

Fields and Galois Theory  
MATH5245

Andrew Hubery  
ahubery@maths.leeds.ac.uk

# Chapter 1

## Introduction

Galois Theory has its origins in the study of roots of polynomials. It is not concerned with *finding* the roots, which can be done using the **Newton-Raphson Method** (see also [here](#) for an analysis of various techniques used in computing); rather, Galois Theory is interested in the *form* that the roots can take.

In particular, we can ask which polynomials are **solvable by radicals**: given a polynomial  $f = X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n \in \mathbb{Q}[X]$ , we say  $f$  is solvable by radicals if we can express a root of  $f$  using only the coefficients  $a_i$  and the field operations  $+$ ,  $-$ ,  $\times$ ,  $\div$ , together with extraction of  $r$ -th roots  $\sqrt[r]{\phantom{x}}$ . Is there a general formula giving the roots of all polynomials of degree  $n$ ? Such a general formula exists if  $n \leq 4$ , but not if  $n \geq 5$ .

For a quadratic equation  $f = X^2 + 2pX + q$ , one learns in school to complete the square and write  $f = (X + p)^2 + q - p^2$ , from which we see that the roots are  $-p \pm \sqrt{p^2 - q}$ . This was essentially known to the Babylonians (ca. 1600BC).

In the sixteenth century, more complicated formulae were found for the cubic, by Ferro and Fontana (nicknamed Tartaglia because of his stutter), and then for the quartic, by Ferrari. These methods were published by Cardano, Ferrari's mentor, in his *Ars Magna* (1545).

In 1770, Lagrange unified these methods for  $n \leq 4$  using Lagrange resolvents. Starting from a quartic, one obtains an auxiliary equation which is a cubic, and applying the procedure once more yields a quadratic. The method fails for quintic equations, though, since the auxiliary equation then has degree six.

The idea behind Lagrange resolvents is to use slight modifications (involving roots of unity) of the symmetric functions. Consider  $\mathbb{Q}[X_1, \dots, X_n]$ , the ring of polynomials in  $n$  variables. We let the symmetric group  $S_n$  act on the set of indeterminates  $X_i$  via  $\sigma(X_i) := X_{\sigma(i)}$ . This extends to a  $\mathbb{Q}$ -linear ring isomorphism of  $\mathbb{Q}[X_1, \dots, X_n]$ . For example, if  $n = 3$  and  $\sigma = (1\ 2)$ , then  $\sigma(X_2^2 - 4X_1X_3) = X_1^2 - 4X_2X_3$ . A polynomial  $g$  is called **symmetric** if  $\sigma(g) = g$  for all permutations  $\sigma$ .

The **elementary symmetric functions** are defined to be

$$\mathbf{e}_1 := \sum_i X_i, \quad \mathbf{e}_2 := \sum_{i < j} X_i X_j, \quad \mathbf{e}_3 := \sum_{i < j < k} X_i X_j X_k, \quad \dots, \quad \mathbf{e}_n := \prod_i X_i.$$

Observe that these are indeed symmetric functions.

Now consider a polynomial  $f = X^n + a_1 X^{n-1} + \dots + a_{n-1} X + a_n \in \mathbb{Q}[X]$ . Over the complex numbers, this factorises as  $f = (X - \alpha_1) \cdots (X - \alpha_n)$ , say, where the  $\alpha_i$  are the roots of  $f$ . Expanding  $f$ , we see that

$$a_1 = -\sum_i \alpha_i, \quad a_2 = \sum_{i < j} \alpha_i \alpha_j, \quad \dots, \quad a_n = (-1)^n \prod_i \alpha_i.$$

We observe that

$$a_i = (-1)^i \mathbf{e}_i(\alpha_1).$$

That is, the coefficients of  $f$  are given (up to sign) by the elementary symmetric functions, evaluated at the point  $(X_1, \dots, X_n) = (\alpha_1, \dots, \alpha_n)$ .

A more interesting symmetric function is given by the discriminant. Consider

$$\delta := \prod_{i < j} (X_i - X_j).$$

We observe that  $\sigma(\delta) = \text{sgn}(\sigma)\delta$ . It follows that

$$\Delta := \delta^2 = (-1)^{\binom{n}{2}} \prod_{i \neq j} (X_i - X_j)$$

is a symmetric function. Evaluating this at the roots  $\alpha_i$  of  $f$ , we obtain the **discriminant**  $\Delta(f)$ .

The next theorem will be proved later in the course.

**Theorem 1.1** (Fundamental Theorem of Symmetric Functions). *Every symmetric function in the  $X_i$  can be written as a polynomial in the elementary symmetric functions  $\mathbf{e}_i$ .*

In particular, any symmetric function of the roots can be expressed in terms of the coefficients of the polynomial.

## 1.1 The Quadratic

Consider  $f = X^2 + 2pX + q$ . Over  $\mathbb{C}$  we can write this as  $f = (X - \alpha)(X - \beta)$ . Thus

$$\mathbf{e}_1 = \alpha + \beta = -2p, \quad \mathbf{e}_2 = \alpha\beta = q.$$

We know that every symmetric function of  $\alpha, \beta$  can be expressed in terms of  $\mathbf{e}_1, \mathbf{e}_2$ . For example,

$$\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = \mathbf{e}_1^2 - 2\mathbf{e}_2 = 4p^2 - 2q.$$

$\delta := \alpha - \beta$  is not symmetric, since it changes sign when we swap  $\alpha, \beta$ . The discriminant is symmetric, and we have

$$\Delta := \delta^2 = (\alpha - \beta)^2 = \alpha^2 + \beta^2 - 2\alpha\beta = \mathbf{e}_1^2 - 4\mathbf{e}_2 = 4(p^2 - q).$$

To find the roots of  $f$ , we first complete the square by applying the linear change of variables  $Y = X + p$ . This is an example of a Tschirnhaus transformation (Tschirnhaus, 1683). This yields the equation  $g = Y^2 + q - p^2$ . The roots of  $g$  are clearly  $\pm\sqrt{p^2 - q} = \pm\frac{1}{2}\sqrt{\Delta}$ , so the roots of  $f$  are  $\alpha, \beta = -p \pm \sqrt{p^2 - q}$ .

## 1.2 The Cubic

Consider  $f = X^3 + aX^2 + bX + C$ . By applying the linear change of variables  $Y = X + a/3$  (another Tschirnhaus transformation, also called completing the cube), we reduce to solving a polynomial with no  $X^2$  term. Thus we may assume that our polynomial is of the form  $f = X^3 + 3pX + 2q$ . Over  $\mathbb{C}$  we can write this as  $f = (X - \alpha)(X - \beta)(X - \gamma)$ , so that

$$\mathbf{e}_1 = \alpha + \beta + \gamma = 0, \quad \mathbf{e}_2 = \alpha\beta + \beta\gamma + \gamma\alpha = 3p, \quad \mathbf{e}_3 = \alpha\beta\gamma = -2q.$$

Again, any function symmetric in  $\alpha, \beta, \gamma$  can be expressed in terms of  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ . For example<sup>1</sup>

$$\begin{aligned} \alpha^2 + \beta^2 + \gamma^2 &= \mathbf{e}_1^2 - 2\mathbf{e}_2 = -6p \\ \alpha^3 + \beta^3 + \gamma^3 &= \mathbf{e}_1^3 - 3\mathbf{e}_1\mathbf{e}_2 + 3\mathbf{e}_3 = -6q. \end{aligned}$$

We again define  $\delta := (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$  and the discriminant  $\Delta := \delta^2$ . This is symmetric, and in fact we have the expression

$$\Delta = \mathbf{e}_1^2\mathbf{e}_2^2 - 4\mathbf{e}_1^3\mathbf{e}_3 - 4\mathbf{e}_2^3 + 18\mathbf{e}_1\mathbf{e}_2\mathbf{e}_3 - 27\mathbf{e}_3^2 = -108(p^3 + q^2).$$

To find the roots  $\alpha, \beta, \gamma$  of  $f$ , we can make the substitution  $X = Y - pY^{-1}$ . This yields  $f = Y^3 + 2q - p^3Y^{-3}$ , and hence gives the polynomial  $g = Y^6 + 2qY^3 - p^3$ ,

<sup>1</sup>One way we can find such formulae is as follows. Consider  $\alpha^3 + \beta^3 + \gamma^3$ . This is homogeneous of degree 3, and the only such symmetric functions are  $\mathbf{e}_1^3, \mathbf{e}_1\mathbf{e}_2, \mathbf{e}_3$ . Thus

$$\alpha^3 + \beta^3 + \gamma^3 = \lambda\mathbf{e}_1^3 + \mu\mathbf{e}_1\mathbf{e}_2 + \nu\mathbf{e}_3$$

for some rational numbers  $\lambda, \mu, \nu$ . We can find these by specialisation:

$(\alpha, \beta, \gamma)$	$(\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3)$	$\alpha^3 + \beta^3 + \gamma^3$
$(1, 0, 0)$	$(1, 0, 0)$	$\lambda = 1$
$(1, 1, 0)$	$(2, 1, 0)$	$8\lambda + 2\mu = 2$
$(1, 1, 1)$	$(3, 3, 1)$	$27\lambda + 9\mu + \nu = 3$

Thus  $(\lambda, \mu, \nu) = (1, -3, 3)$ .

a quadratic in  $Y^3$ . Thus we can take

$$Y = \sqrt[3]{-q + \sqrt{p^3 + q^2}}$$

and

$$X = Y - pY^{-1} = \sqrt[3]{-q + \sqrt{p^3 + q^2}} + \sqrt[3]{-q - \sqrt{p^3 + q^2}}.$$

In fact, just as there are two square roots of a number, related by  $\pm 1$ , there are three cube roots of a number, related via  $1, \omega, \omega^2$ , where  $\omega = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$ , so  $\omega^3 = 1$ . Thus the three roots of  $f$  are given by

$$\alpha = Y - pY^{-1}, \quad \beta = \omega Y - p\omega^2 Y^{-1}, \quad \gamma = \omega^2 Y - p\omega Y^{-1}.$$

One should note that this method is not always useful. This is clearly perceived when we already know one solution. For example, consider the polynomial

$$f = X^3 - 15X - 4.$$

This has an integer root 4, whereas the method described above yields  $(p, q) = (-5, -2)$ , so

$$Y = \sqrt[3]{-q + \sqrt{p^3 + q^2}} = \sqrt[3]{2 + \sqrt{-121}} = \sqrt[3]{2 + 11i}.$$

Only knowing that  $(2 + i)^3 = 2 + 11i$  can we substitute in  $Y = 2 + i$  and  $-pY^{-1} = 2 - i$ , and hence obtain  $\alpha = Y - pY^{-1} = 4$ .

### 1.3 The Quartic

Finally, consider the quartic  $f = X^4 + aX^3 + bX^2 + cX + d$ . By applying the Tschirnhaus transformation  $Y = X + a/4$ , we may assume that  $f$  has no  $X^3$  term. Thus we may assume that  $f = X^4 + bX^2 + cX + d$ . Note that

$$\mathbf{e}_1 = 0, \quad \mathbf{e}_2 = b, \quad \mathbf{e}_3 = -c, \quad \mathbf{e}_4 = d.$$

To find the roots of  $f$ , suppose we can express  $f$  as a product of two quadratics. Using that  $f$  has no  $X^3$  term, we can write

$$f = X^4 + bX^2 + cX + d = (X^2 - mX + p)(X^2 + mX + q),$$

and comparing coefficients gives

$$b + m^2 = p + q, \quad c/m = p - q, \quad d = pq.$$

We can eliminate  $p, q$  via

$$(b + m^2)^2 - (c/m)^2 = (p + q)^2 - (p - q)^2 = 4pq = 4d.$$

This gives the cubic in  $m^2$

$$g = m^6 + 2bm^4 + (b^2 - 4d)m^2 - b^2,$$

which we can solve by the previous method.

Taking the square root, we can find  $m$ , and then we can find  $p$  and  $q$  via

$$p = b + m^2 + c/m, \quad q = b + m^2 - c/m.$$

We note that the two possible square roots of  $m^2$  just swap the two quadratics in  $(X^2 - m + p)(X^2 + m + q)$ .

## 1.4 The General Polynomial

Almost 300 years later, Ruffini (1799) and Abel (1824) proved that there is no general formula to express the root of a quintic in terms of radicals. This did not mean, however, that given a particular quintic, there was no such formula. In fact, formulae obviously exist for certain polynomials, for example those of the form  $X^n - a$ , which have the root  $\sqrt[n]{a}$ . It could even have been true that for each quintic over  $\mathbb{Q}$  some such formula could be found. The Abel-Ruffini Theorem just shows that no single formula can work for every such quintic.

Évariste Galois (1832) went much further. He showed how to associate to each polynomial a subgroup of the symmetric group which completely determines whether or not this polynomial has a solution by radicals: if and only if the group itself is solvable. Indeed, this is the origin of the term solvable group. The group associated to the polynomial  $f$  is called the Galois group in his honour, and written  $\text{Gal}(f)$ .

**Theorem 1.2** (Galois). *The polynomial  $f$  is solvable by radicals if and only if the group  $\text{Gal}(f)$  is solvable.*

We also have the following result.

**Theorem 1.3.** *Let  $f$  be an irreducible polynomial of degree  $n$ . Then  $\text{Gal}(f)$  is a transitive subgroup of the symmetry group  $S_n$ . Moreover, there exists an irreducible polynomial  $f$  over  $\mathbb{Q}$  such that  $\text{Gal}(f) = S_n$ .*

Since there are quintic polynomials over  $\mathbb{Q}$  whose Galois group is the full symmetric group  $S_5$ , and since this group is not solvable, there exist quintics over  $\mathbb{Q}$  which are not solvable in radicals. In fact, it is relatively easy to construct such examples.

From a more modern viewpoint, we replace the study of a polynomial by the study of the field extension generated by its roots. For example, if  $f \in \mathbb{Q}[X]$  is a polynomial with rational coefficients, and having roots  $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ , then we can consider the subfield  $K$  of  $\mathbb{C}$  generated by the  $\alpha_i$  (equivalently the smallest

subfield of  $\mathbb{C}$  containing each  $\alpha_i$ ). The Galois group  $\text{Gal}(f)$  equals the group of all field automorphisms of  $K$ .

In fact, the Galois group describes the internal structure of  $K$ . More precisely, there is a order preserving bijection between the poset of subfields of  $K$  and the poset of subgroups of  $\text{Gal}(f)$ . This is called the **Galois Correspondence**, and is one of the main results of this course. As a consequence, we see that there are only finitely many subfields of  $K$ , a fact which is far from obvious.

This passing between subgroups and subfields is an important and extremely useful observation. One should remark that group theory was in its infancy at that time, and in fact the abstract notion of a group had yet to be given. Galois was one of the first to appreciate the fundamental importance of groups, and nowadays this idea of studying an object by first understanding its symmetries is prevalent in modern mathematics and physics.

Let us discuss our approach to proving Galois' Theorem. Recall that a polynomial  $f$  is solvable by radicals if we can express a root of  $f$  in terms of  $+, -, \times, \div, \sqrt[r]{\phantom{x}}$ . More generally, we say that a field extension  $K/\mathbb{Q}$  is a **radical extension** if there exists a chain of subfields

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n = K$$

such that  $K_{i+1}$  is formed from  $K_i$  by extracting an  $r_i$ -th root of an element in  $K_i$ . In other words, we adjoin an element  $\lambda_i$  such that  $\lambda_i^{r_i} \in K_i$ . We observe that if  $K/\mathbb{Q}$  is radical, then every element of  $K$  can be obtained by repeated use of  $+, -, \times, \div, \sqrt[r]{\phantom{x}}$ .

The Galois correspondence furnishes us with a bijection between towers of field extensions  $L/K/\mathbb{Q}$  and subgroups  $\{1\} \leq \text{Gal}(L/K) \leq \text{Gal}(L/\mathbb{Q})$ . Recall that a finite group  $G$  is **solvable** if there exists a chain of subgroups

$$\{1\} = G_0 \leq \cdots \leq G_1 \leq G_0 = G$$

such that  $G_i \triangleleft G_{i-1}$  is a normal subgroup and the factor group  $G_{i-1}/G_i$  is cyclic of order  $r_i$ . Moreover, subgroups of solvable groups are solvable, and if  $N \triangleleft G$  is normal, then  $G$  is solvable if and only if both  $N$  and  $G/N$  are solvable.

We would like to say that if  $L/K$  is formed by adjoining an  $r$ -th root, then  $\text{Gal}(L/K)$  is a cyclic group of order  $r$ . Unfortunately this is not true in general, and we need to make an extra assumption: namely, we require that we have enough primitive roots of unity in the base field  $K$ . Since the only roots of unity in  $\mathbb{Q}$  are  $\pm 1$ , we have to apply a few tricks to prove the theorem.

## 1.5 Examples.

Let us illustrate this fundamental idea of passing from roots of polynomials to fields to automorphisms in some simple examples.

Consider the polynomial  $f = X^2 + 1 \in \mathbb{R}[X]$ . The roots of  $f$  in  $\mathbb{C}$  are  $\pm i$ , and the smallest subfield of  $\mathbb{C}$  containing  $i$  and  $\mathbb{R}$  is  $\mathbb{C}$  itself. In other words we can

construct  $\mathbb{C}$  from  $\mathbb{R}$  by ‘adding in’ a solution  $i$  to the equation  $X^2 + 1 = 0$ . Note that  $\mathbb{C}$  is a two dimensional real vector space with basis  $\{1, i\}$ . Complex conjugation is a field automorphism of  $\mathbb{C}$  of order 2 which fixes  $\mathbb{R}$  and, apart from the identity, is the only such. Also, complex conjugation permutes the two roots  $i, -i$  of  $f$ . In a certain sense, this symmetry exists because, from the point of view of  $\mathbb{R}$ , we cannot tell which root is which.

The same happens with  $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subset \mathbb{R}$ . From the point of view of  $\mathbb{Q}$  we cannot tell the difference between  $\sqrt{2}$  and  $-\sqrt{2}$ , and we have a field automorphism of  $\mathbb{Q}(\sqrt{2})$  induced by  $\sqrt{2} \mapsto -\sqrt{2}$ .

Now consider  $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ . This has no non-trivial automorphisms since  $\sqrt[3]{2}$  is the only real root of the polynomial  $X^3 - 2$ . This is why we need to consider the field generated by all the roots of a polynomial  $f$  in order to have the Galois correspondence.

## Chapter 2

# Background Material

### 2.1 Rings, Ideals and Homomorphisms

We will only consider commutative, unital rings.

An **integral domain** is a non-trivial ring  $R$  with no **zero-divisors**, i.e.  $ab = 0$  implies  $a = 0$  or  $b = 0$ . Equivalently,  $R$  has **cancellation**, so that if  $ax = bx$  with  $x \neq 0$ , then  $a = b$ .

If  $R$  is an integral domain, then we can form the **quotient field**, or **field of fractions**,  $\text{Quot}(R)$  of  $R$ . Its elements are written  $x/y$  for  $x, y \in R$  and  $y \neq 0$ , where  $x/y = x'/y'$  if  $xy' = x'y$ . The ring structure is given via

$$x/y + x'/y' := (xy' + x'y)/yy', \quad (x/y)(x'/y') := (xx')/(yy')$$

We identify  $R$  with the subring  $\{x/1 : x \in R\}$  of  $\text{Quot}(R)$ .

If  $A$  and  $B$  are subsets of a ring  $R$ , we write

$$A + B := \{a + b : a \in A, b \in B\} \quad \text{and} \quad AB := \{ab : a \in A, b \in B\}.$$

An **ideal**  $I \triangleleft R$  is an additive subgroup closed under multiplication by elements of  $R$ ; that is,  $RI \subset I$ . Since  $I$  is an additive subgroup of  $R$ , we have the factor group  $R/I$  whose elements are the additive cosets  $\bar{a} = a + I$ . This is again an abelian group with zero  $\bar{0} = I$ . We define a multiplication on  $R/I$  via  $(a + I)(b + I) := (ab) + I$ , or  $\bar{a} \cdot \bar{b} := \overline{ab}$ . Then  $R/I$  is again a ring, with unit  $\bar{1}$ , called the **factor ring** of  $R$  by  $I$ .

**Examples.**

1.  $\text{Quot}(\mathbb{Z}) = \mathbb{Q}$ .
2. If  $R$  is an integral domain, then  $R$  is a subring of  $\text{Quot}(R)$  but not an ideal.
3.  $n\mathbb{Z}$  is an ideal of  $\mathbb{Z}$ , so that  $\mathbb{Z}/n\mathbb{Z}$  is again a ring.

4.  $\{0\}$  and  $R$  are ideals of  $R$ .
5. Let  $I \triangleleft R$ . Write  $I[X]$  for the set of polynomials in  $R[X]$ , all of whose coefficients lie in  $I$ . Then  $I[X] \triangleleft R[X]$ .
6. Let  $S$  be a subset of a ring  $R$ . We write  $(S)$  for the smallest ideal containing  $S$ . Its elements are finite  $R$ -linear combinations of elements of  $S$ . If  $S = \{a_1, \dots, a_n\}$  is finite, we also write  $(S) = (a_1, \dots, a_n) = Ra_1 + \dots + Ra_n$ .

Let  $R$  and  $S$  be two rings. A (unital) **ring homomorphism**  $f: S \rightarrow R$  is a map preserving addition, multiplication and units; in other words,  $f$  is an additive group homomorphism such that  $f(1_S) = 1_R$  and  $f(ab) = f(a)f(b)$  for all  $a, b \in S$ . The ring homomorphism  $f$  is a **ring isomorphism** if there exists a ring homomorphism  $g: R \rightarrow S$  such that  $fg = \text{id}_R$  and  $gf = \text{id}_S$ , which is if and only if  $f$  is bijective.

The **kernel** of  $f$  is  $\text{Ker}(f) := \{a \in S : f(a) = 0 \in R\}$ ; it is an ideal of  $S$ . The **image** of  $f$  is  $\text{Im}(f) := \{f(a) \in R : a \in S\}$ ; it is a subring of  $R$ .

**Lemma 2.1.** 1. If  $S \leq R$  is a subring, then the inclusion  $\iota_S: S \hookrightarrow R$  is an injective ring homomorphism.

2. If  $I \triangleleft R$  be an ideal, then the canonical map  $\pi_I: R \rightarrow R/I$ ,  $a \mapsto a + I$ , is a surjective ring homomorphism.

**Theorem 2.2** (Isomorphism Theorems). 1. Let  $f: S \rightarrow R$  be a ring homomorphism and  $I \triangleleft S$  an ideal. If  $I \subset \text{Ker}(f)$ , then there exists a unique ring homomorphism  $\bar{f}: S/I \rightarrow R$  such that  $f = \bar{f}\pi_I$ . In particular, there exists a ring isomorphism

$$S/\text{Ker}(f) \cong \text{Im}(f), \quad a + \text{Ker}(f) \mapsto f(a).$$

2. Let  $I \triangleleft R$ . There exists a bijection between ideals of  $R$  containing  $I$  and ideals of  $R/I$ . If  $I \subset J \triangleleft R$ , then there is a ring isomorphism

$$(R/I)/(J/I) \cong R/J.$$

3. Let  $S \leq R$  be a subring and  $I \triangleleft R$  an ideal. Then  $S + I$  is a subring of  $R$ . Moreover,  $I \triangleleft (S + I)$  and  $(S \cap I) \triangleleft S$ , and there exists a ring isomorphism

$$(S + I)/I \cong S/(S \cap I).$$

### Examples.

1. Let  $I \triangleleft R$ , so that  $I[X] \triangleleft R[X]$ . There is a ring homomorphism  $R[X] \rightarrow (R/I)[X]$ ,  $aX^n \mapsto \bar{a}X^n$ . This is surjective with kernel  $I[X]$ . Thus there exists a ring isomorphism  $R[X]/I[X] \cong (R/I)[X]$ .

2. Let  $S \subset R$  be a subring and  $\alpha \in R$ . There exists a ring homomorphism  $\text{ev}_\alpha: S[X] \rightarrow R$ ,  $X \mapsto \alpha$ , called **evaluation** at  $\alpha$ . If  $f \in R[X]$ , we write  $f(\alpha)$  for  $\text{ev}_\alpha(f)$ . The image of  $\text{ev}_\alpha$  is denoted  $S[\alpha]$ , and is the smallest subring of  $R$  containing  $S$  and  $\alpha$ .

Let  $I \triangleleft R$ . We call  $I$

- proper** if  $I \neq R$ .
- trivial** if  $I = \{0\}$ .
- maximal** if  $I$  is proper, and  $I \subset J \triangleleft R$  implies  $J = I$  or  $J = R$ .
- prime** if  $xy \in I$  implies  $x \in I$  or  $y \in I$ .
- principal** if there exists  $x \in I$  such that  $I = (x) = Rx = \{rx : r \in R\}$ .

**Proposition 2.3.** *Let  $R$  be a ring and  $I \triangleleft R$  an ideal of  $R$ . Then*

- (1)  $R/I$  is a field if and only if  $I$  is maximal.
- (1)'  $R$  is a field if and only if  $(0)$  and  $R$  are the only ideals of  $R$ .
- (2)  $R/I$  is an integral domain if and only if  $I$  is prime.
- (2)'  $R$  is an integral domain if and only if  $(0)$  is prime.
- (3)  $I$  maximal implies  $I$  prime.
- (3)'  $R$  a field implies  $R$  an integral domain.

**Lemma 2.4.** *Let  $K$  be a field and  $R$  a non-trivial ring. Then every ring homomorphism  $f: K \rightarrow R$  is injective.*

*Proof.*  $\text{Ker}(f)$  is an ideal of  $K$ , so either  $(0)$  or  $K$  itself. If  $\text{Ker}(f) = (0)$ , then  $f$  is injective. If  $\text{Ker}(f) = K$ , then  $1_R = f(1_K) = 0_R$ , so that  $R$  is trivial.  $\square$

## 2.2 Division and Factorisation

In a ring  $R$ , we say that  $a$  **divides**  $b$ , written  $a|b$ , if there exists  $x \in R$  such that  $b = ax$ . Equivalently,  $b \in (a)$ , or  $(b) \subset (a)$ . Note that 1 divides every other element, and each element divides 0.

If  $R$  is an integral domain, then  $a|b$  and  $b|a$  if and only if there exists a unit  $u \in R^\times$  such that  $b = au$ . For, there exist  $u, v \in R$  such that  $b = au$  and  $a = bv$ . If  $b = 0$  then  $a = 0$ . Otherwise, since  $b = buv$  and  $R$  is an integral domain, we can cancel  $b$  to get  $uv = 1$ , so  $u, v \in R^\times$  are units.

A **principal ideal domain** is an integral domain  $R$  for which every ideal is generated by a single element, so of the form  $(a)$  for some  $a \in R$ .

**Proposition 2.5.** *Let  $K$  be a field. Then the polynomial ring  $K[X]$  is a principal ideal domain.*

*Proof.* Let  $I \triangleleft K[X]$  be a non-zero ideal, and let  $g \in I$  be chosen such that  $\deg(g) \geq 0$  is minimal. Let  $f \in I$ . By the division algorithm, there exist polynomials  $q, r$  such that  $f = qg + r$  and  $\deg(g) > \deg(r)$ . Now,  $r = f - qg \in I$ , so the minimality of  $g$  gives  $\deg(r) = -\infty$ ; i.e.  $r = 0$ . Therefore  $g$  divides  $f$ , so  $f \in (g)$ . It follows that  $I = (g)$  is principal.  $\square$

We call a non-constant polynomial  $f \in K[X]$  **irreducible** if, whenever  $f = gh$ , either  $g \in K$  or  $h \in K$ . We call  $f$  **monic** provided its leading coefficient is 1.

**Proposition 2.6.** *A prime ideal of  $K[X]$  is either  $(0)$  or of the form  $(f)$  with  $f \in K[X]$  monic and irreducible. Conversely, if  $f \in K[X]$  is monic and irreducible, then  $(f)$  is a maximal ideal.*

*Proof.* Since  $K[X]$  is an integral domain,  $(0)$  is a prime ideal. Let  $I \triangleleft K[X]$  be a non-zero prime ideal. Since  $K[X]$  is a principal ideal domain,  $I = (f)$  for some  $f$ . Moreover, we may assume that  $f$  is monic (and hence uniquely determined by  $I$ ). To see that  $f$  is irreducible, suppose  $f = gh$ . Then  $gh \in (f)$ , and since  $(f)$  is prime we may assume  $h \in (f)$ . Thus  $h = uf$  for some  $u$ , so  $f = gh = fgu$ . Cancelling  $f$  gives  $gu = 1$ , so  $g \in K^\times$  is a unit. Thus  $f$  is irreducible.

Now let  $f$  be monic and irreducible. Take  $g \in K[X]$  such that  $\bar{g} \neq 0$  in  $K[X]/(f)$ . Since  $K[X]$  is a principal ideal domain,  $(f, g) = (d)$  for some  $d$ , and there exist polynomials  $x, y$  such that  $fx + gy = d$ . Now,  $d$  is the greatest common divisor of  $f$  and  $g$ , and since  $f$  is irreducible, we have either  $d = 1$  or  $d = f$ . If  $d = f$ , then  $f$  divides  $g$ , so that  $g \in (f)$  and  $\bar{g} = 0$ , a contradiction. Thus  $d = 1$ , and from  $fx + gy = 1$  we deduce  $\bar{g}\bar{y} = \bar{1}$ , so that  $\bar{g}$  is invertible. Therefore  $K[X]/(f)$  is a field, so  $(f)$  is maximal.  $\square$

**Theorem 2.7.** *Every polynomial  $f \in K[X]$  can be written as  $f = af_1 \cdots f_n$ , where  $a \in K$  and  $f_i \in K[X]$  are monic and irreducible. Moreover, such an expression is unique up to the ordering of the  $f_i$ .*

*Proof.* Let  $f \in K[X]$  be non-zero. We can write  $f = a\bar{f}$ , where  $a \in K$  and  $\bar{f}$  is monic. If  $\bar{f}$  is not irreducible, then there exists some expression  $\bar{f} = gh$  with  $g, h$  non-constant polynomials. Then  $0 < \deg(g), \deg(h) < \deg(f)$ . Moreover, by examining leading coefficients, we may assume that both  $g$  and  $h$  are monic. By induction on degree, we can express both  $g$  and  $h$  as a product of monic irreducible polynomials, hence we can write  $f$  in the desired form.

Suppose now that  $f = af_1 \cdots f_m = bg_1 \cdots g_n$ , where  $a, b \in K$  and  $f_i, g_j \in K[X]$  are monic and irreducible. By Proposition 2.6,  $K[X]/(f_1)$  is a field. Also,  $\bar{b}\bar{g}_1 \cdots \bar{g}_n = \bar{f} = 0$  in  $K[X]/(f_1)$ , so that  $\bar{g}_i = 0$  for some  $i$ . After reordering, we may assume that  $\bar{g}_1 = 0$ . Thus  $g_1 \in (f_1)$ , the kernel, so  $g_1 = uf_1$  for some  $u$ . Since  $g_1$  is irreducible and  $f_1 \notin K$ , we must have  $u \in K$ . Finally, since  $f_1$  and  $g_1$  are monic, we must have  $u = 1$ , so that  $f_1 = g_1$ .

Since  $K[X]$  is an integral domain, we may cancel terms to deduce  $af_2 \cdots f_m = bg_2 \cdots g_n$ , so by induction (and relabelling) we have  $m = n$ ,  $f_i = g_i$  for all  $i$ , and  $a = b$ .  $\square$

**Lemma 2.8.** *Let  $\alpha \in K$ . Then the kernel of the evaluation map  $\text{ev}_\alpha: K[X] \rightarrow K$  is the ideal  $(X - \alpha)$ . In particular,  $\alpha$  is a root of a polynomial  $f$  if and only if  $X - \alpha$  divides  $f$ , and  $f$  has at most  $\deg(f)$  distinct roots in  $K$ .*

*Proof.* Let  $I = \text{Ker}(\text{ev}_\alpha)$ . Then  $(X - \alpha) \subset I$ , and  $(X - \alpha)$  is a maximal ideal by Proposition 2.6. Since  $I$  is a proper ideal, we must have  $I = (X - \alpha)$ .

Now,  $\alpha$  is a root of a polynomial  $f$  if and only if  $0 = f(\alpha) = \text{ev}_\alpha(f)$ , which is if and only if  $f \in \text{Ker}(\text{ev}_\alpha) = (X - \alpha)$ , which is if and only if  $X - \alpha$  divides  $f$ .

Let  $\alpha$  be a root of  $f$ , so  $f = (X - \alpha)f_1$ . If  $\beta \neq \alpha$  is another root of  $f$ , then  $0 = f(\beta) = (\beta - \alpha)f_1(\beta)$ , and since  $\alpha \neq \beta$  we must have  $f_1(\beta) = 0$ . Therefore  $\beta$  is a root of  $f_1$ , so  $f_1 = (X - \beta)f_2$ , and  $f = (X - \alpha)(X - \beta)f_2$ . It follows that  $f$  has at most  $\deg(f)$  distinct roots in  $K$ .  $\square$

## 2.3 Irreducibility of Polynomials

We call  $f = a_0X^d + \cdots + a_{d-1}X + a_d \in \mathbb{Z}[X]$  **primitive** if  $\gcd(a_i) = 1$ . In particular, all monic polynomials are primitive.

**Lemma 2.9** (Gauss' Lemma). *If  $f \in \mathbb{Z}[X]$  is primitive, then it is irreducible over  $\mathbb{Z}$  if and only if it is irreducible over  $\mathbb{Q}$ .*

**Lemma 2.10** (Eisenstein's Criterion). *Let  $f = a_0X^d + \cdots + a_{d-1}X + a_d \in \mathbb{Z}[X]$  be primitive. Suppose that there exists a prime  $p$  such that  $p|a_i$  for  $i = 1, \dots, d$ , but  $p \nmid a_0$  and  $p^2 \nmid a_d$ . Then  $f$  is irreducible.*

**Lemma 2.11** (Rational Root Test). *Let  $f = a_0X^n + \cdots + a_n \in \mathbb{Z}[X]$ . If  $\alpha = p/q \in \mathbb{Q}$  is a root of  $f$  such that  $\gcd(p, q) = 1$ , then  $p|a_n$  and  $q|a_0$ .*

In general, it is difficult to determine whether a given polynomial is irreducible or not, and to find its decomposition into irreducible factors. One can compare this to the problem of determining whether a given number is prime, and to finding its prime factorisation.

Let  $K$  be a field and  $f \in K[X]$ . Clearly if  $\deg(f) = 1$ , then  $f$  is irreducible. Also, if  $\deg(f) = 2$  or  $3$ , then  $f$  is irreducible if and only if it has no linear factor, which is if and only if it has no root in  $K$ . If  $\deg(f) = 4$ , though, it could have a decomposition into two irreducible quadratic polynomials.

Suppose  $K = \mathbb{Q}$ . Clearing denominators, we may assume  $f \in \mathbb{Z}[X]$  is primitive. By Gauss' Lemma,  $f$  is irreducible over  $\mathbb{Q}$  if and only if it is irreducible over  $\mathbb{Z}$ . Moreover, by the Rational Root Test, we know the possible rational roots of  $f$ . In particular, if  $f$  is monic, then any rational root is in fact integral.

For higher degrees, we can also use Eisenstein's Criterion. This is particularly useful if we combine it with a linear change of variables  $Y = X - a$ .

Another powerful method is reduction modulo a prime  $p$ . We write  $\mathbb{F}_p$  for the field  $\mathbb{Z}/p\mathbb{Z}$ . Consider the surjective ring homomorphism  $\mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$ ,  $f \mapsto \bar{f}$ . Clearly if  $f = gh \in \mathbb{Z}[X]$ , then  $\bar{f} = \bar{g}\bar{h} \in \mathbb{F}_p[X]$ . Thus if  $\bar{f}$  is irreducible over

$\mathbb{F}_p$  for some prime  $p$ , then  $f$  itself must be irreducible over  $\mathbb{Z}$ . Now, it is a finite problem to find a factorisation over  $\mathbb{F}_p$ , so we can use a computer. However, this problem grows exponentially in the degree of the polynomial. (Reference?)

Variations of this idea can also be applied. For example, suppose that we are given  $f \in \mathbb{Z}[X]$  of degree 4. Using the Rational Root Test, we may assume that  $f$  has no linear factors, so that if  $f = gh$  has a proper factorisation, then  $\deg(g) = \deg(h) = 2$ . Now suppose that  $\bar{f} \in \mathbb{F}_p[X]$  factors as  $\bar{f} = rs$  with  $r, s$  irreducible,  $\deg(r) = 1, \deg(s) = 3$ . This is incompatible with any factorisation  $f = gh$  with  $\deg(g) = \deg(h) = 2$ , so  $f$  must itself be irreducible.

**Examples.**

1.  $f = X^2 - 2 \in \mathbb{Z}[X]$ . Eisenstein tells us that  $f$  is irreducible over  $\mathbb{Z}$ , so by Gauss' Lemma,  $f$  is irreducible over  $\mathbb{Q}$ . In other words,  $\sqrt{2}$  is not a rational number.
2.  $f = \frac{2}{9}X^5 + \frac{5}{3}X^4 + X^3 + \frac{1}{3}$ . Clearing denominators we have  $g = 9f = 2X^5 + 15X^4 + 9X^3 + 3$ . We can use Eisenstein's Criterion with  $p = 3$  to deduce that  $g$ , and hence  $f$ , is irreducible.
3.  $f = X^3 - 7X^2 + 3X + 3$ . The only possible rational roots are  $\pm 1, \pm 3$ . Checking, we see that  $f = (X-1)(X^2-6X-3)$  as a product of irreducibles.
4.  $f = X^4 + 15X^3 + 7$ . Working over  $\mathbb{F}_2$ , we have  $\bar{f} = X^4 + X^3 + 1$ . This has no linear factor, since neither 0, 1 are roots of  $\bar{f}$  over  $\mathbb{F}_2$ . Suppose

$$\begin{aligned} \bar{f} &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a+c)X^3 + (b+ac+d)X^2 + (ad+bc)X + bd. \end{aligned}$$

From the constant term we see that  $b = d = 1$ . Therefore the the coefficient of  $X$  gives  $a + c = 0$ , whereas the coefficient of  $X^3$  gives  $a + c = 1$ , a contradiction. So  $\bar{f}$  is irreducible over  $\mathbb{F}_2$ , whence  $f$  is irreducible over  $\mathbb{Z}$ .

5. Consider  $f = X^4 + 1$  and its factorisations over various finite fields:

$p$	$\bar{f}$	$p$	$\bar{f}$
2	$(X+1)^4$	7	$(X^2+3X+1)(X^2-3X+1)$
3	$(X^2+X-1)(X^2-X-1)$	11	$(X^2+3X-1)(X^2-3X-1)$
5	$(X^2+2)(X^2-2)$	13	$(X^2+5)(X^2-5)$

Either  $f$  is irreducible or else the product of two irreducible quadratics, but the above data give no further information. However, if we consider  $Y = X - 1$ , then we obtain  $(Y + 1)^4 + 1 = Y^4 + 4Y^3 + 6Y^2 + 4Y + 2$ . Applying Eisenstein with  $p = 2$ , we see that  $f$  is irreducible.

[Since  $(X^4 - 1)f = X^8 - 1$ , the roots of  $f$  are eighth roots of unity. In fact they are precisely the primitive eighth roots of unity, of which there are four, corresponding to the four numbers  $1 \leq r < 8$  which are prime to 8. We will discuss roots of unity later, as an application of Galois Theory.]

## Chapter 3

# Field Extensions

Let  $L$  be a field and  $K \subset L$  a subfield. We write  $L/K$  and call  $L$  a field extension of  $K$ . We observe that  $L$  is naturally a  $K$ -vector space, using the given addition and multiplication in  $L$ . We denote its dimension by  $[L : K]$ , and call this the **degree** of the extension. We say that  $L/K$  is a **finite** field extension if  $[L : K] < \infty$ . Clearly  $L = K$  if and only if  $[L : K] = 1$ .

If  $L/K$  is a field extension, an **intermediate field** is a subfield  $E$  of  $L$  containing  $K$ , so  $L/E/K$  is a **tower** of field extensions.

**Theorem 3.1** (Tower Law). *Let  $L/K/k$  be a tower of field extensions. Then  $L/k$  is a field extension and*

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

*In particular,  $L/k$  is finite if and only if both  $L/K$  and  $K/k$  are finite.*

*Proof.* Let  $\{\alpha_i\}_{i \in I}$  be a  $K$ -basis of  $L$  and  $\{\beta_j\}_{j \in J}$  a  $k$ -basis of  $K$ . Then the set of products  $\{\alpha_i \beta_j\}_{(i,j) \in I \times J}$  is a  $k$ -basis of  $L$ .

Linear Independence: Suppose that  $\sum_{i,j} \lambda_{ij} \alpha_i \beta_j = 0$ , where  $\lambda_{ij} \in k$ , almost all zero. Set  $\mu_i := \sum_j \lambda_{ij} \beta_j \in K$ , so almost all  $\mu_i$  are zero. Then  $\sum_i \mu_i \alpha_i = 0$ , so  $\mu_i = 0$  for all  $i$ . Thus  $\sum_j \lambda_{ij} \beta_j = 0$  for all  $i$ , so  $\lambda_{ij} = 0$  for all  $i, j$ .

