  $N_{L/K}(y) = y^p$ . Otherwise, since  $[L : K]$  is prime,  $K(y) = L$ , and in particular, if  $y = \sum a_i x^i$  then  $y^p = (\sum a_i x^i)^p = \sum a_i (x^p)^i \in K$ . So the minimal polynomial of  $y$  is  $T^p - y^p$ . Applying the previous proposition, the result follows.  $\square$

### Proposition 6.8

Let  $L/K$  be a finite separable extension of degree  $n$ . Let  $\sigma_1, \dots, \sigma_n : L \rightarrow M$  be the distinct  $K$ -homomorphisms of  $L$  into a normal closure  $M$  for  $L/K$ . Then

$$\text{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x); \quad N_{L/K}(x) = \prod_{i=1}^n \sigma_i(x); \quad f_{x,L/K} = \prod_{i=1}^n (T - \sigma_i(x))$$

**Remark.** If  $L/K$  is finite and Galois, then  $\text{Tr}_{L/K}(x) = \sum_{\sigma \in \text{Gal}(L/K)} \sigma(x)$ , and the other results are similar.

*Proof.* It suffices to show the result for the characteristic polynomial. Let  $e_1, \dots, e_n$  be a basis for  $L/K$ . Let  $P = (\sigma_i(e_j)) \in \text{Mat}_{n,n}(M)$ . Recall that the  $\sigma_i$  are linearly independent, so there exist no  $y_i \in M$  such that for all  $j$ ,  $\sigma_i(e_j) = 0$ . Hence  $P$  is nonsingular. Let  $A = (a_{ij})$  be the matrix of  $U_x$ , so  $x e_j = \sum_r a_{rj} e_r$ . Applying  $\sigma_i$ , we have

$$\sigma_i(x) \sigma_i(e_j) = \sum_r \sigma_i(e_r) a_{rj}$$

So if  $S$  is the diagonal matrix with  $(i, i)$ th entry  $\sigma_i(x)$ , then the given equation can be rewritten as  $SP = PA$ . Therefore  $S = PAP^{-1}$ . So  $S$  and  $A$  are conjugate matrices and hence have the same characteristic polynomial. We explicitly find that the characteristic polynomial of  $S$  is  $\prod (T - \sigma_i(x))$  and the characteristic polynomial of  $A$  is  $f_{x,L/K}$ . So they are equal as required.  $\square$

Note that since the trace  $\text{Tr}_{L/K} : L \rightarrow K$  is  $K$ -linear, it is either the zero map or surjective.

### Theorem 6.9

Let  $L/K$  be a finite extension. Then,  $L/K$  is separable if and only if  $\text{Tr}_{L/K}$  is surjective.

**Remark.** If  $\text{char } K = 0$ ,  $\text{Tr}_{L/K}(1) = n \neq 0$ , so the result holds easily.

*Proof.* Suppose  $L/K$  is separable, and  $\sigma_1, \dots, \sigma_n$  are the  $K$ -homomorphisms of  $L$  into a normal closure  $M$  of  $L/K$ . Then  $\text{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x)$ . As the  $\sigma_i$  are linearly independent, there exists  $x$  such that  $\sum_{i=1}^n \sigma_i(x) \neq 0$ . So  $\text{Tr}_{L/K}(x) \neq 0$ , and in particular, it must be surjective as it is  $K$ -linear.

Now suppose  $L/K$  is inseparable. Then there exists  $x \in L$  such that  $K(x) \subsetneq K(x^p)$  from example 7 on example sheet 2. As we have shown,  $\text{Tr}_{K(x)/K(x^p)} = 0$ , so

$$\text{Tr}_{L/K} = \text{Tr}_{L/K(x)} \circ \text{Tr}_{K(x)/K(x^p)} \circ \text{Tr}_{K(x^p)/K} = 0$$

$\square$

### Example 6.10

Consider the extension of finite fields  $\mathbb{F}_{q^n}/\mathbb{F}_q$  for  $q = p^r$ . This is separable, so there exists  $x \in \mathbb{F}_{q^n}$  such that  $\text{Tr}(x) = 1$ . It is also possible to prove this directly by using the fact that the multiplicative group is cyclic.

**Remark.** This criterion can be used to give another proof that if  $M/K$  and  $L/K$  are separable,  $M/L$  is also separable.

### 7.1. Definition.

#### Definition 7.1

A field  $K$  is *algebraically closed* if every non-constant polynomial over  $K$  splits into linear factors over  $K$ .

**Remark.** An equivalent condition is that the only irreducible polynomials are linear.

#### Example 7.2

The complex numbers  $\mathbb{C}$  form an algebraically closed field due to the fundamental theorem of algebra.

#### Proposition 7.3

The following are equivalent.

- (1)  $K$  is algebraically closed.
- (2) If  $L/K$  is a field extension and  $x \in L$  is algebraic over  $K$ , then  $x \in K$ .
- (3) If  $L/K$  is an algebraic extension,  $L = K$ .

*Proof.* (i) implies (ii). Let  $L/K$  be a field extension and  $x \in L$  algebraic over  $K$ . Let  $f$  be the minimal polynomial for  $x$  over  $K$ . Then  $f$  is linear, so  $x \in K$ .