Spanning: Let  $\theta \in L$ . We can write  $\theta = \sum_i \mu_i \alpha_i$ , where  $\mu_i \in K$ , almost all zero. Now write  $\mu_i = \sum_j \lambda_{ij} \beta_j$ , where  $\lambda_{ij} \in k$ , almost all zero. Then  $\theta = \sum_{i,j} \lambda_{ij} \alpha_i \beta_j$ .  $\square$

Let  $L/K$  be a field extension and  $S \subset L$ . We write  $K[S]$  for the smallest subring of  $L$  containing  $K$  and  $S$ , and  $K(S)$  for the smallest subfield of  $L$  containing  $K$  and  $S$ . Since  $L$  is a field,  $K[S]$  is an integral domain, so  $K(S) = \text{Quot}(K[S])$ .

This definition makes sense, since if  $M_i \subset L$  are subrings containing both  $K$  and  $S$ , then their intersection  $\bigcap_i M_i \subset L$  is again a subring containing both  $K$  and  $S$ . Hence we can define  $K[S]$  to be the intersection of all subrings of  $L$  containing  $K$  and  $S$ . Similarly for  $K(S) = \text{Quot}(K[S])$ .

If  $L = K(S)$  for some finite subset  $S$ , then we call  $L/K$  **finitely generated**. If  $L = K(\alpha)$ , then we call  $L/K$  **simple**.

We observe that for a field extension  $L/K$ , if  $S \subset L$  and  $\alpha \in L$ , then  $K(S \cup \{\alpha\}) = K(S)(\alpha)$ . For, a subfield of  $L$  contains  $K$ ,  $S$  and  $\alpha$  if and only if it contains  $K(S)$  and  $\alpha$ .

Now suppose that  $E, F$  are two subfields of  $L$ . The **compositum**  $EF$  of  $E$  and  $F$  in  $L$  is the smallest subfield of  $L$  containing both  $E$  and  $F$ . Thus  $EF = E(F) = F(E)$  in the above notation.

We remark that in all of the above constructions, we need the ambient field  $L$ . This is philosophically a problem since we are interested in roots of polynomials, in which case we begin with  $f \in K[X]$  and want to construct a field extension in which  $f$  has a root, or even better a field extension of  $K$  which contains all the roots of  $f$ .

### 3.1 The Minimal Polynomial

Let  $L/K$  be a field extension and  $\alpha \in L$ . Recall that we have the evaluation homomorphism  $\text{ev}_\alpha: K[X] \rightarrow L$ ,  $X \mapsto \alpha$ . This sends a polynomial  $f \in K[X]$  to  $f(\alpha)$ .

The element  $\alpha$  is called **algebraic** over  $K$  if there exists a non-zero polynomial  $f \in K[X]$  such that  $f(\alpha) = 0$  in  $L$ . Otherwise  $\alpha$  is called **transcendental**.

The next theorem is essentially equivalent to Proposition 2.6.

**Theorem 3.2.** *Let  $L/K$  be a field extension and  $\alpha \in L$ . Then there are two possibilities:*

1. (i)  $\alpha$  algebraic over  $K$ .  
(ii)  $\text{Ker}(\text{ev}_\alpha) = (m_{\alpha/K})$  for some monic irreducible polynomial  $m_{\alpha/K}$ .  
(iii)  $K[\alpha] = K(\alpha)$ .  
(iv)  $[K(\alpha) : K] = \deg(m_{\alpha/K}) < \infty$ .
2. (i)  $\alpha$  transcendental over  $K$ .  
(ii)  $\text{ev}_\alpha$  injective.  
(iii)  $K[\alpha] \neq K(\alpha)$ .  
(iv)  $[K(\alpha) : K] = \infty$ .

*Proof.* Consider  $\text{ev}_\alpha: K[X] \rightarrow L$ . This has image  $K[\alpha]$ , which is an integral domain since it is a subring of the field  $L$ . Therefore  $I := \text{Ker}(\text{ev}_\alpha)$  is a prime ideal. By Proposition 2.6, either  $I = (0)$  and  $\text{ev}_\alpha$  is injective, or else  $I = (m_{\alpha/K})$  for some monic irreducible polynomial  $m_{\alpha/K}$ , uniquely determined by  $I$  (equivalently  $\alpha$ ), and  $I$  is maximal, whence  $K[\alpha] = K(\alpha)$  is a field.

In summary, if the kernel is zero, then  $K[\alpha] \cong K[X]$  is not a field, so  $K[\alpha] \neq K(\alpha)$ ;  $[K(\alpha) : K] \geq [K[\alpha] : K] = \infty$ ;  $\alpha$  is transcendental.

Otherwise, if the kernel is non-zero, then it is generated by some monic irreducible polynomial  $m_{\alpha/K}$ ;  $K[\alpha] = K(\alpha)$  is a field;  $\alpha$  is algebraic. To see that  $[K(\alpha) : K] = \deg(m_{\alpha/K}) < \infty$ , we observe that the elements  $\alpha^r$  for  $0 \leq r < \deg(m_{\alpha/K})$  form a  $K$ -basis of  $K[\alpha]$ .  $\square$

For  $L/K$  and  $\alpha \in L$  algebraic over  $K$ , we call the monic irreducible polynomial  $m_{\alpha/K} \in K[X]$  the **minimal polynomial** of  $\alpha$  over  $K$ . It is uniquely determined by  $\alpha$  and  $K$ .

**Corollary 3.3.** *Let  $K$  be a field.*

1.  $K(X) := \text{Quot}(K[X])$  is a simple extension of  $K$  and  $X$  is transcendental over  $K$ .
2. Let  $f \in K[X]$  be monic and irreducible, and set  $L := K[X]/(f)$ ,  $\alpha := X + (f) \in L$ . Then  $L = K(\alpha)$  is a finite simple extension of  $K$ ,  $[L : K] = \deg(f)$ , and  $m_{\alpha/K} = f$ .

*Proof.* For (1) we just need to recall that  $K(X) = \text{Quot}(K[X])$ . Therefore  $K[X] \hookrightarrow K(X)$ .

For (2) we first note that  $K[X]/(f)$  is a field by Proposition 2.6, and contains  $K$  as a subfield. (More precisely, we may identify  $K$  with its image in  $K[X]/(f)$ .) Now the evaluation map  $\text{ev}_\alpha$  is just the canonical ring homomorphism  $K[X] \rightarrow K[X]/(f) = L$ , so in particular has kernel  $(f)$ .  $\square$

This gives us a way of constructing field extensions of a given field  $K$  without reference to another field. In particular, we have the following result, solving the first part of our philosophical problem discussed earlier.

**Corollary 3.4** (Kronecker). *Let  $f \in K[X]$  be non-constant. Then there exists a field extension  $L/K$  in which  $f$  has a root. Moreover,  $[L : K] \leq \deg(f)$ .*

*Proof.* Let  $g$  be a monic irreducible factor of  $f$  in  $K[X]$ . Consider the field extension  $L = K[X]/(g)$  of  $K$ , and set  $\alpha := X + (g)$ . As in the previous corollary,  $\alpha$  has minimal polynomial  $g$ , so  $\alpha$  is a root of  $g$ , hence a root of  $f$ . Note that  $[L : K] = \deg(g) \leq \deg(f)$ .  $\square$

**Examples.**

1.  $\mathbb{C}/\mathbb{R}$  and  $i \in \mathbb{C}$ . Then  $m_{i/\mathbb{R}} = X^2 + 1$ .
2.  $\mathbb{C}/\mathbb{Q}$  and  $\sqrt{2} \in \mathbb{C}$ . Then  $m_{\sqrt{2}/\mathbb{Q}} = X^2 - 2$ .
3.  $\mathbb{C}/\mathbb{R}$  and  $\sqrt{2} \in \mathbb{R}$ . Then  $m_{\sqrt{2}/\mathbb{R}} = X - \sqrt{2}$ .
4.  $\mathbb{C}/\mathbb{Q}$  and  $\zeta = \exp(2\pi i/5) \in \mathbb{C}$ . Then  $m_{\zeta/\mathbb{Q}} = X^4 + X^3 + X^2 + X + 1$ .
5.  $\pi, e \in \mathbb{R}$  are transcendental over  $\mathbb{Q}$  (hard).

In fact, **Hilbert's Seventh Problem**, from his address to the ICM in 1900, posed the following problem:

If  $a$  and  $b$  are algebraic, with  $a \neq 0, 1$  and  $b$  irrational, then is  $a^b$  necessarily transcendental?

This was proved in 1934, independently by **Gelfond and Schneider**. For example, the number  $\sqrt{2}^{\sqrt{2}}$  is transcendental (but note that  $(\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = 2$  is again rational).

**Remark.** The definition of a compositum of two fields requires an ambient field. If  $E$  and  $F$  are field extensions of  $K$ , we could instead consider the tensor product  $E \otimes_K F$  and take a maximal ideal  $I$ . Then  $E \otimes_K F/I$  is again a field and we have embeddings  $E, F \rightarrow E \otimes_K F/I$ . The problem is that this definition depends on the choice of  $I$ . For example, if

$$E \cong F \cong \mathbb{Q}[X]/(X^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2}),$$

then

$$\begin{aligned} E \otimes_K F &\cong \mathbb{Q}[X, Y]/(X^3 - 2, X^3 - Y^3) \\ &\cong \mathbb{Q}[X, Y]/(X^3 - 2, (X - Y)(X^2 + XY + Y^2)). \end{aligned}$$

We have maximal ideals

$$I = (X^3 - 2, X - Y) \quad \text{and} \quad J = (X^3 - 2, X^2 + XY + Y^2),$$

and

$$\begin{aligned} E \otimes_K F/I &\cong \mathbb{Q}[X]/(X^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2}), \\ E \otimes_K F/J &\cong \mathbb{Q}[X, Z]/(X^3 - 2, Z^2 + Z + 1) \cong \mathbb{Q}(\sqrt[3]{2}, \omega). \end{aligned}$$

Here we have made the substitution  $Z = Y/X$  and written  $\omega$  for a primitive cube root of unity. In particular,

$$[E \otimes_K F/I : \mathbb{Q}] = 3 \quad \text{and} \quad [E \otimes_K F/J : \mathbb{Q}] = 6,$$

so the fields are non-isomorphic.

## 3.2 The Norm and Trace

Let  $L/K$  be a finite field extension and  $\alpha \in L$ . Then multiplication by  $\alpha$  induces a  $K$ -linear endomorphism  $A$  of  $L$ . The **Cayley-Hamilton Theorem** says that every endomorphism satisfies its own characteristic equation  $\chi_A(X) = \det(X - A) \in K[X]$ ; that is,  $\chi_A(A)$  is the zero-map on  $L$ . We observe that  $A^r(\beta) = \alpha^r \beta$  for all  $\beta \in L$ , so that  $\chi_A(A)$  acts on  $L$  as multiplication by  $\chi_A(\alpha)$ . Therefore  $\alpha$  is a root of the polynomial  $\chi_A(X)$ .

Note that the characteristic polynomial  $\chi_A(X)$  is a monic polynomial and is independent of the choice of basis, so depends only on  $\alpha$  and  $L/K$ . We denote it by  $\chi_{\alpha/K}^L$  and call it the field equation of  $\alpha/K$  with respect to  $L$ .

**Theorem 3.5.** *Let  $L/k$  be a finite field extension and let  $\alpha \in L$ . Then*

$$\chi_{\alpha/k}^{k(\alpha)} = m_{\alpha/k} \quad \text{and} \quad \chi_{\alpha/k}^L = (m_{\alpha/k})^{[L:k(\alpha)]}.$$

*Proof.* Suppose first that  $L = k(\alpha)$ . Since  $\alpha$  is a root of the polynomial  $\chi_{\alpha/k}^L$ , we know that  $m_{\alpha/k}$  divides  $\chi_{\alpha/k}^L$ . Since they are both monic polynomials of degree  $[k(\alpha) : k]$ , they must be equal. This proves the first result.

Now let  $K = k(\alpha)$  (or more generally any subfield of  $L$  containing  $k(\alpha)$ ). Let  $\{u_i\}_i$  be a  $K$ -basis of  $L$  and  $\{v_p\}_p$  a  $k$ -basis of  $K$ . Then  $\{u_i v_p\}_{(i,p)}$  is a  $k$ -basis of  $L$ . Let  $A: L \rightarrow L$  and  $B: K \rightarrow K$  be the  $k$ -linear maps corresponding to multiplication by  $\alpha$ . Let  $B = (b_{pq})$  be the matrix with respect to  $\{v_p\}$  and  $A = (a_{ipjq})$  the matrix with respect to  $\{u_i v_p\}$ . Then

$$\sum_{i,p} a_{ipjq} u_i v_p = \alpha u_j v_q = u_j \alpha v_q = \sum_p b_{pq} u_j v_p.$$

Hence  $a_{ipjq} = \delta_{ij} b_{pq}$ , so  $A$  can be written in block-diagonal form, with  $[L : K]$  copies of  $B$  on the diagonal. This proves the second statement.  $\square$

**Remark.** A different proof can be constructed using the following general result from linear algebra: if  $V$  is a  $k$ -vector space,  $A: V \rightarrow V$  a  $k$ -linear endomorphism of  $V$  and  $U \leq V$  a subspace such that  $A(U) \subset U$ , then  $A$  induces endomorphisms  $B: U \rightarrow U$  and  $C: V/U \rightarrow V/U$ . Choosing a basis for  $U$  and extending to a basis for  $V$ , we can write the matrix for  $A$  in block form, with the matrices for  $B$  and  $C$  on the diagonal, and zero in the bottom left corner. Thus  $\chi_A = \chi_B \chi_C$ . Let  $L/K$  be a finite field extension,  $\alpha \in L$  and  $A$  the  $K$ -linear automorphism of  $L$  induced by multiplication by  $\alpha$ . We define the **norm** of  $\alpha$  in  $L/K$  to be  $N_K^L(\alpha) := \det(A)$  and the **trace** of  $\alpha$  in  $L/K$  to be  $\text{Tr}_K^L(\alpha) := \text{Tr}(A)$ .

**Proposition 3.6.** *Let  $L/K$  be a finite field extension and  $\alpha, \beta \in L$ . Then*

1.  $N_K^L: L^* \rightarrow K^*$  is a group homomorphism between multiplicative groups. In particular,  $N_K^L(\alpha\beta) = N_K^L(\alpha)N_K^L(\beta)$ .
2.  $\text{Tr}_K^L: L \rightarrow K$  is a group homomorphism between additive groups. In particular,  $\text{Tr}_K^L(\alpha + \beta) = \text{Tr}_K^L(\alpha) + \text{Tr}_K^L(\beta)$ .

*Proof.* Let  $A$  and  $B$  be the  $K$ -linear automorphisms of  $L$  induced by multiplication by  $\alpha$  and  $\beta$  respectively. Then  $AB$  corresponds to multiplication by  $\alpha\beta$ , so

$$N_K^L(\alpha\beta) = \det(AB) = \det(A)\det(B) = N_K^L(\alpha)N_K^L(\beta).$$

If  $\alpha \in L$  is non-zero, then  $A$  is invertible, so that  $N_K^L(\alpha) = \det(A) \neq 0$ . If  $\alpha = 1$ , then  $A = \text{id}_L$  so that  $N_K^L(1) = 1$ . This shows that  $N_K^L: L^* \rightarrow K^*$  is a group homomorphism.

Similarly,  $A + B$  corresponds to multiplication by  $\alpha + \beta$ , so

$$\text{Tr}_K^L(\alpha + \beta) = \text{Tr}(A + B) = \text{Tr}(A) + \text{Tr}(B) = \text{Tr}_K^L(\alpha) + \text{Tr}_K^L(\beta).$$

If  $\alpha = 0$ , then  $A = 0$  so  $\text{Tr}_K^L(0) = 0$ . Thus  $\text{Tr}_K^L: L \rightarrow K$  is a group homomorphism.  $\square$

**Theorem 3.7.** *Let  $L/K/k$  be finite field extensions. Then*

$$N_k^L = N_k^K \circ N_K^L \quad \text{and} \quad \text{Tr}_k^L = \text{Tr}_k^K \circ \text{Tr}_K^L.$$

A proof of this is outlined in the exercises, although we will provide a different proof later on using Galois Theory in the special case when  $L/k$  is separable.

### 3.3 Algebraic Field Extensions

A field extension  $L/K$  is called **algebraic** if each element  $\alpha \in L$  is algebraic over  $K$ .

**Lemma 3.8.** *All finite field extensions are algebraic. Conversely, a field extension  $L/K$  is finite if and only if it is finitely generated by algebraic elements.*

*Proof.* Let  $L/K$  be finite and let  $\alpha \in L$ . Then  $[K(\alpha) : K]$  is finite by the **Tower Law**, so  $\alpha$  is algebraic over  $K$  by Theorem 3.2. Hence  $L/K$  is algebraic. It is clearly finitely generated, for example by the elements of a  $K$ -basis of  $L$ .

Conversely, suppose that  $L = K(\alpha_1, \dots, \alpha_n)$  with each  $\alpha_i$  algebraic over  $K$ . Set  $L' := L(\alpha_1, \dots, \alpha_{n-1})$ , so  $L = L'(\alpha_n)$ . By induction,  $[L' : K]$  is finite. Also, since  $\alpha_n$  is algebraic over  $K$ , it is *a fortiori* algebraic over  $L'$ , so  $[L' : L]$  is finite by Theorem 3.2. Hence  $[L : K] = [L : L'][L' : K]$  is finite by the **Tower Law**.  $\square$

**Theorem 3.9.** *Let  $L/K$  be a field extension and write  $L^{\text{alg}/K}$  for the subset of  $L$  consisting of those elements which are algebraic over  $K$ . Then  $L^{\text{alg}/K}$  is a subfield of  $L$ , and is an algebraic field extension of  $K$ .*

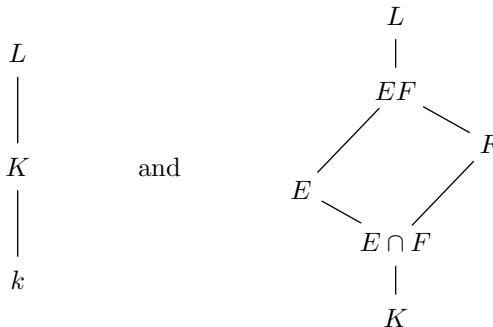
*Proof.* We need to show that if  $\alpha, \beta \in L^{\text{alg}/K}$  and  $\beta \neq 0$ , then  $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in L^{\text{alg}/K}$ . Since  $\alpha, \beta$  are algebraic over  $K$ ,  $K(\alpha, \beta)/K$  is finite, hence algebraic, by Lemma 3.8. Thus  $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha, \beta)$  are all algebraic over  $K$ .  $\square$

**Theorem 3.10.** *1. Let  $L/K/k$  be field extensions. Then  $L/k$  is algebraic if and only if both  $L/K$  and  $K/k$  are algebraic. Similarly for finite instead of algebraic.*

*2. Let  $E, F$  be two intermediate fields of  $L/K$ . Then  $E/K$  algebraic implies  $EF/F$  algebraic. Similarly for finite instead of algebraic.*

*3. Let  $E, F$  be two intermediate fields of  $L/K$ . Then both  $E/K$  and  $F/K$  algebraic implies both  $EF/K$  and  $E \cap F/K$  algebraic. Similarly for finite instead of algebraic.*

We usually draw the following pictures of these field extensions.



*Proof.* (1) The result for finite field extensions follows immediately from the **Tower Law**, since  $[L : k] = [L : K][K : k]$ .

Let  $L/k$  be algebraic. Then clearly both  $L/K$  and  $K/k$  are algebraic. Conversely, suppose that  $L/K$  and  $K/k$  are algebraic. Given  $\alpha \in L$ , we know that it is algebraic over  $K$ , so has a minimal polynomial  $m_{\alpha/K} = X^d + a_{d-1}X^{d-1} + \dots + a_0 \in K[X]$ . Hence  $\alpha$  is algebraic over the subfield  $K' = k(a_0, \dots, a_{d-1})$  of  $K$ . Since  $K/k$  is algebraic, each  $a_i$  is algebraic over  $k$ , so  $K'/k$  is finite by Lemma 3.8. Thus  $K'(\alpha)/k$  is finite by the **Tower Law**, so  $\alpha$  is algebraic over  $k$ .

(2) Let  $E/K$  be algebraic and consider  $(EF)^{\text{alg}/F}$ . This is a subfield of  $EF$  containing  $F$ . Moreover, since each element of  $E$  is algebraic over  $K$ , it is *a fortiori* algebraic over  $F$ . Therefore  $(EF)^{\text{alg}/F}$  also contains  $E$ , hence equals  $EF$ .

Now suppose that  $E/K$  is finite, so algebraic and finitely generated. Write  $E = K(\alpha_1, \dots, \alpha_n)$ . Then  $EF = F(\alpha_1, \dots, \alpha_n)$  is finitely generated and also algebraic from above. Thus  $EF/F$  is finite by Lemma 3.8.

(3) This is immediate from (1) and (2). □

It is not true that  $EF/F$  algebraic implies  $E/K$  algebraic. For example, let  $E = F = K(X)$  be simple transcendental over  $K$ . Then  $EF = F$ , so  $EF/F$  is finite of degree 1, but  $E/K$  is transcendental.

## Chapter 4

# Field Embeddings

The modern approach to Galois Theory involves replacing the roots of a polynomial by the field they generate, and replacing the symmetries of the roots by the automorphisms of the field. One reason for this is that a field has much more structure than just the set of roots of a polynomial, since we can apply all the field operations like addition and multiplication. This approach is also more general, since one can study arbitrary field extensions.

In the previous chapter we looked at field extensions and showed how to construct a field extension in which a given polynomial has a root. We now turn our attention to homomorphisms between fields, and in particular automorphisms of a field.

As a motivating example, let  $f \in \mathbb{R}[X]$  be a non-constant polynomial. Then all the roots of  $f$  lie in the field of complex numbers. Moreover, we have a natural field automorphism of  $\mathbb{C}$  given by complex conjugation. We observe that complex conjugation induces a permutation of the set of roots of  $f$ . For, if  $z \in \mathbb{C}$  is a root of  $f = a_0X^n + \cdots + a_{n-1}X + a_n \in \mathbb{R}[X]$ , so that  $f(z) = 0$ , then

$$\begin{aligned} f(\bar{z}) &= a_0\bar{z}^n + \cdots + a_{n-1}\bar{z} + a_n \\ &= \bar{a}_0\bar{z}^n + \cdots + \bar{a}_{n-1}\bar{z} + \bar{a}_n = \overline{f(z)} = 0. \end{aligned}$$

Let  $K, L'$  be fields. Recall that a field homomorphism  $\iota: K \rightarrow L'$  preserves the addition and multiplication, and the elements 0 and 1. Furthermore, all field homomorphisms are injective, or **embeddings**, and a field homomorphism is an isomorphism if and only if it is bijective. Thus, if we set  $K' := \iota(K)$ , then  $K'$  is a subfield of  $L'$  and  $\iota: K \xrightarrow{\sim} K'$  is a field isomorphism.

Let  $\sigma: L \rightarrow L'$  be a field embedding. If  $K \subset L$  is a subfield, then  $\sigma$  restricts to a field embedding  $\iota := \sigma|_K: K \rightarrow L'$ . Conversely, if  $\iota: K \rightarrow L'$  is a field embedding, then an **extension** of  $\iota$  to  $L$  is a field embedding  $\sigma: L \rightarrow L'$  such that  $\sigma|_K = \iota$ . In other words,  $\sigma(x) = \iota(x)$  for all  $x \in K$ .

As a special case, if  $L$  and  $L'$  are two field extensions of  $K$ , then  $\sigma: L \rightarrow$

$L'$  is called a  $K$ -**embedding** if  $\sigma|_K = \text{id}$ , so  $\sigma$  extends the identity on  $K$ . For example, complex conjugation is an  $\mathbb{R}$ -automorphism of  $\mathbb{C}$ . Note that a  $K$ -embedding is automatically an injective map of  $K$ -vector spaces, so  $[L : K] \leq [L' : K]$ . In particular, for finite field extensions, a  $K$ -embedding  $\sigma$  is an isomorphism if and only if  $[L : K] = [L' : K]$ .

We shall frequently make use of the following observation. Let  $\iota : K \xrightarrow{\sim} K'$  be a field isomorphism. Then we can extend  $\iota$  to a ring isomorphism  $\iota : K[X] \xrightarrow{\sim} K'[X]$  via  $X \mapsto X$ . Note that  $f \in K[X]$  is monic (respectively irreducible) if and only if  $\iota(f) \in K'[X]$  is monic (respectively irreducible).

## 4.1 Artin's Extension Theorem

**Lemma 4.1.** *Let  $L/K$  be a field extension and  $\sigma : L \rightarrow L'$  a field embedding. Set  $K' := \sigma(K)$ . If  $\alpha \in L$  is a root of a polynomial  $f \in K[X]$ , then  $\sigma(\alpha) \in L'$  is a root of  $\sigma(f) \in K'[X]$ .*

*Proof.* Let  $f = a_0X^n + \cdots + a_{n-1}X + a_n \in K[X]$ . Then

$$0 = \sigma(f(\alpha)) = \sigma(a_0)\sigma(\alpha)^n + \cdots + \sigma(a_n) = \sigma(f)(\sigma(\alpha)).$$

Thus  $\sigma(\alpha) \in L'$  is a root of  $\sigma(f) \in K'[X]$ . □

The next result tells us when we can extend a given embedding to a larger field.

**Theorem 4.2** (Artin's Extension Theorem). *Let  $L/K$  and  $L'/K'$  be field extensions and  $\iota : K \xrightarrow{\sim} K'$  an isomorphism. Let  $\alpha \in L$  be algebraic over  $K$  and  $\alpha' \in L'$  be algebraic over  $K'$ .*

*We can extend  $\iota$  to an isomorphism  $\sigma : K(\alpha) \rightarrow K'(\alpha')$  such that  $\sigma(\alpha) = \alpha'$  if and only if  $m_{\alpha'/K'} = \iota(m_{\alpha/K})$ .*

We usually think of this theorem using the following diagram.

$$\begin{array}{ccc} L & & L' \\ | & & | \\ K(\alpha) & \xrightarrow{\sigma} & K'(\alpha') \\ | & & | \\ K & \xrightarrow{\iota} & K' \end{array}$$

*Proof.* For simplicity write  $m = m_{\alpha/K} \in K[X]$  and  $m' = m_{\alpha'/K'} \in K'[X]$ .

Suppose first that  $\iota$  can be extended to an isomorphism  $\sigma : K(\alpha) \xrightarrow{\sim} K'(\alpha')$  such that  $\sigma(\alpha) = \alpha'$ . Then the previous lemma tells us that  $\alpha'$  is a root of  $\sigma(m) = \iota(m)$ . Thus  $m'$  divides  $\iota(m)$ , and since both polynomials are monic and irreducible, we must have  $m' = \iota(m)$ .

Conversely, suppose  $m' = \iota(m)$ . Extend  $\iota$  to an isomorphism  $\iota: K[X] \xrightarrow{\sim} K'[X]$  via  $X \mapsto X$ . We know that  $\text{ev}_\alpha$  induces a  $K$ -isomorphism  $K[X]/(m_{\alpha/K}) \xrightarrow{\sim} K(\alpha)$ , and that  $\text{ev}_{\alpha'}$  induces a  $K'$ -isomorphism  $K'[X]/(m_{\alpha'/K'}) \xrightarrow{\sim} K'(\alpha')$ .

Since  $m' = \iota(m)$ , the isomorphism  $\iota: K[X] \xrightarrow{\sim} K'[X]$  induces an isomorphism of fields  $\bar{\iota}: K[X]/(m) \xrightarrow{\sim} K'[X]/(m')$ , and clearly  $\bar{\iota}$  extends  $\iota$ . Now define  $\sigma := \text{ev}_{\alpha'} \circ \bar{\iota} \circ \text{ev}_\alpha^{-1}$ . Pictorially:

$$\begin{array}{ccccc}
 & L & & & L' \\
 & \downarrow & & & \downarrow \\
 K(\alpha) & \xleftarrow{\text{ev}_\alpha} & K[X]/(m) & \xrightarrow{\bar{\iota}} & K'[X]/(m') & \xrightarrow{\text{ev}_{\alpha'}} & K'(\alpha') \\
 & \downarrow & \downarrow & & \downarrow & & \downarrow \\
 K & \xlongequal{\quad} & K & \xrightarrow{\iota} & K' & \xlongequal{\quad} & K'
 \end{array}$$

Thus  $\sigma: K(\alpha) \xrightarrow{\sim} K'(\alpha')$  is an isomorphism extending  $\iota$  and  $\sigma(\alpha) = \alpha'$ .  $\square$

If  $\alpha \in L$  is algebraic, then the roots of  $m_{\alpha/K}$  in  $L$  are called the  $K$ -conjugates of  $\alpha$  in  $L$ .

One should remember that, although we take  $\alpha \in L$  to begin with, we are looking for all the different  $K$ -embeddings of  $K(\alpha)$  into  $L$ . It may be better to think of these as distinct embeddings of  $K[X]/(m_{\alpha/K})$  into  $L$ .

**Corollary 4.3.** *Let  $L/K$  be a field extension and  $\alpha \in L$  algebraic over  $K$ . Then there is a bijection*

$$\{K\text{-embeddings } K(\alpha) \rightarrow L\} \longleftrightarrow \{\text{roots of } m_{\alpha/K} \text{ in } L\}.$$

*In particular, there are at most  $\deg(m_{\alpha/K}) = [K(\alpha) : K]$  such  $K$ -embeddings.*

*Proof.* By **Artin's Extension Theorem**, if  $\sigma: K(\alpha) \rightarrow L$  is a  $K$ -embedding, then  $\alpha' := \sigma(\alpha)$  is a root of  $m_{\alpha/K}$  in  $L$ . Conversely, if  $\alpha' \in L$  is a root of  $m_{\alpha/K}$ , then there exists a  $K$ -embedding  $\sigma: K(\alpha) \rightarrow L$  such that  $\sigma(\alpha) = \alpha'$ .  $\square$

We observe that we have precisely  $[K(\alpha) : L]$   $K$ -embeddings  $K(\alpha) \rightarrow L$  if and only if  $m_{\alpha/K} = (X - \alpha_1) \cdots (X - \alpha_d) \in L[X]$  splits into distinct linear factors over  $L$  (with  $\alpha = \alpha_1$ , say). In the next chapters we shall discuss the conditions under which  $m_{\alpha/K}$  splits into linear factors, and when these factors are distinct.

**Corollary 4.4.** *Let  $L/K$  and  $L'/K$  be field extensions with  $L/K$  finite. Then the number of  $K$ -embeddings  $L \rightarrow L'$  is at most  $[L : K]$ .*

*Proof.* Since  $L/K$  is finite, we can write  $L = K(\alpha_1, \dots, \alpha_n)$  with each  $\alpha_i$  algebraic over  $K$ . Set  $M := K(\alpha_1, \dots, \alpha_{n-1})$ , so  $L = M(\alpha_n)$ . Let  $m$  be the minimal polynomial of  $\alpha_n$  over  $M$ , so  $[L : M] = \deg(m)$ .

Each  $K$ -embedding  $L \rightarrow L'$  restricts to a  $K$ -embedding  $M \rightarrow L'$ . By induction, we know that there are at most  $[M : K]$   $K$ -embeddings  $\iota: M \rightarrow L'$ , and by **Artin's Extension Theorem**, each such  $\iota$  may be extended in at most  $\deg(m) = [L : M]$  ways to a  $K$ -embedding  $L \rightarrow L'$  (corresponding to the distinct roots of  $\iota(m)$  in  $L'$ ). Thus there are at most  $[L : M][M : K] = [L : K]$   $K$ -embeddings  $L \rightarrow L'$ .  $\square$

We end with a nice result concerning automorphisms of algebraic extensions.

**Proposition 4.5.** *Let  $L/K$  be algebraic and  $\sigma: L \rightarrow L$  a  $K$ -embedding. Then  $\sigma$  is an automorphism of  $L$ .*

*Proof.* We recall that the  $K$ -embedding  $\sigma: L \rightarrow L$  is an automorphism if and only if it is bijective. Now, we know that  $\sigma$  is injective, so we just need to show that it is also surjective.

Let  $\alpha \in L$  have minimal polynomial  $m := m_{\alpha/K}$ . Let  $\alpha = \alpha_1, \dots, \alpha_n$  be the roots of  $m$  in  $L$  and write  $F = K(\alpha_1, \dots, \alpha_n)$ . Then  $F/K$  is finitely generated and algebraic, so finite by Lemma 3.8.

Since  $\sigma$  maps each root of  $m$  to a root of  $m$ ,  $\sigma(F) \subset F$ . Thus  $\sigma(F)$  is an intermediate field of  $F/K$ . Moreover, since  $\sigma: F \rightarrow \sigma(F)$  is bijective, it is an isomorphism. In particular,  $[F : K] = [\sigma(F) : K]$ , so  $[F : \sigma(F)] = 1$  by the **Tower Law**. Hence  $\sigma(F) = F$ , so  $\alpha \in \sigma(L)$  and  $\sigma$  is surjective as required.  $\square$

## 4.2 Examples

Artin's Extension Theorem is actually very easy to use.

1. Let  $\sqrt{2} \in \mathbb{C}$ . Then  $m_{\sqrt{2}/\mathbb{Q}} = X^2 - 2$ . This has roots  $\pm\sqrt{2}$  in  $\mathbb{C}$ . We therefore have two embeddings  $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{C}$  extending the identity of  $\mathbb{Q}$ . These are given by  $\sqrt{2} \mapsto \sqrt{2}$  (the identity) and  $\sqrt{2} \mapsto -\sqrt{2}$ .

2. Let  $\omega := \exp(2\pi i/3) = \frac{1}{2}(-1 + i\sqrt{3}) \in \mathbb{C}$ . Then  $\omega^2 = \exp(4\pi i/3) = \frac{1}{2}(-1 - i\sqrt{3})$  and  $m_{\omega/\mathbb{Q}} = X^2 + X + 1$ . We have two embeddings  $\mathbb{Q}(\omega) \rightarrow \mathbb{C}$  extending the identity on  $\mathbb{Q}$ . These are given by  $\omega \mapsto \omega$  (the identity) and  $\omega \mapsto \omega^2$  (complex conjugation).

3. Let  $\alpha = \sqrt[3]{2} \in \mathbb{R}$ . Then  $m_{\alpha/\mathbb{Q}} = X^3 - 2$ . This has a unique root in  $\mathbb{R}$ , so there is only the identity map  $\mathbb{Q}(\alpha) \rightarrow \mathbb{R}$ . On the other hand,  $X^3 - 2$  has roots  $\alpha, \omega\alpha, \omega^2\alpha$  in  $\mathbb{C}$ , so we have three embeddings  $\mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ . These are given by  $\alpha \mapsto \alpha$ ,  $\alpha \mapsto \omega\alpha$  and  $\alpha \mapsto \omega^2\alpha$ . Note that  $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\omega\alpha)$ , since  $\mathbb{Q} \subset \mathbb{R}$  but  $\omega\alpha \in \mathbb{C} \setminus \mathbb{R}$ . In fact, all three fields  $\mathbb{Q}(\alpha), \mathbb{Q}(\omega\alpha), \mathbb{Q}(\omega^2\alpha)$  are distinct, and the intersection of any two is just  $\mathbb{Q}$ .

4. Let  $\beta = \sqrt[4]{2} \in \mathbb{R}$ , so that  $\beta^2 = \sqrt{2}$ . Then  $m_{\beta/\mathbb{Q}} = X^4 - 2$  and this factors as  $(X^2 - \sqrt{2})(X^2 + \sqrt{2})$  over  $\mathbb{Q}(\sqrt{2})$ . Since  $\beta, i\beta \notin \mathbb{Q}(\sqrt{2})$ , these polynomials are irreducible. Hence  $m_{\beta/\mathbb{Q}(\sqrt{2})} = X^2 - \sqrt{2}$ .

Recall that there are two embeddings  $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{R}$ , namely  $\text{id}: \sqrt{2} \mapsto \sqrt{2}$  and  $\sigma: \sqrt{2} \mapsto -\sqrt{2}$ .

We now apply Artin's Extension Theorem to compute extensions of  $\text{id}$  and  $\sigma$  to  $\mathbb{Q}(\beta)$ . Since  $\text{id}(m_{\beta/\mathbb{Q}(\sqrt{2})}) = X^2 - \sqrt{2}$ , there are two extensions of  $\text{id}$  to  $\mathbb{Q}(\beta) \rightarrow \mathbb{R}$ , namely  $\text{id}: \beta \rightarrow \beta$  and  $\theta: \beta \rightarrow -\beta$ . On the other hand, since  $\sigma(m_{\beta/\mathbb{Q}(\sqrt{2})}) = X^2 + \sqrt{2}$ , which has no real roots, there are no extensions of  $\sigma$  to  $\mathbb{Q}(\beta) \rightarrow \mathbb{R}$ .

There are, however, two extensions of  $\sigma$  to  $\mathbb{Q}(\beta) \rightarrow \mathbb{C}$  given by  $\phi: \beta \mapsto i\beta$  and  $\bar{\phi}: \beta \mapsto -i\beta$ .

5. We can also compute all embeddings  $\mathbb{Q}(\alpha, \omega) \rightarrow \mathbb{C}$ , where  $\alpha = \sqrt[3]{2}$  and  $\omega = \exp(2\pi i/3)$  as above. We begin by noting that  $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6$ . For, we know that  $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$  and that  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ . It follows from the **Tower Law** that both 2 and 3, and hence 6, divide  $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]$ . On the other hand, we know that  $\alpha$  is a root of  $X^3 - 2$  over  $\mathbb{Q}(\omega)$ , so  $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] \leq 3$ , whence  $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] \leq 6$ .

In particular, we note that  $X^3 - 2$  is the minimal polynomial of  $\alpha$  over  $\mathbb{Q}(\omega)$ .

We have already computed all embeddings  $\mathbb{Q}(\omega) \rightarrow \mathbb{C}$ , namely  $\text{id}$  and complex conjugation  $\tau: \omega \mapsto \omega^2$ . Clearly both  $\text{id}$  and  $\tau$  fix the minimal polynomial  $X^3 - 2$  of  $\alpha$ , and since this polynomial has three distinct roots in  $\mathbb{C}$ , we see that there are three extensions of  $\text{id}$  to  $\mathbb{Q}(\alpha, \omega) \rightarrow \mathbb{C}$  and three extensions of  $\tau$  to  $\mathbb{Q}(\alpha, \omega) \rightarrow \mathbb{C}$ . Hence there are precisely six embeddings  $\mathbb{Q}(\alpha, \omega) \rightarrow \mathbb{C}$ .

We illustrate these embeddings in a table showing their actions on  $\alpha, \omega$ .

id	$\sigma$	$\sigma^2$	$\tau$	$\sigma\tau$	$\sigma^2\tau$
$\omega \mapsto \omega$	$\omega \mapsto \omega$	$\omega \mapsto \omega$	$\omega \mapsto \omega^2$	$\omega \mapsto \omega^2$	$\omega \mapsto \omega^2$
$\alpha \mapsto \alpha$	$\alpha \mapsto \omega\alpha$	$\alpha \mapsto \omega^2\alpha$	$\alpha \mapsto \alpha$	$\alpha \mapsto \omega\alpha$	$\alpha \mapsto \omega^2\alpha$

Note that  $\tau$  still denotes complex conjugation. Also, the images of each of these embeddings is contained in  $\mathbb{Q}(\alpha, \omega)$ , so that all six embeddings induce automorphisms of  $\mathbb{Q}(\alpha, \omega)$ . In particular, we may compose them, and in fact we have used this when labelling the automorphisms. For example,

$$\sigma^2(\omega) = \sigma(\omega) = \omega, \quad \sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\omega\alpha) = \sigma(\omega)\sigma(\alpha) = \omega \cdot \omega\alpha = \omega^2\alpha.$$

Similarly,

$$\sigma\tau(\omega) = \sigma(\omega^2) = \sigma(\omega)^2 = \omega^2, \quad \sigma\tau(\alpha) = \sigma(\alpha) = \omega\alpha.$$

Moreover, since

$$\tau\sigma(\omega) = \tau(\omega) = \omega^2, \quad \tau\sigma(\alpha) = \tau(\omega\alpha) = \tau(\omega)\tau(\alpha) = \omega^2\alpha,$$

we have that  $\tau\sigma = \sigma^2\tau$ . Since we also have  $\sigma^3 = \text{id} = \tau\omega^2$ , we deduce that the set of all such embeddings forms a group isomorphic to  $S_3$ . Note that  $|S_3| = 6 = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]$ .

### 4.3 Linear Independence of Characters

A **character** of a group  $G$  in an arbitrary field  $K$  is a group homomorphism  $\chi: G \rightarrow K^*$ . The **trivial character** is the homomorphism  $\chi(g) = 1$  for all  $g \in G$ . (Such a character is called an irreducible character of degree one in courses on representations of groups.)

If  $\chi_1, \dots, \chi_n$  are characters of  $G$  and  $\lambda_1, \dots, \lambda_n \in K$ , then we can form the linear combination  $\lambda_1\chi_1 + \dots + \lambda_n\chi_n$ , which sends  $g \in G$  to  $\sum_i \lambda_i\chi_i(g)$ . We say that the  $\chi_i$  are **linearly independent over  $K$**  if, whenever  $\lambda_i \in K$  satisfy  $\lambda_1\chi_1 + \dots + \lambda_n\chi_n = 0$ , then  $\lambda_i = 0$  for all  $i$ .

Let  $L/K$  and  $M/K$  be field extensions. Then each  $K$ -embedding  $L \rightarrow M$  yields a character of the multiplicative group  $L^*$  in  $M$ .

**Theorem 4.6** (Dedekind). *Let  $K$  be a field,  $G$  a group and  $\chi_1, \dots, \chi_n$  distinct characters  $G \rightarrow K^*$ . Then the  $\chi_i$  are linearly independent over  $K$ .*

*Proof.* Suppose we have a non-trivial expression  $\sum_{i=1}^n \lambda_i\chi_i = 0$  with  $\lambda_i \in K$ . Assume further that such an expression has a minimum number of non-zero coefficients  $\lambda_i$ . Relabelling if necessary, we may assume that  $\lambda_n \neq 0$ , and dividing through, we may assume that  $\lambda_n = -1$ .

We therefore have an expression  $\chi_n = \sum_{i=1}^{n-1} \lambda_i\chi_i$ , and this has the same number of non-zero coefficients as our original expression. Observe that  $\lambda_i \neq 0$  for some  $i < n$ . For otherwise we would have  $\chi_n = 0$ , but  $\chi_n(1) = 1$ , a contradiction. Hence, after relabelling, we may assume that  $\lambda_1 \neq 0$ .

Now, since  $\chi_1$  and  $\chi_n$  are distinct, there exists  $g \in G$  such that  $\chi_1(g) \neq \chi_n(g)$ . Set  $\mu_i := \chi_n(g) - \chi_i(g)$  and consider the linear expression  $\sum_{i=1}^{n-1} \lambda_i\mu_i\chi_i$ . For each  $h \in G$  we have

$$\begin{aligned} \sum_{i=1}^{n-1} \lambda_i\mu_i\chi_i(h) &= \sum_{i=1}^{n-1} \lambda_i\chi_n(g)\chi_i(h) - \sum_{i=1}^{n-1} \lambda_i\chi_i(g)\chi_i(h) \\ &= \chi_n(g) \sum_{i=1}^{n-1} \lambda_i\chi_i(h) - \sum_{i=1}^{n-1} \lambda_i\chi_i(gh) \\ &= \chi_n(g)\chi_n(h) - \chi_n(gh) = 0, \end{aligned}$$

using that characters are multiplicative. Hence we have obtained a new equation of linear dependence  $\sum_{i=1}^{n-1} \lambda_i\mu_i\chi_i = 0$ . This has fewer terms than the original equation, so by our minimality assumption each coefficient must be zero. On the other hand,  $\mu_1 \neq 0$ , a contradiction.

We deduce that  $\lambda_i = 0$  for all  $i$ , so that the  $\sigma_i$  are linearly independent.  $\square$

## Chapter 5

# Splitting Fields and Normal Extensions

Let  $L/K$  be a field extension. We say that a polynomial  $f \in K[X]$  **splits** over  $L$  if there exist  $c \in K$  and  $\alpha_i \in L$  such that  $f = c \prod_i (X - \alpha_i) \in L[X]$ . More generally, if  $S \subset K[X]$  is a set of polynomials, then  $S$  splits over  $L$  if each polynomial  $f \in S$  splits over  $L$ .

Let  $L/K$  be a field extension and  $S \subset K[X]$ . We call  $L/K$  a **splitting field extension** for  $S$  if  $S$  splits over  $L$ , but  $S$  does not split over any proper intermediate field  $L'$  (i.e.  $K \subset L' \subset L$ ).

**Theorem 5.1** (Existence and Uniqueness of Splitting Fields). *Let  $f \in K[X]$  be a non-constant polynomial. Then there exists a splitting field extension  $L/K$  for  $f$ . Moreover,  $[L : K] \leq \deg(f)!$ .*

*If  $\iota: K \xrightarrow{\sim} K'$  is an isomorphism and if  $L'/K'$  is a splitting field for  $\iota(f)$ , then we can extend  $\iota$  to an isomorphism  $\sigma: L \xrightarrow{\sim} L'$ .*

*Proof.* We prove by induction on  $n := \deg(f)$  that there exists an extension  $M/K$  of degree at most  $n!$  over which  $f$  splits. If  $n = 1$  there is nothing to prove, so suppose  $n \geq 2$ . Using Corollary 3.4, we first construct a field  $K'/K$  with  $[K' : K] \leq n$  in which  $f$  has a root, say  $\alpha$ . Then  $f = (X - \alpha)g \in K'[X]$  and  $\deg(g) = n - 1$ . By induction, there exists an extension  $M/K'$  with  $[M : K'] \leq (n - 1)!$  over which  $g$  splits. Hence  $f$  splits over  $M$  and  $[M : K] \leq n!$ .

Now write  $f = c \prod_{i=1}^n (X - \alpha_i) \in M[X]$  and set  $L := K(\alpha_1, \dots, \alpha_n)$ . Then  $L$  is a splitting field for  $f$ . For,  $f$  clearly splits over  $L$ , and if  $f$  splits over some field  $L'$  with  $M/L'/K$ , then  $L'$  must contain each  $\alpha_i$ , so  $L \subset L'$ . Since  $M/L/K$  we have  $[L : K] \leq n!$  by the **Tower Law**.

Suppose that  $\iota: K \xrightarrow{\sim} K'$  is an isomorphism and that  $L'/K'$  is a splitting field extension for  $f' := \iota(f)$ . Write  $L' = K'(\alpha'_1, \dots, \alpha'_n)$  with  $f' = c' \prod_i (X - \alpha'_i) \in L'[X]$ . We wish to extend  $\iota$  to an isomorphism  $\sigma: L \xrightarrow{\sim} L'$ . We again do this

by induction on  $n := \deg(f)$ .

Consider  $K(\alpha_n) \subset L$  and let  $m = m_{\alpha_n/K}$  be its minimal polynomial. Since  $\alpha_n$  is a root of  $f$ ,  $m$  divides  $f$ . Therefore  $m' := \iota(m)$  divides  $f'$  and since  $f'$  splits in  $L'$ , so does  $m'$ . Relabelling if necessary, we may assume that  $\alpha'_n$  is a root of  $m'$  in  $L'$ . By [Artin's Extension Theorem](#), we can extend  $\iota$  to an isomorphism  $\tilde{\iota}: K(\alpha_n) \xrightarrow{\sim} K'(\alpha'_n)$  via  $\alpha_n \mapsto \alpha'_n$ .

Define  $g := f/(X - \alpha) \in K(\alpha_n)[X]$  and  $g' := f'/(X - \alpha'_n) \in K'(\alpha'_n)[X]$ , so that  $g' = \tilde{\iota}(g)$  and  $\deg(g) = n - 1$ . Also,  $L/K(\alpha_n)$  is a splitting field for  $g$ , and  $L'/K'(\alpha'_n)$  is a splitting field for  $g'$ . By induction we can extend  $\tilde{\iota}: K(\alpha_n) \xrightarrow{\sim} K'(\alpha'_n)$  to an isomorphism  $\sigma: L \xrightarrow{\sim} L'$ . Then  $\sigma$  is of course an extension of  $\iota$ , so we are done.  $\square$

We observe that if  $f \in K[X]$  splits in  $M/K$  with roots  $\alpha_1, \dots, \alpha_n$ , then the splitting field extension of  $f$  in  $M$  is  $L = K(\alpha_1, \dots, \alpha_n)$ , the subfield generated by the roots of  $f$  in  $M$ .

**Corollary 5.2.** *Let  $S \subset K[X]$  be a finite subset. Then there exists a splitting field extension for  $S$  over  $K$ , and this is unique up to isomorphism.*

*Proof.* If  $S = \{f_1, \dots, f_n\}$ , then  $L/K$  is a splitting field extension for  $S$  if and only if it is a splitting field extension for  $f = f_1 \cdots f_n$ .  $\square$

A much harder result is that splitting field extensions exist and are unique up to isomorphism for arbitrary subsets  $S \subset K[X]$ . This follows from the existence of the algebraic closure of a field. See [Appendix C](#).

## 5.1 Normal Extensions

An algebraic extension  $L/K$  is called **normal** provided that every *irreducible* polynomial  $f \in K[X]$  which has a root in  $L$ , splits over  $L$ . Equivalently,  $L/K$  is normal if for every  $\alpha \in L$ , its minimal polynomial  $m_{\alpha/K}$  splits over  $L$ .

We begin by relating normal extensions to the seemingly weaker condition of splitting field extensions.

**Theorem 5.3.** *Let  $L/K$  be finite. Then  $L/K$  is normal if and only if it is the splitting field of some monic polynomial  $f \in K[X]$ .*

*Proof.* Let  $L/K$  be finite and normal. Since  $L/K$  is finite, it is algebraic and finitely generated, say  $L = K(\alpha_1, \dots, \alpha_n)$ . Let  $m_i \in K[X]$  be the minimal polynomial of  $\alpha_i$  over  $K$ . Each  $m_i$  has a root in  $L$ , namely  $\alpha_i$ . Since  $L/K$  is normal, each  $m_i$  splits over  $L$ . Write  $m = m_1 \cdots m_n$ , a monic polynomial in  $K[X]$  which splits over  $L$ . Then  $L/K$  is a splitting field of  $m$ . For, if  $m$  splits over an intermediate field  $L'$ , then each  $\alpha_i \in L'$ , so  $L' = L$ .

Conversely, suppose that  $L/K$  is the splitting field extension for some monic polynomial  $f \in K[X]$ . Let  $g \in K[X]$  be irreducible. We wish to show that, if  $g$

has a root in  $L$ , then  $g$  splits over  $L$ . To this end, let  $M/L$  be the splitting field extension of  $g$ .

We observe that if  $E$  is an intermediate field of  $M/K$ , then the composite  $EL$  is the splitting field of  $f$  over  $E$ . For, let  $\alpha_1, \dots, \alpha_n \in M$  be the roots of  $f$ . Then  $L = K(\alpha_1, \dots, \alpha_n)$  is the splitting field of  $f$  over  $K$ , and  $E(\alpha_1, \dots, \alpha_n) = EL$  is the splitting field of  $f$  over  $E$ .

In particular, if  $\beta \in M$  is a root of  $g$ , then  $L(\beta)$  is the splitting field of  $f$  over  $K(\beta)$ .

Now let  $\gamma \in M$  be another root of  $g$ . We claim that there exists a  $K$ -isomorphism  $L(\beta) \xrightarrow{\sim} L(\gamma)$  with  $\beta \mapsto \gamma$ , and hence  $[L(\beta) : K] = [L(\gamma) : K]$ .

By **Artin's Extension Theorem** there exists a  $K$ -isomorphism  $\iota : K(\beta) \xrightarrow{\sim} K(\gamma)$  with  $\iota(\beta) = \gamma$ . Clearly  $\iota(f) = f$ . So, since  $L(\beta)/K(\beta)$  and  $L(\gamma)/K(\gamma)$  are splitting fields of  $f$ , Theorem 5.1 says that we can extend  $\iota$  to a  $K$ -isomorphism  $L(\beta) \xrightarrow{\sim} L(\gamma)$ . This proves the claim.

To see that  $L/K$  is normal, suppose that  $\beta \in L$ , so that  $g$  has a root in  $L$ . Then  $L(\beta) = L$ , so the **Tower Law** gives

$$[L : K] = [L(\beta) : K] = [L(\gamma) : K] = [L(\gamma) : L][L : K].$$

Thus  $[L(\gamma) : L] = 1$ , so  $L(\gamma) = L$ . Hence each root  $\gamma \in M$  of  $g$  actually lies in  $L$ , so  $g$  splits over  $L$ .  $\square$

One has to be careful here since the property of being a normal extension is not transitive; that is, we can have  $M/L/K$  with both  $M/L$  and  $L/K$  normal, but  $M/K$  not normal. For example,  $K = \mathbb{Q}$ ,  $L = \mathbb{Q}(\sqrt{2})$  and  $M = \mathbb{Q}(\sqrt[4]{2})$ . Then  $L/\mathbb{Q}$  is the splitting field of  $X^2 - 2$  and  $M/L$  is the splitting field of  $X^2 - \sqrt{2}$ . However,  $M/\mathbb{Q}$  is not normal. For, the minimal polynomial of  $\sqrt[4]{2}$  over  $\mathbb{Q}$  is  $m := X^4 - 2$ , which decomposes as  $(X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2})$  over  $M$ . Since  $M \subset \mathbb{R}$  but the roots of  $X^2 + \sqrt{2}$  are complex, we see that  $m$  has a root in  $M$ , but does not split over  $M$ . Hence  $M/\mathbb{Q}$  is not normal.

For this reason, we make the following definition. Let  $L/K$  be algebraic. A field extension  $M/L$  is called a **normal closure** of  $L/K$  if  $M/K$  is normal, but  $M'/K$  is not normal for any proper intermediate field  $M'$  of  $M/L$ . (Note the relevant base fields.)

**Theorem 5.4** (Existence and Uniqueness of Normal Closures). *Let  $L/K$  be finite. Then there exists a normal closure  $M/L$  of  $L/K$ , and it is unique up to isomorphism. Moreover,  $[M : L]$  is finite.*

*Proof.* Since  $L/K$  is finite, we can write  $L = K(\alpha_1, \dots, \alpha_n)$  with each  $\alpha_i$  algebraic over  $K$ . Let  $m_i \in K[X]$  be the minimal polynomial of  $\alpha_i$  and set  $m := m_1 \cdots m_n$ . We will show that  $M/L$  is a normal closure of  $L/K$  if and only if it is a splitting field of  $m$ . It will follow immediately from Theorem 5.1 that  $[M : L]$  is finite and  $M/L$  is unique up to isomorphism.

Let  $M/L$  be the splitting field of  $m$ . We claim that  $M/K$  is the splitting field of  $m$ , hence normal by Theorem 5.3. Clearly  $m$  splits over  $M$ , so let  $M' \subset M$

be the splitting field of  $m$  over  $K$ . Clearly each  $\alpha_i \in M'$ , so  $L \subset M'$ . Therefore  $M'/L$  is a splitting field for  $m$ , so  $M' = M$ .

To see that  $M/L$  is a normal closure, suppose we have  $M/M'/L$  with  $M'/K$  normal. Then  $\alpha_i \in M'$  for each  $i$ , so each  $m_i$  splits over  $M'$ . Thus  $m$  splits over  $M'$ , so that  $M' = M$ . Thus  $M/L$  is a normal closure of  $L/K$ .

Conversely, let  $N/L$  be a normal closure of  $L/K$ . Then each  $m_i$  must split over  $N$ , so  $m$  splits over  $N$ . Let  $N' \subset N$  be the splitting field of  $m$  over  $L$ . As above,  $N'/L$  is also a normal closure of  $L/K$ , so  $N' = N$ .  $\square$

The next theorem will play a central role.

**Theorem 5.5.** *Let  $M/L/K$  be field extensions with  $M/K$  finite and normal. Then any  $K$ -embedding  $L \rightarrow M$  can be extended to a  $K$ -automorphism of  $M$ .*

*Proof.* By Theorem 5.3  $M/K$  is the splitting field of some  $f \in K[X]$ . Then clearly  $M/L$  is also the splitting field of  $f$ . Given a  $K$ -embedding  $\iota: L \rightarrow M$ , set  $L' := \iota(L)$ . Note that  $\iota(f) = f$ , so  $M/L'$  is also the splitting field of  $f$ . Therefore, by Theorem 5.1, we can extend  $\iota$  to a  $K$ -automorphism of  $M$ .  $\square$

A sort of converse is given by the following.

**Proposition 5.6.** *Let  $M/L/K$  be field extensions with  $L/K$  normal. Then any  $K$ -embedding  $\sigma: M \rightarrow M$  restricts to a  $K$ -automorphism of  $L$ .*

*Proof.* Since  $L/K$  is normal, it is algebraic. Let  $\alpha \in L$ . Then  $\sigma(\alpha)$  is also a root of  $m_{\alpha/K}$  by **Artin's Extension Theorem**, hence lies in  $L$ . Thus  $\sigma$  restricts to a  $K$ -embedding  $\sigma|_L: L \rightarrow L$ . This is a  $K$ -automorphism by Proposition 4.5.  $\square$

We also have the following nice result.

**Proposition 5.7.** *Let  $M/L/K$  be field extensions with  $L/K$  finite and  $M/K$  normal. Let  $\sigma_1, \dots, \sigma_r$  be the distinct  $K$ -embeddings  $L \rightarrow M$ . Then the compositum of the fields  $\sigma_i(L)$  is a normal closure of  $L/K$ .*

*Proof.* Let  $N \subset M$  be the normal closure of  $L/K$ . Clearly, if  $\sigma: L \rightarrow M$  is a  $K$ -embedding and if  $\alpha \in L$ , then  $\alpha$  and  $\sigma(\alpha)$  are  $K$ -conjugates, so  $\sigma(\alpha) \in N$ . Hence each  $\sigma(L)$  is contained in  $N$ .

Conversely, we saw in the proof of Theorem 5.4 that if  $L = K(\alpha_1, \dots, \alpha_n)$ , then  $N/K$  is generated by the  $K$ -conjugates of the  $\alpha_i$ . Let  $\beta_i$  be a conjugate of  $\alpha_i$ . By **Artin's Extension Theorem** there exists a  $K$ -isomorphism  $\iota: K(\alpha_i) \xrightarrow{\sim} K(\beta_i)$  sending  $\alpha_i \mapsto \beta_i$ . We claim that we can extend  $\iota$  to a  $K$ -embedding  $\sigma: L \rightarrow M$ . For, applying Theorem 5.5, we can extend  $\iota$  to a  $K$ -automorphism  $\tilde{\sigma}$  of  $N$ . This restricts to a  $K$ -embedding  $\sigma := \tilde{\sigma}|_L: L \rightarrow M$ . It follows that  $\beta_i \in \sigma(L)$ , and hence that  $N$  is contained in the composite of all such  $\sigma(L)$ .  $\square$

To return to one of our standard examples, let  $\alpha = \sqrt[3]{2} \in \mathbb{R}$  and  $K = \mathbb{Q}(\alpha)$ . Then there are three embeddings  $K \rightarrow \mathbb{C}$  given by  $\alpha \mapsto \alpha$ ,  $\alpha \mapsto \omega\alpha$  and  $\alpha \mapsto \omega^2\alpha$ . Therefore the normal closure of  $K/\mathbb{Q}$  is precisely  $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbb{Q}(\alpha, \omega)$ . The next theorem is the analogue for normal extensions of Theorem 3.10. Recall that the property of being normal is not transitive, so (1) is necessarily weaker, and (3) is no longer a consequence of (1) and (2).

- Theorem 5.8.**
1. Let  $L/K/k$  be field extensions. Then  $L/k$  normal implies  $L/K$  normal.
  2. Let  $E, F$  be two intermediate fields of  $L/K$ . Then  $E/K$  normal implies  $EF/F$  normal.
  3. Let  $E, F$  be two intermediate fields of  $L/K$ . Then both  $E/K$  and  $F/K$  normal implies both  $EF/K$  and  $E \cap F/K$  normal.

*Proof.* (1) Since  $L/k$  is normal, it is algebraic, so  $L/K$  is also algebraic by Theorem 3.10. To show that  $L/K$  is normal, we therefore need to show that for all  $\alpha \in L$ ,  $m_{\alpha/K}$  splits over  $L$ . We know, however, that  $m_{\alpha/K}$  divides  $m_{\alpha/k}$  in  $K[X]$ , and since  $m_{\alpha/k}$  splits over  $L$  (since  $L/k$  is normal), so too does  $m_{\alpha/K}$ .

(2) Since  $E/K$  is normal, it is algebraic, so  $EF/F$  is algebraic by Theorem 3.10. We again need to show that for all  $\alpha \in EF$ ,  $m_{\alpha/F}$  splits over  $EF$ . Write  $\alpha = x_1y_1 + \cdots + x_ry_r$  with  $x_i \in E$  and  $y_i \in F$ . Using Theorem 5.4, let  $E_0 \subset E$  be the normal closure of  $K(x_1, \dots, x_r)/K$ . Then  $E_0/K$  is finite and normal, so the splitting field of some  $f \in K[X]$  by Theorem 5.3. We can therefore write  $E_0 = K(\beta_1, \dots, \beta_s)$ , where the  $\beta_i$  are the roots of  $f$ .

Now consider the compositum  $E_0F = F(\beta_1, \dots, \beta_s)$ . This is the splitting field over  $F$  of  $f$ , so is normal by Theorem 5.3. Since  $\alpha \in E_0F$ , we have that  $m_{\alpha/F}$  splits over  $E_0F$ , and hence also over  $EF$ . Thus  $EF/F$  is normal.

(3) We proceed as in the previous part. Let  $\alpha = x_1y_1 + \cdots + x_ry_r \in EF$ , where  $x_i \in E$  and  $y_i \in F$ . Let  $E_0 \subset E$  be the normal closure of  $K(x_1, \dots, x_r)/K$  and similarly  $F_0 \subset F$  the normal closure of  $K(y_1, \dots, y_r)/K$ . Then  $E_0/K$  is the splitting field of some  $f \in K[X]$ , say  $E_0 = K(\beta_1, \dots, \beta_s)$ , where the  $\beta_i$  are the roots of  $f$ . Similarly  $F_0/K$  is the splitting field of some  $g \in K[X]$ , say  $F_0 = K(\gamma_1, \dots, \gamma_t)$ , where the  $\gamma_i$  are the roots of  $g$ .

Now consider the compositum  $E_0F_0 = K(\beta_1, \dots, \beta_s, \gamma_1, \dots, \gamma_t)$ . This is the splitting field over  $K$  of the polynomial  $fg$ , hence is normal. Since  $\alpha \in E_0F_0$ , we have that  $m_{\alpha/K}$  splits over  $E_0F_0$ , and hence also over  $EF$ . Thus  $EF/K$  is normal.

To see that  $E \cap F/K$  is normal, take  $\alpha \in E \cap F$ . Since  $E/k$  is normal,  $m_{\alpha/k}$  splits over  $E$ . Similarly, since  $F/k$  is normal,  $m_{\alpha/k}$  splits over  $F$ . Thus the roots of  $m_{\alpha/k}$  all lie in  $E \cap F$ , so  $m_{\alpha/k}$  splits over  $E \cap F$ . Thus  $E \cap F/K$  is normal.  $\square$

## Chapter 6

# Separable Extensions

In this chapter we discuss when a polynomial has distinct roots in a splitting field.

Let  $f \in K[X]$ . We call  $f$  **separable** over  $K$  if each irreducible factor of  $f$  has distinct roots in some splitting field extension  $L/K$  for  $f$ . Since splitting field extensions are unique up to isomorphism, this definition depends only on  $f$  and  $K$ . More generally, if  $L/K$  is a field extension and  $\alpha \in L$  is algebraic over  $K$ , then we say that  $\alpha$  is separable over  $K$  if  $m_{\alpha/K} \in K[X]$  is a separable polynomial. We call an algebraic extension  $L/K$  separable if each  $\alpha \in L$  is separable over  $K$ .

### 6.1 The Frobenius Homomorphism

In order to characterise separable polynomials, we will need some results on fields of positive characteristic. In particular, we need to introduce the Frobenius homomorphism.

Let  $K$  be a field of characteristic  $p > 0$ . Consider the map  $\text{Fr}: K \rightarrow K$ ,  $x \mapsto x^p$ , called the **Frobenius homomorphism**.

**Lemma 6.1.** *The Frobenius homomorphism is a homomorphism of fields. In particular, it is injective.*

*Proof.* We need to check that

$$(x + y)^p = x^p + y^p, \quad (xy)^p = x^p y^p, \quad 0^p = 0 \quad \text{and} \quad 1^p = 1.$$

The last three are obvious, so we just need to check that  $(x + y)^p = x^p + y^p$ . Using the binomial formula, we have

$$(x + y)^p = \sum_{r=0}^p \binom{p}{r} x^r y^{p-r}.$$

Since  $\binom{p}{r} = p!/r!(p-r)!$  and  $p|p!$  but  $p \nmid r!$  for  $0 \leq r < p$ , we deduce that  $p|\binom{p}{r}$  for  $0 < r < p$ . Since  $\text{char}(K) = p$ , we get  $(x+y)^p = x^p + y^p$  as required.  $\square$

Note that, by induction,  $(x_1 + \cdots + x_n)^p = x_1^p + \cdots + x_n^p$ .

**Lemma 6.2.** *Each field endomorphism of a finite field is an automorphism. In particular, this holds for the Frobenius homomorphism.*

*Proof.* Each field endomorphism  $f: K \rightarrow K$  is necessarily injective. If  $K$  is finite as a set, then  $f$  must also be surjective, hence an automorphism.  $\square$

As usual, we may extend the Frobenius homomorphism to the polynomial ring  $K[X]$ : if  $f = a_0X^n + \cdots + a_{n-1}X + a_n$ , then  $\text{Fr}(f) = a_0^pX^n + \cdots + a_{n-1}^pX + a_n^p$ .

**Lemma 6.3.** *Let  $f \in K[X]$ . Then  $\text{Fr}(f)(X^p) = f(X)^p$ .*

*Proof.* Write  $f = a_0X^n + \cdots + a_{n-1}X + a_n$ . Since non-trivial multinomial coefficients are divisible by  $p$  we have

$$f(X)^p = a_0^pX^{pn} + \cdots + a_{n-1}^pX^p + a_n^p = \text{Fr}(f)(X^p). \quad \square$$

## 6.2 Separability

We now give a criterion for when a polynomial is separable.

**Theorem 6.4.** *Let  $f \in K[X]$  be irreducible. Then the following are equivalent.*

1.  $f$  is inseparable over  $K$ .
2.  $\text{gcd}(f, f') \neq 1$  in  $K[X]$ .
3.  $f' = 0$ .
4.  $\text{char}(K) = p > 0$  and  $f(X) = g(X^p)$  for some irreducible  $g \in K[X]$ .

*Proof.* (1)  $\Rightarrow$  (2) Let  $f$  be inseparable over  $K$  and let  $L/K$  be its splitting field extension. Then  $f$  has a repeated root over  $L$ , say  $f = (X - \alpha)^2h(X) \in L[X]$ . Therefore  $f' = (X - \alpha)[2h(X) + (X - \alpha)h'(X)] \in L[X]$ . Thus  $X - \alpha$  divides both  $f$  and  $f'$  over  $L$ . Now let  $g = \text{gcd}(f, f') \in K[X]$ , and write  $g = rf + sf'$  for polynomials  $r, s \in K[X]$ . Then  $g(\alpha) = r(\alpha)f(\alpha) + s(\alpha)f'(\alpha) = 0$  in  $L$ , so that  $(X - \alpha)|g$  in  $L[X]$ , whence  $\deg(g) \geq 1$ .

(2)  $\Rightarrow$  (3) Since  $f$  is irreducible, if  $\text{gcd}(f, f') \neq 1$ , then it must equal  $f$ . Therefore  $f|f'$  but  $\deg(f) > \deg(f')$ . This can only happen if  $f' = 0$ .

(3)  $\Rightarrow$  (4) Write  $f = \sum_n a_nX^n \in K[X]$ . Then  $f' = \sum_n na_nX^{n-1} = 0$ , so that  $na_n = 0 \in K$  for all  $n$ . If  $\text{char}(K) = 0$ , then  $a_n = 0$  for all  $n \geq 1$ , so that  $f = a_0 \in K$  is constant, contradicting the assumption that  $f$  is irreducible. Thus  $\text{char}(K) = p > 0$  and  $a_n = 0$  unless  $p|n$ , so that  $f(X) = g(X^p)$  with

$g = \sum_r a_{pr} X^r \in K[X]$ . To see that  $g$  is irreducible, suppose that  $g = h_1 h_2 \in K[X]$ . Then  $f(X) = g(X^p) = h_1(X^p) h_2(X^p) \in K[X]$ . Since  $f$  is irreducible,  $\deg(h_i) = 0$  for some  $i$ . Hence  $g$  is irreducible.

(4)  $\Rightarrow$  (1). Let  $\text{char}(K) = p > 0$  and  $f(X) = g(X^p) \in K[X]$ . Let  $L/K$  be the splitting field extension for  $f$ . If  $\alpha \in L$  is a root of  $f$ , then  $0 = f(\alpha) = g(\alpha^p)$ . Hence  $\alpha^p$  is a root of  $g$ , so  $(X - \alpha^p) | g(X)$ , which implies that  $(X^p - \alpha^p)$  divides  $g(X^p) = f(X)$ . Since  $\text{char}(L) = p$ ,  $X^p - \alpha^p = (X - \alpha)^p \in L[X]$ . Therefore  $(X - \alpha)^p | f(X)$ , so  $f$  is inseparable.  $\square$

We call a field  $K$  **perfect** if every irreducible polynomial  $f \in K[X]$  is separable. We observe that all fields of characteristic 0 are separable. Also, all algebraically closed fields are perfect (since all irreducible polynomials are linear). We shall see below that all finite fields are perfect as well.

**Corollary 6.5.** *Let  $f \in K[X]$  be irreducible with  $\text{char}(K) = p > 0$ . Then there exists a unique  $r \geq 0$  and a unique separable irreducible  $g \in K[X]$  such that  $f(X) = g(X^{p^r})$ .*

*In particular, given an algebraic extension  $L/K$  and  $\alpha \in L$ , there exists  $r$  such that  $\alpha^{p^r}$  is separable over  $K$ .*

*Proof.* Existence: If  $f$  is separable, then setting  $r = 0$  and  $g = f$ , we are done. If  $f$  is inseparable, then we can write  $f(X) = g(X^p)$  for some irreducible  $g \in K[X]$ . Since  $\deg(g) = \deg(f)/p$ , we are done by induction on degree.

Uniqueness: Let  $f(X) = g(X^{p^r}) = h(X^{p^s})$  with  $g, h \in K[X]$  separable and irreducible and  $r \geq s$ . Then  $h(X) = g(X^{p^{r-s}}) \in K[X]$  and since  $h$  is separable,  $r = s$  by Theorem 6.4. Thus  $g = h$ .

For the last statement, let  $f = m_{\alpha/K}$ . If  $\alpha$  is inseparable over  $K$ , then  $f(X) = g(X^p)$  with  $g$  irreducible, and monic since  $f$  is monic. Observe that  $g(\alpha^p) = f(\alpha) = 0$ , so  $g = m_{\alpha^p/K}$  is the minimal polynomial of  $\alpha^p$  over  $K$ . The result follows by induction.  $\square$

**Lemma 6.6.** *Let  $L/K$  be algebraic with  $\text{char}(K) = p > 0$ . Then for  $\alpha \in L$*

1.  $\alpha$  is separable over  $K$  if and only if  $[K(\alpha) : K(\alpha^p)] = 1$ .
2.  $\alpha$  is inseparable over  $K$  if and only if  $[K(\alpha) : K(\alpha^p)] = p$ .

*Proof.* If  $\alpha$  is inseparable over  $K$ , then  $m_{\alpha/K}(X) = m_{\alpha^p/K}(X^p)$ , as in the previous proof. Hence

$$[K(\alpha) : K(\alpha^p)] = \frac{[K(\alpha) : K]}{[K(\alpha^p) : K]} = \frac{\deg(m_{\alpha/K})}{\deg(m_{\alpha^p/K})} = p.$$

Conversely, let  $\alpha$  be separable over  $K$ . Then *a fortiori*  $\alpha$  is separable over  $K(\alpha^p)$ . Set  $m$  to be the minimal polynomial of  $\alpha$  over  $K(\alpha^p)$ . Now,  $\alpha$  is clearly a root of  $X^p - \alpha^p \in K(\alpha^p)[X]$ , so  $m | (X^p - \alpha^p)$ . Since  $X^p - \alpha^p = (X - \alpha)^p$

over  $K(\alpha)$ , by Lemma 6.3, we deduce that  $m = (X - \alpha)^r$  for some  $r$  over  $K(\alpha)$  by unique factorisation. Since  $m$  is separable, we must have  $r = 1$ , so  $[K(\alpha) : K(\alpha^p)] = \deg(m) = 1$ .  $\square$

**Proposition 6.7.** *All finite fields are perfect.*

*Proof.* Let  $K$  be a finite field of characteristic  $p > 0$ , and let  $L/K$  be algebraic. For  $\alpha \in L$ , we wish to show that  $\alpha \in K(\alpha^p)$ , and hence that  $\alpha$  is separable over  $K$  by Lemma 6.6.

Consider  $K(\alpha^p)$ . This is a finite extension of  $K$ , so is again a finite field. By Lemma 6.2 we know that the Frobenius map is an automorphism of  $K(\alpha^p)$ , and hence there exists  $\gamma \in K(\alpha^p)$  such that  $\alpha^p = \text{Fr}(\gamma) = \gamma^p$ . Thus, over  $L$ , we have that  $0 = \alpha^p - \gamma^p = (\alpha - \gamma)^p$ , hence  $\alpha = \gamma \in K(\alpha^p)$  as required.  $\square$

On the other hand, inseparable extensions do exist.

**Proposition 6.8.** *Let  $k$  be a field of characteristic  $p > 0$ ,  $L = k(x)$  a simple transcendental extension of  $k$  and  $K = k(x^p)$ . Then  $L/K$  is inseparable.*

*Proof.* Clearly  $L = K(x)$  and  $x$  is a root of the polynomial  $X^p - x^p \in K[X]$ . Thus  $L/K$  is simple algebraic. To see that  $L/K$  is inseparable, we can either show that  $X^p - x^p$  is irreducible over  $K$ , or else that  $x \notin K$ , using Lemma 6.6. Suppose that  $x \in K$ . Then there exist polynomials  $f, g \in k[X]$  such that  $x = f(x^p)/g(x^p)$ . Thus  $xg(x^p) = f(x^p)$ , and since  $x$  is transcendental over  $k$ , this yields the polynomial identity  $Xg(X^p) = f(X^p)$ . In particular,  $p \deg(f) = 1 + p \deg(g)$ , a contradiction.

Alternatively, set  $y := x^p$  and note that  $y$  is transcendental over  $k$ . Consider  $m = X^p - y \in k(y)[X]$ . By Gauss' Lemma,  $m$  is irreducible in  $k(y)[X]$  if and only if it is irreducible in  $k[y][X] = k[y, X]$ , if and only if it is irreducible in  $k(X)[y]$ . Since  $m$  is linear in  $y$ , it is irreducible in  $k(X)[y]$ , so we are done.  $\square$

The next theorem is an analogue for separability of Theorem 3.9.

**Theorem 6.9.** *Let  $L/K$  be a field extension and write  $L^{\text{sep}/K}$  for the subset of  $L$  consisting of those elements which are separable over  $K$ . Then  $L^{\text{sep}/K}$  is a subfield of  $L$ , and is a separable field extension of  $K$ .*

*Proof.* This is trivial when  $\text{char}(K) = 0$ , so suppose  $\text{char}(K) = p > 0$ . The main idea is to show that for  $\alpha, \beta \in L$  algebraic over  $K$ , we have

$$K(\alpha^p, \beta^p) = K(\alpha, \beta) \quad \text{if and only if} \quad \alpha, \beta \text{ are separable over } K.$$

This follows from the Tower Law and Lemma 6.6, once we have proved that

$$[K(\beta^p) : K] \leq [K(\beta) : K] \quad \text{and} \quad [K(\alpha^p, \beta^p) : K(\beta^p)] \leq [K(\alpha, \beta) : K(\beta)].$$

The first is Lemma 6.6. For the second, let  $m \in K(\beta)[X]$  denote the minimal polynomial of  $\alpha$  over  $K(\beta)$ . Applying the Frobenius homomorphism, we have

$\text{Fr}(m) \in K(\beta^p)[X]$ . Also, since  $\text{Fr}(m)(X^p) = m(X)^p$ , we have  $0 = m(\alpha)^p = \text{Fr}(m)(\alpha^p)$ , so the minimal polynomial of  $\alpha^p$  over  $K(\beta^p)$  divides  $\text{Fr}(m)(X)$ , so has degree at most  $\deg(m)$ .

Now let  $\alpha, \beta \in L^{\text{sep}/K}$  with  $\beta \neq 0$ , and let  $\gamma$  denote any one of  $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ . Using the above, we have

$$K(\beta, \gamma) = K(\alpha, \beta) = K(\alpha^p, \beta^p) = K(\beta^p, \gamma^p).$$

Thus  $\gamma$  is also separable over  $K$ .  $\square$

An important property is that normal closures of separable extensions are themselves separable.

**Theorem 6.10.** *Let  $L/K$  be a finite, separable extension, and let  $M/L$  be its normal closure. Then  $M/K$  is again finite and separable.*

*In particular, if  $f \in K[X]$  is a separable polynomial, then its splitting field  $L/K$  is finite, separable and normal.*

*Proof.* Let  $L = K(\alpha_1, \dots, \alpha_n)$ . Let  $m_i \in K[X]$  be the minimal polynomial of  $\alpha_i$ , and set  $m := m_1 \cdots m_n$ . Then, as in Theorem 5.4,  $M/K$  is the splitting field of  $m$ , so finite. Now, since each  $m_i$  is separable over  $K$ ,  $m$  is separable over  $K$ . Since  $M$  is generated over  $K$  by the roots of  $m$ ,  $M/K$  is separable by Theorem 6.9.  $\square$

The following is the analogue for separable extensions of Theorems 3.10 and 5.8.

**Theorem 6.11.** *1. Let  $L/K/k$  be field extensions. Then  $L/k$  is separable if and only if both  $L/K$  and  $K/k$  are separable.*

*2. Let  $E, F$  be two intermediate fields  $L/K$ . Then  $E/K$  separable implies  $EF/F$  separable.*

*3. Let  $E, F$  be two intermediate fields  $L/K$ . Then both  $E/K$  and  $F/K$  separable implies both  $EF/K$  and  $E \cap F/K$  separable.*

*Proof.* (1) If  $\text{char}(K) = 0$ , then there is nothing to prove, so assume  $\text{char}(K) = p > 0$ . Clearly if  $L/k$  is separable, then both  $L/K$  and  $K/k$  are separable, so suppose that both  $L/K$  and  $K/k$  are separable, hence algebraic. Then  $L/k$  is algebraic by Theorem 3.10. Let  $\alpha \in L$ .

On the one hand,  $\alpha$  is separable over  $K$ , so each  $\alpha^{p^r}$  is separable over  $K$  by Theorem 6.9. Therefore  $K(\alpha) = K(\alpha^{p^r})$  by repeated use of Lemma 6.6. On the other hand, there exists  $r$  such that  $\alpha^{p^r}$  is separable over  $k$  by Corollary 6.5, whence  $K(\alpha^{p^r})/k$  is separable by Theorem 6.9, so  $\alpha$  is separable over  $k$ .

(2) Consider  $(EF)^{\text{sep}/F}$ . This obviously contains every element of  $F$ , and since  $E/K$  is separable, it must contain every element of  $E$ . Hence  $(EF)^{\text{sep}/F} = EF$ .

(3) This is immediate from (1) and (2).  $\square$

# Chapter 7

## Galois Extensions

Let  $L/K$  be an algebraic field extension. We define the **Galois group**  $\text{Gal}(L/K)$  of  $L/K$  to be the set of  $K$ -automorphisms of  $L$  under composition:

$$\text{Gal}(L/K) := \{\sigma: L \xrightarrow{\sim} L : \sigma(x) = x \text{ for all } x \in K\}.$$

We remark that this is a group under composition. For

- if  $\sigma, \tau \in \text{Gal}(L/K)$ , then  $\sigma\tau: L \rightarrow L$ ,  $x \mapsto \sigma(\tau(x))$  is again an automorphism of  $L$ , and if  $x \in K$ , then  $\sigma(\tau(x)) = \sigma(x) = x$ , so it is a  $K$ -automorphism of  $L$ .
- composition of automorphisms is associative.
- the identity  $\text{id}: L \rightarrow L$  is the identity element of  $\text{Gal}(L/K)$ .
- each  $K$ -automorphism has an inverse, which is again a  $K$ -automorphism.

Note that by Proposition 4.5, since  $L/K$  is algebraic, each  $K$ -endomorphism of  $L$  is necessarily a  $K$ -automorphism.

Conversely, let  $G$  be any group of automorphisms of a field  $L$ . We define the **fixed field**  $L^G$  of  $G$  to be the set of elements of  $L$  fixed by each automorphism in  $G$ :

$$L^G := \{x \in L : \sigma(x) = x \text{ for all } \sigma \in G\}.$$

We remark that this is a subfield of  $L$ . For

- $\sigma(0) = 0$  and  $\sigma(1) = 1$  since  $\sigma$  is a field homomorphism, so  $0, 1 \in L^G$ .
- if  $x, y \in L^G$ , then  $\sigma(x+y) = \sigma(x) + \sigma(y) = x + y$  and  $\sigma(xy) = \sigma(x)\sigma(y) = xy$ , so  $x + y, xy \in L^G$ .
- similarly if  $0 \neq x \in L^G$ , then  $\sigma(-x) = -x$  and  $\sigma(1/x) = 1/x$ , so  $-x, 1/x \in L^G$ .

Observe that  $K \subset L^{\text{Gal}(L/K)}$ , and if  $F$  is a subfield of  $L/K$ , then  $\text{Gal}(L/F) \leq \text{Gal}(L/K)$ .

We say that  $L/K$  is a **Galois extension** if there exists some *finite* group  $G$  of automorphisms of  $L$  such that  $K = L^G$ . It necessarily follows that  $G$  is a subgroup of  $\text{Gal}(L/K)$ , and hence that  $K = L^{\text{Gal}(L/K)}$ .

**Warning.**

It is not true in general that for a field extension  $L/K$  we have  $K = L^{\text{Gal}(L/K)}$ . For example, let  $L = \mathbb{Q}(\sqrt[3]{2})$  and  $K = \mathbb{Q}$ . Then we have already seen (using Artin's Extension Theorem), that there are no non-trivial  $K$ -automorphisms of  $L$ . Thus  $\text{Gal}(L/K) = \{\text{id}\}$ , so  $L^{\text{Gal}(L/K)} = L$ .