(ii) implies (iii). An extension  $L/K$  is algebraic when all  $x \in L$  are algebraic over  $K$ . So  $x \in K$  by (ii).

(iii) implies (i). Let  $f$  be an irreducible polynomial, and  $L = K[T]/(f)$ , so  $L/K$  is a finite algebraic extension. Then  $L = K$ , so  $f$  is linear.  $\square$

#### Proposition 7.4

Let  $L/K$  be an algebraic extension such that every irreducible polynomial  $f \in K[T]$  splits into linear factors in  $L$ . Then  $L$  is algebraically closed.

Such a field is called an *algebraic closure* of  $K$ .

*Proof.* Let  $M/L$  be an extension, and let  $x \in M$  be algebraic over  $L$ . Then  $x$  is algebraic over  $K$ . By hypothesis, its minimal polynomial  $m_{x,K} \in K[T]$  splits into linear factors over  $L$ . So  $x \in L$ . By criterion (ii) in the previous proposition,  $L$  is algebraically closed.  $\square$

**Remark.** An algebraic closure of  $K$  is the same as an algebraic extension of  $K$  which is algebraically closed.

#### Corollary 7.5

The field  $\overline{\mathbb{Q}}$  of algebraic complex numbers is algebraically closed. In particular,  $\overline{\mathbb{Q}}$  is an algebraic closure of  $\mathbb{Q}$ .

*Proof.* We apply the previous result to the extension  $\overline{\mathbb{Q}}/\mathbb{Q}$ . The extension is algebraic, so it suffices to check that every irreducible polynomial  $f \in \mathbb{Q}[T]$  splits into linear factors in  $\overline{\mathbb{Q}}$ . By the fundamental theorem of algebra,  $f$  splits in  $\mathbb{C}$ . By definition of  $\overline{\mathbb{Q}}$ , we have  $f = \prod (T - x_i)$  where each  $x_i \in \overline{\mathbb{Q}}$  as required.  $\square$

### 7.2. Algebraic closures of countable fields.

#### Proposition 7.6

Let  $K$  be a countable field. Then  $K$  has an algebraic closure.

*Proof.* If  $K$  is a countable field, then  $K[T]$  is a countable ring. We will enumerate the monic irreducible polynomials  $f_i \in K[T]$  for  $i \geq 1$ . Let  $L_0 = K$ , and inductively define  $L_i$  to be a splitting field for  $f_i$  over  $L_{i-1}$ .

One can perform this in such a way that no choices need to be made in the construction of the splitting fields. We may also assume that  $L_{i-1} \subseteq L_i$  for each  $i \geq 1$ , because if  $\sigma: L_{i-1} \rightarrow L_i$  is the extension, we can replace  $L_i$  with  $L_{i-1} \sqcup (L_i \setminus \sigma(L_{i-1}))$ . Let  $L = \bigcup L_i$  be their union. By construction, every  $f_i$  splits in  $L$ , so  $L$  is an algebraic closure of  $K$ .  $\square$

#### Example 7.7

$\mathbb{F}_p$  has an algebraic closure.

**7.3. Zorn's lemma.** For a general field, we need to apply some set-theoretic machinery.

#### Definition 7.8

A binary relation  $\preceq$  on a set  $S$  is a *partial order* if it is reflexive, transitive, and antisymmetric. Explicitly, for all  $x, y, z \in S$ , we have

$$x \preceq x; \quad x \preceq y, y \preceq z \implies x \preceq z; \quad x \preceq y, y \preceq x \implies z = y$$

We say  $(S, \preceq)$  is a *partially ordered set*, or a *poset*. It is *totally ordered* if the order is total;  $x \preceq y$  or  $y \preceq x$  for all  $x, y \in S$ .

#### Definition 7.9

Let  $S$  be a partially ordered set. A *chain* in  $S$  is a totally ordered subset. An *upper bound* for a subset  $T$  of  $S$  is an element  $z \in S$  such that for all  $x \in T$ , we have  $x \preceq z$ . A *maximal element* of  $S$  is an element  $y \in S$  such that for all  $x \in S$ ,  $y \preceq x$  implies  $y = x$ .

If  $S$  is totally ordered,  $S$  has at most one maximal element.

**Lemma 7.10 (Zorn)**

Let  $S$  be a nonempty partially ordered set. Suppose that every chain in  $S$  has an upper bound in  $S$ . Then  $S$  has a maximal element.

This can be proven using the axiom of choice.

**Example 7.11**

Let  $V$  be a vector space over  $K$ . Then  $V$  has a basis; a set  $B \subseteq V$  such that any finite subset of  $B$  is linearly independent, and for all  $v \in V$ , there exists  $b_1, \dots, b_k \in B$  and  $a_1, \dots, a_k \in K$  such that  $v = \sum_{i=1}^k a_i b_i$ . If  $V = 0$ , the result is trivial by taking  $V = \emptyset$ . Otherwise, let  $S$  be the set of all subsets  $X \subseteq V$  where finite subsets of  $X$  are linearly independent.  $S$  is ordered by inclusion; this is a partial order.  $S$  is nonempty since  $V \neq 0$ . Each chain  $T \subseteq S$  has an upper bound by taking its union  $Y = \bigcup_{X \in T} X$ . This upper bound indeed lies in  $S$ , since we only need to check finite subsets of  $Y$  for linear independence. Then by Zorn's lemma,  $S$  has a maximal element  $B$ , which can be seen to be a basis.

**Proposition 7.12**

Let  $L/K$  be an algebraic extension, and let  $M$  be algebraically closed. Let  $\sigma: K \rightarrow M$ . Then there exists  $\bar{\sigma}: L \rightarrow M$  extending  $\sigma$ .

*Proof.* First, consider the case  $L = K(x)$  where  $x$  is algebraic over  $K$  with minimal polynomial  $m_{x,K} = f$ . Then  $\sigma f \in M[T]$ . Since  $M$  is algebraically closed,  $\sigma f$  splits in  $M$ . Therefore there exists such a  $\bar{\sigma}: K(x) \rightarrow M$  extending  $\sigma$ . We can obtain one homomorphism for each root of  $\sigma f$  in  $M$ .

Now consider the general case. Suppose  $K \subseteq L$  without loss of generality, by replacing  $K$  with its image in  $L$ . Let

$$S = (F, \tau) \mid K \subseteq F \subseteq L, \tau: F \rightarrow M, \tau|_K = \sigma$$

This has a partial order given by  $(F, \tau) \preceq (F', \tau')$  where  $F \subseteq F'$  and  $\tau'|_F = \tau$ . Therefore,  $S$  is a partially ordered set. It contains  $(K, \sigma)$ , so it is not empty.

Let  $T = (F_i, \tau_i)_{i \in I}$  be a chain in  $S$ . If  $T$  is empty, we can vacuously upper bound it with  $(K, \sigma)$ . Otherwise, we define  $F' = \bigcup_{i \in I} F_i$ . This is a field since  $T$  is a chain; in particular, for all  $i, j \in I$ , we have either  $F_i \subseteq F_j$  or  $F_j \subseteq F_i$ . Now define  $\tau': F' \rightarrow M$  by mapping  $x$  to  $\tau_i(x)$  where  $x \in F_i$ ; this is independent of the choice of  $i$  since  $\tau_j|_{F_i} = \tau_i$  and  $T$

is a chain. This is an upper bound in  $S$  for the chain.

Then, by Zorn's lemma,  $S$  has a maximal element. Let  $(F, \tau)$  be this maximal element. We will show  $F = L$ ; in this case,  $\tau = \bar{\sigma}$  is an extension as required.

Clearly  $F \subseteq L$ . If  $x \in L$ , then by the first part applied to  $F(x)/F$ , we can extend the homomorphism  $\tau: F \rightarrow M$  into a homomorphism  $\bar{\tau}: F(x) \rightarrow M$ . Then  $(F(x), \bar{\tau}) \in S$ , and  $(F, \tau) \preceq (F(x), \bar{\tau})$ . By maximality,  $F(x) = F$ , so  $x \in F$ . Hence  $F = L$  as required.  $\square$

**7.4. Algebraic closures of general fields.** One can construct an algebraic closure of a field using Zorn's lemma, obtaining a field that extends all algebraic extensions of a given field. However, difficulties arise since the class of algebraic extensions of a field does not form a set. Zorn's lemma can be utilised inside a suitably well-behaved set, but instead, we will construct the algebraic closure via the maximal ideal theorem.

**Theorem 7.13 (maximal ideal theorem)**

Let  $R$  be a non-zero commutative ring with a 1. Then  $R$  has a maximal ideal.

*Proof sketch.* Let  $S$  be the set of all proper ideals  $I \subset R$ , partially ordered by inclusion. A maximal ideal is a maximal element of  $S$ . We apply Zorn's lemma. Let  $T$  be a nonempty chain, since anything is an upper bound for an empty chain. Then  $J = \bigcup_{I \in T} I$  is an ideal. As  $1 \notin I$  for all  $I \in T$ , we conclude  $1 \notin J$ . So  $J$  is a proper ideal, and hence is an upper bound.  $\square$

**Theorem 7.14**

Let  $K$  be a field. Then  $K$  has an algebraic closure  $\bar{K}$ . If  $\sigma: K \rightarrow K'$  is an isomorphism, and  $\bar{K}, \bar{K}'$  are any algebraic closures of  $K, K'$ , then  $\sigma$  extends to an isomorphism  $\bar{\sigma}: \bar{K} \rightarrow \bar{K}'$ .

**Remark.** The extension  $\bar{\sigma}$  is not generally unique.

*Proof.* We begin by proving the existence of the algebraic closure. Let  $P$  be the set of monic irreducible polynomials in  $K[T]$ , and construct  $K_1$  such that every  $f \in P$  has a root in  $K_1$ . First, we will find a ring in which every  $f \in P$  has a root.

Let  $R = K[T_f]_{f \in P}$  be the set of finite  $K$ -linear combinations of monomials  $T_{f_1}^{m_1} \dots T_{f_k}^{m_k}$  for  $f_i \in P$ . Let  $I$  be the ideal generated by  $f(T_f)$  for each  $f \in P$ . Now, in  $R/I$ ,  $T_f + I$  is a root of  $f$ .