**Examples.**

1. The field extension  $\mathbb{C}/\mathbb{R}$  is Galois, with Galois group  $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \sigma\}$ , where  $\sigma(x) = \bar{x}$  is complex conjugation.
2. The extension  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  is Galois, with Galois group  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\text{id}, \sigma\}$ , where  $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$  for  $a, b \in \mathbb{Q}$ .
3. More generally, let  $L/K$  be a field extension of degree 2 with  $\text{char}(K) \neq 2$ . Then  $L/K$  is Galois. For, take  $\alpha \in L \setminus K$ . Then  $\alpha$  has minimal polynomial of degree 2. Completing the square, we may assume that  $\alpha^2 \in K$ , so  $\alpha$  has minimal polynomial  $X^2 - \alpha^2$ . This is separable, since  $\text{char}(K) \neq 2$ , with roots  $\pm\alpha$ . The field  $L$  has  $K$ -basis  $\{1, \alpha\}$ , and  $\text{Gal}(L/K) = \{\text{id}, \sigma\}$ , where  $\sigma(a + b\alpha) = a - b\alpha$  for  $a, b \in K$ .
4. In Section 4.2 we computed the Galois group of  $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$ , where  $\alpha = \sqrt[3]{2} \in \mathbb{R}$  and  $\omega = \exp(2\pi i/3)$ . We showed that the Galois group is isomorphic to the symmetry group  $S_3$ , with generators  $\sigma$  and  $\tau$ . Since  $\tau$  corresponded to complex conjugation, the fixed field must be real, so contained in  $\mathbb{Q}(\alpha)$ . This has degree 3 over  $\mathbb{Q}$ , so the fixed field is either  $\mathbb{Q}$  or  $\mathbb{Q}(\alpha)$  by the Tower Law. Since  $\alpha$  is not fixed by  $\sigma$ , the fixed field is  $\mathbb{Q}$ . Hence  $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$  is Galois.

The following theorem can be interpreted as saying that Galois extensions are those having the maximum possible number of symmetries.

**Theorem 7.1.** *Let  $L/K$  be Galois with respect to the finite group  $G$ . Then  $|G| = [L : K]$  and  $G = \text{Gal}(L/K)$ .*

*Proof.* We will first show that  $[L : K] \leq |G|$ . The proof is similar to that of Theorem 4.6, showing the linear independence of characters.

Let  $G = \{\sigma_1, \dots, \sigma_n\}$ . Suppose  $[L : K] > n$ , so there exist  $x_1, \dots, x_{n+1} \in L$ , linearly independent over  $K$ . Forming the  $n \times (n+1)$ -matrix  $(\sigma_i(x_j))$  with entries in  $L$ , we see that this has non-zero kernel. In other words, there exist  $\lambda_1, \dots, \lambda_{n+1} \in L$  not all zero such that  $\sum_j \lambda_j \sigma_r(x_j) = 0$  for all  $r$ . We take such a vector  $(\lambda_i)$  having a minimal number of non-zero terms. Relabelling if

necessary, we may assume that  $\lambda_{n+1} \neq 0$ , and dividing through, we may assume that  $\lambda_{n+1} = -1$ . Thus, for all  $r$ ,

$$\sigma_r(x_{n+1}) = \lambda_1 \sigma_r(x_1) + \cdots + \lambda_n \sigma_r(x_n).$$

Now, since  $\sigma_r = \text{id}$  for some  $r$ , and since the  $x_j$  are linearly independent over  $K$ , we must have  $\lambda_i \in L \setminus K$  for some  $i \leq n$ . Relabelling, we may assume that  $i = 1$ . Since  $K = L^G$ ,  $\lambda_1$  is not fixed by  $G$ , so there exists  $s$  such that  $\sigma_s(\lambda_1) \neq \lambda_1$ . Applying  $\sigma_s$  to the previous expression, we obtain

$$\sigma_s \sigma_r(x_{n+1}) = \sigma_s(\lambda_1) \sigma_s \sigma_r(x_1) + \cdots + \sigma_s(\lambda_n) \sigma_s \sigma_r(x_n)$$

for all  $r$ . Moreover, since  $G$  is a group, left multiplication in  $G$  by  $\sigma_s$  is bijective. In other words, we have  $\sigma_s \sigma_r = \sigma_t$  for some  $t$ , and every  $\sigma_t$  arises in such a way. Therefore, for all  $r$ ,

$$\sigma_r(x_{n+1}) = \sigma_s(\lambda_1) \sigma_r(x_1) + \cdots + \sigma_s(\lambda_n) \sigma_r(x_n).$$

Subtracting this from our original expression yields

$$0 = (\lambda_1 - \sigma_s(\lambda_1)) \sigma_r(x_1) + \cdots + (\lambda_n - \sigma_s(\lambda_n)) \sigma_r(x_n)$$

for all  $r$ . Thus the vector  $(\lambda_i - \sigma_s(\lambda_i))$  also lies in the kernel. Moreover, this element is non-zero, since  $\lambda_1 \neq \sigma_s(\lambda_1)$ , but has fewer non-zero terms, contradicting our minimality assumption.

We deduce that  $[L : K] \leq |G|$ . In particular,  $L/K$  is finite. Since  $G$  fixes every element in  $K$ , each  $\sigma_r$  is a  $K$ -automorphism of  $L$ , so  $G \leq \text{Gal}(L/K)$ . We can now use Corollary 4.4 with  $L = L'$  to deduce that  $|\text{Gal}(L/K)| \leq [L : K]$ . Hence  $|G| = [L : K] = |\text{Gal}(L/K)|$ , and  $G = \text{Gal}(L/K)$ .  $\square$

The next theorem relates Galois extensions with all that we have done so far.

**Theorem 7.2.** *A field extension  $L/K$  is Galois if and only if it is finite, separable and normal.*

*In particular, if  $f \in K[X]$  is separable, then its splitting field  $L/K$  is Galois.*

Let  $f \in K[X]$  be separable and let  $L/K$  be the splitting field of  $f$ . We sometimes write  $\text{Gal}(f)$  for  $\text{Gal}(L/K)$ .

*Proof.* Let  $L/K$  be Galois and set  $G := \text{Gal}(L/K)$ . By Theorem 7.1 we have  $[L : K] = |G|$  so that  $L/K$  is finite.

Now let  $\alpha \in L$ , and set

$$G' := \text{Stab}_G(\alpha) = \{\sigma : \sigma(\alpha) = \alpha\} \leq G.$$

Let  $\{\sigma_1, \dots, \sigma_n\}$  be a complete set of left coset representatives of  $G'$  in  $G$ . Then

$$\text{Orb}_G(\alpha) = \{\sigma(\alpha) : \sigma \in G\} = \{\sigma_1(\alpha), \dots, \sigma_n(\alpha)\}.$$

In particular, given  $\sigma \in G$  we have  $\{\sigma\sigma_i(\alpha)\} = \{\sigma_i(\alpha)\}$ .  
 Consider the polynomial

$$f(X) := \prod_i (X - \sigma_i(\alpha)) = X^n + a_1X^{n-1} + \cdots + a_n \in L[X].$$

Given  $\sigma \in G$  we have

$$\sigma(f) = \prod_i (X - \sigma\sigma_i(\alpha)) = \prod_i (X - \sigma_i(\alpha)) = f.$$

Therefore, for each  $i$ ,  $\sigma(a_i) = a_i$  for all  $\sigma \in G$ , whence  $a_i \in L^G = K$ . Thus  $f \in K[X]$ . Moreover, by construction,  $f$  is separable over  $K$  and splits over  $L$ . Now,  $\alpha \in \text{Orb}_G(\alpha)$ , so  $\alpha = \sigma_i(\alpha)$  for some  $i$ . Hence  $\alpha$  is a root of  $f$ . It follows that  $m_{\alpha/K}$  divides  $f$ , so  $m_{\alpha/K}$  is separable over  $K$  and splits over  $L$ . This holds for all  $\alpha \in L$ , so  $L/K$  is separable and normal.

Conversely let  $L/K$  be finite, separable and normal. By Corollary 4.4 we know that  $|\text{Gal}(L/K)| \leq [L : K]$ , so that  $G := \text{Gal}(L/K)$  is a finite group.

Let  $\alpha \in L \setminus K$ . Then its minimal polynomial  $m_{\alpha/K}$  has degree at least two, and by assumption is separable and splits over  $L$ . Thus it has another root  $\beta \neq \alpha$  in  $L$ . By Artin's Extension Theorem, there exists a  $K$ -embedding  $\iota: K(\alpha) \rightarrow L$  sending  $\alpha \mapsto \beta$ . Furthermore, Theorem 5.5 implies that  $\iota$  extends to a  $K$ -automorphism  $\sigma$  of  $L$ . Thus  $\sigma \in G$  and  $\sigma(\alpha) = \beta \neq \alpha$ , so  $\alpha \notin L^G$ . Therefore  $G$  has fixed field precisely  $K$ , so  $L/K$  is Galois.

If  $f \in K[X]$  is separable, then its splitting field  $L/K$  is finite, separable and normal by Theorem 6.10, hence Galois.  $\square$

One part of the proof is worth emphasising.

**Corollary 7.3.** *Let  $L/K$  be Galois. If  $\alpha$  and  $\beta$  are  $K$ -conjugates in  $L$ , then there exists  $\sigma \in \text{Gal}(L/K)$  such that  $\sigma(\alpha) = \beta$ .*

## 7.1 The Galois Correspondence

**Theorem 7.4** (Fundamental Theorem of Galois Theory). *Let  $L/K$  be Galois with Galois group  $\text{Gal}(L/K)$ . Then there is a bijection between the subgroups of  $G$  and the set of intermediate fields of  $L/K$ . This bijection is given as*

$$\theta: H \leq G \mapsto L^H, \quad \phi: F \mapsto \text{Gal}(L/F) \leq \text{Gal}(L/K).$$

*Proof.* The maps are well-defined, since if  $F$  is an intermediate field, then  $\text{Gal}(L/F) \leq \text{Gal}(L/K)$ , and if  $H \leq \text{Gal}(L/K)$ , then  $L^H$  is an intermediate field of  $L/K$ .

To see that  $\phi\theta = \text{id}$ , let  $H \leq \text{Gal}(L/K)$ . Then  $H$  is a finite group, so  $L/L^H$  is Galois by definition, hence  $H = \text{Gal}(L/L^H)$  by Theorem 7.1.

To see that  $\theta\phi = \text{id}$ , let  $F$  be an intermediate field of  $L/K$ . Then  $L/F$  is finite, separable and normal by Theorems 3.10, 5.8 and 6.11, so is Galois by Theorem 7.2. Hence  $F = L^{\text{Gal}(L/F)}$ .

If  $H$  is a subgroup of  $\text{Gal}(L/K)$ , then  $L/L^H$  is Galois, so  $H = \text{Gal}(L/L^H)$  by Theorem 7.1. Also, since  $H$  fixes each element of  $K$ , we have  $K \subset L^H$ . Thus  $L^H$  is an intermediate field of  $L/K$ .

This shows that our two maps are well-defined. Moreover, since  $L^{\text{Gal}(L/F)} = F$  and  $\text{Gal}(L/L^H) = H$ , we see that these maps are mutually inverse.

If  $E \subset F$  are intermediate fields of  $L/K$ , then clearly  $\text{Gal}(L/F) \leq \text{Gal}(L/E)$ . Conversely, if  $H \leq H'$  are subgroups of  $\text{Gal}(L/K)$ , then each element of  $L^{H'}$  is fixed by  $H$ , so  $L^{H'} \subset L^H$ . Thus the maps above reverse inclusions between subgroups and intermediate fields.  $\square$

Let  $L/K$  be Galois. We often use the following terminology. If  $F$  is an intermediate field, then  $\text{Gal}(L/F)$  is the subgroup **associated** to  $F$ . If  $H \leq \text{Gal}(L/K)$  is a subgroup, then  $L^H$  is the intermediate field **belonging** to  $H$ .

**Theorem 7.5** (Galois Correspondence). *Let  $L/K$  be Galois. Let  $F, F_1, F_2$  be intermediate fields with associated groups  $H, H_1, H_2$ . Then*

1.  $|H| = [L : F]$ .
2.  $F_1 \subset F_2$  if and only if  $H_1 \supset H_2$ .
3. The intersection  $F_1 \cap F_2$  has associated subgroup  $\langle H_1, H_2 \rangle$ , the smallest subgroup of  $\text{Gal}(L/K)$  containing both  $H_1$  and  $H_2$ .
4. The composite  $F_1F_2$  has associated group  $H_1 \cap H_2$ .
5. Given  $\sigma \in \text{Gal}(L/K)$ ,  $\sigma(F)$  has associated subgroup  $\sigma H \sigma^{-1}$ .
6.  $F/K$  is Galois if and only if it is normal, which is if and only if  $H \triangleleft \text{Gal}(L/K)$  is a normal subgroup. In this case,  $\text{Gal}(F/K) \cong \text{Gal}(L/K)/H$ .

In particular, this shows that the two maps

$$H \leq \text{Gal}(L/K) \mapsto L^H \quad \text{and} \quad F \mapsto \text{Gal}(L/F)$$

induce an order-reversing bijection between the lattice of subgroups of  $\text{Gal}(L/K)$  and the lattice of intermediate fields of  $L/K$ .

Note that property (6) is the reason for the term *normal subgroup*.

*Proof.* (1) This follows from Theorem 7.1, noting that  $H = \text{Gal}(L/F)$ .

(2) This is contained in Theorem 7.4.

(3) Clearly  $F_1 \cap F_2 \subset F_i$ , so that  $H_i \leq \text{Gal}(L/F_1 \cap F_2)$ , hence  $\langle H_1, H_2 \rangle \leq \text{Gal}(L/F_1 \cap F_2)$ . On the other hand,  $H_i \leq \langle H_1, H_2 \rangle$ , so that  $L^{\langle H_1, H_2 \rangle} \subset F_i$ ,

whence  $L^{\langle H_1, H_2 \rangle} \subset F_1 \cap F_2$ . Applying (2) yields the reverse inclusion  $\text{Gal}(L/F_1 \cap F_2) \leq \langle H_1, H_2 \rangle$ .

(4) This is similar to (3). We have  $F_i \subset F_1 F_2$ , so that  $\text{Gal}(L/F_1 F_2) \leq H_i$ , hence  $\text{Gal}(L/F_1 F_2) \leq H_1 \cap H_2$ . Conversely,  $H_1 \cap H_2 \leq H_i$ , so  $F_i \subset L^{H_1 \cap H_2}$ , whence  $F_1 F_2 \subset L^{H_1 \cap H_2}$ . Applying (2) yields the reverse inclusion  $H_1 \cap H_2 \leq \text{Gal}(L/F_1 F_2)$ .

(5) Let  $\tau \in H$  and  $x \in L$ . Then  $(\sigma\tau\sigma^{-1})(\sigma(x)) = \sigma\tau(x)$ , so  $\sigma(x)$  is fixed by  $\sigma\tau\sigma^{-1}$  if and only if  $x$  is fixed by  $\tau$ . Thus  $L^{\sigma H \sigma^{-1}} = \sigma(L^H) = \sigma(F)$ .

(6) Since  $L/K$  is finite and separable, the same is true of  $F/K$ . Thus  $F/K$  is Galois if and only if it is normal.

Suppose  $F/K$  is normal. If  $\sigma \in \text{Gal}(L/K)$ , then  $\sigma(F) = F$  by Proposition 5.6, so (5) implies  $\sigma H \sigma^{-1} = H$ . Thus  $H \triangleleft \text{Gal}(L/K)$  is a normal subgroup.

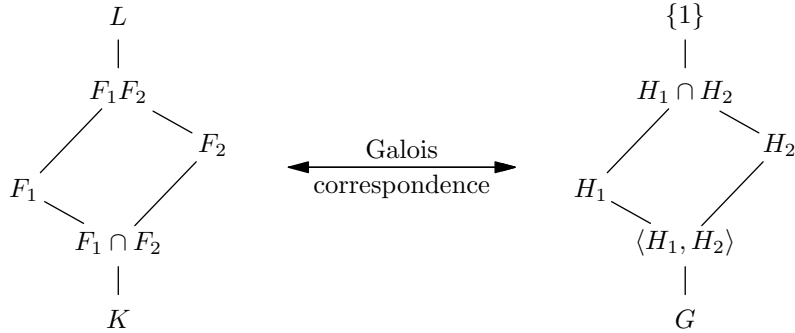
Conversely, if  $H$  is a normal subgroup, then for all  $\sigma \in \text{Gal}(L/K)$  we have  $\sigma H \sigma^{-1} = H$ , and hence from (5) that  $\sigma(F) = F$ . Thus each  $\sigma \in \text{Gal}(L/K)$  restricts to an automorphism of  $F$ . Now let  $\alpha, \beta \in L$  be conjugates. By Corollary 7.3 there exists  $\sigma \in \text{Gal}(L/K)$  such that  $\sigma(\alpha) = \beta$ . So, if  $\alpha \in F$ , then  $\beta \in F$  too. Hence  $F/K$  is normal.

Consider the group homomorphism

$$\text{Gal}(L/K) \rightarrow \text{Gal}(F/K), \quad \sigma \mapsto \sigma|_F.$$

This has kernel  $\{\sigma \in \text{Gal}(L/K) : \sigma|_F = \text{id}\} = \text{Gal}(L/F) = H$ . On the other hand, if  $\iota \in \text{Gal}(F/K)$ , then we can extend this to  $\sigma \in \text{Gal}(L/K)$  by Theorem 5.5. Hence the map is also surjective.  $\square$

We have the following two pictures representing properties (3) and (4) above.



The following is the analogue for Galois extensions of Theorems 3.10, 5.8 and 6.11. Given groups  $G, G'$  and  $H$ , and group homomorphisms  $\theta: G \rightarrow H$  and  $\theta': G' \rightarrow H$ , we define the fibred product to be

$$G \times_H G' := \{(g, g') \in G \times G' : \theta(g) = \theta'(g') \in H\} \leq G \times G'.$$

**Theorem 7.6.** 1. Let  $L/K/k$  be field extensions. Then  $L/k$  Galois implies  $L/K$  Galois, in which case  $\text{Gal}(L/K) \leq \text{Gal}(L/k)$ .

2. Let  $E, F$  be two intermediate fields of  $L/K$ . Then  $E/K$  Galois implies  $EF/F$  Galois, in which case we have a group isomorphism

$$\text{Gal}(EF/F) \xrightarrow{\sim} \text{Gal}(E/E \cap F), \quad \sigma \mapsto \sigma|_E.$$

3. Let  $E, F$  be two intermediate fields of  $L/K$ . Then both  $E/K$  and  $F/K$  Galois implies both  $EF/K$  and  $E \cap F/K$  Galois, in which case we have a group isomorphism

$$\text{Gal}(EF/K) \xrightarrow{\sim} \text{Gal}(E/K) \times_{\text{Gal}(E \cap F/K)} \text{Gal}(F/K), \quad \sigma \mapsto (\sigma|_E, \sigma|_F).$$

*Proof.* (1) This is contained in Theorem 7.4.

(2) Since  $E/K$  is finite, separable and normal, so is  $EF/F$  by Theorems 3.10, 5.8 and 6.11. Thus  $EF/F$  is Galois. Let  $\sigma \in \text{Gal}(EF/F)$ . Then  $\sigma(E) = E$  by Proposition 5.6, and  $\sigma|_{E \cap F} = \text{id}$ . We therefore have a group homomorphism  $\text{Gal}(EF/F) \rightarrow \text{Gal}(E/E \cap F)$ ,  $\sigma \mapsto \sigma|_E$ .

If  $\sigma|_E = \text{id}$ , then  $\sigma$  acts as the identity on all elements of  $E$  and all elements of  $F$ , hence on all elements of  $EF$ . Thus  $\sigma = \text{id}$  in  $\text{Gal}(EF/F)$ , so the group homomorphism is injective. Conversely, if  $x \in E$  is fixed by all elements in the image, then it is fixed by all elements of  $\text{Gal}(EF/F)$ , so lies in  $F$ . Thus  $x \in E \cap F$  and the map is surjective.

(3) Since  $E/K$  and  $F/K$  are both finite, separable and normal, so are both  $EF/K$  and  $E \cap F/K$  by Theorems 3.10, 5.8 and 6.11. Thus  $EF/K$  and  $E \cap F/K$  are both Galois. Let  $\theta: \text{Gal}(EF/K) \rightarrow \text{Gal}(E/K) \times \text{Gal}(F/K)$  be the group homomorphism sending  $\sigma$  to  $(\sigma|_E, \sigma|_F)$ . To see that  $\theta$  is injective, suppose that  $\theta(\sigma) = (\text{id}_E, \text{id}_F)$ . Then  $\sigma$  fixes each element of  $E$  and  $F$ , hence fixes each element of  $EF$ , so  $\sigma = \text{id}_{EF}$ .

Now, since  $E \cap F/K$  is Galois, we have a surjective group homomorphism

$$\text{Gal}(E/K) \rightarrow \text{Gal}(E \cap F/K), \quad \tau \mapsto \tau|_{E \cap F}$$

by Theorem 7.5 (6). Moreover, if  $\sigma \in \text{Gal}(EF/K)$ , then it is clear that  $(\sigma|_E)|_{E \cap F} = \sigma|_{E \cap F}$ . Analogous results hold for  $F$  instead of  $E$ . Therefore, since  $\theta(\sigma) = (\sigma|_E, \sigma|_F)$ , we deduce that  $\theta(\sigma) \in H := \text{Gal}(E/K) \times_{\text{Gal}(E \cap F/K)} \text{Gal}(F/K)$ .

The proof of the surjectivity of  $\theta$  is somewhat indirect. (Alternatively one can prove this by counting arguments.) By (2), we know that  $\text{Gal}(EF/E \cap F) \xrightarrow{\sim} \text{Gal}(E/E \cap F)$ . Hence the image of  $\theta$  contains  $\text{Gal}(E/E \cap F) \times \{\text{id}\}$ . Similarly for  $F$ , so it contains  $\text{Gal}(E/E \cap F) \times \text{Gal}(F/E \cap F)$ . This proves that

$$\text{Gal}(EF/E \cap F) \xrightarrow{\sim} \text{Gal}(E/E \cap F) \times \text{Gal}(F/E \cap F).$$

Now, suppose that  $(\sigma_1, \sigma_2) \in H$ , and let  $\tau = \sigma_i|_{E \cap F}$  be their common image in  $\text{Gal}(E \cap F/K)$ . By Theorem 5.5 there exists  $\tilde{\tau} \in \text{Gal}(EF/K)$  extending  $\tau$ . Let  $\theta(\tilde{\tau}) = (\tau_1, \tau_2) \in H$ . Then  $(\sigma_1 \tau_1^{-1}, \sigma_2 \tau_2^{-1})$  is an element of the subgroup  $\text{Gal}(E/E \cap F) \times \text{Gal}(F/E \cap F)$  of  $H$ . From what we showed above, there exists

$\rho \in \text{Gal}(EF/K)$  such that  $\theta(\rho) = (\sigma_1\tau_1^{-1}, \sigma_2\tau_2^{-1})$ . Therefore, setting  $\sigma := \rho\tilde{\tau}$ , we have that  $\theta(\sigma) = (\sigma_1, \sigma_2)$  as required. Thus  $\theta$  is surjective.  $\square$

**Corollary 7.7.** *Let  $L/K$  be a field extension,  $E, F$  intermediate fields and suppose that  $E/K$  is Galois. Then  $[EF : F]$  divides  $[E : K]$ .*

*Proof.* We have  $[EF : F] = |\text{Gal}(EF/F)| = |\text{Gal}(E/E \cap F)|$ , and this divides  $|\text{Gal}(E/K)| = [E : K]$  by Lagrange's Theorem.  $\square$

By induction, we can also prove the following corollary.

**Corollary 7.8.** *Let  $L/K$  be a field extension.*

1. *Let  $F_1, \dots, F_n$  be intermediate fields of  $L/K$  with  $F_i/K$  Galois and  $F_i \cap (F_1 \cdots F_{i-1}) = K$  for all  $i$ . Then the composite  $F_1 \cdots F_n$  is Galois over  $K$  with Galois group isomorphic to the product  $\prod_{i=1}^n \text{Gal}(F_i/K)$ .*
2. *If  $L/K$  is Galois with Galois group  $\text{Gal}(L/K) \cong \prod_{i=1}^n G_i$ , then letting  $F_j$  be the intermediate subfield belonging to the subgroup  $\prod_{i \neq j} G_i$ , we have that  $F_i/K$  is Galois with Galois group  $G_i$ ,  $L = F_1 \cdots F_n$  and  $F_i \cap (F_1 \cdots F_{i-1}) = K$  for all  $i$ .*

## 7.2 The Primitive Element Theorem

Recall that  $L/K$  is simple if there exists some  $\alpha \in L$  such that  $L = K(\alpha)$ . We call such an  $\alpha$  a **primitive element** for  $L/K$ . We now give a criterion showing when a finite field extension is simple, and show that this always holds for finite separable extensions.

**Theorem 7.9** (Primitive Element). *Let  $L/K$  a finite extension. Then  $L/K$  is simple if and only if  $L/K$  has only finitely many intermediate fields.*

*Proof for  $K$  infinite.* Suppose that  $L/K$  has only finitely many intermediate fields. We show that, given  $\alpha, \beta \in L$ , there exists  $\lambda \in K$  such that  $K(\alpha, \beta) = K(\alpha + \lambda\beta)$ . We write  $\theta_\lambda$  for  $\alpha + \lambda\beta$ .

Since  $L/K$  has only finitely many intermediate fields, but  $K$  is infinite, there exists  $\lambda \neq \mu \in K$  such that  $K(\theta_\lambda) = K(\theta_\mu)$ . Thus both

$$\beta = \frac{\theta_\lambda - \theta_\mu}{\lambda - \mu} \quad \text{and} \quad \alpha = \frac{\mu\theta_\lambda - \lambda\theta_\mu}{\mu - \lambda}$$

lie in  $K(\theta_\lambda)$ , so that  $K(\alpha, \beta) = K(\theta_\lambda)$ .

By induction, given  $\alpha_1, \dots, \alpha_n \in L$ , there exist  $\lambda_2, \dots, \lambda_n \in K$  such that

$$K(\alpha_1, \dots, \alpha_n) = K(\alpha_1 + \lambda_2\alpha_2 + \cdots + \lambda_n\alpha_n).$$

Since  $L/K$  is finite, it is finitely generated and hence simple.

Conversely, let  $L = K(\alpha)$  be simple and write  $m = m_{\alpha/K} \in K[X]$ . We claim that there is an injection from the intermediate fields of  $L/K$  to the divisors of  $m$  over  $L$ .

Given a subfield  $F$ , we have  $L = F(\alpha)$ . If  $f \in F[X]$  is the minimal polynomial of  $\alpha$  over  $F$ , then  $f$  divides  $m$  over  $F$  and hence also over  $L$ . This determines a map  $\phi$  from intermediate fields  $F$  of  $L/K$  to divisors  $f$  of  $m$  over  $L$ .

Given a factor  $f$  of  $m$  over  $L$ , let  $F$  be the subfield of  $L/K$  generated by the coefficients of  $f$ . This determines a map  $\psi$  from divisors  $f$  of  $m$  over  $L$  to intermediate fields  $F$  of  $L/K$ .

We now show that  $\psi$  is a left inverse for  $\phi$ , whence  $\phi$  is injective. Let  $F$  be an intermediate field of  $L/K$  and let  $f$  be the minimal polynomial of  $\alpha$  over  $F$ . Then  $\psi\phi(F) = F'$  is the intermediate field of  $L/K$  generated by the coefficients of  $f$ . Since  $f \in F[X]$ , we must have  $F' \subset F$ . On the other hand, the minimal polynomial of  $\alpha$  over  $F'$  must equal  $f$ , so that  $[L : F] = \deg(f) = [L : F']$ . Since  $F' \subset F$ , we have equality  $F' = F$ .  $\square$

If  $K$  is a finite field, then we can use a completely different proof, based on the following lemma.

**Lemma 7.10.** *Let  $G$  be a finite group such that, for all  $m \geq 1$ , there are at most  $m$  elements  $x \in G$  such that  $x^m = 1$ . Then  $G$  is cyclic.*

*In particular, if  $G$  is a finite subgroup of the multiplicative group  $K^\times$  of some field  $K$ , then  $G$  is cyclic. If  $K$  is a finite field, then  $K^\times$  is a cyclic group.*

*Proof.* Let  $G$  be a finite group of order  $n$ . Write  $\theta(d)$  for the number of elements of  $G$  of order  $d$ . Using Lagrange's Theorem we have  $n = \sum_{d|n} \theta(d)$ .

If  $G$  is cyclic, then there exists a unique subgroup of order  $d$  for  $d|n$ . Thus  $\theta(d) = \phi(d)$ , where  $\phi$  is Euler's totient (or phi) function:

$$\phi(d) := |\{1 \leq r \leq d : \gcd(r, d) = 1\}|.$$

Suppose now that  $G$  satisfies our condition and let  $d|n$ . If  $\theta(d) \neq 0$ , then there exists some element  $g \in G$  of order  $d$ . Consider the cyclic group  $\langle g \rangle \leq G$ . This has  $d$  elements, all of which satisfy  $x^d = 1$ . Hence there can be no other elements in  $G$  with  $x^d = 1$ . Hence  $\theta(r) = \phi(r)$  for all  $r|d$ . It follows that, given  $d|n$ , either  $\theta(d) = \phi(d)$  or  $\theta(d) = 0$ . Since

$$\sum_{d|n} \theta(d) = n = \sum_{d|n} \phi(d),$$

we deduce that  $\theta(d) = \phi(d)$  for all  $d|n$ . In particular,  $\theta(n) = \phi(n) \geq 1$ , so that  $G$  is cyclic.

If  $K$  is a field, then there are at most  $m$  solutions to the equation  $X^m = 1$  in  $K$ . Thus each finite subgroup of  $K^\times$  is cyclic. If  $K$  is a finite field, then  $K^\times$  itself is a finite group, so cyclic.  $\square$

We can now prove the Primitive Element Theorem for finite fields.

*Proof for  $K$  finite.* Since  $K$  is a finite field and  $L/K$  is a finite field extension,  $L$  is also a finite field. There are only finitely many subsets of  $L$ , so only finitely many subfields of  $L$ . On the other hand, if  $\alpha$  is a generator for the multiplicative group  $L^\times$ , then clearly  $L = K(\alpha)$ .  $\square$

An important corollary of the **Primitive Element Theorem** is that all finite separable extensions are simple.

**Theorem 7.11.** *Let  $L/K$  be finite and separable. Then  $L/K$  is simple.*

*Proof.* Let  $L/K$  be finite and separable, and let  $M/L$  be its normal closure. Then by Theorem 6.10,  $M/K$  is finite, separable and normal, hence Galois by Theorem 7.2. By the **Fundamental Theorem of Galois Theory**, there is a bijection between the intermediate fields of  $M/K$  and the subgroups of  $\text{Gal}(M/K)$ . Since  $\text{Gal}(M/K)$  is a finite group, it has only finitely many subgroups, so there are only finitely many intermediate fields of  $M/K$ . In particular,  $L/K$  has only finitely many intermediate fields. Hence  $L/K$  is primitive, by the **Primitive Element Theorem**.  $\square$

It is illuminating to find an example of a finite field extension  $L/K$  which has infinitely many intermediate fields. This must be an inseparable extension, but of course there are many examples of inseparable extensions which are simple. Another nice consequence of the Primitive Element Theorem is the following.

**Proposition 7.12.** *Let  $L/K$  be Galois with Galois group  $G$ . Then  $L \otimes_K L \cong L^{[L:K]}$  as  $K$ -algebras.*

*Proof.* Since  $L/K$  is Galois, we can use the **Primitive Element Theorem** to write  $L = K(\alpha)$ . Set  $f := m_{\alpha/K}$ , so  $L \cong K[X]/(f)$ . Now, since  $L = K(\alpha)$  is simple, the elements  $\sigma(\alpha)$  for  $\sigma \in G$  are all distinct. These are precisely the roots of  $f$ , by **Artin's Extension Theorem**, so over  $L$  we can write

$$f = \prod_{\sigma \in G} (X - \sigma(\alpha)).$$

Using the **Chinese Remainder Theorem**, we have

$$L \otimes_K L \cong L \otimes K[X]/(f) \cong L[X]/(f) \cong \prod_{\sigma \in G} L[X]/(X - \sigma(\alpha)) \cong L^{[L:K]}.$$

The isomorphism  $L \otimes_K L \xrightarrow{\sim} L^{[L:K]}$  is given explicitly by  $x \otimes y \mapsto (x\sigma(y))_{\sigma \in G}$ .  $\square$

### 7.3 Transitivity

We now show that each Galois group can be considered as a transitive subgroup of some symmetric group  $S_n$ . Recall that a subgroup  $G \leq S_n$  is called **transitive** if, given  $1 \leq i, j \leq n$ , there exists  $\sigma \in G$  such that  $\sigma(i) = j$ .

**Proposition 7.13.** *Let  $L/K$  be the splitting field of a separable polynomial  $f \in K[X]$ . Let  $\{\alpha_1, \dots, \alpha_n\}$  be the roots of  $f$  in  $L$ . Then the map  $\text{Gal}(L/K) \rightarrow S_n$  induced by  $\sigma(\alpha_i) = \alpha_{\bar{\sigma}(i)}$  is an injective group homomorphism.*

*If  $f$  is irreducible, then the image of  $\text{Gal}(L/K)$  is a transitive subgroup of  $S_n$ .*

*Proof.* Each  $\sigma \in \text{Gal}(L/K)$  induces a permutation  $\bar{\sigma}$  of the roots of  $f$ . Clearly  $\bar{\text{id}} = \text{id}$ , and

$$\alpha_{\overline{\sigma\tau}(i)} = \sigma\tau(\alpha_i) = \sigma(\alpha_{\bar{\tau}(i)}) = \alpha_{\bar{\sigma}\bar{\tau}(i)},$$

so that  $\overline{\sigma\tau} = \bar{\sigma}\bar{\tau}$ . Therefore we have a group homomorphism  $\text{Gal}(L/K) \rightarrow S_n$ ,  $\sigma \mapsto \bar{\sigma}$ . To see that this is injective, suppose  $\sigma(\alpha_i) = \alpha_i$  for all  $i$ . Then, since  $L = K(\alpha_1, \dots, \alpha_n)$  is generated by the roots of  $f$ , we must have that  $\sigma = \text{id}$ .

Now suppose that  $f$  is irreducible, so that the  $\alpha_i$  are all conjugates. By Corollary 7.3, given  $i$  and  $j$  there exists  $\sigma \in \text{Gal}(L/K)$  such that  $\sigma(\alpha_i) = \alpha_j$ . Hence the image of  $\text{Gal}(L/K)$  is a transitive subgroup of  $S_n$ .  $\square$

We recall some results above transitive groups.

**Lemma 7.14.** *Let  $G$  be a transitive subgroup of  $S_p$  for some prime  $p$ . If  $G$  contains a transposition, then  $G = S_p$ .*

*Proof.* Since  $G$  is transitive,  $|\text{Orb}_G(1)| = p$ , so  $p$  divides  $|G|$  by the **Orbit-Stabiliser Theorem**. Then  $G$  contains a  $p$ -cycle by **Cauchy's Theorem**. Suppose  $G$  also contains a transposition. By relabelling, we may assume that  $G$  contains  $(1\ 2 \cdots p)$  and  $(1\ r)$ . By taking the  $(r-1)$ -st power of the  $p$ -cycle, we may further assume that  $r = 2$ . By repeatedly conjugating the transposition, we see that  $G$  contains  $(1\ 2), (2\ 3), \dots, (p-1\ p)$ . It is well-known that these transpositions generate  $S_p$ .  $\square$

For convenience, we recall the following classification.

**Proposition 7.15.** 1.  $S_2$  has no proper transitive subgroups.

2.  $A_3 \cong \mathbb{Z}/3\mathbb{Z}$  is the unique proper, transitive subgroup of  $S_3$ .

3. The proper, transitive subgroups of  $S_4$  up to conjugation are

$$A_4, \quad D_8, \quad \langle(1234)\rangle \cong \mathbb{Z}/4\mathbb{Z},$$

$$V = \{\text{id}, (12)(34), (13)(24), (14)(23)\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

$V$  is the Klein four-group (Kleinsche Vierergruppe);  $D_8$  is the dihedral group with 8 elements, or symmetry group of a square, given for example as  $\langle(1234), V\rangle$

## 7.4 Norm and Trace Revisited

In this section we relate the minimal polynomial and the field equation of an element  $\alpha$  to its conjugates  $\sigma(\alpha)$ . This is often easier to work with than the original definition.

We begin with a useful observation, which generalises Theorem 7.5 (6). Let  $L/K$  be finite, with normal closure  $M/L$ . Let  $\mathcal{E}$  denote the set of  $K$ -embeddings  $L \rightarrow M$ . We let  $\text{Gal}(M/K)$  act (on the left) on  $\mathcal{E}$  via  $\sigma \cdot \tau: L \rightarrow M, x \mapsto \sigma(\tau(x))$ . Note that  $\sigma \cdot \text{id} = \sigma|_L$ .

**Proposition 7.16.**  *$\text{Gal}(M/K)$  acts transitively on  $\mathcal{E}$ , and the stabiliser of  $\text{id} \in \mathcal{E}$  equals  $\text{Gal}(M/L)$ . In particular, the map  $\text{Gal}(M/K) \rightarrow \mathcal{E}, \sigma \mapsto \sigma|_L$  induces a natural bijection between the cosets of  $\text{Gal}(M/L)$  in  $\text{Gal}(M/K)$  and  $\mathcal{E}$ .*

*Proof.* Let  $\tau \in \mathcal{E}$ . By Theorem 5.5, we can extend  $\tau$  to  $\sigma \in \text{Gal}(M/K)$ . In particular,  $\sigma \cdot \text{id} = \sigma|_L = \tau$ , so  $\text{Gal}(M/K)$  acts transitively on  $\mathcal{E}$ . Clearly  $\sigma \cdot \text{id} = \text{id}$  if and only if  $\sigma \in \text{Gal}(M/L)$ , so by the **Orbit-Stabiliser Theorem** the map  $\sigma \mapsto \sigma \cdot \text{id} = \sigma|_L$  induces a bijection between the cosets of  $\text{Gal}(M/L)$  in  $\text{Gal}(M/K)$  and  $\mathcal{E}$  as required.  $\square$

We observe that the number  $|\mathcal{E}|$  of distinct  $K$ -embeddings  $L \rightarrow M$  equals the index of  $\text{Gal}(M/L)$  in  $\text{Gal}(M/K)$ . If  $L/K$  is separable, then  $M/K$  is Galois, so  $|\mathcal{E}| = [L : K]$  by the **Fundamental Theorem of Galois Theory**. This proves the next corollary.

**Corollary 7.17.** *Let  $L/K$  be finite and separable, with normal closure  $M/L$ . Then there are precisely  $[L : K]$  distinct  $K$ -embeddings  $L \rightarrow M$ .*

[In fact, this has a converse:  $L/K$  is separable if and only if there are precisely  $[L : K]$  distinct  $K$ -embeddings  $L \rightarrow M$ . This leads some authors *define*  $L/K$  to be separable if there are  $[L : K]$  distinct  $K$ -embeddings  $L \rightarrow M$ .]

**Proposition 7.18.** *Let  $L/K$  be finite and separable, with normal closure  $M/L$ . Let  $\sigma_1, \dots, \sigma_n$  be the distinct  $K$ -embeddings  $L \rightarrow M$ . Then for  $\alpha \in L$  we have*

$$\chi_{\alpha/K}^L = (X - \sigma_1(\alpha)) \cdots (X - \sigma_n(\alpha)).$$

*In particular,*

$$N_K^L(\alpha) = \prod_j \sigma_j(\alpha) \quad \text{and} \quad \text{Tr}_K^L(\alpha) = \sum_j \sigma_j(\alpha).$$

*Proof.* Let  $M/K$  be Galois, say with Galois group  $G := \text{Gal}(M/K)$ . For an intermediate field  $L$  let  $\sigma_1, \dots, \sigma_n$  be the distinct  $K$ -embeddings  $L \rightarrow M$ . We know that  $n = [L : K]$  by Corollary 7.17. For  $\alpha \in L$  define

$$f_{\alpha/K}^L := \prod_{i=1}^n (X - \sigma_i(\alpha)).$$

We wish to show that  $f_{\alpha/K}^L = \chi_{\alpha/K}^L$  for all  $L$  and all  $\alpha \in L$ .

We observe that

$$f_{\alpha/K}^M = \prod_{\sigma \in G} (X - \sigma(\alpha)),$$

whereas by Artin's Extension Theorem

$$f_{\alpha/K}^{K(\alpha)} = m_{\alpha/K},$$

since the distinct  $K$ -embeddings  $K(\alpha) \rightarrow M$  are in bijection with the roots of  $m_{\alpha/K}$ .

For  $\alpha \in L$  we can apply Proposition 7.16 to deduce that  $f_{\alpha/K}^M = (f_{\alpha/K}^L)^{[M:L]}$ . For, the value of  $\sigma(\alpha)$  depends only on the restriction  $\sigma|_L$ . In particular, for  $L = K(\alpha)$  we have  $f_{\alpha/K}^M = (m_{\alpha/K})^{[M:K(\alpha)]}$ , so  $f_{\alpha/K}^M = \chi_{\alpha/K}^M$  by Theorem 3.5. From this it follows that

$$(\chi_{\alpha/K}^L)^{[M:L]} = \chi_{\alpha/K}^M = f_{\alpha/K}^M = (f_{\alpha/K}^L)^{[M:L]}.$$

Therefore  $\chi_{\alpha/K}^L = f_{\alpha/K}^L$  by unique factorisation in  $L[X]$ .

By definition, if  $\chi_{\alpha/K}^L = X^n - a_1X^{n-1} + \dots + (-1)^n a_n$ , then  $\text{Tr}_K^L(\alpha) = a_1$  and  $N_K^L(\alpha) = a_n$ .  $\square$

Note that, by Proposition 7.16,  $\sum_j \sigma_j(\alpha)$  and  $\prod_j \sigma_j(\alpha)$  are fixed by  $\text{Gal}(M/K)$ , so these elements really do lie in  $K$ . Also, we may write  $\text{Tr}_K^L = \sum_j \sigma_j$  as a linear combination of the characters  $\sigma_j$ .

As promised, we can now prove transitivity of norm and trace for separable extensions.

**Theorem 7.19.** *Let  $L/K/k$  be finite, separable extensions. Then for  $\alpha \in L$  we have*

$$N_k^L(\alpha) = N_k^K(N_K^L(\alpha)) \quad \text{Tr}_k^L(\alpha) = \text{Tr}_k^K(\text{Tr}_K^L(\alpha)).$$

*Proof.* Let  $M/L$  be the normal closure of  $L/K$  and consider the chain of subgroups  $\text{Gal}(M/L) \leq \text{Gal}(M/K) \leq \text{Gal}(M/k)$ . Let  $\sigma_j$  be coset representatives of  $\text{Gal}(M/L)$  in  $\text{Gal}(M/K)$ , and let  $\tau_i$  be coset representatives of  $\text{Gal}(M/K)$  in  $\text{Gal}(M/k)$ . Thus  $1 \leq i \leq [K:k]$  and  $1 \leq j \leq [L:K]$ .

We claim that the  $\tau_i \sigma_j$  are coset representatives for  $\text{Gal}(M/L)$  in  $\text{Gal}(M/k)$ . [This is actually quite general, applying to all finite groups.] For, suppose  $\tau_i \sigma_j = \tau_r \sigma_s$ . We know that  $\sigma_j \text{Gal}(M/L) \subset \text{Gal}(M/K)$ . Since the  $\tau_i \text{Gal}(M/K)$  are distinct inside  $\text{Gal}(M/k)$ , we must therefore have  $i = r$ . Then since the  $\sigma_j \text{Gal}(M/L)$  are distinct in  $\text{Gal}(M/K)$ , we must have  $j = s$ . Therefore the  $\tau_i \sigma_j$  represent distinct cosets. Since there are  $[L:K][K:k] = [L:k]$  of them, we are done.

Now, using Proposition 7.18, we can write

$$N_k^K(N_K^L(\alpha)) = \prod_i \tau_i\left(\prod_j \sigma_j(\alpha)\right) = \prod_{i,j} \tau_i(\sigma_j(\alpha)) = \prod_{i,j} (\tau_i \sigma_j)(\alpha) = N_k^L(\alpha),$$

and similarly for  $\text{Tr}$ . □

## Chapter 8

# Calculating Galois Groups

### 8.1 Example 1.

Let us begin with our favourite example  $f = X^3 - 2 \in \mathbb{Q}[X]$ . Let  $L = \mathbb{Q}(\alpha, \omega)$  be the splitting field of  $f$  over  $\mathbb{Q}$ , where  $\alpha = \sqrt[3]{2}$  and  $\omega = \exp(2\pi i/3)$ . Then  $\text{Gal}(f) \cong \text{Sym}_3$ , as worked out in Chapter 3. This has generators  $\sigma$  and  $\tau$ , where  $\sigma(\alpha) = \omega\alpha$  and  $\sigma(\omega) = \omega$ , and  $\tau$  is complex conjugation, so that  $\tau(\alpha) = \alpha$  and  $\tau(\omega) = \omega^2$ . Moreover,  $\alpha + \omega$  is a primitive element for  $L/\mathbb{Q}$ . For, it takes the following six values under  $\text{Gal}(f)$ :

$$\begin{array}{ll} \text{id}(\alpha + \omega) = \alpha + \omega & \tau(\alpha + \omega) = \alpha + \omega^2 \\ \sigma(\alpha + \omega) = \omega\alpha + \omega & \sigma\tau(\alpha + \omega) = \omega\alpha + \omega^2 \\ \sigma^2(\alpha + \omega) = \omega^2\alpha + \omega & \sigma^2\tau(\alpha + \omega) = \omega^2\alpha + \omega^2 \end{array}$$

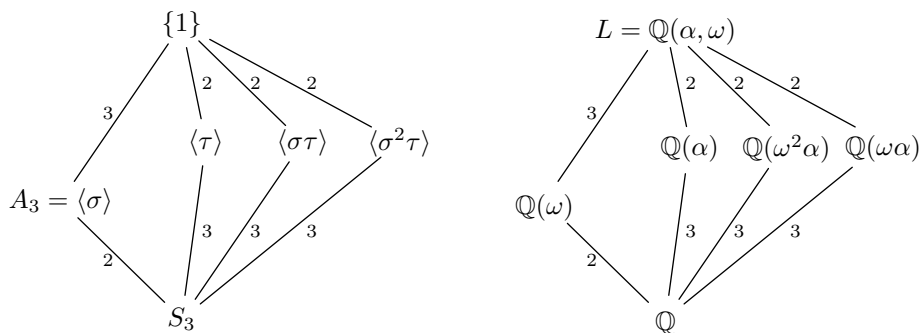
It follows that the minimal polynomial of  $\alpha + \omega$  over  $\mathbb{Q}$  is the product of the six linear factors with these roots. We calculate that

$$\begin{aligned} (X - (\alpha + \omega))(X - (\omega\alpha + \omega))(X - (\omega^2\alpha + \omega)) \\ = (X - \omega)^3 - \alpha^2 = X^3 - 3\omega X^2 + 3\omega^2 X - 3. \end{aligned}$$

Thus

$$m_{\alpha+\omega} = X^6 + 3X^5 + 6X^4 + 3X^3 + 9X + 9.$$

We now consider the Galois correspondence between the subgroups and intermediate fields. We illustrate this by drawing the respective lattices.



We have labelled the edges to indicate the index of the subgroup, respectively the degree of the field extension.

To compute the subgroup lattice is relatively easy, so how do we compute the corresponding fixed field? As an example, consider  $A_3 = \langle \sigma \rangle$  and denote its fixed field by  $K$ . Then  $\omega \in K$ , and since  $|A_3| = 3 = [L : \mathbb{Q}(\omega)]$ , we must have that  $K = \mathbb{Q}(\omega)$ .

We also observe that  $\sigma \langle \tau \rangle \sigma^{-1} = \langle \sigma \tau \sigma^{-1} \rangle = \langle \sigma^2 \tau \rangle$ , so that the fixed field of  $\langle \sigma^2 \tau \rangle$  equals  $\mathbb{Q}(\sigma(\alpha)) = \mathbb{Q}(\omega\alpha)$ .

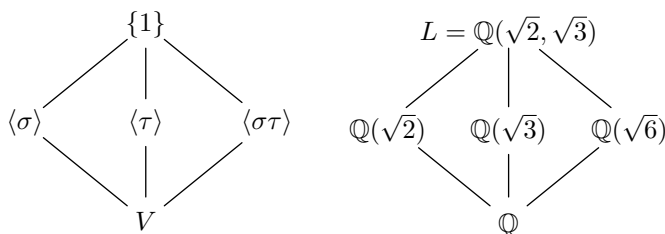
We observe that  $A_3$  is the only proper normal subgroup of  $S_3$ , and  $\mathbb{Q}(\omega)/\mathbb{Q}$  is the only normal extension. It is the splitting field extension of  $X^2 + X + 1$ .

## 8.2 Example 2.

Our next example is  $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ . We know that this is a field extension of degree 4, and is normal since it is the splitting field extension of  $f = (X^2 - 2)(X^2 - 3)$  over  $\mathbb{Q}$ . We calculate the Galois group using Artin's Extension Theorem. We let  $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  and  $K_p = \mathbb{Q}(\sqrt{p})$  for  $p = 2, 3$ . The minimal polynomial of  $\sqrt{p}$  over  $\mathbb{Q}$  is  $X^2 - p$ .

We observe that  $K_p/\mathbb{Q}$  is Galois, with Galois group  $\mathbb{Z}/2\mathbb{Z}$ . Moreover,  $K_2 \cap K_3 = \mathbb{Q}$  and  $L = K_2 K_3$ . Therefore we can apply Theorem 7.6 to deduce that  $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 = V$ , the Klein four-group. The Galois group is generated by  $\sigma$  and  $\tau$ , where  $\sigma(\sqrt{2}) = -\sqrt{2}$ ,  $\sigma(\sqrt{3}) = \sqrt{3}$  and  $\tau(\sqrt{2}) = \sqrt{2}$ ,  $\tau(\sqrt{3}) = -\sqrt{3}$ .

We again draw the lattices of subgroups and intermediate fields. Note that all inclusions of subgroups have index 2.



We observe that  $\sqrt{2} + \sqrt{3}$  is a primitive element for  $L/\mathbb{Q}$ , since its conjugates under  $V$  are

$$\sqrt{2} + \sqrt{3}, \quad -\sqrt{2} + \sqrt{3}, \quad \sqrt{2} - \sqrt{3}, \quad -\sqrt{2} - \sqrt{3}.$$

It follows that the minimal polynomial of  $\sqrt{2} + \sqrt{3}$  over  $\mathbb{Q}$  equals

$$\begin{aligned} m_{\sqrt{2}+\sqrt{3}} &= (X - (\sqrt{2} + \sqrt{3}))(X - (-\sqrt{2} + \sqrt{3}))(X - (\sqrt{2} - \sqrt{3}))(X - (-\sqrt{2} - \sqrt{3})) \\ &= X^4 - 10X^2 + 1. \end{aligned}$$

In this example, the Galois group is abelian, so all subgroups are normal.

More generally, if  $L = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$  for distinct primes  $p_i$ , then

$$\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n.$$

For, we use Corollary 7.8 with  $K_i := \mathbb{Q}(\sqrt{p_i})$ .

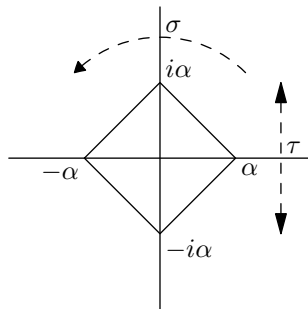
Note how easy this is, compared with Exercise 9.

### 8.3 Example 3.

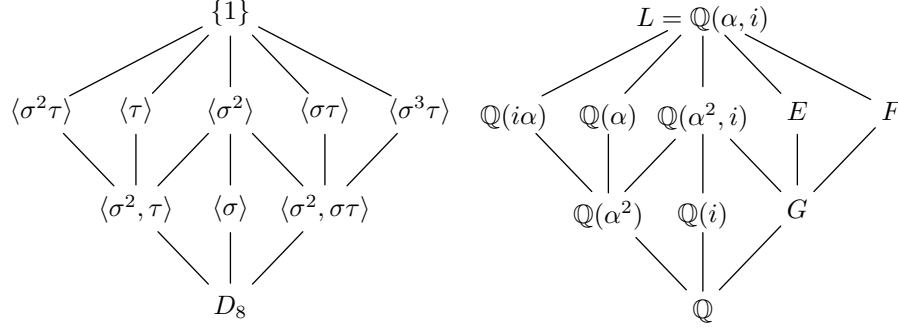
Now consider  $f = X^4 - 2 \in \mathbb{Q}[X]$ . This has splitting field  $L = \mathbb{Q}(\alpha, i)$ , where  $\alpha = \sqrt[4]{2}$ . Set  $K = \mathbb{Q}(\alpha)$ , and note that  $\alpha$  has minimal polynomial  $f$  over  $\mathbb{Q}$ . We have four embeddings  $K \rightarrow L$ , given by  $\alpha \mapsto i^r \alpha$  for  $0 \leq r \leq 3$ . The minimal polynomial of  $i$  over  $K$  must be  $X^2 + 1$ , since  $[L : K] \leq 2$  and  $L \neq K$  since  $K \subset \mathbb{R}$ . We therefore have two extensions of each  $\sigma^r$  to  $L$ , sending  $i \mapsto \pm i$ . Thus

$$\sigma^r : \alpha \mapsto i^r \alpha, \quad i \mapsto i \quad \text{and} \quad \sigma^r \tau : \alpha \mapsto i^r \alpha, \quad i \mapsto -i,$$

where  $\tau$  is complex conjugation. Note that  $\sigma$  has order 4,  $\tau$  has order 2 and  $\tau\sigma = \sigma^3\tau$ . Hence  $\text{Gal}(L/\mathbb{Q}) \cong D_8$ , the dihedral group with 8 elements, or symmetry group of the square. In fact, the four roots  $i^r \alpha$  of  $f$  in  $\mathbb{C}$  form the four vertices of a square, with diagonals along the real and imaginary axes. In this picture,  $\sigma$  is just the rotation anticlockwise by  $\pi/2$  and  $\tau$  is reflection in the real axis.



We again calculate the lattices of subgroups and intermediate fields. Again, all inclusions of subgroups have index 2.



Most of these fixed fields are easy to find. For example, it is clear that  $L^{\langle \sigma \rangle} = \mathbb{Q}(i)$  since one inclusion is obvious and  $|\langle \sigma \rangle| = 4 = [L : \mathbb{Q}(i)]$ . Similarly,  $L^{\langle \tau \rangle} = \mathbb{Q}(\alpha)$ . Using that  $\sigma \langle \tau \rangle \sigma^{-1} = \langle \sigma \tau \sigma^{-1} \rangle = \langle \sigma^2 \tau \rangle$ , we see that

$$L^{\langle \sigma^2 \tau \rangle} = \mathbb{Q}(\sigma(\alpha)) = \mathbb{Q}(i\alpha).$$

Next,  $\mathbb{Q}(\alpha) \cap \mathbb{Q}(i\alpha) = \mathbb{Q}(\alpha^2)$ . Again, one inclusion is obvious and we have the correct degrees. Thus this is the intermediate field belonging to  $\langle \tau, \sigma^2 \tau \rangle = \langle \sigma^2, \tau \rangle$ . It now follows that the subfield belonging to  $\langle \sigma^2 \rangle$  must equal  $\mathbb{Q}(\alpha^2, i)$ .

It remains to calculate the intermediate fields  $E, F$  and  $G$ .

The subfield  $G$  is of degree 2 over  $\mathbb{Q}$ , and after a little thought, we see that this must be  $\mathbb{Q}(i\alpha^2) = \mathbb{Q}(i\sqrt{2})$ . This has degree two over  $\mathbb{Q}$ , and is quickly checked to be fixed by  $G$ .

Consider  $\sigma\tau$ . Viewing the four roots  $i^r \alpha$  of  $f$  as the points of a square in  $\mathbb{C}$ , we observe that  $\sigma\tau$  fixes the midpoint of the side connecting  $\alpha$  with  $i\alpha$ . Thus  $\sigma\tau$  fixes the point  $\alpha(1+i)$ . This is quickly checked:

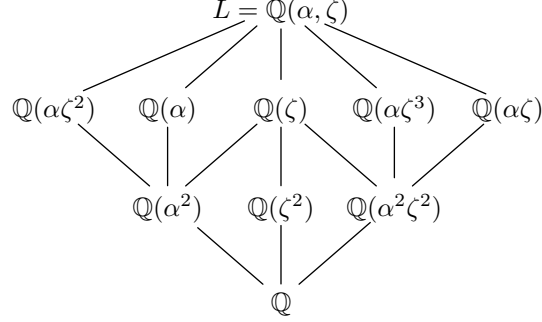
$$\sigma\tau(\alpha) = \sigma(\alpha) = i\alpha, \quad \sigma\tau(i\alpha) = \sigma(-i\alpha) = -i\sigma(\alpha) = \alpha.$$

Thus  $E = L^{\langle \sigma\tau \rangle}$  contains  $\mathbb{Q}(\alpha(1+i))$ . They are equal since they both have degree 4 over  $\mathbb{Q}$  ( $\alpha(1+i)$  has the four distinct conjugates  $\pm\alpha(1+i), \pm\alpha(1-i)$ ). It follows that  $F = \sigma(E) = \mathbb{Q}(\alpha(-1+i))$ .

We now seem to have lost some symmetry in our diagram of intermediate fields. We can reclaim this by applying some more thought to the fields  $E$  and  $F$ . We begin by noting that the primitive 8-th root of unity  $\zeta := \exp(2\pi i/8)$  can be written as  $\zeta = \frac{1}{\sqrt{2}}(1+i) = (1+i)/\alpha^2$ . Thus  $L = \mathbb{Q}(\alpha, \zeta)$ . Furthermore,  $\zeta^2 = i$  and  $\alpha^2 = \zeta + \zeta^{-1}$ , so  $\mathbb{Q}(\alpha^2, i) = \mathbb{Q}(\zeta)$ . Also,  $E$  is generated by  $\alpha(1+i) = \alpha^3\zeta$ , hence also by  $(\alpha^3\zeta)^3 = 4\alpha\zeta^3$ . Thus  $E = \mathbb{Q}(\alpha\zeta^3)$ , and similarly  $F = \mathbb{Q}(\alpha\zeta)$ . Observe that

$$\begin{aligned} \sigma(\zeta) &= \sigma(1+i)/\sigma(\alpha)^2 = -(1+i)/\alpha^2 = -\zeta = \zeta^5 \\ \tau(\zeta) &= (1-i)/\alpha^2 = -\zeta^3 = \zeta^7. \end{aligned}$$

We can therefore rewrite the lattice of intermediate fields as



The proper normal subgroups of  $D_8$  are

$$\langle \sigma^2, \tau \rangle, \quad \langle \sigma \rangle, \quad \langle \sigma^2, \sigma\tau \rangle, \quad \langle \sigma \rangle.$$

The corresponding fixed fields are normal over  $\mathbb{Q}$

$$\mathbb{Q}(\alpha^2), \quad \mathbb{Q}(i), \quad \mathbb{Q}(i\alpha^2), \quad \mathbb{Q}(\zeta).$$

These are the splitting field extensions of the irreducible polynomials

$$X^2 - 2, \quad X^2 + 1, \quad X^2 + 2, \quad X^4 + 1.$$

## 8.4 Example 4.

Let  $\alpha = \sqrt{(2 + \sqrt{2})(3 + \sqrt{3})}$ . We shall show that  $L = \mathbb{Q}(\alpha)$  is Galois over  $\mathbb{Q}$  and has Galois group  $Q_8$ , the quaternion group.

Observe that  $\alpha^2 = (2 + \sqrt{2})(3 + \sqrt{3}) = 6 + 3\sqrt{2} + 2\sqrt{3} + \sqrt{6}$ . Thus  $\mathbb{Q}(\alpha^2) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , which is Galois over  $\mathbb{Q}$  with Galois group  $V$ . Let  $\bar{\sigma}, \bar{\tau} \in V$  be such that

$$\begin{array}{ll}
 \bar{\sigma}(\sqrt{2}) = -\sqrt{2} & \bar{\tau}(\sqrt{2}) = \sqrt{2} \\
 \bar{\sigma}(\sqrt{3}) = \sqrt{3} & \bar{\tau}(\sqrt{3}) = -\sqrt{3}.
 \end{array}$$

Thus  $V = \{1, \bar{\sigma}, \bar{\tau}, \bar{\sigma}\bar{\tau}\}$ . Consider the four conjugates of  $\alpha^2$ , namely

$$\begin{array}{ll}
 6 + 3\sqrt{2} + 2\sqrt{3} + \sqrt{6}, & 6 - 3\sqrt{2} + 2\sqrt{3} - \sqrt{6} \\
 6 + 3\sqrt{2} - 2\sqrt{3} - \sqrt{6}, & 6 - 3\sqrt{2} - 2\sqrt{3} + \sqrt{6}.
 \end{array}$$

Since  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$  is a  $\mathbb{Q}$ -basis for  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ , we observe that these four elements are all distinct. Thus  $\alpha^2$  is a primitive element for  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . In particular,  $\mathbb{Q}(\alpha^2)/\mathbb{Q}$  is Galois with Galois group  $V$ .

Clearly  $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] \leq 2$ , so to prove equality, we must show that  $\alpha \notin \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Suppose for a contradiction that  $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$  and

consider  $\alpha\bar{\tau}(\alpha)$ . This must lie in the fixed field of  $\langle\bar{\tau}\rangle$ , namely  $\mathbb{Q}(\sqrt{2})$ . On the other hand

$$(\alpha\bar{\tau}(\alpha))^2 = \alpha^2\bar{\tau}(\alpha^2) = (2 + \sqrt{2})(3 + \sqrt{3}) \cdot (2 + \sqrt{2})(3 - \sqrt{3}) = 6(2 + \sqrt{2})^2.$$

Thus

$$6 = \left(\frac{\alpha\bar{\tau}(\alpha)}{2 + \sqrt{2}}\right)^2, \quad \text{so that} \quad \sqrt{6} = \pm \frac{\alpha\bar{\tau}(\alpha)}{2 + \sqrt{2}} \in \mathbb{Q}(\sqrt{2}).$$

This yields the required contradiction. Hence  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$ .

We next show that  $\mathbb{Q}(\alpha)/\mathbb{Q}$  is normal. The minimal polynomial of  $\alpha$  over  $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  is simply  $X^2 - (2 + \sqrt{2})(3 + \sqrt{3})$ . The eight  $\mathbb{Q}$ -embeddings  $\mathbb{Q}(\alpha) \rightarrow \mathbb{C}$  are found by extending each of the four  $\mathbb{Q}$ -embeddings  $\mathbb{Q}(\alpha^2) \rightarrow \mathbb{C}$  as in Artin's Extension Theorem. For example, we can extend the identity to  $\alpha \mapsto \pm\alpha$ . Similarly,

$$\bar{\sigma}(X^2 - (2 + \sqrt{2})(3 + \sqrt{3})) = X^2 - (2 - \sqrt{2})(3 - \sqrt{3}).$$

Thus we can extend  $\bar{\sigma}$  to  $\alpha \mapsto \pm\sqrt{(2 - \sqrt{2})(3 + \sqrt{3})}$ . We deduce that the eight conjugates of  $\alpha$  in  $\mathbb{C}$  are

$$\pm\sqrt{(2 \pm \sqrt{2})(3 \pm \sqrt{3})},$$

where we can choose the signs independently of one another. Moreover, we can now find the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ , since this is the polynomial of degree eight having precisely these roots. We calculate

$$m := m_{\alpha/\mathbb{Q}} = X^8 - 24X^6 + 144X^4 - 288X^2 + 144.$$

Now,

$$\frac{\sqrt{2 + \sqrt{2}}}{2 + \sqrt{2}} = \frac{1}{\sqrt{2 + \sqrt{2}}} = \frac{\sqrt{2 - \sqrt{2}}}{\sqrt{(2 + \sqrt{2})(2 - \sqrt{2})}} = \frac{\sqrt{2 - \sqrt{2}}}{\sqrt{2}}.$$

Similarly

$$\frac{\sqrt{3 + \sqrt{3}}}{3 + \sqrt{3}} = \frac{\sqrt{3 - \sqrt{3}}}{\sqrt{6}}.$$

Since  $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , we see that  $\sqrt{2}, \sqrt{3}, \sqrt{6} \in \mathbb{Q}(\alpha)$ . Therefore

$$\begin{aligned} \sqrt{(2 - \sqrt{2})(3 + \sqrt{3})} &= \frac{\alpha\sqrt{2}}{2 + \sqrt{2}} = \frac{\alpha}{1 + \sqrt{2}} \\ \sqrt{(2 + \sqrt{2})(3 - \sqrt{3})} &= \frac{\alpha\sqrt{6}}{3 + \sqrt{3}} = \frac{\alpha\sqrt{2}}{1 + \sqrt{3}} \\ \sqrt{(2 - \sqrt{2})(3 - \sqrt{3})} &= \frac{\alpha\sqrt{2}}{(1 + \sqrt{2})(1 + \sqrt{3})} = \frac{2\sqrt{3}}{\alpha} \end{aligned}$$

and so each of the eight conjugates of  $\alpha$  again lies in  $\mathbb{Q}(\alpha)$ . Thus  $\mathbb{Q}(\alpha)/\mathbb{Q}$  is the splitting field extension of  $m$ , so is normal.

We have already calculated the eight elements of the Galois group. We now show that this is isomorphic to the quaternion group  $Q_8$ . Define  $\sigma$  and  $\tau$  to be the following extensions of  $\bar{\sigma}$  and  $\bar{\tau}$  respectively:

$$\begin{aligned}\sigma(\alpha) &:= \sqrt{(2 - \sqrt{2})(3 + \sqrt{3})} = \frac{\alpha}{1 + \sqrt{2}} \\ \tau(\alpha) &:= \sqrt{(2 + \sqrt{2})(3 - \sqrt{3})} = \frac{\alpha\sqrt{2}}{1 + \sqrt{3}}.\end{aligned}$$

Then

$$\begin{aligned}\sigma^2(\alpha) &= \frac{\sigma(\alpha)}{\sigma(1 + \sqrt{2})} = \frac{\alpha/(1 + \sqrt{2})}{1 - \sqrt{2}} = -\alpha \\ \tau^2(\alpha) &= \frac{\tau(\alpha\sqrt{2})}{\tau(1 + \sqrt{3})} = \frac{2\alpha/(1 + \sqrt{3})}{1 - \sqrt{3}} = -\alpha.\end{aligned}$$

Hence  $\sigma^2 = \tau^2$  and  $\sigma^4 = 1$ . Also

$$\begin{aligned}\tau\sigma(\alpha) &= \frac{\tau(\alpha)}{\tau(1 + \sqrt{2})} = \frac{\alpha\sqrt{2}/(1 + \sqrt{3})}{1 + \sqrt{2}} = \frac{\alpha\sqrt{2}}{(1 + \sqrt{2})(1 + \sqrt{3})} \\ \sigma\tau(\alpha) &= \frac{\sigma(\alpha\sqrt{2})}{\sigma(1 + \sqrt{3})} = \frac{-\alpha\sqrt{2}/(1 + \sqrt{2})}{1 + \sqrt{3}} = \frac{-\alpha\sqrt{2}}{(1 + \sqrt{2})(1 + \sqrt{3})}.\end{aligned}$$

Thus  $\tau\sigma = \sigma^3\tau$ . It follows from the discussion below that  $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong Q_8$ .

We recall that the quaternions are given as

$$\mathbb{H} := \{a + bi + cj + dk : i^2 = j^2 = k^2 = ijk = -1, \quad a, b, c, d \in \mathbb{Q}\}.$$

Note that  $ij = -ijk^2 = k$ . Similarly  $jk = i$  and  $ki = j$ . On the other hand,  $ji = j^2k = -k$ , so that  $ij \neq ji$ . Thus  $\mathbb{H}$  is a non-commutative ring. (Discovered by Hamilton. See webpages...)

The quaternion group  $Q_8$  is given as the multiplicative subgroup

$$Q_8 := \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}.$$

It has the following presentation:

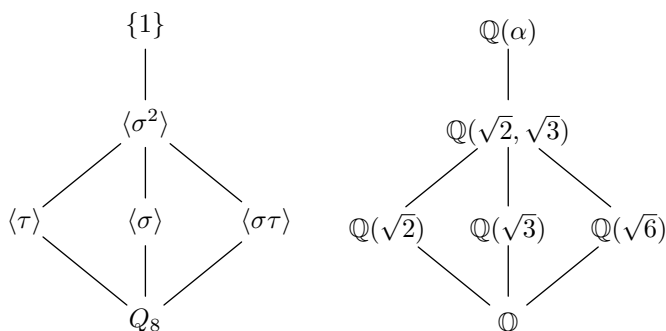
$$Q_8 = \langle \sigma, \tau : \sigma^2 = \tau^2, \sigma^4 = 1, \tau\sigma = \sigma^3\tau \rangle.$$

The subgroup  $Z = \langle \sigma^2 \rangle$  is central, so normal, and the quotient group  $Q_8/Z$  is isomorphic to the Klein four-group  $V \cong (\mathbb{Z}/2\mathbb{Z})^2$ .

Using this, we see that the subgroups of  $Q_8$  containing  $Z$  are in bijection with the subgroups of  $V$ . This yields the subgroups  $\langle \sigma \rangle$ ,  $\langle \tau \rangle$  and  $\langle \sigma\tau \rangle$ , each of which is isomorphic to  $\mathbb{Z}/4\mathbb{Z}$ . It is now clear that these, together with  $Z$ , are the only

proper subgroups of  $Q_8$ . [Let  $G \leq Q_8$  be a proper subgroup and take  $1 \neq g \in G$ . Then either  $g^2 = \sigma^2$ , or  $g^2 = 1$ , in which case  $g = \sigma^2$ . Hence  $\sigma^2 \in G$  and  $G$  must be one of the subgroups in our list.]

We now draw the lattices of subgroups and intermediate fields. Again, all indices equal 2, so are omitted.



Since  $\sigma^2(\alpha) = -\alpha$ , we have  $\sigma^2(\alpha^2) = \alpha^2$ . Thus the field belonging to  $\langle \sigma^2 \rangle$  is just  $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . The rest follows immediately, using the identification of the Galois group of  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  over  $\mathbb{Q}$  with the quotient group  $Q_8/\langle \sigma^2 \rangle$ .

All subgroups are normal, so all intermediate fields are normal over  $\mathbb{Q}$ .

## 8.5 Example 5.

Consider the polynomial  $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$ , irreducible by Eisenstein's Criterion. Now,  $f$  has at least three real roots, since  $f(-2) = -22 < 0$ ,  $f(0) = 2 > 0$ ,  $f(1) = -1 < 0$  and  $f(2) = 26 > 0$ . On the other hand, it has at most three real roots since  $f' = 5X^4 - 4$ , so  $f$  has only two turning points. Thus  $f$  has precisely three real roots, and so two complex roots, which must form a conjugate pair. Hence  $\text{Gal}(f)$  is a transitive subgroup of  $\text{Sym}_5$  and contains a transposition, corresponding to complex conjugation. Hence  $\text{Gal}(f) = \text{Sym}_5$  by Lemma 7.14.

In fact, for all  $n$ , there exists an irreducible polynomial  $f \in \mathbb{Q}[X]$  of degree  $n$  such that  $\text{Gal}(f) \cong \text{Sym}_n$ . On the other hand, since each finite group  $G$  of order  $n$  is isomorphic to a subgroup of  $\text{Sym}_n$ , there exists a Galois extension  $L/\mathbb{Q}$  and an intermediate field  $K$  such that  $\text{Gal}(L/K) \cong G$ . It is an open problem whether we can take  $K = \mathbb{Q}$ .

This leads to the Inverse Galois Problem: Given a field  $K$ , which finite groups can be realised as  $\text{Gal}(L/K)$  for some Galois extension  $L/K$ ?

1. Every finite group is realisable over  $\mathbb{C}(x)$ , the function field in one variable over  $\mathbb{C}$ .
2. All symmetric groups and alternating groups are realisable over  $\mathbb{Q}$ .

3. Every cyclic group is realisable over  $\mathbb{Q}$ . More generally, every solvable group is realisable over  $\mathbb{Q}$ .
4. All but possibly one of the 26 sporadic finite simple groups is realisable over  $\mathbb{Q}$ . In particular, the Monster group is realisable over  $\mathbb{Q}$ .

## Chapter 9

# Radical Extensions

We now come back to our motivating question of whether we can express the roots of an irreducible polynomial as radical expressions in the coefficients of the polynomial. We shall begin by studying two special cases — cyclotomic extensions, given by adjoining a primitive  $n$ -th root of unity, and cyclic extensions, given by adjoining an arbitrary  $n$ -th under the assumption that the base field already contains a primitive  $n$ -th root of unity. Both of these cases are relatively easy to study, and have far reaching generalisations to abelian Kummer theory and class field theory.

We then come back to an arbitrary base field (of characteristic zero), and show that a Galois extension is contained in a radical extension if and only if its Galois group is a soluble group. The main difficulty in the proof is that the base field does not contain enough roots of unity. We therefore have to adjoin these in order to make our deductions.

In this chapter, all fields will be of characteristic zero unless explicitly stated otherwise.

### 9.1 Cyclotomic Extensions

Recall that  $\zeta \in K$  is called a **primitive  $n$ -th root of unity** if  $\zeta^n = 1$  but  $\zeta^d \neq 1$  for all  $1 \leq d < n$ . For example, we could take  $\zeta = \exp(2\pi i/n) \in \mathbb{C}$ . Recall also Euler's phi function

$$\phi(n) = |\{1 \leq r \leq n : \gcd(r, n) = 1\}|.$$

Let  $\zeta \in K$  be a primitive  $n$ -th root of unity. We make the following observations.

1. The  $n$  numbers  $\zeta^r$  for  $1 \leq r \leq n$  are all distinct. For, if  $\zeta^r = \zeta^s$  with  $1 \leq r < s \leq n$ , then  $\zeta^{s-r} = 1$  and  $1 \leq s - r < n$ , contradicting the fact that  $\zeta$  was a primitive  $n$ -th root of unity.

2. The set  $\mu_n := \{\zeta^r : 1 \leq r \leq n\}$  is a group under multiplication, isomorphic to the additive group  $\mathbb{Z}/n\mathbb{Z}$ . For, it is cyclic, generated by  $\zeta$ , and has order  $n$ .
3. If  $1 \leq r \leq n$ , then  $\zeta^r$  is a primitive  $n/d$ -th root of unity, where  $d = \gcd(r, n)$ . For, the same holds in  $\mathbb{Z}/n\mathbb{Z}$ .
4.  $\mu_n$  contains  $\mu_d$  for all  $d|n$ . In particular, if  $\xi$  is an  $n/d$ -th root of unity, then  $\xi = \zeta^{ds}$  for some  $1 \leq s \leq n/d$ .

We define the  $n$ -th **cyclotomic polynomial** as

$$\Phi_n(X) := \prod_{\substack{1 \leq r \leq n \\ \gcd(r, n) = 1}} (X - \zeta^r) = \prod_{\substack{\xi \text{ primitive } n\text{-th} \\ \text{root of unity}}} (X - \xi).$$

We therefore have the factorisation

$$X^n - 1 = \prod_{1 \leq r \leq n} (X - \zeta^r) = \prod_{d|n} \Phi_d(X).$$

**Theorem 9.1.**  $\Phi_n(X) \in \mathbb{Z}[X]$  is irreducible of degree  $\phi(n)$ .

If  $\zeta \in \mathbb{C}$  is a primitive  $n$ -th root of unity, then  $\mathbb{Q}(\zeta)/\mathbb{Q}$  is Galois with Galois group isomorphic to  $(\mathbb{Z}/n\mathbb{Z})^\times$ , where  $\sigma_r(\zeta) := \zeta^r$  for  $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ . In particular, it is abelian.

*Proof.* We recall from Gauss' Lemma that if  $f, g \in \mathbb{Q}[X]$  are monic and  $fg \in \mathbb{Z}[X]$ , then both  $f, g \in \mathbb{Z}[X]$ .

Clearly  $\Phi_n(X)$  is monic for all  $n$  and  $\Phi_1(X) = X - 1$ . By induction, each  $\Phi_d(X)$  with  $d < n$  has integer coefficients. Since  $\Phi_n(X) = (X^n - 1) / \prod_{d|n, d < n} \Phi_d(X)$ , it has rational coefficients. Hence  $\Phi_n(X) \in \mathbb{Z}[X]$  by Gauss' Lemma.

Now let  $f \in \mathbb{Q}[X]$  be the minimal polynomial of  $\zeta$ , a primitive  $n$ -th root of unity. We claim that if  $\xi$  is any root of  $f$ , then so is  $\xi^p$  for all primes  $p \nmid n$ . It will follow that  $\zeta^r$  is a root of  $f$  for all  $1 \leq r \leq n$  with  $\gcd(r, n) = 1$ . Hence  $\Phi_n(X) = f$  is irreducible.

Since  $\zeta$  is a root of  $X^n - 1$ , we can write  $X^n - 1 = f(X)g(X)$ . Then  $g = (X^n - 1)/f$  is monic with rational coefficients. By Gauss' Lemma,  $f, g \in \mathbb{Z}[X]$ . Let  $\xi$  be a root of  $f$ ,  $p$  a prime not dividing  $n$  and assume for contradiction that  $\xi^p$  is not a root of  $f$ . Then  $\xi^p$  must be a root of  $g(X)$ , so that  $\xi$  is a root of  $g(X^p)$ . Since  $f$  is the minimal polynomial of  $\xi$ , it divides  $g(X^p)$ . Hence  $g(X^p) = f(X)h(X)$ . By Gauss' Lemma,  $h \in \mathbb{Z}[X]$  and is monic.

Now reduce coefficients modulo  $p$ . Denote by  $\bar{f}, \bar{g}$  and  $\bar{h}$  the images of  $f, g$  and  $h$  in  $\mathbb{F}_p[X]$ . By Lemma 6.3,  $\bar{g}(X)^p = \bar{g}(X^p) = \bar{f}(X)\bar{h}(X)$ . Thus  $\gcd(\bar{f}, \bar{g}) \neq 1$ . Since  $X^n - 1 = \bar{f}(X)\bar{g}(X)$ , we see that  $X^n - 1$  has repeated roots. It follows that  $X^n - 1$  and its derivative  $nX^{n-1}$  have a common divisor which, since  $p \nmid n$ , clearly cannot happen. This proves the claim.

We have shown that  $\Phi_n(X)$  is the minimal polynomial of  $\zeta$  over  $\mathbb{Q}$ . Thus  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_n) = \phi(n)$ . Since all  $n$ -th roots of unity (primitive or not) are powers of  $\zeta$ , we see that  $\mathbb{Q}(\zeta)/\mathbb{Q}$  is the splitting field extension of  $\Phi_n$  (or equivalently of  $X^n - 1$ ). Hence  $\mathbb{Q}(\zeta)/\mathbb{Q}$  is Galois.

Let  $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ . Then  $|G| = \phi(n)$ . Let  $\sigma \in G$ . Since  $\zeta$  is a primitive element for  $\mathbb{Q}(\zeta)/\mathbb{Q}$ ,  $\sigma$  is completely determined by  $\sigma(\zeta)$ . Thus by Artin's Extension Theorem, the elements of  $G$  correspond to the roots of  $\Phi_n$ , so

$$G = \{\sigma_r : 1 \leq r \leq n, \gcd(r, n) = 1\}, \quad \sigma_r(\zeta) = \zeta^r.$$

Consider the bijection  $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow G, r \mapsto \sigma_r$ . Since  $1 \mapsto \sigma_1 = \text{id}$  and  $\sigma_r \sigma_s(\zeta) = \sigma_r(\zeta)^s = \zeta^{rs}$ , this map is a group isomorphism.  $\square$

**Corollary 9.2.** *Let  $L/K$  be a finite field extension and let  $\zeta \in L$  be a primitive  $n$ -th root of unity. Then  $K(\zeta)/K$  is Galois and  $\text{Gal}(K(\zeta)/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ .*

*Proof.* Since  $K$  is of characteristic zero, it contains  $\mathbb{Q}$ . Thus  $K(\zeta)$  is the compositum of  $\mathbb{Q}(\zeta)$  and  $K$ . By Theorem 7.6,  $K(\zeta)/K$  is Galois with  $\text{Gal}(K(\zeta)/K)$  isomorphic to a subgroup of  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ .  $\square$

## 9.2 Cyclic Extensions

We now study the equation  $X^n - a \in K[X]$  under the assumption that  $K$  contains a primitive  $n$ -th root of unity. We will show that  $L/K$  is Galois with cyclic Galois group of order dividing  $n$  if and only if  $L/K$  is the splitting field of some  $X^n - a \in K[X]$ .