We must check that  $I \neq R$ . If  $I = R$ , then in particular  $1 \in I$ . In other words, for some finite subset  $Q \subseteq P$ , there exists  $r_f \in R$  for  $f \in Q$

such that  $1 = \sum_{f \in Q} r_f f(T_f)$ . Enlarging  $Q$  if necessary, we can assume that each  $r_f$  is a polynomial in  $T_g \mid g \in Q$ . Let  $L/K$  be a splitting field for  $\prod_{f \in Q} f$ , and  $a_f \in L$  be a root of  $f$  for each  $f \in Q$ . Consider the homomorphism  $\varphi: R \rightarrow L$  such that  $\varphi|_K = \text{id}$  and  $\varphi(T_f) = a_f$  for  $f \in Q$ , and  $\varphi(T_f) = 0$  for  $f \notin Q$ . Then

$$1 = \varphi(1) = \sum_{f \in Q} \varphi(r_f f(T_f)) = \sum_{f \in Q} \varphi(r_f) f(a_f) = 0$$

This is a contradiction, so  $I$  is in fact a proper ideal.

By the maximal ideal theorem, the ring  $R/I$  has a maximal ideal  $\bar{J}$ . Equivalently, there exists a maximal ideal  $J$  of  $R$  containing  $I$ , since the ideals of  $R/I$  are in bijection with the ideals of  $R$  containing  $I$  by the isomorphism theorem. Now let  $K_1 = R/J$ . This is a field since  $J$  is maximal. Let  $x_f = T_f + J \in K_1$ , then  $K_1/K$  is generated by the  $x_f$ , and  $f(x_f) = 0$  by construction. So  $K_1/K$  is an algebraic extension of  $K$  in which every  $f \in P$  has a root.

Let  $P_1$  be the set of monic irreducibles in  $K_1[T]$ . We apply the same procedure to  $K_1$  and  $P_1$  to obtain a field  $K_2$ , and so on. We then obtain a tower  $K \subseteq K_1 \subseteq K_2 \subseteq \dots$  such that if  $f \in K_n[T]$  is non-constant, it has a root in  $K_{n+1}$ .

Now, suppose  $f \in K[T]$  is non-constant. Then we can write  $f = (T - x_1)f_1$  where  $x_1 \in K_1, f_1 \in K_1[T]$ , and so on. So  $f$  splits in  $K_{\deg f - 1}$ . Therefore, the union  $\bigcup_{n \in \mathbb{N}} K_n$  is algebraically closed, and hence is an algebraic closure of  $K$ .

We now prove uniqueness. Let  $K \subseteq \bar{K}$  and  $K' \subseteq \bar{K}'$  be algebraic closures, and let  $\sigma: K \rightarrow K'$  be an isomorphism. Then by the previous result, as  $\bar{K}/K$  is algebraic,  $\sigma$  extends to a homomorphism  $\bar{\sigma}: \bar{K} \rightarrow \bar{K}'$ . It suffices to show that  $\sigma$  is an isomorphism. We have  $K' \subseteq \sigma(\bar{K}) \subseteq \bar{K}'$ , so  $\bar{K}'/\sigma(\bar{K})$  is algebraic.  $\bar{K}$  is algebraically closed, so  $\sigma(\bar{K})$  is also algebraically closed. So  $\bar{K}' = \sigma(\bar{K})$  by part (iii) of a previous result.  $\square$

## 8. CUBICS, QUARTICS, AND QUINTICS

**8.1. Cubics.** Let  $f \in K[T]$  be a monic separable cubic. Then  $G = \text{Gal}(f/K) \leq S_3$  acting on the roots  $x_1, x_2, x_3$  in a splitting field  $L$  of  $K$ . If  $f$  is reducible,  $f$  is either a product of three linear factors, in which case  $G$  is trivial, or  $f$  is a linear factor multiplied by a quadratic, in which case  $G$  is isomorphic to  $S_2$ .

Now suppose  $f$  is irreducible. We will assume that  $\text{char } K \neq 2, 3$ . We have  $G = S_3$  or  $G = A_3$ . We know that  $G = A_3$  if and only if the discriminant  $\text{Disc}(f)$  is a square in  $K^\times$ . In general, the Galois correspondence yields

$$\begin{array}{ccc} L = K(x_1, x_2, x_3) & & 1 \\ \downarrow \text{3 if } f \text{ irreducible, else 1} & & \uparrow \\ K(\Delta) = L^{G \cap A_3} & & G \cap A_3 \\ \downarrow \text{2 or 1} & & \uparrow \\ K & & G \end{array}$$

Then  $K_1 = K(\sqrt{\text{Disc}(f)})$ , and  $K_1 = L$  if  $f$  is reducible.

In the irreducible case,  $L/K_1$  is Galois with  $\text{Gal}(L/K_1) \simeq \mathbb{Z}/3\mathbb{Z}$ . Recall that if  $\omega \in K_1$  is a primitive third root of unity, then  $L = K_1(y)$  where  $y^3 \in K_1$ , by Kummer theory.