**Theorem 9.3** (Hilbert's Theorem 90). *Let  $L/K$  be Galois with Galois group  $\text{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$ . Let  $\sigma$  be a generator for  $\text{Gal}(L/K)$ . Then for  $\beta \in L$  we have  $N_K^L(\beta) = 1$  if and only if there exists  $\alpha \in L$  such that  $\beta = \sigma(\alpha)/\alpha$ .*

*Proof.* Suppose that  $\beta = \sigma(\alpha)/\alpha$ . Then since  $\sigma^n = \text{id}$  we have by Proposition 7.18 that

$$N_K^L(\beta) = \beta \sigma(\beta) \cdots \sigma^{n-1}(\beta) = \frac{\sigma(\alpha)}{\alpha} \frac{\sigma^2(\alpha)}{\sigma(\alpha)} \cdots \frac{\sigma^n(\alpha)}{\sigma^{n-1}(\alpha)} = \frac{\sigma^n(\alpha)}{\alpha} = 1.$$

This proves one direction. Note also that  $\sigma(\alpha) = \alpha\beta$ , so by induction

$$\sigma^i(\alpha) = \alpha(\beta\sigma(\beta) \cdots \sigma^{i-1}(\beta)).$$

Using that  $N_K^L(\beta) = 1$ , set

$$\lambda_i := \sigma^i(\beta) \cdots \sigma^{n-1}(\beta) = \frac{1}{\beta\sigma(\beta) \cdots \sigma^{i-1}(\beta)},$$

so that  $\lambda_0 = N_K^L(\beta) = 1$ ,  $\lambda_1 = \beta^{-1}$ ,  $\lambda_n = N_K^L(\beta)^{-1} = 1$  and  $\lambda_i \sigma^i(\alpha) = \alpha$ . Thus

$$\sum_{i=0}^{n-1} \lambda_i \sigma^i(\alpha) = n\alpha \neq 0.$$

Now, to prove the converse, suppose that  $N_K^L(\beta) = 1$ . As above, define  $\lambda_i := \sigma^i(\beta) \cdots \sigma^{n-1}(\beta)$ . By Theorem 4.6, the  $\sigma^i$  for  $0 \leq i < n$  are linearly independent over  $L$ . Hence there exists  $\gamma \in L$  such that

$$\alpha := \sum_{i=0}^{n-1} \lambda_i \sigma^i(\gamma) \neq 0.$$

Since  $\sigma(\lambda_i) = \lambda_{i+1} \sigma^n(\beta) = \beta \lambda_{i+1}$  and  $\lambda_n \sigma^n(\gamma) = \gamma = \lambda_0 \gamma$ , we have

$$\sigma(\alpha) = \sum_{i=0}^{n-1} \sigma(\lambda_i) \sigma^{i+1}(\gamma) = \beta \sum_{i=0}^{n-1} \lambda_{i+1} \sigma^{i+1}(\gamma) = \alpha \beta.$$

Therefore  $\beta = \sigma(\alpha)/\alpha$  as required.  $\square$

As an application, let  $d \in \mathbb{Q}$  be a non-square. Then  $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$  is a Galois extension with Galois group  $\mathbb{Z}/2\mathbb{Z}$ , generated by  $\sigma(a - b\sqrt{d}) = a + b\sqrt{d}$ . The norm of an element  $\beta = x + y\sqrt{d}$  is

$$N(\beta) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

Thus, the solutions of  $x^2 - dy^2 = 1$  are all of the form

$$x + y\sqrt{d} = \frac{a + b\sqrt{d}}{a - b\sqrt{d}} = \frac{(a + b\sqrt{d})^2}{a^2 - db^2} = \frac{a^2 + db^2}{a^2 - db^2} + \frac{2ab}{a^2 - db^2} \sqrt{d}.$$

If  $d$  is a positive integer, we obtain all solutions to Pell's Equation

$$x^2 - dy^2 = 1 \quad \Leftrightarrow \quad (x, y) = \left( \frac{a^2 + db^2}{a^2 - db^2}, \frac{2ab}{a^2 - db^2} \right) \quad \text{for } a, b \in \mathbb{Q}.$$

We immediately see that if  $(a, b)$  is a solution, then so is  $(a^2 + db^2, 2ab)$ .

Note that this gives rational solutions, not integral solutions. For that, the best method is to use convergents to the continued fraction expression for  $\sqrt{d}$ . By Dirichlet's Theorem, if  $\epsilon$  is the first such solution, then all other solutions are of the form  $\pm \epsilon^n$  for  $n \in \mathbb{Z}$ .

On the other hand, if  $d = -1$ , then  $\mathbb{Q}(i)$  is the field of Gaussian numbers and

$$x^2 + y^2 = 1 \quad \Leftrightarrow \quad (x, y) = \left( \frac{a^2 - b^2}{a^2 + b^2}, \frac{2ab}{a^2 + b^2} \right) \quad \text{for } a, b \in \mathbb{Q}.$$

Hence all Pythagorean triples can be written in the form

$$x^2 + y^2 = z^2 \quad \Leftrightarrow \quad (x, y, z) = \frac{1}{c} (a^2 - b^2, 2ab, a^2 + b^2) \quad \text{for } a, b, c \in \mathbb{Q}.$$

With a little extra work, one obtains that all integer solutions can be written in the form

$$x^2 + y^2 = z^2 \iff (x, y, z) = (a^2 - b^2, 2ab, a^2 + b^2) \text{ for } a, b \in \mathbb{Z}.$$

**Theorem 9.4.** *Let  $K$  contain a primitive  $n$ -th root of unity  $\zeta$ .*

1. *If  $L/K$  is Galois with  $\text{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$ , then  $L/K$  is the splitting field extension of some  $X^n - a \in K[X]$ .*
2. *Conversely, let  $f = X^n - a \in K[X]$ , let  $L/K$  be its splitting field extension and let  $\alpha \in L$  be a root of  $f$ . Then  $L = K(\alpha)$  and has cyclic Galois group of order  $d := [K(\alpha) : K]$ . Moreover,  $d$  divides  $n$  and  $\alpha^d \in K$ .*

*Proof.* (1) Let  $\sigma$  be a generator for  $\text{Gal}(L/K)$ . Clearly  $N(\zeta) = \zeta^n = 1$ , so by Hilbert's Theorem 90, there exists  $\alpha \in L$  such that  $\sigma(\alpha) = \alpha\zeta$ , whence  $\sigma^i(\alpha) = \alpha\zeta^i$  for all  $i$ . These elements are all distinct, so  $\alpha$  has precisely  $n$  conjugates. Hence  $\alpha$  is a primitive element for  $L/K$  and  $L/K$  is the splitting field extension of  $m_{\alpha/K}$ . Finally, by Proposition 7.18, we have

$$\begin{aligned} m_{\alpha/K} &= (X - \alpha)(X - \sigma(\alpha)) \cdots (X - \sigma^{n-1}(\alpha)) \\ &= (X - \alpha)(X - \alpha\zeta) \cdots (X - \alpha\zeta^{n-1}) \\ &= \alpha^n ((X/\alpha) - 1)((X/\alpha) - \zeta) \cdots ((X/\alpha) - \zeta^{n-1}) \\ &= \alpha^n ((X/\alpha)^n - 1) = X^n - \alpha^n. \end{aligned}$$

(2) Since  $\alpha \in L$  is a root of  $f$ , so is  $\alpha\zeta^i$  for each  $i$ . Hence all roots of  $f$  lie in  $K(\alpha)$ , so  $L = K(\alpha)$ . Let  $d = [K(\alpha) : K]$  and let  $G = \text{Gal}(K(\alpha)/K)$ . Let  $\sigma \in G$ . Then  $\sigma(\alpha)$  is again a root of  $f$ , so  $\sigma(\alpha) = \alpha\zeta^i$  for some  $i$ . If  $\tau(\alpha) = \alpha\zeta^j$ , then  $\sigma\tau(\alpha) = \sigma(\alpha\zeta^j) = \alpha\zeta^{i+j}$ . This determines an injective group homomorphism  $G \rightarrow \mathbb{Z}/n\mathbb{Z}$ , where  $\sigma \mapsto i$  such that  $\sigma(\alpha) = \alpha\zeta^i$ . Thus  $G$  is isomorphic to a subgroup of a cyclic group, so is itself cyclic. Since  $|G| = d$ , we have  $G \cong \mathbb{Z}/d\mathbb{Z}$ , and that  $d = |G|$  divides  $n = |\mathbb{Z}/n\mathbb{Z}|$ . Thus  $G$  is generated by  $\sigma$  where  $\sigma(\alpha) = \alpha\zeta^{n/d}$ . Note that  $\zeta^{n/d}$  is a primitive  $d$ -th root of unity. As in the proof of (1) for  $d$  instead of  $n$ , we see that the minimal polynomial of  $\alpha$  over  $K$  is  $X^d - \alpha^d \in K[X]$ .  $\square$

### 9.3 Radical Extensions

A field extension  $L/K$  is called **radical** if there exists a tower  $L = K_n/\cdots/K_0 = K$  such that each  $K_i = K_{i-1}(\alpha_i)$  is simple and with  $\alpha_i^{r_i} \in K_{i-1}$  for some positive integer  $r_i$ . We call such a tower a **radical tower** for  $L/K$ . Note that all radical extensions are necessarily finite.

Let  $L = K_n/\cdots/K_0 = K$  be a radical tower for  $L/K$ , where  $K_i = K_{i-1}(\alpha_i)$  with  $\alpha_i^{r_i} \in K_{i-1}$ . Let  $r = \text{lcm}(r_1, \dots, r_n)$ . Then  $\alpha_i^r \in K_{i-1}$  for all  $i$ , so we may assume that at each stage we have adjoined an  $r$ -th root for some common  $r$ .

We shall call such an  $r$  an **exponent** of the radical extension  $L/K$ . (N.B. This is non-standard terminology, but useful.) If  $L/K$  is radical of exponent  $r$ , then it is also radical of exponent  $t$  for all multiples  $t$  of  $r$ .

**Theorem 9.5.** 1. Let  $L/K/k$  be field extensions. If both  $L/K$  and  $K/k$  are radical (of exponents  $r$  and  $s$ ), then  $L/k$  is radical (of exponent  $\text{lcm}(r, s)$ ).

2. Let  $L/K$  be a field extension and  $E, F$  two intermediate fields. Then  $E/K$  radical (of exponent  $r$ ) implies  $EF/F$  radical (of exponent  $r$ ). In particular, if  $L/K/k$  are field extensions, then  $L/k$  radical implies  $L/K$  radical.

*Proof.* (1) Let  $L/K$  and  $K/k$  be radical of exponents  $r$  and  $s$ . Then they are both radical of exponent  $t := \text{lcm}(r, s)$ . Let  $L = K_m/\cdots/K_0 = K$  and  $K = k_n/\cdots/k_0 = k$  be radical towers of exponent  $t$ . Juxtaposing these yields a radical tower for  $L/k$  of exponent  $t$ .

(2) Let  $E = K_n/\cdots/K_0 = K$  be a radical tower of exponent  $r$ . Define  $F_i := FK_i$  to be the compositum. We have  $K_i = K_{i-1}(\alpha_i)$  for some  $\alpha_i$  with  $\alpha_i^r \in K_{i-1}$ . Therefore

$$F_i = FK_i = FK_{i-1}(\alpha_i) = F_{i-1}(\alpha_i) \quad \text{and} \quad \alpha_i^r \in K_{i-1} \subset F_{i-1}.$$

Since  $F_n = EF$  and  $F_0 = F$  we have that  $EF = F_n/\cdots/F_0 = F$  is a radical tower of exponent  $r$ .

For the second part we have  $L/k$  is radical, so  $L = LK$  is radical over  $K$ .  $\square$

### Warning

If  $L/k$  is radical and  $K$  an intermediate field, then  $K/k$  is not in general radical. However, for most of the time it is usually sufficient to ask that, given  $K/k$ , there exists  $L/K$  such that  $L/k$  is radical.

**Theorem 9.6.** Let  $L/K$  be finite, with normal closure  $M/L$ . Then  $L/K$  radical implies  $M/K$  radical.

*Proof.* Let  $\sigma_1, \dots, \sigma_m$  be the distinct  $K$ -embeddings  $L \rightarrow M$ . Then  $M$  equals the compositum  $\sigma_1(L)\cdots\sigma_m(L)$ . Moreover, if  $L = K_n/\cdots/K_0 = K$  is a radical tower of exponent  $r$ , then so too is  $\sigma_j(L) = \sigma_j(K_n)/\cdots/\sigma_j(K_0) = K$ . For, writing  $K_i = K_{i-1}(\alpha_i)$  with  $\alpha_i^r \in K_{i-1}$ , then  $\sigma_j(K_i) = \sigma_j(K_{i-1})(\sigma_j(\alpha_i))$  with  $\sigma_j(\alpha_i)^r = \sigma_j(\alpha_i^r) \in \sigma_j(K_{i-1})$ .

Using Theorem 9.5 we have that  $\sigma_1(L)\sigma_2(L)$  is radical over  $\sigma_2(L)$ , and since  $\sigma_2(L)/K$  is radical we deduce that  $\sigma_1(L)\sigma_2(L)/K$  is radical. By induction, each compositum  $\sigma_1(L)\cdots\sigma_j(L)$  is radical over  $K$ , so in particular  $M/K$  is radical.  $\square$

As motivation for the next section we make the following observations.

Let  $L/K$  be normal and radical, say with radical tower  $L = K_n/\cdots/K_0 = K$ . Note that  $L/K_i$  is Galois for all  $i$  (all extensions are separable since we are in

characteristic zero). Set  $G_i := \text{Gal}(L/K_i)$ , so that we have a chain of subgroups  $\{1\} = G_n \leq \dots \leq G_0 = \text{Gal}(L/K)$ .

**Proposition 9.7.** *Let  $L/K$  be normal and radical. Let  $L = K_n/\dots/K_0 = K$  be a radical tower of exponent  $r$  and set  $G_i := \text{Gal}(L/K_i)$ . If  $K$  contains a primitive  $r$ -th root of unity, then each  $K_i/K_{i-1}$  is Galois with cyclic Galois group, hence each  $G_i \triangleleft G_{i-1}$  is normal with cyclic quotient.*

*Proof.* By the Galois correspondence,  $K_i/K_{i-1}$  is Galois if and only if  $G_i \triangleleft G_{i-1}$  is normal, in which case  $\text{Gal}(K_i/K_{i-1}) \cong G_{i-1}/G_i$ .

Since  $L = K_n/\dots/K_0 = K$  is a radical tower of exponent  $r$ , we can write  $K_i = K_{i-1}(\alpha_i)$  for some  $\alpha_i$  with  $\alpha_i^r \in K_{i-1}$ . Since  $K$  contains a primitive  $r$ -th root of unity, so too does  $K_{i-1}$ . Thus by Theorem 9.4,  $K_i/K_{i-1}$  is Galois with cyclic Galois group (of order dividing  $r$ ).  $\square$

**Proposition 9.8** (Vandermonde-Gauss). *Let  $\zeta$  be a primitive  $n$ -th root of unity. Then  $K(\zeta)$  is contained in a radical extension of  $K$ .*

*Proof.* Since  $K(\zeta)$  is the compositum of  $K$  and  $\mathbb{Q}(\zeta)$ , it is enough to prove that  $\mathbb{Q}(\zeta)$  is contained in a radical extension of  $\mathbb{Q}$ , by Theorem 9.5. If  $n = ab$  with  $a, b$  coprime, then  $\zeta^a$  is a primitive  $b$ -th root of unity and  $\zeta^b$  is a primitive  $a$ -th root of unity. Moreover, by Euclid's Algorithm, there exist  $x, y$  such that  $ax + by = 1$ . Hence  $\zeta = (\zeta^a)^x (\zeta^b)^y$ , so that  $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^a, \zeta^b)$ . Again by Theorem 9.5, it is enough to prove that both  $\mathbb{Q}(\zeta^a)$  and  $\mathbb{Q}(\zeta^b)$  are contained in radical extensions.

This reduces to the case when  $n = p^a$  is a prime power. If  $a \geq 2$ , then  $\zeta$  is a root of  $X^p - \zeta^p$  and  $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^p)$  has degree  $\phi(p^a)/\phi(p^{a-1}) = p$  by the Tower Law. Thus  $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^p)$  is Galois with Galois group  $\mathbb{Z}/p\mathbb{Z}$ , and since  $\mathbb{Q}(\zeta^p)$  contains a primitive  $p$ -th root of unity, namely  $\zeta^{p^{a-1}}$ , we have that  $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta^p)$  is radical by Theorem 9.4. Hence by Theorem 9.5, if  $\mathbb{Q}(\zeta^p)$  is contained in a radical extension, then so is  $\mathbb{Q}(\zeta)$ .

We have therefore reduced the problem to showing that  $\mathbb{Q}(\zeta)$  is contained in a radical extension whenever  $\zeta$  is a primitive  $p$ -th root of unity for some prime  $p$ .

In this case, let  $\theta$  be a primitive  $(p-1)$ -st root of unity. Then  $\zeta\theta$  is a primitive  $p(p-1)$ -st root of unity, so that  $\mathbb{Q}(\zeta\theta)$  is a field extension of  $\mathbb{Q}(\theta)$  of degree  $\phi(p(p-1))/\phi(p-1) = \phi(p) = p-1$  by the Tower Law. It follows from Corollary 9.2 that  $\mathbb{Q}(\zeta\theta)/\mathbb{Q}(\theta)$  is Galois with Galois group  $\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ . Since  $\theta$  is a primitive  $(p-1)$ -st root of unity, we can apply Theorem 9.4 to deduce that  $\mathbb{Q}(\zeta\theta)/\mathbb{Q}(\theta)$  is a radical extension. By induction,  $\mathbb{Q}(\theta)$  is contained in a radical extension, whence  $\mathbb{Q}(\zeta\theta)$  is contained in a radical extension by Theorem 9.5, so  $\mathbb{Q}(\zeta)$  is contained in a radical extension as required.  $\square$

The point of this result is that if  $\zeta$  is a primitive  $p$ -th root of unity, we should not allow  $\zeta = \sqrt[p]{1}$  to be our radical expression: for one thing,  $\mathbb{Q}(\zeta)/\mathbb{Q}$  has degree  $\phi(p) = p-1$ , which is less than the exponent  $p$  used. This result is also more

in keeping with such expressions as

$$\begin{aligned}\exp(2\pi i/3) &= -\frac{1 + \sqrt{-3}}{2}, \\ \exp(2\pi i/4) &= \sqrt{-1}, \\ \exp(2\pi i/5) &= \frac{-1 + \sqrt{5} + \sqrt{-10 - 2\sqrt{5}}}{4}.\end{aligned}$$

The latter comes from writing

$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1 = X^2(X^2 + X + 1 + X^{-1} + X^{-2}) = X^2(u^2 + u - 1),$$

where  $u := X + X^{-1}$ , corresponding to  $2 \cos(2\pi i/5) = \exp(2\pi i/5) + \exp(-2\pi i/5)$ .

We can solve the quadratic for  $u$  to get

$$2 \cos(2\pi i/5) = u = \frac{-1 + \sqrt{5}}{2} = 1/\Phi, \quad \text{where } \Phi \text{ is the Golden Ratio.}$$

We now solve for  $\exp(2\pi i/5)$ , since this is a root of the quadratic  $X^2 - uX + 1$ , getting

$$\exp(2\pi i/5) = \frac{u + \sqrt{u^2 - 4}}{2} = \frac{-1 + \sqrt{5} + \sqrt{-10 - 2\sqrt{5}}}{4}.$$

Similar tricks only work for  $n < 11$ , but in 1771 Vandermonde found the expression

$$\begin{aligned}5 \exp(2\pi i/11) &= \\ &\sqrt[5]{\frac{11}{4}(89 + 25\sqrt{5} + 5\sqrt{\alpha} - 45\sqrt{\beta})} + \sqrt[5]{\frac{11}{4}(89 + 25\sqrt{5} - 5\sqrt{\alpha} + 45\sqrt{\beta})} \\ &+ \sqrt[5]{\frac{11}{4}(89 - 25\sqrt{5} + 5\sqrt{\alpha} + 45\sqrt{\beta})} + \sqrt[5]{\frac{11}{4}(89 - 25\sqrt{5} - 5\sqrt{\alpha} - 45\sqrt{\beta})},\end{aligned}$$

where

$$\alpha = -5 + 2\sqrt{5} \quad \text{and} \quad \beta = -5 - 2\sqrt{5}.$$

## 9.4 Solvable Groups

Given a finite group  $G$ , a chain of subgroups  $\{1\} = G_n \leq \dots \leq G_0 = G$  is called a **subnormal series** if  $G_i \triangleleft G_{i+1}$  for all  $i$ . The factor groups  $G_i/G_{i+1}$  are called the subquotients of the subnormal series. A chain is called a **normal series** if each  $G_i$  is a normal subgroup of  $G$ . (Some authors call a subnormal series a normal series, but then have no name for a normal series.)

A finite group  $G$  is called **solvable** provided there exists a subnormal series for  $G$  such that all subquotients are cyclic. We observe that a simple group is solvable if and only if it is cyclic of prime order.

The interest in such groups arises from Proposition 9.7, which states that if  $L/K$  is normal and radical, and if  $K$  contains enough roots of unity, then  $\text{Gal}(L/K)$  is a solvable group. A more general version of this result will be given in the next section, where we also prove a partial converse. Hence  $\text{Gal}(L/K)$  is solvable if and only if we can ‘solve’ the field extension  $L/K$  using radical expressions.

**Proposition 9.9.** *Let  $G$  be a finite group and  $H \leq G$  a subgroup. Let  $\{1\} = G_n \triangleleft \cdots \triangleleft G_0 = G$  be a subnormal series for  $G$ . Setting  $H_i := H \cap G_i$ , then  $\{1\} = H_n \triangleleft \cdots \triangleleft H_0 = H$  is a subnormal series for  $H$ . Moreover,  $H_i/H_{i+1} \leq G_i/G_{i+1}$ .*

*In particular, if each  $G_i/G_{i+1}$  is abelian (respectively cyclic), then so is each  $H_i/H_{i+1}$ . Hence  $G$  solvable implies  $H$  is solvable.*

*Proof.* We have  $H_i \leq G_i$ ,  $G_{i+1} \triangleleft G_i$  and  $H_{i+1} = H_i \cap G_{i+1}$ , so by the **Third Isomorphism Theorem**,  $H_{i+1} \triangleleft H_i$  and  $H_i/H_{i+1} \cong (H_i G_{i+1})/G_{i+1} \leq G_i/G_{i+1}$ .

For the second part, we observe that subgroups of abelian (respectively cyclic) groups are again abelian (respectively cyclic).  $\square$

**Proposition 9.10.** *Let  $G$  be a finite group and  $H \triangleleft G$  a normal subgroup. Let  $\{1\} = G_n \triangleleft \cdots \triangleleft G_0 = G$  be a subnormal series for  $G$ . Setting  $\bar{G}_i := (G_i H)/H$ , then  $\{1\} = \bar{G}_n \triangleleft \cdots \triangleleft \bar{G}_0 = G/H$  is a subnormal series for  $G/H$ . Moreover,  $G_i/G_{i+1} \twoheadrightarrow \bar{G}_i/\bar{G}_{i+1}$ .*

*In particular, if each  $G_i/G_{i+1}$  is abelian (respectively cyclic), then so is each  $\bar{G}_i/\bar{G}_{i+1}$ . Hence  $G$  solvable implies  $G/H$  is solvable.*

*Proof.* Set  $H_i := H \cap G_i$ . Then both  $G_{i+1}H_i, H_i \triangleleft G_i$  are normal subgroups, so also  $G_{i+1}H_i \triangleleft G_i$ . By the Second Isomorphism Theorem, we have

$$G_i/(G_{i+1}H_i) \cong (G_i/H_i)/(G_{i+1}H_i/H_i),$$

whereas by the Third Isomorphism Theorem we have

$$G_i/H_i \cong (G_i H)/H = \bar{G}_i.$$

Combining these gives an epimorphism

$$G_i H \twoheadrightarrow G_i/H_i \twoheadrightarrow G_i/(G_{i+1}H_i), \quad gh \mapsto g(G_{i+1}H_i).$$

This therefore has kernel  $G_{i+1}H$ , so  $G_{i+1}H \triangleleft G_i H$  is a normal subgroup. By the Second Isomorphism Theorem we now have  $\bar{G}_{i+1} \triangleleft \bar{G}_i$  and

$$\bar{G}_i/\bar{G}_{i+1} \cong (G_i H)/(G_{i+1}H) \cong G_i/(G_{i+1}H_i).$$

Finally, by the First Isomorphism Theorem, we have an epimorphism

$$G_i/G_{i+1} \twoheadrightarrow G_i/(G_{i+1}H_i) \cong \bar{G}_i/\bar{G}_{i+1}$$

as required. The second part follows as in the previous proposition.  $\square$

**Theorem 9.11.** *Let  $H \leq G$  be finite groups. Then  $G$  solvable implies  $H$  solvable. Moreover, if  $H \triangleleft G$ , then  $G$  is solvable if and only if both  $H$  and  $G/H$  are solvable.*

*Proof.* Using the propositions above, it only remains to prove that  $H$  and  $G/H$  both solvable implies  $G$  is solvable.

Let  $\{1\} = H_n \triangleleft \cdots \triangleleft H_m = H$  be a subnormal series for  $H$  and let  $\{1\} = \bar{G}_m \triangleleft \cdots \triangleleft \bar{G}_0 = G/H$  be a subnormal series for  $G/H$ . Define  $G_i := H_i$  for  $m \leq i \leq n$  and  $G_i := \pi^{-1}(\bar{G}_i)$  for  $0 \leq i \leq m$ , where  $\pi: G \rightarrow G/H$  is the canonical epimorphism. Since  $\pi^{-1}(\bar{G}_m) = H$ , this definition is consistent. Also,  $\pi^{-1}(\bar{G}_0) = G$ .

Then  $\{1\} = G_n \triangleleft \cdots \triangleleft G_0 = G$  is a subnormal series for  $G$ . Moreover,  $G_i/G_{i+1} \cong H_i/H_{i+1}$  for  $m \leq i < n$  and  $G_i/G_{i+1} \cong \bar{G}_i/\bar{G}_{i+1}$  for  $0 \leq i < m$ . The first of these is clear, and the second follows from the Second Isomorphism Theorem.

In particular, if each  $H_i/H_{i+1}$  and  $\bar{G}_i/\bar{G}_{i+1}$  is abelian (respectively cyclic), then so is each  $G_i/G_{i+1}$ . It follows that if both  $H$  and  $G/H$  are solvable, then so is  $G$ .  $\square$

We say that a chain of subgroups  $\{1\} = G'_n \leq \cdots \leq G'_0 = G$  is a **refinement** of a chain  $\{1\} = G_m \leq \cdots \leq G_0 = G$  provided that each  $G_i$  occurs as some  $G'_j$ .

**Corollary 9.12.** *A group is solvable if and only if it has a subnormal series whose subquotients are all cyclic of prime order, which is if and only if it has a subnormal series whose subquotients are all abelian.*

*Proof.* All finite abelian groups are direct products of cyclic groups, and all cyclic groups have a normal series whose subquotients are cyclic of prime order. Thus, given a subnormal series with abelian subquotients, we can refine it to a subnormal series whose subquotients are cyclic of prime order.  $\square$

**Theorem 9.13.** *Let  $p$  be a prime and  $G$  a finite  $p$ -group, so having  $p^r$  elements for some  $r$ . Then there exists a normal series  $\{1\} = Z^0 \triangleleft Z^1 \triangleleft \cdots \triangleleft Z^n = G$ , where  $Z^{i+1}/Z^i = Z(G/Z^i)$  is the centre of  $G/Z^i$ . In particular,  $G$  is solvable (in fact nilpotent).*

*Proof.* We let  $G$  act on itself by conjugation. The orbits of size one are given by the elements of the centre  $Z = Z(G) = Z^1$  of  $G$ , and note that  $|Z| \geq 1$  since  $1 \in Z$ . Let  $X$  be a set of representatives for the conjugacy classes of size at least 2. For  $x \in X$  let  $G_x = \text{Stab}_G(x)$  be the stabiliser of  $x$ , so the orbit of  $x$  has size  $[G : G_x] > 1$ . Since  $G$  is a  $p$ -group, we see that  $p$  divides each  $[G : G_x]$ . Now,  $|G| = |Z| + \sum_{x \in X} [G : G_x]$ , so  $p$  divides  $|Z|$ . In particular,  $G$  has non-trivial centre. Since  $Z \triangleleft G$  and  $G/Z$  is again a  $p$ -group we are done by induction.  $\square$

More generally, we have the following famous theorem. John Thompson was recently awarded the **Abel Prize** for this and other work on finite groups.

**Theorem 9.14** (Feit-Thompson). *Every finite group of odd order is solvable. In particular, if  $G$  is a finite simple group, then either  $G$  is cyclic of prime order or else  $|G|$  is even.*

We shall need the following result, concerning the solvability of the symmetric and alternating groups.

**Theorem 9.15.** *The alternating group  $A_n$  is solvable if  $n \leq 4$  and simple if  $n \geq 5$ . In particular, the symmetric group  $S_n$  is solvable if and only if  $n \leq 4$ .*

*Proof.* For  $n = 4$  we have the normal series  $\{1\} \triangleleft V \triangleleft A_4 \triangleleft S_4$ , where  $V = \{\text{id}, (12)(34), (13)(24), (14)(23)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$ . Since each quotient is abelian, we have the result. Moreover, since  $S_4/V \cong S_3$ , we also obtain that  $S_3$  is solvable.

On the other hand, if  $n \geq 5$ , then  $A_n$  is simple but not cyclic, so not solvable. (This was on the third exercise sheet.) Since  $A_n \triangleleft S_n$ , the full symmetric group  $S_n$  is not solvable for  $n \geq 5$ .  $\square$

## 9.5 Solvable Galois Extensions

We now come to one of the highlights of Galois Theory.

**Theorem 9.16.** *Let  $L/K$  be finite and normal. Then  $\text{Gal}(L/K)$  is solvable if and only if there exists a finite extension  $M/L$  with  $M/K$  normal and radical.*

*Proof.* Let  $L/K$  be Galois and let  $M/L$  be a field extension such that  $M/K$  is Galois and radical of exponent  $r$ . Let  $\zeta$  be a primitive  $r$ -th root of unity (in a splitting field of  $X^r - 1$  over  $M$ ). We observe that  $M(\zeta)$  is the compositum of  $M$  and  $K(\zeta)$ .

Since  $M/K$  and  $K(\zeta)/K$  are both Galois,  $M(\zeta)/K$  is Galois by Theorem 7.6. Moreover, Theorem 9.5 implies that  $M(\zeta)/K(\zeta)$  is radical of exponent  $r$ , and since  $\zeta$  is a primitive  $r$ -th root of unity, we must have that  $\text{Gal}(M(\zeta)/K(\zeta))$  is solvable, Proposition 9.7. Since this is a normal subgroup of  $\text{Gal}(M(\zeta)/K)$  with quotient the abelian group  $\text{Gal}(K(\zeta)/K)$  (Corollary 9.2), we deduce from Theorem 9.11 that  $\text{Gal}(M(\zeta)/K)$  is a solvable group.

Now,  $L/K$  is Galois, and by Theorem 7.5 we have an epimorphism of groups  $\text{Gal}(M(\zeta)/K) \twoheadrightarrow \text{Gal}(L/K)$ . Therefore  $\text{Gal}(L/K)$  is solvable by Theorem 9.11.

Conversely, let  $G = \text{Gal}(L/K)$  be solvable group of order  $r = [L : K]$ , and let  $\{1\} = G_n \triangleleft \cdots \triangleleft G_0 = G$  be a subnormal series for  $G$  with cyclic subquotients. Let  $K_i$  be the intermediate field of  $L/K$  belonging to  $G_i$ , so that  $L = K_n/\cdots/K_0 = K$  is a tower of field extensions. Then  $K_i/K_{i-1}$  is Galois with Galois group  $G_{i-1}/G_i$  cyclic of order dividing  $r$ .

Now let  $M$  be the splitting field extension of  $X^r - 1$  over  $L$  and let  $\zeta \in M$  be a primitive  $r$ -th root of unity. Note that  $M$  is the compositum of  $L$  and  $K(\zeta)$ , so  $M/K$  is Galois by Theorem 7.6.

Set  $M_i := K_i(\zeta)$ , so that we have a tower  $M = M_n/\cdots/M_0 = K(\zeta)$ . By Theorem 7.6 again,  $M_i/M_{i-1}$  is Galois and  $\text{Gal}(M_i/M_{i-1}) \leq \text{Gal}(K_i/K_{i-1})$ , so that the Galois group is cyclic of order dividing  $r$ . By Theorem 9.4,  $M_i = M_{i-1}(\alpha_i)$  with  $\alpha_i^r \in M_{i-1}$ . Hence  $M = M_n/\cdots/M_0 = K(\zeta)$  is a radical tower of exponent  $r$ .

Finally, since  $K(\zeta)/K$  is radical by Proposition 9.8, we deduce from Theorem 9.5 that  $M/K$  is normal and radical.  $\square$

We say that an irreducible polynomial  $f \in K[X]$  is **solvable by radicals** if there exists a radical extension  $M/K$  containing a root of  $f$ . Since the normal closure of a radical extension is again radical, Theorem 9.6, it is equivalent to assume that there exists a radical Galois extension  $M/K$  containing a root of  $f$ . In this case,  $M$  contains all roots of  $f$ , so contains the splitting field extension  $L$  of  $f$  over  $K$ .

We remark once again that  $L/K$  will not be radical in general.

**Theorem 9.17** (Galois). *An irreducible polynomial  $f$  is solvable by radicals if and only if  $\text{Gal}(f)$  is a solvable group.*

*Proof.* Let  $f \in K[X]$  be irreducible and let  $L/K$  be its splitting field extension, so that  $\text{Gal}(f) = \text{Gal}(L/K)$ . Then  $f$  is solvable by radicals if and only if there exists a finite extension  $M/L$  with  $M/K$  normal and radical, which by Theorem 9.16 is if and only if  $\text{Gal}(L/K)$  is solvable.  $\square$

**Corollary 9.18.** *A general quintic is not solvable by radicals.*

*Proof.* We saw in Example 6 of the previous chapter that  $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$  is irreducible and has Galois group  $S_5$ . Therefore  $\text{Gal}(f)$  is not solvable, so  $f$  is not solvable by radicals.  $\square$

## Chapter 10

# Explicit Formulae for Cubics and Quartics

In this chapter we apply the above considerations to the cubic and quartic polynomials, and in so doing obtain radical expressions for roots of cubics and quartics. In particular, we recover Cardano's formula from the introduction, and motivate the constructions involved. The formula for the quartic is due to Ferrari, a student of Cardano.

### 10.1 Solving the Cubic

Let  $f = X^3 - \mathbf{e}_1 X^2 + \mathbf{e}_2 X - \mathbf{e}_3 \in K[X]$  be irreducible and let  $\alpha_i$  for  $i = 1, 2, 3$  be the roots of  $f$  in its splitting field extension  $L$ . Thus the  $\mathbf{e}_i$  are the elementary symmetric functions

$$\mathbf{e}_1 = \alpha_1 + \alpha_2 + \alpha_3, \quad \mathbf{e}_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1, \quad \mathbf{e}_3 = \alpha_1\alpha_2\alpha_3.$$

The Galois group  $G$  of  $f$  is a subgroup of  $S_3$ , and we have the subnormal series  $\{1\} \triangleleft A_3 \triangleleft S_3$  with cyclic subquotients. In fact,  $A_3 \cong \mathbb{Z}/3\mathbb{Z}$  and  $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ .

In order to solve the cubic, we first adjoin primitive square and cube roots of unity (since 2 and 3 are the orders of the cyclic subquotients). Since  $-1 \in K$ , it is enough to adjoin a primitive cube root of unity  $\omega$ . So, from now on we assume that  $\omega \in K$ .

We define

$$\delta = \prod_{i < j} (\alpha_i - \alpha_j) = (\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) - (\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2),$$

so that the discriminant of  $f$  is

$$\Delta(f) = \mathbf{e}_1^2\mathbf{e}_2^2 - 4\mathbf{e}_1^3\mathbf{e}_3 - 4\mathbf{e}_2^3 + 18\mathbf{e}_1\mathbf{e}_2\mathbf{e}_3 - 27\mathbf{e}_3^2.$$

We have already observed that an element of  $G$  fixes  $\delta$  if and only if it is an even permutation. Thus  $\text{Gal}(L/K(\delta)) = G \cap A_3$ .

Since  $\text{Gal}(L/K(\delta)) = A_3$  and  $\omega \in K$ , we know that there exists some  $u \in L$  such that  $u^3 \in K(\delta)$ . In fact, by Theorem 9.4, this element  $u$  must satisfy  $u/\sigma(u) = \omega$ , where  $\sigma = (123): \alpha_i \mapsto \alpha_{i+1}$  is a generator for  $A_3$ . The obvious choice is to consider  $u = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$ , for then  $\sigma(u) = \omega^2u$ , so that  $u/\sigma(u) = \omega$ .

It remains to calculate  $u^3$ , which we know from the introduction equals

$$(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 6\alpha_1\alpha_2\alpha_3 + 3\omega(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + 3\omega^2(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2).$$

Using that

$$(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1) + (\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) = \mathbf{e}_1\mathbf{e}_2 - 3\mathbf{e}_3,$$

we can write

$$\begin{aligned} u^3 &= (\mathbf{e}_1^3 - 3\mathbf{e}_1\mathbf{e}_2 + 9\mathbf{e}_3) + \frac{3}{2}\omega(\mathbf{e}_1\mathbf{e}_2 - 3\mathbf{e}_3 + \delta) + \frac{3}{2}\omega^2(\mathbf{e}_1\mathbf{e}_2 - 3\mathbf{e}_3 - \delta) \\ &= \mathbf{e}_1^3 - \frac{9}{2}\mathbf{e}_1\mathbf{e}_2 + \frac{27}{2}\mathbf{e}_3 + \frac{3}{2}(\omega - \omega^2)\delta \\ &= \frac{1}{2}(\lambda + 3(\omega - \omega^2)\delta), \quad \text{where } \lambda = 2\mathbf{e}_1^3 - 9\mathbf{e}_1\mathbf{e}_2 + 27\mathbf{e}_3. \end{aligned}$$

Note that  $\omega - \omega^2 = \sqrt{-3}$ . Similarly, we can form the sum  $v = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3$  and see that

$$v^3 = \frac{1}{2}(\lambda - 3(\omega - \omega^2)\delta), \quad uv = \mathbf{e}_1^2 - 3\mathbf{e}_2.$$

We can now solve for  $\alpha_i$  using the three expressions

$$\mathbf{e}_1 = \sum_i \alpha_i, \quad u = \sum_i \omega^{i-1}\alpha_i, \quad v = \sum_i \omega^{2(i-1)}\alpha_i.$$

In this way we recover the formula given in the introduction: we have

$$\alpha_1 = \frac{1}{3}(\mathbf{e}_1 + u + v), \quad \alpha_2 = \frac{1}{3}(\mathbf{e}_1 + \omega^2u + \omega v), \quad \alpha_3 = \frac{1}{3}(\mathbf{e}_1 + \omega u + \omega^2v),$$

and  $u^3$  and  $v^3$  are the roots of the resolvent quadratic

$$g := X^2 - \lambda X + \frac{1}{4}(\lambda^2 + 27\Delta), \quad \lambda := 2\mathbf{e}_1^3 - 9\mathbf{e}_1\mathbf{e}_2 + 27\mathbf{e}_3.$$

[This is essentially the same formula, but we have not assumed that  $\mathbf{e}_1 = 0$  and we have that the  $u$  in the introduction is one third of the  $u$  here.]

We also have the following criterion for the Galois group of an irreducible cubic  $f \in K[X]$ .

$\sqrt{\Delta}$	$\text{Gal}(f)$
not in $K$	$S_3$
in $K$	$A_3$

## 10.2 Solving the Quartic

We now carry out a similar analysis for an irreducible quartic polynomial  $f = X^4 - \mathbf{e}_1 X^3 + \mathbf{e}_2 X^2 - \mathbf{e}_3 X + \mathbf{e}_4 \in K[X]$ . Let  $L$  be a splitting field extension and let  $\alpha_i$  for  $i = 1, 2, 3, 4$  be the roots of  $f$  in  $L$ . Let  $G \leq S_4$  be the Galois group of  $f$ .

Recall that  $S_4$  is a solvable group. In fact, we have the normal series  $\{\text{id}\} \triangleleft T \triangleleft V \triangleleft A_4 \triangleleft S_4$  whose subquotients are cyclic of order 2, 2, 3, 2 respectively. Here we have written  $T$  for the subgroup generated by (12)(34), although we could have used any of the non-trivial elements in  $V$ . Since the cyclic subquotients are of orders 2 and 3, it is again enough to adjoin a primitive cube root of unity  $\omega$ .

We have

$$\begin{aligned} \delta &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_4) \\ &= \sum_{\sigma \in A_4} \alpha_{\sigma(1)}^3 \alpha_{\sigma(2)}^2 \alpha_{\sigma(3)} - \sum_{\sigma \in A_4} \alpha_{\sigma(1)} \alpha_{\sigma(2)}^2 \alpha_{\sigma(3)}^3, \end{aligned}$$

and since  $\sigma \in G$  fixes  $\delta$  if and only if  $\sigma$  is even, we see that the group associated to  $K(\delta)$  is  $G \cap A_4$ .

We next want to calculate the fixed field of  $G \cap V$ . This will be a Galois extension of  $K(\delta)$  with Galois group a subgroup of  $A_4/V \cong \mathbb{Z}/3\mathbb{Z}$ . Since  $V = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$ , we are led to consider the elements

$$a = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \quad b = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4), \quad c = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).$$

We observe that

$$a + b + c = 2\mathbf{e}_2, \quad ab + bc + ca = \mathbf{e}_2^2 + \mathbf{e}_1\mathbf{e}_3 - 4\mathbf{e}_4, \quad abc = -\mathbf{e}_3^2 - \mathbf{e}_1^2\mathbf{e}_4 + \mathbf{e}_1\mathbf{e}_2\mathbf{e}_3$$

so that  $a, b, c$  are the roots of the resolvent cubic

$$g := X^3 - 2\mathbf{e}_2 X^2 + (\mathbf{e}_2^2 + \mathbf{e}_1\mathbf{e}_3 - 4\mathbf{e}_4)X + (\mathbf{e}_3^2 + \mathbf{e}_1^2\mathbf{e}_4 - \mathbf{e}_1\mathbf{e}_2\mathbf{e}_3).$$

This has coefficients in  $K$ , and so  $K(a, b, c)$  is the splitting field extension for  $g$ , hence is Galois.

We also observe that

$$\begin{aligned} a - b &= (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4), \\ b - c &= -(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4), \\ a - c &= -(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4), \end{aligned}$$

so that

$$\prod_{i < j} (\alpha_i - \alpha_j) = (a - b)(a - c)(b - c).$$

Thus  $f$  and  $g$  have the same discriminant  $\Delta$ . Since the roots of  $f$  are distinct,  $\Delta \neq 0$ , so the roots of  $g$  must also be distinct. Note however that  $g$  may not be irreducible.

We can now calculate the subgroup associated to  $K(a, b, c)$ . For, since  $a, b, c$  are all distinct,  $\sigma \in G$  fixes  $a$  if and only if  $\sigma$  is one of the elements

$$\text{id}, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)$$

(which form the elements of a group of type  $D_8$ ). Doing this for  $b$  and  $c$  as well, we deduce that the group associated to  $K(a, b, c)$  is precisely  $G \cap V$ .

We remark that  $K(a, b, c)/K$  is Galois with Galois group  $\text{Gal}(g) = G/(G \cap V)$ . This is naturally a subgroup of  $S_3 \cong S_4/V$ .

Moreover, since  $f$  and  $g$  have the same discriminant, we can substitute the coefficients of  $g$  into the formula for the discriminant of a cubic to obtain the formula for the discriminant of a quartic:

$$\begin{aligned} \Delta(f) &= e_1^2 e_2^2 e_3^2 - 4e_1^3 e_3^3 - 4e_2^3 e_3^2 - 4e_1^2 e_2^3 e_4 - 6e_1^2 e_3^2 e_4 + 16e_2^4 e_4 \\ &\quad + 18e_1^3 e_2 e_3 e_4 + 18e_1 e_2 e_3^3 - 27e_1^4 e_4^2 - 27e_3^4 - 80e_1 e_2^2 e_3 e_4 - 128e_2^2 e_4^2 \\ &\quad + 144e_1^2 e_2 e_4^2 + 144e_2 e_3^2 e_4 - 192e_1 e_3 e_4^2 + 256e_4^3. \end{aligned}$$

We already know how to solve the cubic  $g$ : we consider

$$2\mathbf{e}_2 = a + b + c, \quad u = a + \omega b + \omega^2 c, \quad v = a + \omega^2 b + \omega c.$$

Then

$$u^3 = \frac{1}{2}(\lambda + 3(\omega - \omega^2)\delta),$$

where as before

$$\begin{aligned} \lambda &= 2(a + b + c)^3 - 9(a + b + c)(ab + bc + ca) + 27abc \\ &= 16\mathbf{e}_2^3 - 18\mathbf{e}_2(\mathbf{e}_2^2 + \mathbf{e}_1\mathbf{e}_3 - 4\mathbf{e}_4) + 27(\mathbf{e}_1\mathbf{e}_2\mathbf{e}_3 - \mathbf{e}_3^2 - \mathbf{e}_1^2\mathbf{e}_4) \\ &= 2\mathbf{e}_2^3 + 27\mathbf{e}_3^2 + 27\mathbf{e}_1^2\mathbf{e}_4 - 72\mathbf{e}_2\mathbf{e}_4 - 9\mathbf{e}_1\mathbf{e}_2\mathbf{e}_3. \end{aligned}$$

(Note that we used the symmetric functions in the elements  $a, b, c$  in the formula for  $\lambda$ .)

We next want to calculate the fixed field of  $G \cap T$ . This is an extension of  $K(a, b, c)$  of degree at most 2. We will show that this always equals  $L := K(a, b, c, \alpha_1 + \alpha_2, \alpha_1\alpha_2)$ . Let  $H$  be the subgroup associated to  $L$ . It is clear that  $(G \cap T) \leq H \leq (G \cap V)$ , so the result follows if we can show that  $H \leq (G \cap T)$ .

Suppose therefore that  $\sigma \in H$ . Since  $\alpha_1 + \alpha_2 = \alpha_1 + \alpha_j$  implies  $j = 2$ , and similarly  $\alpha_1 + \alpha_2 = \alpha_i + \alpha_2$  implies  $i = 1$ , we see that  $\alpha_1 + \alpha_2 \neq \alpha_3 + \alpha_4$  implies  $\sigma \in \langle (12), (34) \rangle \cap V = T$ . Similarly for  $\alpha_1\alpha_2$ . Therefore, if  $\sigma \notin G \cap T$ , then we must have both  $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 =: \theta$  and  $\alpha_1\alpha_2 = \alpha_3\alpha_4 =: \phi$ . Hence we have four distinct roots of the quadratic  $X^2 - \theta X + \phi$ , a contradiction.

We note that  $\alpha_1 + \alpha_2$  and  $\alpha_3 + \alpha_4$  are the roots of the quadratic  $X^2 - \mathbf{e}_1 X + a$ , whereas  $\alpha_1 \alpha_2$  and  $\alpha_3 \alpha_4$  are the roots of the quadratic  $X^2 - (\mathbf{e}_2 - a)X + \mathbf{e}_4$ . Also,  $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$  implies  $\mathbf{e}_1 = 2(\alpha_1 + \alpha_2)$  and  $a = (\alpha_1 + \alpha_2)^2 = \frac{1}{4}\mathbf{e}_1^2 \in K$ . Thus, provided that  $g$  has no root in  $K$ , we have  $L = K(a, b, c, \alpha_1 + \alpha_2)$ . Otherwise we may assume that  $g$  has a root  $a \in K$ . Then  $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$  if and only if  $\mathbf{e}_1^2 = 4a$ , and  $\alpha_1 \alpha_2 = \alpha_3 \alpha_4$  if and only if  $(\mathbf{e}_2 - a)^2 = 4\mathbf{e}_4$ . Thus we can always write either  $L = K(a, b, c, \alpha_1 + \alpha_2)$  or  $L = K(a, b, c, \alpha_1 \alpha_2)$ .

In particular, to obtain  $L$  from  $K(a, b, c)$ , we only need to adjoin either a square root of  $\mathbf{e}_1^2 - 4a$  or a square root of  $(\mathbf{e}_2 - a)^2 - 4\mathbf{e}_4$ .

Finally, to obtain  $\alpha_1$  and  $\alpha_2$ , we can solve the quadratic

$$X^2 - (\alpha_1 + \alpha_2)X + \alpha_1 \alpha_2$$

by adjoining a square root of  $(\alpha_1 + \alpha_2)^2 - 4\alpha_1 \alpha_2$ .

We remark that  $\alpha_1 \alpha_2$  and  $\alpha_1 + \alpha_2$  are related by the formula

$$8\mathbf{e}_3 - 4\mathbf{e}_1 \mathbf{e}_2 + \mathbf{e}_1^3 = -(2(\alpha_1 + \alpha_2) - \mathbf{e}_1)(8\alpha_1 \alpha_2 + 4(a - \mathbf{e}_2) - \mathbf{e}_1(2(\alpha_1 + \alpha_2) - \mathbf{e}_1)).$$

This expression seems to be new — at least I couldn't find it in the standard literature. One can easily check it in the simple case when  $\mathbf{e}_1 = 0$ . For, making the substitution  $-\alpha_4 = \alpha_1 + \alpha_2 + \alpha_3$  one obtains

$$a - \mathbf{e}_2 = -\alpha_1 \alpha_2 - \alpha_3 \alpha_4 = -\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 + \alpha_3^2$$

and

$$\mathbf{e}_3 = -(\alpha_1 + \alpha_2)(\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 + \alpha_3^2) = -(\alpha_1 + \alpha_2)(2\alpha_1 \alpha_2 + a - \mathbf{e}_2).$$

The general formula follows after applying the Tschirnhaus transformation  $Y = X + a/4$ .

A different approach, the standard method for solving a quartic and yielding simpler formulae, involves finding expressions for  $\alpha_1 + \alpha_3$  and  $\alpha_1 + \alpha_4$  as well as for  $\alpha_1 + \alpha_2$ . We thus solve the three quadratics

$$X^2 - \mathbf{e}_1 X + a, \quad X^2 - \mathbf{e}_1 X + b, \quad X^2 - \mathbf{e}_1 X + c.$$

We may choose square roots such that

$$\begin{aligned} p &= \sqrt{\mathbf{e}_1^2 - 4a} = 2(\alpha_1 + \alpha_2) - \mathbf{e}_1 = (\alpha_1 + \alpha_2) - (\alpha_3 + \alpha_4) \\ q &= \sqrt{\mathbf{e}_1^2 - 4b} = 2(\alpha_1 + \alpha_3) - \mathbf{e}_1 = (\alpha_1 + \alpha_3) - (\alpha_2 + \alpha_4) \\ r &= \sqrt{\mathbf{e}_1^2 - 4c} = 2(\alpha_1 + \alpha_4) - \mathbf{e}_1 = (\alpha_1 + \alpha_4) - (\alpha_2 + \alpha_3), \end{aligned}$$

which gives us the compatibility condition

$$\begin{aligned}
pqr &= \sqrt{\mathbf{e}_1^2 - 4a}\sqrt{\mathbf{e}_1^2 - 4b}\sqrt{\mathbf{e}_1^2 - 4c} \\
&= (\alpha_1^3 + \alpha_2^3 + \alpha_3^3 + \alpha_4^3) + 2(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4) \\
&\quad - (\alpha_1^2\alpha_2 + \alpha_1^2\alpha_3 + \alpha_1^2\alpha_4 + \alpha_2^2\alpha_3 + \alpha_2^2\alpha_4 + \alpha_3^2\alpha_4) \\
&\quad - (\alpha_1\alpha_2^2 + \alpha_1\alpha_3^2 + \alpha_1\alpha_4^2 + \alpha_2\alpha_3^2 + \alpha_2\alpha_4^2 + \alpha_3\alpha_4^2) \\
&= (\mathbf{e}_1^3 - 3\mathbf{e}_1\mathbf{e}_2 + 3\mathbf{e}_3) + 2\mathbf{e}_3 - (\mathbf{e}_1\mathbf{e}_2 - 3\mathbf{e}_3) \\
&= 8\mathbf{e}_3 - 4\mathbf{e}_1\mathbf{e}_2 + \mathbf{e}_1^3.
\end{aligned}$$

Having this, we can now solve for  $\alpha_1$ , since

$$2\alpha_1 + e_1 = (\alpha_1 + \alpha_2) + (\alpha_1 + \alpha_3) + (\alpha_1 + \alpha_4) = \frac{1}{2}(3\mathbf{e}_1 + p + q + r).$$

Note that with this method we have to solve one extra quadratic, and also have to introduce a compatibility condition, both of which are avoided using the previous method following the theory. On the other hand, the formulae are easier. We also observe the connection between the two methods, since

$$\begin{aligned}
p &= 2(\alpha_1 + \alpha_2) - \mathbf{e}_1, \\
qr &= -(8\alpha_1\alpha_2 + 4(a - \mathbf{e}_2) - \mathbf{e}_1(2(\alpha_1 + \alpha_2) - \mathbf{e}_1)).
\end{aligned}$$

In summary, given a quartic

$$f = X^4 - \mathbf{e}_1X^3 + \mathbf{e}_2X^2 - \mathbf{e}_3X + \mathbf{e}_4 \in K[X],$$

where  $K$  contains a primitive cube root of unity, we form the resolvent cubic

$$g = X^3 - 2\mathbf{e}_2X^2 + (\mathbf{e}_2^2 + \mathbf{e}_1\mathbf{e}_3 - 4\mathbf{e}_4)X + (\mathbf{e}_3^2 + \mathbf{e}_1^2\mathbf{e}_4 - \mathbf{e}_1\mathbf{e}_2\mathbf{e}_3)$$

having roots  $a, b, c$ . We then take square roots

$$p = \sqrt{\mathbf{e}_1^2 - 4a}, \quad q = \sqrt{\mathbf{e}_1^2 - 4b}, \quad r = \sqrt{\mathbf{e}_1^2 - 4c}$$

with signs chosen such that

$$pqr = 8\mathbf{e}_3 - 4\mathbf{e}_1\mathbf{e}_2 + \mathbf{e}_1^3.$$

The roots of  $f$  are then given by

$$\begin{aligned}
\alpha_1 &= \frac{1}{4}(\mathbf{e}_1 + p + q + r) & \alpha_3 &= \frac{1}{4}(\mathbf{e}_1 - p + q - r) \\
\alpha_2 &= \frac{1}{4}(\mathbf{e}_1 + p - q - r) & \alpha_4 &= \frac{1}{4}(\mathbf{e}_1 - p - q + r).
\end{aligned}$$

It is also possible to give simple criteria for determining the Galois group of a quartic  $f$  (following Kappe and Warren). Note that we only need the third column to distinguish between  $D_8$  and  $\mathbb{Z}/4\mathbb{Z}$ . In these two cases  $g$  has a root in  $K$ , which we may assume to be  $a$ .

$\sqrt{\Delta}$	$g \in K[X]$	$\sqrt{(\mathbf{e}_2 - a)^2 - 4\mathbf{e}_4}, \sqrt{\mathbf{e}_1^2 - 4a}$	$\text{Gal}(f)$
not in $K$	irreducible		$S_4$
not in $K$	root $a$	not both in $K(\sqrt{\Delta})$	$D_8$
not in $K$	root $a$	both in $K(\sqrt{\Delta})$	$\mathbb{Z}/4\mathbb{Z}$
in $K$	irreducible		$A_4$
in $K$	splits		$V$

Recall that the fixed field of  $G \cap A_4$  is  $K(\sqrt{\Delta})$  and the fixed field of  $G \cap V$  is  $K(a, b, c)$ , the splitting field of  $g$ . The degree of  $K(a, b, c)/K$  equals the index of  $G \cap V$  in  $G$ .

If  $\sqrt{\Delta} \in K$ , then  $G$  is a subgroup of  $A_4$ , so either  $A_4$  or  $V$ . If  $G = A_4$ , then  $[K(a, b, c) : K] = 3$ , so that  $g$  is irreducible. If  $G = V$ , then  $K(a, b, c) = K$  and  $g$  splits over  $K$ . We observe that  $g$  splits over  $K$  if and only if  $g$  has a root in  $K$ .

Otherwise, if  $\sqrt{\Delta} \notin K$ , then  $G$  is one of  $S_4$ ,  $D_8$  or  $\mathbb{Z}/4\mathbb{Z}$ . If  $G = S_4$ , then  $[K(a, b, c) : K] = 6$  and  $g$  is irreducible over  $K$  (in fact,  $\text{Gal}(g) \cong S_3$ .) If  $G = D_8$  or  $G = \mathbb{Z}/4\mathbb{Z}$ , then  $G \cap V = G \cap A_4$ . ( $G \cap A_4$  equals  $V$  if  $G = D_8$  and is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$  if  $G = \mathbb{Z}/4\mathbb{Z}$ .) Thus  $K(a, b, c) = K(\sqrt{\Delta})$  and  $g$  has a root in  $K$ , which we may assume to be  $a$ . N.B. Making this choice means that  $G$  contains the 4-cycle (1324).

To distinguish between  $D_8$  and  $\mathbb{Z}/4\mathbb{Z}$ , set

$$h := (X^2 - \mathbf{e}_1 X + a)(X^2 - (\mathbf{e}_2 - a)X + \mathbf{e}_4).$$

This has roots  $\alpha_1 + \alpha_2$ ,  $\alpha_3 + \alpha_4$ ,  $\alpha_1 \alpha_2$ ,  $\alpha_3 \alpha_4$ . As above, the splitting field of  $h$  over  $K(a, b, c) = K(\sqrt{\Delta})$  is precisely the fixed field of  $G \cap T$ . Now, if  $G = D_8$ , then  $G \cap T = T \neq V = G \cap V$ . Thus  $h$  does not split over  $K(\sqrt{\Delta})$ . On the other hand, if  $G = \mathbb{Z}/4\mathbb{Z}$ , then  $G \cap T = T = G \cap V$ , so  $h$  does split over  $K(\sqrt{\Delta})$ .

We remark that the standard analysis is based on the fact that, provided that  $\sqrt{\Delta} \notin K$  and  $g$  has a root in  $K$ , we have  $G \cong D_8$  if and only if  $f$  is irreducible over  $K(\sqrt{\Delta})$ . Checking the irreducibility of a quartic, however, is non-trivial. Our method only requires one to check whether  $\mathbf{e}_1^2 - 4a$  and  $(\mathbf{e}_2 - a)^2 - 4\mathbf{e}_4$  have square roots in  $K(\sqrt{\Delta})$ , a much easier problem.

As a special case, we note that if  $f = X^4 + e_2 X^2 + e_4 \in K[X]$  is irreducible, with roots  $\pm\alpha, \pm\beta$ , then

1.  $\text{Gal}(f) \cong V$  if and only if  $e_4$  is a square in  $K$  if and only if  $\alpha\beta \in K$ ;
2.  $\text{Gal}(f) \cong \mathbb{Z}/4\mathbb{Z}$  if and only if  $e_4(e_2^2 - 4e_4)$  is a square in  $K$  if and only if  $\alpha\beta \in K(\alpha^2) \setminus K$ ;
3.  $\text{Gal}(f) \cong D_8$  if and only if neither  $e_4, e_4(e_2^2 - 4e_4)$  are squares in  $K$  if and only if  $\alpha\beta \notin K(\alpha^2)$ .

For,  $\Delta = 16\mathbf{e}_4(\mathbf{e}_2^2 - 4\mathbf{e}_4)^2$ , so  $\Delta$  is a square if and only if  $\mathbf{e}_4$  is a square. Also,  $g = X(X^2 - 2\mathbf{e}_2X + (\mathbf{e}_2^2 - 4\mathbf{e}_4))$ , so has roots 0 and  $\mathbf{e}_2 \pm 2\sqrt{\mathbf{e}_4}$ . In particular, we can always take  $a = 0 \in K$ , so the possible Galois groups are  $V$ ,  $D_8$  and  $\mathbb{Z}/4\mathbb{Z}$ . Note that  $\mathbf{e}_1^2 - 4a = 0$  always has a square root in  $K$ .

Now,  $G = V$  if and only if  $\sqrt{\mathbf{e}_4} \in K$ . On the other hand, suppose that  $\sqrt{\mathbf{e}_4} \notin K$ . Then  $\mathbf{e}_2^2 - 4\mathbf{e}_4$  is a square in  $K(\sqrt{\mathbf{e}_4})$  if and only if  $\mathbf{e}_4(\mathbf{e}_2^2 - 4\mathbf{e}_4)$  is a square in  $K$ . For, writing  $\mathbf{e}_2^2 - 4\mathbf{e}_4 = (x + y\sqrt{\mathbf{e}_4})^2$  with  $x, y \in K$ , we see that  $2xy\sqrt{\mathbf{e}_4} = (\mathbf{e}_2^2 - 4\mathbf{e}_4) - x^2 - y^2\mathbf{e}_4 \in K$ . Hence  $xy = 0$ , so either  $x = 0$  and  $\mathbf{e}_4(\mathbf{e}_2^2 - 4\mathbf{e}_4) = y^2\mathbf{e}_4^2$ , or else  $y = 0$  and  $\mathbf{e}_2^2 - 4\mathbf{e}_4 = x^2$ . In this latter case, we would have the factorisation  $f = (X^2 + \frac{1}{2}(\mathbf{e}_2 + x))(X^2 + \frac{1}{2}(\mathbf{e}_2 - x))$ , so  $f$  would not be irreducible.

The statements involving the roots follow from the expressions

$$\mathbf{e}_2 = -(\alpha^2 + \beta^2), \quad \mathbf{e}_4 = \alpha^2\beta^2, \quad \mathbf{e}_2^2 - 4\mathbf{e}_4 = (\alpha^2 - \beta^2)^2.$$

Another nice exercise is to use this criterion to study the polynomial  $f = X^4 + pX + p \in \mathbb{Z}[X]$  for  $p$  a prime. This has Galois group  $S_4$  if  $p \neq 3, 5$ , has Galois group  $D_8$  if  $p = 3$  and has Galois group  $\mathbb{Z}/4\mathbb{Z}$  if  $p = 5$ .

# Chapter 11

## Applications

### 11.1 Symmetric Functions

Let  $L = k(x_1, \dots, x_n)$  with each  $x_i$  transcendental over  $k(x_1, \dots, x_{i-1})$ . In other words, we have a tower  $L = k_n/\dots/k_0 = k$  such that  $k_i = k_{i-1}(x_i)$  is a simple transcendental field extension. (We say that the  $x_i$  are algebraically independent, since they satisfy no algebraic relation. C.f. linear independence.)

Let  $S_n$  act on  $L$  as  $k$ -automorphisms, where  $\sigma(x_i) := x_{\sigma(i)}$ . We define the elementary symmetric functions to be

$$\mathbf{e}_r := \sum_{i_1 < \dots < i_r} x_{i_1} \cdots x_{i_r} = \sum_{\substack{I \subset \{1, \dots, n\} \\ |I|=r}} \prod_{i \in I} x_i, \quad 1 \leq r \leq n.$$

We now observe that  $S_n$  acts on the set of subsets  $I \subset \{1, \dots, n\}$  of size  $r$ . Hence  $\sigma(\mathbf{e}_r) = \mathbf{e}_r$  for all  $\sigma \in S_n$ , so that  $\mathbf{e}_r \in L^{S_n}$ . Define  $K := k(\mathbf{e}_1, \dots, \mathbf{e}_n)$ .

**Theorem 11.1** (Fundamental Theorem of Symmetric Functions).  *$L/K$  is Galois with Galois group  $S_n$ . In particular, any rational function in the  $x_i$  which is invariant under  $S_n$  can be expressed as a rational function of the  $\mathbf{e}_i$ .*

*Moreover, any polynomial in the  $x_i$  which is invariant under  $S_n$  can be expressed as a polynomial in the  $\mathbf{e}_i$ , so  $k[x_1, \dots, x_n]^{S_n} = k[\mathbf{e}_1, \dots, \mathbf{e}_n]$ .*

*Proof.* Since  $S_n$  is a finite group,  $L/L^{S_n}$  is a Galois extension. This gives an epimorphism  $S_n \rightarrow \text{Gal}(L/L^{S_n})$ , which is injective, so an isomorphism. For, if  $\sigma$  acts as the identity on  $L$ , then  $\sigma(x_i) = x_i$  for all  $i$ , so  $\sigma(i) = i$  for all  $i$ , whence  $\sigma = \text{id}$ . Therefore  $[L : L^{S_n}] = |S_n| = n!$  and  $S_n = \text{Gal}(L/L^{S_n})$ .

We showed above that  $K \subset L^{S_n}$ , so  $[L : K] \geq n!$ . Conversely, consider the polynomial

$$F = \prod_i (X - x_i) = X^n - \mathbf{e}_1 X^{n-1} + \mathbf{e}_2 X^{n-2} - \dots + (-1)^n \mathbf{e}_n \in K[X].$$

This has degree  $n$  and roots  $x_i$  for  $1 \leq i \leq n$ . Thus the splitting field extension of  $F$  over  $K$  is precisely  $K(x_1, \dots, x_n) = L$ . By Theorem 5.1, we have  $[L : K] \leq n!$ . Hence  $[L : K] = n!$  and  $L^{S_n} = K$ , proving the first statement.

We now want to prove that  $L$  has  $K$ -basis given by the following set of monomials  $\mathcal{M} := \{x_1^{a_1} \cdots x_n^{a_n} : 0 \leq a_i < i\}$ . We begin by showing that we can write any polynomial  $f \in k[x_1, \dots, x_n]$  as a sum of elements of the form  $x_1^{a_1} \cdots x_n^{a_n} g$  with  $g \in k[\mathbf{e}_1, \dots, \mathbf{e}_n]$  and  $0 \leq a_i < i$  for all  $i$ . We introduce the polynomials

$$F_i(X) := (X - x_1) \cdots (X - x_i) = F(X)/(X - x_{i+1}) \cdots (X - x_n),$$

so that  $F_i$  has degree  $i$  and coefficients involving only  $\mathbf{e}_1, \dots, \mathbf{e}_n$  and  $x_{i+1}, \dots, x_n$ . For example, if  $n = 3$ , then

$$\begin{aligned} F_3 &= F = (X - x_1)(X - x_2)(X - x_3) = X^3 - \mathbf{e}_1 X^2 + \mathbf{e}_2 X - \mathbf{e}_3 \\ F_2 &= (X - x_1)(X - x_2) = \frac{F_3}{(X - x_3)} = X^2 - (\mathbf{e}_1 - x_3)X + (\mathbf{e}_2 - \mathbf{e}_1 x_3 + x_3^2) \\ F_1 &= (X - x_1) = \frac{F_2}{(X - x_2)} = X - (\mathbf{e}_1 - x_2 - x_3). \end{aligned}$$

Since  $x_1$  is a root of  $F_1$  and  $\deg(F_1) = 1$ , we can replace all occurrences in  $f$  of  $x_1$  using  $\mathbf{e}_1, \dots, \mathbf{e}_n$  and  $x_2, \dots, x_n$ . In fact, we know that  $F_1 = X - \mathbf{e}_1 + (x_2 + \cdots + x_n)$ , and we are replacing  $x_1$  with  $\mathbf{e}_1 - (x_2 + \cdots + x_n)$ .

Since  $x_2$  is a root of  $F_2$  and  $\deg(F_2) = 2$ , we can replace all occurrences in  $f$  of  $x_2^d$  for  $d \geq 2$  by a linear polynomial in  $x_2$  with coefficients from  $\mathbf{e}_1, \dots, \mathbf{e}_n$  and  $x_3, \dots, x_n$ . By induction, using that  $\deg(F_i) = i$  and  $x_i$  is a root of  $F_i$ , we can replace all occurrences of  $x_i^d$  for  $d \geq i$  by a polynomial of degree at most  $i - 1$  in  $x_i$  with coefficients from  $\mathbf{e}_1, \dots, \mathbf{e}_n$  and  $x_{i+1}, \dots, x_n$ . In this way, we can write any polynomial in the stated form.

Now, if  $f = f_1/f_2 \in L$  with  $f_1, f_2 \in k[\{x_i\}]$ , then setting  $g_2 = \prod_{\sigma \in S_n \setminus \{1\}} \sigma(f_2)$  we see that  $g_2 f_2$  is symmetric and  $f_1 g_2 \in k[\{x_i\}]$  can be written as a  $k[\{\mathbf{e}_i\}]$ -linear combination of the elements from  $\mathcal{M}$ . Since  $f = f_1 g_2 / f_2 g_2$ , we see that  $\mathcal{M}$  is a spanning set. Since  $|\mathcal{M}| = n!$  it must also be a basis.

Finally, if  $f \in k[\{x_i\}]$  is symmetric, then we can write it as a  $k[\{\mathbf{e}_i\}]$ -linear combination of the elements from  $\mathcal{M}$ . Since  $\mathcal{M}$  is a  $K$ -basis, we must have that  $f \in k[\{\mathbf{e}_i\}]$ .  $\square$

As an example, if  $n = 3$  and  $f = x_1^2 x_3 + x_3^3$ . We will be using the substitutions

$$\begin{aligned} x_1 &= \mathbf{e}_1 - x_2 - x_3 \\ x_2^2 &= -\mathbf{e}_2 + \mathbf{e}_1 x_2 + \mathbf{e}_1 x_3 - x_2 x_3 - x_3^2 \\ x_3^3 &= \mathbf{e}_3 - \mathbf{e}_2 x_3 + \mathbf{e}_1 x_3^2, \end{aligned}$$

found using  $F_1, F_2$  and  $F_3$ . We first replace all occurrences of  $x_1$  to get

$$f = \mathbf{e}_1^2 x_3 - 2\mathbf{e}_1 x_2 x_3 - 2\mathbf{e}_1 x_3^2 + x_2^2 x_3 + 2x_2 x_3^2 + x_2^3 + x_3^3.$$

We next replace all occurrences of  $x_2^2$  to get

$$f = -\mathbf{e}_1\mathbf{e}_2 + (\mathbf{e}_1^2 - \mathbf{e}_2)x_2 + 2\mathbf{e}_1^2x_3 - 2\mathbf{e}_1x_2x_3 - 3\mathbf{e}_1x_3^2 + x_2x_3^2 + x_3^3.$$

Finally we replace all occurrences of  $x_3^2$  to get

$$f = (\mathbf{e}_3 - \mathbf{e}_1\mathbf{e}_2) + (\mathbf{e}_1^2 - \mathbf{e}_2)x_2 + (2\mathbf{e}_1^2 - \mathbf{e}_2)x_3 - 2\mathbf{e}_1x_2x_3 - 2\mathbf{e}_1x_3^2 + x_2x_3^2.$$

We have therefore expressed  $f$  as a linear combination of the elements of  $\mathcal{M} = \{1, x_2, x_3, x_2x_3, x_3^2, x_2x_3^2\}$ , with coefficients in the polynomial ring  $k[\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3]$ .

Another classical problem involves the field  $L = k(x)$  with  $x$  transcendental over  $k$ . Consider the following six  $k$ -automorphisms of  $L$ :

$$f(x) \mapsto f(x), \quad f\left(\frac{1}{x}\right), \quad f(1-x), \quad f\left(\frac{1}{1-x}\right), \quad f\left(1 - \frac{1}{x}\right) = f\left(\frac{x-1}{x}\right), \quad f\left(\frac{x}{x-1}\right).$$

It is not hard to see that these six transformations form a group isomorphic to  $S_3$ . For, if  $\sigma(f(x)) = f(1 - \frac{1}{x})$ , then  $\sigma^2(f(x)) = f(1 - \frac{1}{1-1/x}) = f(\frac{1}{1-x})$  and  $\sigma^3 = \text{id}$ . Similarly, we can let  $\tau(f(x)) = f(\frac{1}{x})$ . Then  $\tau^2 = \text{id}$  and  $\tau\sigma = \sigma^2\tau: f(x) \mapsto f(\frac{x}{x-1})$ .

**Theorem 11.2.**  $L/L^{S_3}$  is a Galois extension with Galois group  $S_3$  and fixed field  $L^{S_3} = k(J)$ , where  $J = \frac{(x^2-x+1)^3}{x^2(x-1)^2}$ .

*Proof.* Since  $S_3$  is a finite group, we know that  $L/L^{S_3}$  is Galois with Galois group  $S_3$ , hence  $[L : L^{S_3}] = |S_3| = 6$ . On the other hand, it is not hard to check that the function  $J = \frac{(x^2-x+1)^3}{x^2(x-1)^2}$  lies in  $L^{S_3}$ . (We only need to check that  $\sigma(J) = J = \tau(J)$ .)

Set  $K = k(J) \subset L^{S_3}$ . Then  $L = K(x)$  and  $x$  is a root of the polynomial  $X^2(X-1)^2 - (X^2 - X + 1)^3 J \in K[X]$ , of degree 6. Thus  $[L : K] \leq 6$ . Since  $[L : L^{S_3}] = 6$  and  $K \subset L^{S_3}$ , it follows that  $L^{S_3} = K$ .  $\square$

In other words, the set of functions  $f$  for which

$$f(x) = f\left(\frac{1}{x}\right) = f(1-x) = f\left(\frac{1}{1-x}\right) = f\left(\frac{x-1}{x}\right) = f\left(\frac{x}{x-1}\right)$$

is precisely the field  $k(J)$  of functions in  $J$ .

This function  $J$  can be found in the study of elliptic curves. The Legendre normal form of an elliptic curve  $E$  is  $Y^2 = X(X-1)(X-\lambda)$  with  $\lambda \in \mathbb{C} \setminus \{0, 1\}$ , and two elliptic curves  $E, E'$  are isomorphic if and only if the numbers  $\lambda, \lambda'$  lie in the same  $S_3$ -orbit. Therefore, given an elliptic curve  $E$ , we define  $J(E) := J(\lambda)$ , and this parameterises the isomorphism classes of elliptic curves. (It is common to define  $j(E) := 2^8 J(E)$  and declare this to be the  $j$ -invariant of the elliptic curve  $E$ .)

Another instance where the  $J$ -invariant occurs is in the cross-ratio. Recall that the cross-ratio of four complex numbers  $(z_1, z_2, w_1, w_2)$  may be defined as

$$[z_1, z_2; w_1, w_2] := \frac{(z_1 - w_1)(z_2 - w_2)}{(z_1 - w_2)(z_2 - w_1)} \in \mathbb{C} \cup \{\infty\}.$$

However, different permutations may give different values. In fact, the symmetry group  $S_4$  acts on the quadruple  $(z_1, z_2, w_1, w_2)$  by place-permutation. Since

$$[z_1, z_2; w_1, w_2] = [z_2, z_1; w_2, w_1] = [w_1, w_2; z_1, z_2] = [w_2, w_1; z_2, z_1]$$

we see that the subgroup  $V$  acts trivially. Now  $V \triangleleft S_4$  is a normal subgroup, and the factor group is isomorphic to  $S_3$ . If we define  $\lambda := [z_1, z_2; w_1, w_2]$ , then

$$[z_1, w_1; z_2, w_2] = 1 - \frac{1}{\lambda} \quad \text{and} \quad [z_1, z_2; w_2, w_1] = \frac{1}{\lambda}.$$

This induces an action of  $S_3$  on the Riemann sphere  $\mathbb{P}^1\mathbb{C} = \mathbb{C} \cup \{\infty\}$ , analogous to the action of  $\text{Sym}_3$  on  $\mathbb{C}(X)$ . More precisely,  $\sigma(\lambda) := 1 - \frac{1}{\lambda}$  and  $\tau(\lambda) := \frac{1}{\lambda}$ . In fact, viewing  $\mathbb{C}(X)$  as the function field of  $\mathbb{P}^1\mathbb{C}$ , these two actions of  $\text{Sym}_3$  are dual to one another.

The Möbius group  $\text{PGL}_2(\mathbb{C})$  acts on  $\mathbb{P}^1\mathbb{C}$  via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) := \frac{az + b}{cz + d}.$$

This action is 3-transitive, since it can take any three distinct points to any other three distinct points. The action also preserves the cross-ratio of any four points. In particular, given any four distinct points  $(z_1, z_2, w_1, w_2)$ , there exists a unique Möbius transformation  $M$  taking these four points to  $(\lambda, 1, 0, \infty)$ , where  $\lambda = [z_1, z_2; w_1, w_2]$ . In fact, we take  $M(x) := [x, z_2; w_1, w_2]$ . This is used in the proof of the former result concerning elliptic curves.

For more interesting facts about cubics, elliptic curves and  $S_3$ , try [here](#).

## 11.2 Finite Fields

A finite field is a field with only finitely many elements. Examples include the fields  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$  for each prime number  $p$ . We begin with an easy lemma.

**Lemma 11.3.** *Let  $F$  be a finite field with  $q$  elements. Then*

1.  $\text{char}(F) = p > 0$  and  $F$  has prime subfield  $\mathbb{F}_p$ ;
2.  $q = p^n$  where  $n = [F : \mathbb{F}_p]$ ;
3.  $F^\times$  is a cyclic group of order  $q - 1$ .

*Proof.* The first part is clear, as is the second using a basis for  $F$  over  $\mathbb{F}_p$ . The third part was proved in Lemma 7.10.  $\square$

Let  $F$  be a finite field with  $q = p^n$  elements. Recall from Lemma 6.2 that the Frobenius homomorphism  $\text{Fr}(x) = x^p$  is a field automorphism of  $F$ . Moreover, since it fixes 1, it fixes every element of the prime subfield  $\mathbb{F}_p$ . Thus  $\text{Fr} \in \text{Gal}(F/\mathbb{F}_p)$ .

**Lemma 11.4.** *Let  $F$  be a finite extension of  $\mathbb{F}_p$  and let  $\text{Fr}$  be the Frobenius homomorphism.*

1. *For  $x \in F$ ,  $\text{Fr}^n(x) = x$  if and only if  $x$  is a root of  $X^{p^n} - X$ .*
2. *The polynomial  $X^{p^n} - X$  is separable and has  $p^n$  distinct roots in its splitting field extension.*
3. *Let  $G = \langle \text{Fr} \rangle \leq \text{Gal}(F/\mathbb{F}_p)$ . Then  $G$  is a finite cyclic group with fixed field  $\mathbb{F}_p$ .*

*Proof.* (1) This is clear, since  $\text{Fr}^n(x) = x^{p^n}$ .

(2) Suppose  $(X - x)^2 | f$  over its splitting field. Then  $X - x$  divides  $f' = -1$ , a contradiction. Thus  $f$  has  $p^n$  distinct roots in its splitting field extension.

(3) The Frobenius homomorphism is an automorphism of the finite set  $F$ , hence has finite order. Thus  $G = \langle \text{Fr} \rangle$  is a finite cyclic group. We know that  $\text{Fr}$  fixes  $\mathbb{F}_p$ . On the other hand,  $x \in F$  is fixed by  $\text{Fr}$  if and only if it is a root of  $X^p - X$ , which has at most  $p$  distinct roots in  $F$ . Thus the fixed field of  $\text{Fr}$  is precisely  $\mathbb{F}_p$ .  $\square$

**Theorem 11.5.** *Let  $p$  be a prime and  $n$  a positive integer. Then there exists a finite field  $F$  with  $p^n$  elements.*

*If  $F$  is any finite field with  $p^n$  elements, then*

1.  *$F/\mathbb{F}_p$  is Galois with cyclic Galois group generated by  $\text{Fr}$ .*
2. *Each element of  $F$  is a root of  $X^{p^n} - X$ . Thus  $F$  is the splitting field extension of  $X^{p^n} - X$ , so is unique up to isomorphism.*
3.  *$F/\mathbb{F}_p$  has an intermediate field  $E$  with  $p^r$  elements if and only if  $r|n$ , in which case  $E$  is the fixed field of  $\text{Fr}^r$ . In particular,  $F/E$  is Galois of degree  $n/r$  and with Galois group generated by  $\text{Fr}^r$ .*

*Proof.* Let  $F$  be the splitting field extension of  $X^{p^n} - X$  over  $\mathbb{F}_p$ . Since this polynomial is separable,  $F$  is a Galois extension of  $\mathbb{F}_p$ . Consider  $\text{Fr}^n \in \text{Gal}(F/\mathbb{F}_p)$ . By the Lemma, this has fixed field the set of roots of  $X^{p^n} - X$  in  $F$ , so equals  $F$ . Thus each element of  $F$  is a root of  $X^{p^n} - X$  and  $F$  has precisely  $p^n$  elements.

Now let  $F$  be any finite field with  $p^n$  elements.

(1) By the lemma,  $G := \langle \text{Fr} \rangle$  is a finite subgroup of  $\text{Gal}(F/\mathbb{F}_p)$  with fixed field  $\mathbb{F}_p$ . Hence by Theorem 7.2,  $F/\mathbb{F}_p$  is Galois with Galois group  $G$ .

(2) Since  $|\text{Gal}(F/\mathbb{F}_p)| = [F : \mathbb{F}_p] = n$ , we see that  $\text{Fr}$  has order  $n$ . Thus  $\text{Fr}^n(x) = x$  for all  $x \in F$ , so each element of  $F$  is a root of  $X^{p^n} - X$ . Since  $F$  has  $p^n$  elements and there are  $p^n$  distinct roots of  $X^{p^n} - X$ , we see that  $F$  is the splitting field of  $X^{p^n} - X$ .

(3) By the Galois Correspondence, the intermediate fields correspond to the subgroups of  $\text{Gal}(F/\mathbb{F}_p) = \langle \text{Fr} \rangle$ . These are of the form  $\langle \text{Fr}^r \rangle$  for  $r|n$ . Since  $\langle \text{Fr}^r \rangle$

has index  $r$  in the Galois group, its fixed field  $E$  has degree  $r$  over  $\mathbb{F}_p$ . Thus  $E$  has  $p^r$  elements, so  $F/E$  is Galois of degree  $n/r$ .  $\square$

We write  $\mathbb{F}_q$  for the finite field with  $q$  elements. If  $q = p^n$ , then we write  $\text{Fr}_q := \text{Fr}^n$ , so that  $\text{Fr}_q(x) = x^q$ . Thus the Galois group of  $\mathbb{F}_{q^r}/\mathbb{F}_q$  is generated by  $\text{Fr}_q$ .

**Corollary 11.6.** *Every finite extension of a finite field is Galois. If  $f \in \mathbb{F}_q[X]$  is irreducible of degree  $n$ , then  $\mathbb{F}_q[X]/(f) \cong \mathbb{F}_{q^n}$  and the roots of  $f$  are of the form  $\alpha^{q^r}$  for  $0 \leq r < n$ .*

*Proof.* Let  $f \in \mathbb{F}_q[X]$  be monic and irreducible of degree  $n$ . Then  $\mathbb{F}_q[X]/(f)$  is a degree  $n$  extension of  $\mathbb{F}_q$ , hence isomorphic to  $\mathbb{F}_{q^n}$ . Since  $\mathbb{F}_{q^n}$  is a Galois extension of  $\mathbb{F}_q$ , we have that  $f$  is separable and splits completely in  $\mathbb{F}_{q^n}$ . The Galois group is generated by  $\text{Fr}_q$ , and this acts transitively on the roots of  $f$  by Proposition 7.13. Since  $f$  has  $n$  roots and  $\text{Fr}_q$  has order  $n$ , the Frobenius map permutes the roots of  $f$  cyclically.  $\square$

**Proposition 11.7.** *Let  $q$  be a prime power. Over  $\mathbb{F}_q$  we have the factorisation*

$$X^{q^n} - X = \prod_{\substack{f \text{ monic, irred} \\ \deg(f) | n}} f.$$

*Proof.* We know that  $X^{p^n} - X$  factorises over  $\mathbb{F}_{q^n}$  as the product  $\prod_{\alpha \in \mathbb{F}_{q^n}} (X - \alpha)$ , and so has no repeated roots.

Let  $\alpha \in \mathbb{F}_{q^n}$ , say with minimal polynomial  $m$  over  $\mathbb{F}_q$ . Since  $\alpha$  is a root of  $X^{p^n} - X \in \mathbb{F}_q[X]$ , we see that  $m$  divides  $X^{p^n} - X$ . Also, the subfield  $\mathbb{F}_q(\alpha)$  of  $\mathbb{F}_{q^n}$  must be of the form  $\mathbb{F}_{q^r}$  for some  $r|n$ , so the minimal polynomial  $m$  of  $\alpha$  over  $\mathbb{F}_q$  has degree  $r$  dividing  $n$ .