We can compute this  $y$  explicitly. Suppose  $f = T^3 + bT + c$  without loss of generality. Then  $\Delta^2 = -4b^3 - 27c^2$ . If  $b = 0$ , the roots of  $f$  are  $\omega^i \sqrt[3]{-c}$ , so let  $y$  be any of them. In the other case  $b \neq 0$ , let  $y$  be a Lagrange resolvent. If the roots of  $f$  in  $L$  are  $x_1, x_2, x_3$ , take  $y = x_1 + \omega^2 x_2 + \omega x_3 = (1 - \omega)(x_1 - \omega x_2)$  as  $x_1 + x_2 + x_3 = 0$ . Then  $L(\omega) = K(\Delta, \omega, y)$  if and only if  $y \neq 0$ , by the proof of the structure of Kummer extensions. Let  $y' = x_1 + \omega x_2 + \omega^2 x_3$ , then  $yy' = -3b \neq 0$  since we are not in characteristic 3. Note that  $y + y' = y + y' + x_1 + x_2 + x_3 = 3x_1$ . One can calculate  $y^3 = \frac{1}{2}(-3\sqrt{-3}\Delta + 27c)$ , so  $x_1 = y - \frac{3b}{y}$ .

If not, let  $L(\omega)$  be the splitting field of  $f \cdot (T^3 - 1)$  over  $K$ . Then  $L(\omega)/K_1(\omega)$  is Galois with Galois group  $\mathbb{Z}/3\mathbb{Z}$  as before. So  $L(\omega) = K_1(\omega, y)$  where  $y^3 \in K_1(\omega)$ .

Therefore, in every case,  $x_i$  lie in the field obtained by adjoining successive square roots and cube roots to  $K$ , since  $\omega = \frac{-1 + \sqrt{-3}}{2}$ . This is a theoretical description of Cardano's solution to the cubic.

**8.2. Quartics.** Let  $f \in K[T]$  be a monic separable quartic, with  $\text{char } K \neq 2, 3$ . Then  $\text{Gal}(f/K) \leq S_4$ . Note that  $S_4$  acts on the partitions  $(12 \mid 34), (13 \mid 24), (14 \mid 23)$  of  $1, 2, 3, 4$ . Then we have a homomorphism  $S_4 \rightarrow S_3$ . The kernel of this homomorphism is the Klein four-group  $V = e, (12)(34), (13)(24), (14)(23) \triangleleft S_4$ . Hence the homomorphism is surjective, as  $|V| \cdot |S_3| = |S_4|$ .

Let  $f$  have splitting field  $L$  with (distinct) roots  $x_1, \dots, x_4$ . Suppose that  $x_1 + \dots + x_4 = 0$  without loss of generality as the characteristic is not 2, so  $f = T^4 + aT^2 + bT + c$ . Since  $V$  is a normal subgroup of  $S_4$ ,  $G \cap V$  is a normal subgroup of  $G$  and contains  $V$ . In particular, we have a homomorphism  $G/G \cap V \hookrightarrow S_4/V \simeq S_3$ . But  $G/G \cap V = \text{Gal}(M/K)$ . So we should be able to write  $M$  as the splitting field of a cubic  $g \in K[T]$ .

Let  $y_{12} = x_1 + x_2 = -(x_3 + x_4) = -y_{34}$ , and let  $y_{13}, y_{24}, y_{14}, y_{23}$  be defined similarly. Note that  $G \cap V$  maps  $y_{12}$  to  $y_{12}$  or  $y_{34} = -y_{12}$ , and so on. So  $y_{12}^2, y_{13}^2, y_{14}^2$  are fixed under  $G \cap V$ . Hence they lie in  $M = L^{G \cap V}$ .

Suppose  $y_{12}^2 = y_{13}^2$ . Then either  $y_{12} = y_{13}$ , so  $x_2 = x_3$ , contradicting separability, or  $y_{12} = -y_{13}$ , so  $2x_1 + x_2 + x_3 = 0$ , giving  $x_1 = x_4$ , also contradicting separability.

So these are distinct elements of  $M$ , and hence are indeed the roots of a separable cubic  $g \in K[T]$ . This is called the *resolvent cubic*.

$M = L^{G \cap V}$  is a splitting field of  $g$ . Note that  $x_1 = \frac{1}{2}(y_{12} + y_{13} + y_{14})$  and similar results hold for  $x_2, x_3, x_4$ . Hence  $L = M(y_{12}, y_{13}, y_{14})$ . We can compute  $g = (T - y_{12}^2)(T - y_{13}^2)(T - y_{14}^2) = T^3 + 2aT^2 + (a^2 - 4c)T - b^2$ . In particular,  $y_{12}y_{13}y_{14} = b$ , hence we can simplify to  $L = M(y_{12}, y_{13})$  where  $y_{12}^2, y_{13}^2 \in M$ .

In conclusion, we have found a way to solve  $f = 0$ . First, we solve the resolvent equation  $g = 0$ , and then we take at most two square roots to obtain the relevant field generators.

**8.3. Solubility by radicals.** Let  $f \in K[T]$  be a monic polynomial in a field  $K$  of characteristic zero. To prove that there is no quintic formula, we must first establish a definition of ‘formula’. The relevant notion is solubility by radicals.

#### Definition 8.1

An irreducible polynomial  $f \in K[T]$  is *soluble by radicals* over  $K$  if there exists a sequence of fields  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$ , with  $x \in K_m$  a root of  $f$ , and each  $K_i$  is obtained from  $K_{i-1}$  by adjoining a root, so  $K_i = K_{i-1}(y_i)$  where  $y_i^{d_i} \in K_{i-1}$ .

**Remark.** This is a generalisation of ruler and compass constructions to permit roots of arbitrary degree.

Note that we can adjoin extra roots if desired. In particular, adjoining roots of unity,  $f$  is soluble by radicals over  $K$  if there exists  $d \geq 1$  and  $K = K_0 \subseteq \dots \subseteq K_m$ , such that  $x \in K_m$  is a root of  $f$ , and  $K_1 = K_0(\zeta_d)$  where  $\zeta_d$  is a primitive  $d$ th root of unity. We can also assume that the other extensions satisfy  $K_i = K_{i-1}(y_i)$  for  $y_i^d = a_i \in K_{i-1}$ . This condition can be easily satisfied by letting  $d$  be the least common multiple of the  $d_i$  that occurs in the tower of fields.

Note that  $K_1/K_0$  is Galois with abelian Galois group.  $K_i/K_{i-1}$  for  $i > 1$  is Galois, where the Galois group is a subgroup of  $\mathbb{Z}/d\mathbb{Z}$  as it is a Kummer extension.

To obtain all roots of  $f$ , we consider a normal closure  $M$  of  $K_m$ ; this will contain a splitting field for  $f$ , since it contains one root and  $f$  is irreducible. To determine  $M$ , let  $K'_i \subseteq M$  be a normal closure of  $K_i$  for each  $i$ . As we are in characteristic zero, an extension is Galois if and only if it is normal. Note that  $K_1$  is Galois, so  $K_1 = K'_1 = K(\zeta_d)$ .

#### Proposition 8.2

$K'_i = K'_{i-1}(\sqrt[d]{\sigma(a_i)} \mid \sigma \in \text{Gal}(K'_{i-1}/K))$ .

*Proof.* Suppose  $\sigma \in \text{Gal}(K'_{i-1}/K)$ . Then we can lift  $\sigma$  to an element  $\bar{\sigma} \in \text{Gal}(K'_i/K)$  such that  $\bar{\sigma}|_{K'_{i-1}} = \sigma$ . Since  $K'_i/K$  is normal, it contains

$\bar{\sigma}(y_i)$ , and  $\bar{\sigma}(y)^d = \sigma(y^d) = \sigma(a_i)$ . So the right hand side is contained in  $K'_i$ .

It suffices to show the right hand side is a normal extension. It is the splitting field over  $K'_{i-1}$  of the polynomial  $g_i = \prod_{\sigma \in \text{Gal}(K'_{i-1}/K)} (T^d - \sigma(a_i))$ . This has coefficients in  $K$ . If  $K'_{i-1}$  is the splitting field of some polynomial  $h_{i-1}$  over  $K$ , then the right hand side is the splitting field of the product  $g_i h_{i-1}$  over  $K$ . So it is normal.  $\square$

#### Proposition 8.3

$\text{Gal}(K'_i/K'_{i-1})$  is abelian.

*Proof.* This proof is a variant on the proof of a previous theorem. Consider the case  $i > 1$ . Let  $A = \text{Gal}(K'_i/K'_{i-1})$ . Let  $\tau \in A$  and  $\sigma \in \text{Gal}(K'_i/K)$ . Then  $\tau(\sqrt[d]{\sigma(a_i)}) = \zeta_d^{m_\sigma} \sqrt[d]{\sigma(a_i)}$  where  $m_\sigma \in \mathbb{Z}/d\mathbb{Z}$ . Hence  $\tau \mapsto (m_\sigma) \in (\mathbb{Z}/d\mathbb{Z})^r$  is an injective homomorphism, where  $r = |\text{Gal}(K'_{i-1}/K)|$ .

If  $i = 1$ , then  $K_1 = K(\zeta_d)$ . So the Galois group is a subgroup of  $(\mathbb{Z}/d\mathbb{Z})^\times$ , so is abelian.  $\square$

Since all of the fields  $K'_i$  are normal closures, the  $N_i$  are normal subgroups of  $G$ .

#### Definition 8.4

A finite group  $G$  is *soluble* if there exists a chain of normal subgroups  $N_i \trianglelefteq G$  with  $G = N_0 \supseteq N_1 \supseteq \dots \supseteq N_m = 1$  such that  $N_i/N_{i+1}$  is abelian for all  $i$ .

#### Example 8.5

Any abelian group is soluble.  $S_3$  is soluble, by considering the chain  $S_3 \supset A_3 \supset 1$ , as  $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$  and  $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ .  $S_4$  is also soluble; the chain  $S_4 \supset A_4 \supset V \supset 1$  suffices. Note that  $S_4/A_4 \simeq \mathbb{Z}/2\mathbb{Z}$ ,  $A_4/V \simeq \mathbb{Z}/3\mathbb{Z}$ ,  $V \simeq (\mathbb{Z}/2\mathbb{Z})^2$ .

We have shown that  $N_i/N_{i+1} = \text{Gal}(K'_i/K'_{i-1})$  is abelian. Hence  $\text{Gal}(M/K)$  is soluble.

#### Lemma 8.6

Every subgroup and quotient of a soluble group is soluble.

*Proof.* Let  $G = N_0 \supset N_1 \supset \dots \supset N_m = 1$ , where the quotients  $N_i/N_{i+1}$  are abelian. Let  $H \leq G$ . Then  $H \cap N_i \trianglelefteq H$ , and there is an injective homomorphism from  $H \cap N_i/H \cap N_{i+1}$  to  $N_i/N_{i+1}$ . Hence the  $H \cap N_i/H \cap N_{i+1}$  are abelian, so  $H$  is soluble.



Now let  $\pi: G \rightarrow \overline{G} = G/H$  for  $H \trianglelefteq G$ . Then  $\pi(N_i) \trianglelefteq \overline{G}$ , and  $N_i/N_{i+1}$  surjects onto  $\pi(N_i)/\pi(N_{i+1})$ .  $\square$

### Theorem 8.7 (Abel–Ruffini)

Let  $f \in K[T]$  be soluble by radicals over  $K$ . Then  $\text{Gal}(f/K)$  is soluble.

*Proof.*  $\text{Gal}(f/K) = \text{Gal}(L/K) \simeq \text{Gal}(M/K)/\text{Gal}(M/L)$ . We know that  $\text{Gal}(M/K)$  is soluble, so the result follows from the fact that quotients of soluble groups are soluble.  $\square$

**Remark.** One can easily show the converse to this theorem.

### Proposition 8.8

If  $n \geq 5$ , then  $S_n$  and  $A_n$  are insoluble.

*Proof.*  $S_n$  and  $A_n$  contain  $A_5$  as a subgroup, so it suffices to show that  $A_5$  is insoluble.  $A_5$  is not abelian, and it is simple, so it is insoluble.  $\square$

### Corollary 8.9

Let  $n = \deg f \geq 5$ , and  $A_n \leq \text{Gal}(f/K)$ . Then  $f$  is not soluble by radicals over  $K$ .

## 8.4. Complex numbers are algebraically closed.

This subsection is non-examinable. We show that  $\mathbb{C}$  is an algebraic closure of  $\mathbb{Q}$ , without using complex analysis. We will only use the following facts:

- (1) every polynomial of odd degree over  $\mathbb{R}$  has a root, due to the intermediate value theorem;
- (2) every quadratic over  $\mathbb{C}$  splits into linear factors, so we can take square roots;
- (3) every finite group  $G$  has a subgroup  $H$  such that  $(G:H)$  is odd and  $|H|$  is a power of 2, by Sylow's theorem for  $p=2$ ;
- (4) if  $G$  is a  $p$ -group, so  $|G| = p^k$  and  $k > 0$ , then  $G$  has a subgroup of index  $p$ , since  $G$  has a non-trivial centre.

Let  $K/\mathbb{C}$  be a finite extension. Let  $L/K$  be a normal closure of  $K$  over  $\mathbb{R}$ , so  $L$  is a Galois extension of  $\mathbb{R}$  containing  $\mathbb{C}$ . Let  $G = \text{Gal}(L/\mathbb{R})$ . We will show that  $L = \mathbb{C}$ .

Let  $H \leq G$  be a Sylow 2-subgroup, and consider  $L^H$ . We have  $[L^H : \mathbb{R}] = (G:H)$ , which is odd. So if  $x \in L^H$ , by (i), its minimal polynomial is linear over  $\mathbb{R}$ , so  $x \in \mathbb{R}$ . Hence  $L^H = \mathbb{R}$ , so  $H = G$ . So  $G$  is a 2-group.

Let  $G \supset G_1 = \text{Gal}(L/\mathbb{C})$ , and  $G_2 \leq G_1$  be a subgroup of index 2, which exists by (iv). Then  $[L^{G_2} : \mathbb{C}] = (G_1 : G_2)$ , contradicting the fact (ii) that quadratics

split in  $\mathbb{C}$ . So there cannot exist a subgroup of index 2, so  $G_1 = e$ , and  $L = \mathbb{C}$ .

## 8.5. Artin's theorem on invariants.

### Theorem 8.10 (Artin)

Let  $L$  be a field and  $G \leq \text{Aut}(L)$  be a finite subgroup of automorphisms of  $L$ . Then  $L^G = x \in L \mid \forall \sigma \in G, \sigma(x) = x$  satisfies  $[L : L^G] = |G|$ .

**Remark.** Unlike in the Galois correspondence, this theorem does not rely on a field extension, just a single field and a finite group of automorphisms. In particular, we find that  $L/L^G$  is finite and Galois, with Galois group  $G$ .

*Proof.* It suffices to show  $L/L^G$  is finite, because then we can apply the Galois correspondence to show  $[L : L^G] = |G|$ . Let  $K = L^G$ , and let  $x \in L$ . Then if  $\sigma_1(x), \dots, \sigma_r(x)$  is the orbit of  $G$  on  $x$ , then  $x$  is a root of  $f = \prod_{i=1}^r (T - \sigma_i(x))$ . But  $f \in L^G[T] = K[T]$ . By construction,  $f$  is separable. Hence  $x$  is algebraic and separable over  $K$ , and  $\deg_K x \leq |G|$ .

Let  $y \in L$  have maximal degree. We claim that  $K(y) = L$ . If not, there exists  $x \in L \setminus K(y)$ . By above,  $x, y$  are algebraic and separable over  $K$ . By the primitive element theorem, there exists  $z \in L$  such that  $K(x, y) = K(z) \supsetneq K(y)$ , so  $\deg_K z > \deg_K y$ . But  $y$  was chosen to have maximal degree, so this is a contradiction.  $\square$

**Remark.** One can prove this theorem directly without appealing to the Galois correspondence or the primitive element theorem. This can then be used as a starting point for Galois theory, which then allows the more complicated theorems to be proven.

### Example 8.11

Let  $k$  be a field, and let  $L = k(X_1, \dots, X_n)$  be the field of rational functions, defined as the fractions of the polynomial ring  $k[X_1, \dots, X_n]$ . Let  $G = S_n$  be the symmetric group permuting the  $X_i$ . Then  $G \leq \text{Aut}(L)$ .

### Theorem 8.12

Let  $k$  be a field and let  $L = k(X_1, \dots, X_n)$ . Then  $L^G = k(s_1, \dots, s_n)$ .

*Proof.* Recall that  $k[X_1, \dots, X_n]^G = k[s_1, \dots, s_n]$  where the  $s_i$  are the elementary symmetric polynomials in the  $X_i$ , and there are no nontrivial relations between the  $s_i$ . In particular,  $k(s_1, \dots, s_n) \subseteq L^G$ .

Conversely, let  $\frac{f}{g} \in L^G$  for  $f, g \in k[X_1, \dots, X_n] = R$ . Without loss of generality let  $f, g$  be coprime.

Then for all  $\sigma \in G$ ,  $\frac{f}{g} = \frac{\sigma f}{\sigma g}$ . By Gauss' lemma,  $R$  is a unique factorisation domain, and the units in  $R$  are the nonzero constants  $\mathbb{k}^\times$ . Hence  $\sigma f = c_\sigma f$  and  $\sigma g = c_\sigma g$  where  $c_\sigma \in \mathbb{k}^\times$ .

Since  $G$  is finite and has order  $N = n!$ ,  $f = \sigma^N f = c_\sigma^N f$ . So  $c_\sigma$  is an  $N$ th root of unity. Then  $fg^{N-1}, g^N$  are invariant under  $\sigma$ , so  $fg^{N-1}, g^N \in R^G = \mathbb{k}[s_1, \dots, s_n]$ . So  $\frac{f}{g} = \frac{fg^{N-1}}{g^N} \in \mathbb{k}(s_1, \dots, s_n)$ .  $\square$

problem is equivalent to asking whether every finite group is a quotient of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . We may also be interested in finding the representations of this group. This leads to the Langlands programme.

### Example 8.13

Let  $L = \mathbb{k}(X_1, \dots, X_n)$ , and let  $K = \mathbb{k}(s_1, \dots, s_n) = L^G$  where  $G = S^n$ . Then by Artin's theorem,  $L/K$  is a finite Galois extension with Galois group  $G$ . Let  $f = T^n - s_1 T^{n-1} + \dots + (-1)^n s_n \in K[T]$ . Then in  $L$ ,  $f = \prod_{i=1}^n (T - X_i)$ . Since the  $X_i$  are different,  $f$  is separable, and  $L/K$  is a splitting field for  $f$ . Hence  $\text{Gal}(f/K) = S^n$ . Informally, the general polynomial of degree  $n$  has Galois group  $S^n$ . It is not difficult to show that for any finite group  $G$ , there exists a Galois extension with Galois group isomorphic to  $G$ .

This is one of a number of theories in *invariant theory*, in which one considers a ring  $R$  and a group  $G \leq \text{Aut}(R)$ , and study  $R^G$ . If  $R$  is a polynomial ring  $\mathbb{k}[X_1, \dots, X_n]$  and  $G \leq S_n$ , then knowing  $R^G$  can help with the computation of Galois groups algorithmically. For example, if  $G = A_n$ , then  $\mathbb{k}[X_1, \dots, X_n]^{A_n} = \mathbb{k}[s_1, \dots, s_n, \Delta]$  where  $\Delta = \prod_{i < j} (X_i - X_j)$ , for  $\text{char } \mathbb{k} \neq 2$ .

Now consider  $R = \mathbb{k}[X_1, X_2]$  and  $G = 1, \sigma$  where  $\sigma(X_i) = -X_i$ . Let  $\text{char } \mathbb{k} \neq 2$ . Then one can show  $R^G = \mathbb{k}[X_1^2, X_2^2, X_1 X_2] = \mathbb{k}[Y_1, Y_2, Y_3] / (Y_1 Y_2 - Y_3^2)$ . Geometrically,  $Y_1 Y_2 = Y_3^2 \subset \mathbb{R}^3$  is a double cone. The point at which the cones meet is known as a singularity; such singularities occur in the study of algebraic geometry.

If  $K$  and  $G$  are fixed, it is not always the case that there exists a Galois extension  $L/K$  such that  $\text{Gal}(L/K) = G$ . For instance, if  $K$  is algebraically closed, it has no nontrivial Galois extensions. If  $K = \mathbb{F}_p$ , then  $\text{Gal}(L/K)$  must be cyclic.

The *inverse Galois problem* asks whether every finite group  $G$  is the Galois group of some Galois extension  $L/\mathbb{Q}$ . This is unsolved in the general case. On the extra example sheet, one shows that every abelian group is in fact the Galois group of some Galois extension  $L/\mathbb{Q}$ . There is a famous theorem by Shafarevich that every finite soluble group is such a Galois group over  $\mathbb{Q}$ . This is also known to hold for most finite simple groups; in particular, due to a theorem of John Thompson, the monster group is known to be a Galois group over  $\mathbb{Q}$ .

Perhaps to solve this problem, it would be better to instead understand  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . The inverse Galois