Conversely, let  $f$  be any monic irreducible polynomial of degree  $r$  for  $r|n$ . We know that  $\mathbb{F}_q[X]/(f) \cong \mathbb{F}_{q^r}$ , which is a subfield of  $\mathbb{F}_{q^n}$ . Since  $f$  splits in  $\mathbb{F}_q[X]/(f)$ , it splits in  $\mathbb{F}_{q^n}$ . Hence every root of  $f$  is also a root of  $X^{p^n} - X$ , so that  $f$  divides  $X^{p^n} - X$ .

This shows that the irreducible factors of  $X^{p^n} - X$  over  $F_q$  are precisely the monic irreducible polynomials of degree dividing  $n$ . Since everything is monic, we have the result.  $\square$

This result is a generalisation of Wilson's Theorem.

For, consider the polynomial  $X^p - X$ . We have seen that the roots of this are precisely the elements of  $\mathbb{F}_p$ , so that

$$X^p - X = X(X + 1)(X + 2) \cdots (X + p - 1).$$

Equating coefficients of  $X$  we deduce Wilson's Theorem, that

$$(p - 1)! \equiv -1 \pmod{p}.$$

Define  $\varphi_d(q)$  to be the number of monic irreducible polynomials of degree  $d$  over  $\mathbb{F}_q$ . We can use the previous proposition to obtain a formula for  $\varphi_d(q)$ . This formula involves the Möbius function  $\mu(n)$ , defined as follows:

$$\mu(n) := \begin{cases} (-1)^r & \text{if } n = p_1 \cdots p_r \text{ is a product of distinct primes;} \\ 0 & \text{if } d^2 | n \text{ for some } d \geq 2. \end{cases}$$

We immediately see that  $\mu(1) = 1$ , that  $\mu(mn) = \mu(m)\mu(n)$  provided  $m$  and  $n$  are coprime (i.e.  $\mu$  is a multiplicative function) and that for a prime  $p$ ,

$$\mu(p^r) = \begin{cases} 1 & \text{if } r = 0; \\ -1 & \text{if } r = 1; \\ 0 & \text{if } r \geq 2. \end{cases}$$

The Möbius function satisfies the formula

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n \geq 2, \end{cases}$$

from which it follows that if we have functions  $f_n$  and  $g_n$  for all positive integers  $n$ , then

$$f_n = \sum_{d|n} g_d \quad \text{if and only if} \quad g_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) f_d.$$

**Proposition 11.8.**

$$\varphi_n(q) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

*Proof.* We have from the proposition that

$$X^{q^n} - X = \prod_{d|n} \prod_{\substack{f \text{ monic, irred} \\ \deg(f)=d}} f.$$

Comparing degrees, we deduce that

$$q^n = \sum_{d|n} d \varphi_d(q).$$

Inverting this formula (with  $f_n(q) = q^n$  and  $g_n(q) = n \varphi_n(q)$ ), we obtain that

$$n \varphi_n(q) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \sum_{d|n} \mu(d) q^{n/d}$$

as required. □

Examples. We know that  $\varphi_1(q) = q$ , and the irreducible polynomials of degree 1 over  $\mathbb{F}_q$  are just the linear polynomials  $X - \alpha$  for  $\alpha \in \mathbb{F}_q$ .

Next, we have

$$\varphi_2(q) = \frac{1}{2}(q^2 - q), \quad \varphi_3(q) = \frac{1}{3}(q^3 - q), \quad \varphi_4(q) = \frac{1}{4}(q^4 - q^2).$$

We can compute the irreducible polynomials over  $\mathbb{F}_2$  or  $\mathbb{F}_3$ , using the **Sieve of Erasthones**, but taking irreducible polynomials over a finite field instead of prime numbers in the integers. (That these methods work is due to the fact that both  $K[X]$  and  $\mathbb{Z}$  are principal ideal domains.)

We have the following irreducible polynomials over  $\mathbb{F}_2$ .

$$\begin{aligned} &X^2 + X + 1 \\ &X^3 + X + 1, \quad X^3 + X^2 + 1 \\ &X^4 + X + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1. \end{aligned}$$

Over  $\mathbb{F}_3$  we have three irreducible quadratics.

$$X^2 + 1, \quad X^2 + X - 1, \quad X^2 - X - 1.$$

Try and find the 8 irreducible cubics and the eighteen irreducible quartics yourselves.

## 11.3 The Normal Basis Theorem

The Normal Basis Theorem is due to Hensel (1888) in the case of finite fields, and Noether (1932) and Deuring (1933) for general Galois extensions. It states that for a Galois extension  $L/K$ , there is a  $K$ -basis of  $L$  given by a single orbit  $\{\sigma(\theta) : \sigma \in \text{Gal}(L/K)\}$  of the Galois group.

This basis has applications to cryptography, since it is easy to manipulate and is computationally very efficient.

**Theorem 11.9** (Normal Basis). *Let  $L/K$  be Galois. Then there exists an element  $\theta \in L$  such that the set  $\{\sigma(\theta) : \sigma \in \text{Gal}(L/K)\}$  is a  $K$ -basis for  $L$ , called a normal basis.*

We shall split the proof into two cases: when the field is infinite, or when the Galois group is cyclic (which includes all finite fields).

### 11.3.1 Proof for infinite fields

Recall that, for an irreducible polynomial  $f \in K[X]$  with roots  $\alpha_1, \dots, \alpha_n$ , we have the discriminant  $\Delta(f) := (-1)^{\binom{n}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j)$ . We can generalise this notion as follows.

Let  $L/K$  be a Galois extension with Galois group  $G = \{\sigma_1, \dots, \sigma_n\}$ . For  $\{\alpha_1, \dots, \alpha_n\} \subset L$  we define

$$\Delta(\alpha_1, \dots, \alpha_n) := \det(\mathrm{Tr}_K^L(\alpha_i \alpha_j)) \in K.$$

We observe that we can rewrite this as follows. Set

$$A := (\sigma_i(\alpha_j)) \in \mathbb{M}_n(L).$$

Then

$$A^t A = \left( \sum_i \sigma_i(\alpha_i \alpha_j) \right) = (\mathrm{Tr}_K^L(\alpha_i \alpha_j)) \in \mathbb{M}_n(K),$$

using that

$$\mathrm{Tr}_K^L = \sum_i \sigma_i,$$

as shown in Proposition 7.18. Therefore

$$\Delta(\alpha_1, \dots, \alpha_n) = \det(A)^2.$$

This definition generalises the discriminant for  $f$ . For, let  $L/K$  be the splitting field of  $f$  and let  $\alpha_1, \dots, \alpha_n$  be the roots of  $f$  in  $L$ . We may assume that the Galois group acts via  $\sigma_i(\alpha_1) = \alpha_i$ . Therefore, using the subset  $\{1, \alpha_1, \dots, \alpha_1^{n-1}\}$ , we obtain as above that

$$A := (\sigma_i(\alpha_1^{j-1})) = (\alpha_i^{j-1}).$$

This is a Van der Monde matrix, so

$$\det(A) = \prod_{i>j} (\alpha_i - \alpha_j), \quad \text{whence} \quad \Delta(1, \alpha_1, \dots, \alpha_1^{n-1}) = \det(A)^2 = \Delta(f).$$

**Proposition 11.10.** *Let  $L/K$  be Galois. Then  $\{\alpha_1, \dots, \alpha_n\}$  is a  $K$ -basis for  $L$  if and only if  $\Delta(\alpha_1, \dots, \alpha_n) \neq 0$ .*

*Proof.* Let  $\mathrm{Gal}(L/K) = \{\sigma_i\}$  and set  $A := (\sigma_i(\alpha_j))$  as before. Then  $A$  is non-singular if and only if  $\Delta(\alpha_1, \dots, \alpha_n) \neq 0$ .

Suppose first that  $A$  is singular. Then there exists  $\lambda_i \in L$  such that  $(\lambda_i)A = 0$ , or in other words,  $\sum_i \lambda_i \sigma_i(\alpha_j) = 0$  for all  $j$ . If the  $\alpha_j$  were a  $K$ -basis, then for any  $\theta \in L$  we could write  $\theta = \sum_j \mu_j \alpha_j$ . Then  $\sum_i \lambda_i \sigma_i(\theta) = 0$ , so that  $\sum_i \lambda_i \sigma_i = 0$ , contradicting the **Linear Independence of Characters**. Hence the  $\alpha_i$  do not form a  $K$ -basis of  $L$ .

Conversely, suppose that  $A$  is non-singular. Then the  $\alpha_i$  are linearly independent over  $K$ . For, if  $\sum_j \lambda_j \alpha_j = 0$  for some  $\lambda_j \in K$ , then applying  $\sigma_i$  yields that  $\sum_j \sigma_i(\alpha_j) \lambda_j = 0$  for all  $i$ . Therefore  $A(\lambda_i) = 0$ . Since  $A$  is non-singular, we deduce that  $\lambda_j = 0$  for all  $i$ .  $\square$

We can now prove the Normal Basis Theorem for infinite fields.

Let  $L/K$  be Galois with Galois group  $\text{Gal}(L/K) = \{\sigma_i\}$ . By the **Primitive Element Theorem**, we can write  $L = K(\alpha)$ . Set  $f \in K[X]$  to be the minimal polynomial of  $\alpha$ . Over  $L$  we have  $f = \prod_i (X - \sigma_i(\alpha))$ , by Proposition 7.18. For convenience we assume that  $\sigma_1 = \text{id}$  and  $\alpha_1 = \alpha$ , and write  $\alpha_i = \sigma_i(\alpha)$ .

The idea is now to use the Chinese Remainder Theorem to obtain

$$L[X]/(f) \cong L^n, \quad X \mapsto (\alpha_1, \dots, \alpha_n) \quad \text{where } n := \deg(f) = [L : K].$$

In particular, we have a complete set of pairwise orthogonal idempotents in  $L^n$  given by  $e_i$  having 1 in place  $i$  and 0 elsewhere.

More explicitly, set

$$g_i := \prod_{j \neq i} \frac{X - \alpha_j}{\alpha_i - \alpha_j}.$$

Then clearly  $g_i(\alpha_j) = 0$  for  $i \neq j$  and  $g_i(\alpha_i) = 1$  (so that  $g_i \mapsto e_i \in L^n$ ). Note also that  $\sigma_i(g_1) = g_i$ . Furthermore, if  $i \neq j$ , then each  $\alpha_i$  is a root of  $gh_i g_j$ , so  $f$  divides  $g_i g_j$  in  $L[X]$  (corresponding to  $e_i e_j = 0$  for  $i \neq j$  in  $L^n$ ). Finally, we have the polynomial identity  $\sum_i g_i = 1$  in  $L[X]$  (corresponding to  $1 = \sum_i e_i$  in  $L^n$ ). For, the left hand side is a polynomial of degree at most  $n - 1$ , and takes the value 1 at each  $\alpha_i$ ; therefore it is identically 1.

Thus, in  $L[X]$ , we have  $g_i g_j \equiv 0 \pmod{f}$  for  $i \neq j$ , and  $g_j = \sum_i g_i g_j \equiv g_j^2 \pmod{f}$ . From this we obtain that, in  $K[X]$ , we have  $\text{Tr}_K^L(g_i g_j) \equiv 0 \pmod{f}$  for  $i \neq j$  and  $\text{Tr}_K^L(g_i^2) \equiv \text{Tr}_K^L(g_i) = 1 \pmod{f}$ . This yields the polynomial identity

$$\Delta(g_i) = \det(\text{Tr}_K^L(g_i g_j)) \equiv 1 \pmod{f},$$

since the off-diagonal entries vanish, and the diagonal entries are all 1.

We can now define a polynomial  $h \in K[X]$  via  $h(X) = \Delta(g_i)$ . As a polynomial, this is non-zero, since it is congruent to 1 modulo  $f$ . Since  $K$  is an infinite field, there exists some  $\lambda \in K$  such that  $h(\lambda) \neq 0$  (and  $h(\lambda) = \Delta(g_i(\lambda))$ ). Setting  $\theta := g_1(\lambda)$ , we have  $g_i(\lambda) = \sigma_i(\theta)$ , and hence  $\Delta(\sigma_i(\theta)) = h(\lambda) \neq 0$ . By the previous Proposition, we deduce that  $\{\sigma_i(\theta)\}$  is a normal basis for  $L/K$ .

As a simple example, consider  $\mathbb{Q}(i)/\mathbb{Q}$ . Then  $f = X^2 + 1$ , and  $g_1 = \frac{1}{2i}(X + i)$  and  $g_2 = \frac{1}{2i}(X - i)$ . Hence

$$\text{Tr}(g_1^2) = -\frac{1}{4} \text{Tr}(X^2 + 2iX - 1) = -\frac{1}{2}(X^2 - 1) = 1 - \frac{1}{2}f.$$

Similarly

$$\text{Tr}(g_2^2) = 1 - \frac{1}{2}f \quad \text{and} \quad \text{Tr}(g_1 g_2) = \frac{1}{2}f,$$

so that

$$h(X) = \det(\text{Tr}(g_i g_j)) = 1 - f = X^2.$$

The result then says that  $\{g_1(\lambda), g_2(\lambda)\} = \{\frac{1}{2i}(\lambda + i), \frac{1}{2i}(\lambda - i)\}$  is a  $\mathbb{Q}$ -basis if and only if  $\lambda \neq 0$ .

### 11.3.2 Proof for cyclic Galois groups

Let  $\sigma \in \text{Gal}(L/K)$  be a generator for the Galois group. We observe that any normal basis for  $L/K$  is of the form  $\{\theta, \sigma(\theta), \dots, \sigma^{n-1}(\theta)\}$ , where  $n = [L : K]$ .

Recall that  $L$  is a  $K$ -vector space of dimension  $n$  and that  $\sigma$  is a  $K$ -linear endomorphism of  $L$ . In particular, we can talk about the characteristic polynomial  $\chi$  of  $\sigma$ , and also its minimal polynomial  $m$ . Clearly  $\sigma^n = 1$ , so that the minimal polynomial  $m$  divides  $X^n - 1$ . On the other hand, by the **Linear Independence of Characters**, we know that  $1, \sigma, \dots, \sigma^{n-1}$  are linearly independent, so that  $\sigma$  does not satisfy any polynomial relation of degree less than  $n$ . Since  $[L : K] = n$  we deduce that  $m = \chi = X^n - 1$ .

The normal basis theorem therefore follows from the a general result in linear algebra. Let  $V$  be a  $K$ -vector space of dimension  $n$  and let  $S \in \text{End}_K(V)$ . A cyclic vector for  $S$  is a vector  $v \in V$  such that  $\{v, S(v), \dots, S^{n-1}(v)\}$  is a  $K$ -basis of  $V$ .

**Theorem 11.11.** *The endomorphism  $S$  has a cyclic vector if and only if its minimal polynomial equals its characteristic polynomial.*

The proof of this is essentially a special case of the rational normal form for matrices. (The rational normal form is a generalisation of the Jordan normal form which works for arbitrary fields, not just algebraically closed fields.) Our approach will be via polynomials.

Let  $\chi = p_1^{r_1} \cdots p_s^{r_s}$  be the characteristic polynomial of  $S$ , where  $p_i \in K[X]$  are pairwise coprime, monic irreducible polynomials. Again, the Chinese Remainder Theorem tells us that

$$K[X]/(\chi) \cong K[X]/(p_1^{r_1}) \times \cdots \times K[X]/(p_s^{r_s}).$$

We again have a complete set of pairwise orthogonal idempotents  $e_i$  having 1 in the  $i$ -th factor and 0 elsewhere.

Explicitly, set

$$f_i := \prod_{j \neq i} p_j^{r_j} = m/p_i^{r_i}.$$

Then  $\gcd(f_1, \dots, f_s) = 1$ , so there exist  $g_i$  with  $\sum_i g_i f_i = 1$ . We observe that  $\chi$  divides  $f_i f_j$  for  $i \neq j$ . Hence  $f_j = \sum_i g_i f_i f_j \equiv g_j f_j^2 \pmod{\chi}$ , so that  $(g_i f_i)^2 \equiv g_i f_i \pmod{\chi}$ . In summary,

$$\tilde{P}_i := g_i f_i, \quad \tilde{P}_i \tilde{P}_j \equiv 0 \pmod{\chi} \text{ for } i \neq j, \quad \tilde{P}_i^2 \equiv \tilde{P}_i \pmod{\chi}.$$

(Thus  $\tilde{P}_i \mapsto e_i$ .)

Set  $P_i := \tilde{P}_i(S) = g_i(S) f_i(S)$ . By the Cayley-Hamilton Theorem, we know that  $\chi(S) = 0$  on  $V$ . Thus

$$P_i^2 = P_i, \quad P_i P_j = 0 \text{ for } i \neq j, \quad \text{and} \quad \sum_i P_i = \text{id}.$$

Using this we can write

$$V = \bigoplus_i V_i, \quad \text{where } V_i = \text{Im}(P_i).$$

For, we know that  $v = \sum_i P_i(v)$ . On the other hand, if  $P_i(v) = P_j(w)$  for some  $v, w \in V$  and some  $i \neq j$ , then  $P_j(w) = P_j^2(w) = P_j P_i(v) = 0$ . This shows that the sum is direct.

Note that  $V_i = \text{Ker}(p_i(S)^{r_i})$ , so that the  $V_i$  are generalised eigenspaces. For, if  $v = P_i(w) \in V_i$ , then since  $p_i^{r_i} f_i = \chi$ , we have  $p_i(S)^{r_i} P_i = 0$ , so  $v \in \text{Ker}(p_i(S)^{r_i})$ . Conversely, if  $p_i(S)^{r_i}(v) = 0$ , then writing  $v = \sum_j P_j(v)$  and using that  $p_i^{r_i}$  divides  $f_j$  for  $i \neq j$ , we see that  $P_j(v) = 0$  for all  $j \neq i$ . Hence  $v = P_i(v) \in V_i$ .

Next we note that each  $V_i$  is  $S$ -invariant; i.e. if  $v \in V_i$ , then  $S(v) \in V_i$ . For,  $P_i S = S P_i$ , which follows from the fact that  $P_i = g_i(S) f_i(S)$  is a polynomial in  $S$ . Therefore  $S$  can be represented as a block diagonal matrix  $S = \text{diag}(S_1, \dots, S_s)$ , where  $S_i$  represents the induced action of  $S$  on  $V_i$ .

We can now reduce to the case when  $V = V_i$  for some  $i$ . For, if  $v_i \in V_i$  is a cyclic vector for  $S_i$  for each  $i$ , then  $v = \sum_i v_i \in V$  is a cyclic vector for  $S$ . To see this, we just note that  $v_i = P_i(v) \in W := \text{Span}\{v, S(v), S^2(v), \dots\}$ . Thus  $V_i \leq W$  for each  $i$ , whence  $W = V$ . Also, the characteristic polynomial  $\chi_i$  of  $S_i$  on  $V_i$  is just  $p_i^{r_i}$ , whereas if the minimal polynomial of  $S$  equals  $m = p_1^{a_1} \cdots p_s^{a_s}$  with  $1 \leq a_i \leq r_i$ , then the minimal polynomial  $m_i$  of  $S_i$  equals  $m_i = p_i^{a_i}$ . So  $m = \chi$  if and only if  $a_i = r_i$  for all  $i$ , which is if and only if  $m_i = \chi_i$  for all  $i$ .

Therefore it is enough to prove the result when  $\chi = p^r$  for some monic irreducible polynomial  $p$ .

Suppose first that  $m \neq \chi$ . Then for each vector  $v \in V$  the subspace  $W := \text{Span}\{v, S(v), S^2(v), \dots\}$  has dimension at most  $\deg(m) < \deg(\chi) = \dim V$ . Therefore  $V$  cannot have a cyclic vector. (As a trivial example, think of  $S = \text{id}$ , which has minimal polynomial  $X - 1$  and characteristic polynomial  $(X - 1)^n$ . If  $n \geq 2$ , then  $S$  does not have a cyclic vector.)

Now suppose that  $m = \chi$ , and consider  $p^{r-1}$ . By definition,  $p(S)^{r-1} \neq 0$ , so there exists  $v \in V$  such that  $p(S)^{r-1}(v) \neq 0$ . We claim that such a vector is a cyclic vector for  $S$ . Again, set  $W := \text{Span}\{v, S(v), S^2(v), \dots\}$ . We know that  $W \leq V$  is an  $S$ -invariant subspace. It follows from the First Isomorphism Theorem that  $S$  induces an action on the quotient  $V/W$ . In particular, we can represent  $S$  as an upper-triangular block matrix

$$S = \begin{pmatrix} S_1 & S_3 \\ 0 & S_2 \end{pmatrix}, \quad \text{where } S_1 = S|_W \in \text{End}_K(W), \quad S_3 = \bar{S} \in \text{End}_K(V/W).$$

Therefore  $\chi = \chi_1 \chi_2$ , where  $\chi_i$  is the characteristic polynomial of  $S_i$ . (We have already mentioned this fact in the Remark following Theorem 3.5 about the norm and trace.) Since  $\chi = p^r$  is a power of an irreducible polynomial, we deduce that  $\chi_1 = p^a$  for some  $1 \leq a \leq r$ . By the Cayley-Hamilton Theorem once

more, we know that  $p(S)^a = 0$  on  $W$ , whereas by construction  $p(S)^{r-1}(v) \neq 0$ . Thus  $a \geq r$ , so that  $a = r$  and  $\dim W = \deg(p^r) = \dim V$ , so that  $V = W$ .

This completes the proof of Theorem 11.11, and hence the proof of the Normal Basis Theorem when the Galois group is cyclic.

# Appendix A

## Background

This is a summary of background material from Introductory Group Theory (MATH 1022) and Rings, Fields and Polynomials (MATH 2032), together with some topics which could (should) have been included.

### A.1 Groups

A **group**  $(G, \cdot, e)$  is a set  $G$  together with a group law  $\cdot : G \times G \rightarrow G$  and an element  $e \in G$  satisfying the following axioms:

$$\begin{array}{ll} \textbf{Associativity} & a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ for all } a, b, c \in G. \\ \textbf{Unit} & a \cdot e = a = e \cdot a \text{ for all } a \in G. \\ \textbf{Inverses} & \forall a \in G \exists a^{-1} \in G \text{ such that } a \cdot a^{-1} = e = a^{-1} \cdot a. \end{array}$$

We often write  $ab$  instead of  $a \cdot b$ .

A group is called **abelian**, or **commutative**, if  $ab = ba$  for all  $a, b \in G$ . In this case we sometimes write the group law additively,  $a + b$ , in which case the inverse of  $a$  is  $-a$  and the unit is  $0$ .

The **order**  $|G|$  of  $G$  is the number (possibly infinite) of elements of  $G$  as a set.

A **subgroup**  $H \leq G$  is a subset  $H \subset G$  such that

$$\begin{array}{ll} \textbf{Non-empty} & e \in H. \\ \textbf{Closure} & ab^{-1} \in H \text{ for all } a, b \in H. \end{array}$$

It follows that  $\cdot$  restricts to a group law  $H \times H \rightarrow H$  and that  $(H, \cdot, e)$  is again a group.

A **left coset** of  $H$  is a subset of the form  $aH := \{ah : h \in H\}$  for some  $a \in G$ . The **index**  $[G : H]$  of  $H$  in  $G$  is the number of distinct left (or right) cosets.

**Theorem A.1** (Lagrange). *Let  $H \leq G$  be a subgroup. Then any two left cosets*

of  $H$  are either disjoint or equal, and each such left coset is in bijection with  $H$  itself. In particular,  $[G : H] = |G|/|H|$ .

Let  $S \subset G$  be a subset of  $G$ . The smallest subgroup of  $G$  containing  $S$  is denoted  $\langle S \rangle$ , called the group **generated** by  $S$ . The elements of  $\langle S \rangle$  are finite products of elements from  $S \cup S^{-1}$ , where  $S^{-1} := \{a^{-1} : a \in S\}$ . A group is called **cyclic** if it is generated by a single element. The **order** of an element  $a$  is the order of the subgroup  $\langle a \rangle$ . Each cyclic group is abelian.

A subgroup  $N \leq G$  is called **normal** if  $aNa^{-1} = N$  (or equivalently  $aN = Na$ ) holds for all  $a \in G$ . We write  $N \triangleleft G$ . In this case we define a multiplication on the set  $G/N$  of cosets of  $N$  via  $(aN)(bN) := (ab)N$ . We sometimes write  $\bar{a}$  for the coset  $aN$ . Then  $(G/N, \cdot, \bar{e})$  is again a group, called the **factor group** of  $G$  by  $N$ .

Each subgroup of an abelian group is normal, and each factor group is again abelian.

### Examples.

1. The integers under addition form an abelian group  $(\mathbb{Z}, +, 0)$ . This is cyclic, generated by either 1 or  $-1$ . For each  $n \in \mathbb{Z}$  we have the cyclic subgroup  $\langle n \rangle = n\mathbb{Z} = \{\dots, -n, 0, n, 2n, \dots\}$ . The factor group  $\mathbb{Z}/n\mathbb{Z}$  has elements  $\bar{0}, \bar{1}, \dots, \overline{n-1}$ .
2. The non-zero complex numbers  $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$  under multiplication form an abelian group  $(\mathbb{C}^\times, \cdot, 1)$ . For each  $n$  we have the cyclic subgroup  $\mu_n := \langle \exp(2\pi i/n) \rangle = \{\exp(2\pi i k/n) : k \in \mathbb{Z}\}$ .
3. The set of symmetries of a geometric figure form a group with respect to composition. The subset of all rotations forms a normal subgroup. This fits nicely with the idea that conjugation  $g \mapsto aga^{-1}$  can be thought of as a **change of point of view**.

Let  $G$  and  $H$  be two groups. A **group homomorphism**  $f: H \rightarrow G$  is a map such that  $f(ab) = f(a)f(b)$  for all  $a, b \in H$ . Note that  $f(e_H) = e_G$  sends the unit of  $H$  to the unit of  $G$ . We call  $f$  a **group isomorphism** if there exists a group homomorphism  $g: G \rightarrow H$  such that  $fg = \text{id}_G$  and  $gf = \text{id}_H$ , which is if and only if  $f$  is bijective.

The **kernel** of  $f$  is  $\text{Ker}(f) := \{a \in H : f(a) = e_G\}$ ; it is a normal subgroup of  $H$ . The **image** of  $f$  is  $\text{Im}(f) := \{f(a) \in G : a \in H\}$ ; it is a subgroup of  $G$ .

**Lemma A.2.** 1. If  $H \leq G$  is a subgroup, then the inclusion map  $\iota_H: H \hookrightarrow G$  is an injective group homomorphism.

2. If  $N \triangleleft G$  is a normal subgroup, then the canonical map  $\pi_N: G \rightarrow G/N$ ,  $a \mapsto aN$ , is a surjective group homomorphism.

**Theorem A.3** (Isomorphism Theorems). 1. Let  $f: H \rightarrow G$  be a group homomorphism and  $N \triangleleft H$  a normal subgroup of  $H$ . If  $N \subset \text{Ker}(f)$ ,

then there exists a unique group homomorphism  $\bar{f}: H/N \rightarrow G$  such that  $f = \bar{f}\pi_N$ . In particular, there is a group isomorphism

$$H/\text{Ker}(f) \cong \text{Im}(f), \quad a \text{Ker}(f) \mapsto f(a).$$

2. Let  $N \triangleleft G$ . There exists a bijection between normal subgroups of  $G$  containing  $N$  and normal subgroups of  $G/N$ . If  $N \subset M \triangleleft G$ , then there is a group isomorphism

$$(G/N)/(M/N) \cong G/M.$$

3. Let  $H \leq G$  and  $N \triangleleft G$ . Then

$$HN := \{hn : h \in H, n \in N\}$$

is a subgroup of  $G$ . Moreover,  $N \triangleleft HN$  and  $H \cap N \triangleleft H$ , and there exists a group isomorphism

$$(HN)/N \cong H/(H \cap N).$$

### Example.

Let  $n \in \mathbb{Z}$  and consider the function  $f: \mathbb{Z} \rightarrow \mathbb{C}^\times$ ,  $k \mapsto \exp(2\pi ik/n)$ . This is a group homomorphism with kernel  $n\mathbb{Z}$  and image  $\mu_n$ . Thus there exists a group isomorphism  $\mathbb{Z}/n\mathbb{Z} \cong \mu_n$ . Note that the group law on the left is written additively, whereas it is written multiplicatively on the right.

Let  $X$  be a set. The **symmetry group**  $\text{Sym}(X)$  of  $X$  is the set of all bijections of  $X$ , with multiplication the usual composition of functions. In particular, when  $X = \{1, 2, \dots, n\}$  we write  $S_n$  for its symmetry group, also called the **permutation group** or **symmetric group**.

A  **$k$ -cycle** in  $S_n$  is a permutation of the form  $\sigma = (a_1 a_2 \cdots a_k)$ , denoting the function

$$a_i \mapsto a_{i+1} \text{ for } 1 \leq i < k, \quad a_k \mapsto a_1, \quad \text{all other elements fixed.}$$

A 2-cycle is also called a **transposition**. Every element of  $S_n$  can be written as a product of disjoint cycles, and every cycle can be written as a product of transpositions. In fact, it is enough to take transpositions of the form  $(i \ i+1)$ .

There is a group homomorphism  $\text{sgn}: S_n \rightarrow \mu_2 = \{\pm 1\}$ , called the **sign** map, sending each  $k$ -cycle to  $(-1)^{k-1}$ . The kernel of the sign map is a normal subgroup of  $S_n$ , denoted  $A_n$  and called the **alternating group**.

We say that a subgroup  $G \leq S_n$  is **transitive** if for all  $1 \leq i, j \leq n$  there exists some  $\sigma \in G$  such that  $\sigma(i) = j$ .

## A.2 Rings

A commutative, unital **ring**  $(R, +, \cdot, 0, 1)$  is a set  $R$  together with two operations  $+: R \times R \rightarrow R$  (addition) and  $\cdot: R \times R \rightarrow R$  (multiplication) together with two elements  $0, 1 \in R$  satisfying the following axioms:

**Addition**  $(R, +, 0)$  is an abelian group

**Multiplication** Multiplication is commutative, associative and has unit 1

**Distributivity**  $a \cdot (b + c) = a \cdot b + a \cdot c$

We will only consider commutative, unital rings, and we shall simply call them rings.

**Examples.**

1. The **integers**  $\mathbb{Z}$ , the **rational numbers**  $\mathbb{Q}$ , the **real numbers**  $\mathbb{R}$  and the **complex numbers**  $\mathbb{C}$  are all rings.
2. If  $R$  is a ring, then we can form the **polynomial ring**  $R[X]$ . Its elements are the polynomials  $f(X) = a_n X^n + \cdots + a_1 X + a_0$  with coefficients  $a_i \in R$ , on which we have the usual addition and multiplication. We write  $\deg(f) = \max\{n : a_n \neq 0\}$  if  $f \neq 0$ , and set  $\deg(0) := -\infty$ .
3. More generally, if  $\{X_i\}$  is a (possibly infinite) set of indeterminates, then  $R[\{X_i\}]$  is a ring whose elements are finite  $R$ -linear combinations of monomials, where each monomial is a finite product of powers of the  $X_i$ . We have  $R[\{X_1, \dots, X_n\}] \cong R[X_1][X_2] \cdots [X_n]$ .
4. If  $0 = 1$  in  $R$ , then  $R = \{0\}$ , called the **trivial ring**. For all other rings we have  $0 \neq 1$ .

We write  $R^\times := \{a \in R : \exists b \in R \text{ with } ab = 1\}$  for the set of **units** of a ring  $R$ . Note that  $(R^\times, \cdot, 1)$  is an abelian group.

A **field** is a non-trivial ring  $K$  with inverses, i.e. such that  $K^\times = K \setminus \{0\}$ .

An **integral domain** is a non-trivial ring  $R$  with no **zero-divisors**, i.e.  $ab = 0$  implies  $a = 0$  or  $b = 0$ . Equivalently,  $R$  has **cancellation**, so that if  $ax = bx$  with  $x \neq 0$ , then  $a = b$ .

**Examples.**

1.  $\mathbb{Q}$ ,  $\mathbb{R}$  and  $\mathbb{C}$  are all fields, and all fields are integral domains.
2.  $\mathbb{Z}$  is an integral domain but not a field.
3. If  $R$  is an integral domain, then so is the polynomial ring  $R[\{X_i\}]$ . By considering degrees of polynomials we obtain that the units of  $R[\{X_i\}]$  are just the units of  $R$ .
4.  $\mathbb{C} \times \mathbb{C}$  with component-wise addition and multiplication is a ring, with zero  $(0, 0)$  and unit  $(1, 1)$ , but is not an integral domain, since  $(1, 0)(0, 1) = (0, 0)$ .

If  $R$  is an integral domain, then we can form the **quotient field**, or **field of fractions**,  $\text{Quot}(R)$  of  $R$ . We first define an equivalence relation on  $R \times (R \setminus \{0\})$  by  $(x, y) \sim (x', y')$  if  $xy' = x'y$ . We denote the equivalence class of  $(x, y)$  by

$x/y$ . Thus  $x/y = x'/y'$  if and only if  $xy' = x'y$ . The set of all equivalence classes is denoted by  $\text{Quot}(R)$ . The ring structure is given via

$$a/b + x/y := (ay + bx)/by, \quad (a/b)(x/y) := (ax)/(by),$$

which is quickly checked to be well-defined. We identify  $R$  with the subring  $\{x/1 : x \in R\}$  of  $\text{Quot}(R)$ . In particular, the unit is  $1/1$  and the zero is  $0/1$ .

If  $A$  and  $B$  are subsets of a ring  $R$ , we write

$$A + B := \{a + b : a \in A, b \in B\} \quad \text{and} \quad AB := \{ab : a \in A, b \in B\}.$$

A (unital) **subring**  $S \leq R$  is an additive subgroup closed under multiplication and containing 1. Then  $(S, +, \cdot, 0, 1)$  is again a ring. If  $S$  is a subset of  $R$ , then it is a subring if and only if  $1 \in S$  and  $S + S, S^2 \subset S$ . The **prime subring** of  $R$  is the smallest subring of  $R$ .

An **ideal**  $I \triangleleft R$  is an additive subgroup closed under multiplication by elements of  $R$ ; that is,  $RI \subset I$ . Since  $I$  is an additive subgroup of  $R$ , we have the factor group  $R/I$  whose elements are the additive cosets  $\bar{a} = a + I$ . This is again an abelian group with zero  $\bar{0} = I$ . We define a multiplication on  $R/I$  via  $(a + I)(b + I) := (ab) + I$ , or  $\bar{a} \cdot \bar{b} := \overline{ab}$ . Then  $R/I$  is again a ring, with unit  $\bar{1}$ , called the **factor ring** of  $R$  by  $I$ .

**Examples.**

1.  $\text{Quot}(\mathbb{Z}) = \mathbb{Q}$ . If  $R$  is an integral domain, then  $R$  is a subring of  $\text{Quot}(R)$ .
2.  $\{0\}$  and  $R$  are ideals of  $R$ .
3.  $n\mathbb{Z}$  is an ideal of  $\mathbb{Z}$ , so that  $\mathbb{Z}/n\mathbb{Z}$  is again a ring.
4. Let  $I \triangleleft R$ . Write  $I[X]$  for the set of polynomials in  $R[X]$ , all of whose coefficients lie in  $I$ . Then  $I[X] \triangleleft R[X]$ .
5. Let  $S$  be a subset of a ring  $R$ . We write  $(S)$  for the smallest ideal containing  $S$ . Its elements are finite  $R$ -linear combinations of elements of  $S$ . If  $S = \{a_1, \dots, a_n\}$  is finite, we also write  $(S) = (a_1, \dots, a_n) = Ra_1 + \dots + Ra_n$ .

Let  $R$  and  $S$  be two rings. A (unital) **ring homomorphism**  $f: S \rightarrow R$  is a map preserving addition, multiplication and units; in other words,  $f$  is an additive group homomorphism such that  $f(1_S) = 1_R$  and  $f(ab) = f(a)f(b)$  for all  $a, b \in S$ . We call  $f$  a **ring isomorphism** if there exists a ring homomorphism  $g: R \rightarrow S$  such that  $fg = \text{id}_R$  and  $gf = \text{id}_S$ , which is if and only if  $f$  is bijective.

The **kernel** of  $f$  is  $\text{Ker}(f) := \{a \in S : f(a) = 0 \in R\}$ ; it is an ideal of  $S$ . The **image** of  $f$  is  $\text{Im}(f) := \{f(a) \in R : a \in S\}$ ; it is a subring of  $R$ .

**Lemma A.4.** 1. If  $S \leq R$  be a subring, then the inclusion  $\iota_S: S \hookrightarrow R$  is an injective ring homomorphism.

2. If  $I \triangleleft R$  be an ideal, then the canonical map  $\pi_I: R \rightarrow R/I, a \mapsto a + I$ , is a surjective ring homomorphism.

**Theorem A.5** (Isomorphism Theorems). 1. Let  $f: S \rightarrow R$  be a ring homomorphism and  $I \triangleleft S$  an ideal. If  $I \subset \text{Ker}(f)$ , then there exists a unique ring homomorphism  $\bar{f}: S/I \rightarrow R$  such that  $f = \bar{f}\pi_I$ . In particular, there exists a ring isomorphism

$$S/\text{Ker}(f) \cong \text{Im}(f), \quad a + \text{Ker}(f) \mapsto f(a).$$

2. Let  $I \triangleleft R$ . There exists a bijection between ideals of  $R$  containing  $I$  and ideals of  $R/I$ . If  $I \subset J \triangleleft R$ , then there is a ring isomorphism

$$(R/I)/(J/I) \cong R/J.$$

3. Let  $S \leq R$  be a subring and  $I \triangleleft R$  an ideal. Then  $S + I$  is a subring of  $R$ . Moreover,  $I \triangleleft (S + I)$  and  $(S \cap I) \triangleleft S$ , and there exists a ring isomorphism

$$(S + I)/I \cong S/(S \cap I).$$

### Examples.

1. Let  $I \triangleleft R$ , so that  $I[X] \triangleleft R[X]$ . There is a ring homomorphism  $R[X] \rightarrow (R/I)[X]$ ,  $aX^n \mapsto \bar{a}X^n$ . This is surjective with kernel  $I[X]$ . Thus there exists a ring isomorphism  $R[X]/I[X] \cong (R/I)[X]$ .
2. Let  $S \subset R$  be a subring and  $\alpha \in R$ . There exists a ring homomorphism  $\text{ev}_\alpha: S[X] \rightarrow R$ ,  $X \mapsto \alpha$ , called **evaluation** at  $\alpha$ . If  $f \in R[X]$ , we write  $f(\alpha)$  for  $\text{ev}_\alpha(f)$ . The image of  $\text{ev}_\alpha$  is denoted  $S[\alpha]$ , and is the smallest subring of  $R$  containing  $S$  and  $\alpha$ .

Let  $I \triangleleft R$ . We call  $I$

- proper** if  $I \neq R$ .
- trivial** if  $I = \{0\}$ .
- maximal** if  $I$  is proper, and  $I \subset J \triangleleft R$  implies  $J = I$  or  $J = R$ .
- prime** if  $xy \in I$  implies  $x \in I$  or  $y \in I$ .
- principal** if there exists  $x \in I$  such that  $I = (x) = Rx = \{rx : r \in R\}$ .

**Proposition A.6.** Let  $R$  be a ring and  $I \triangleleft R$  an ideal of  $R$ . Then

- (1)  $R/I$  is a field if and only if  $I$  is maximal.
- (1)'  $R$  is a field if and only if  $(0)$  and  $R$  are the only ideals of  $R$ .
- (2)  $R/I$  is an integral domain if and only if  $I$  is prime.
- (2)'  $R$  is an integral domain if and only if  $(0)$  is prime.
- (3)  $I$  maximal implies  $I$  prime.
- (3)'  $R$  a field implies  $R$  an integral domain.

**Lemma A.7.** *Let  $K$  be a field and  $R$  a non-trivial ring. Then every ring homomorphism  $f: K \rightarrow R$  is injective.*

*Proof.*  $\text{Ker}(f)$  is an ideal of  $K$ , so either  $(0)$  or  $K$  itself. If  $\text{Ker}(f) = (0)$ , then  $f$  is injective. If  $\text{Ker}(f) = K$ , then  $1_R = f(1_K) = 0_R$ , so that  $R$  is trivial.  $\square$

### A.3 Division and Factorisation

In a ring  $R$ , we say that  $a$  **divides**  $b$ , written  $a|b$ , if there exists  $x \in R$  such that  $b = ax$ . Equivalently,  $b \in (a)$ , or  $(b) \subset (a)$ . Note that 1 divides every other element, and each element divides 0.

If  $R$  is an integral domain, then  $a|b$  and  $b|a$  if and only if there exists a unit  $u \in R^\times$  such that  $b = au$ . For, there exist  $u, v \in R$  such that  $b = au$  and  $a = bv$ . If  $b = 0$  then  $a = 0$ . Otherwise, since  $b = buv$ , we have  $uv = 1$ , so that  $u, v \in R^\times$  are units.

A **principal ideal domain** is an integral domain  $R$  for which every ideal is generated by a single element, so of the form  $(a)$  for some  $a \in R$ .

**Proposition A.8.** *The ring of integers  $\mathbb{Z}$  is a principal ideal domain. In fact, the ideal generated by two integers  $a$  and  $b$  equals the ideal generated by their greatest common divisor  $d$ .*

*Proof.* Let  $I \triangleleft \mathbb{Z}$  be a non-zero ideal, and let  $b > 0$  be minimal such that  $b \in I$ . Let  $a \in I$ . By the Euclidean Algorithm, there exist integers  $q, r$  with  $b > r \geq 0$  such that  $a = qb + r$ . Now,  $r = a - qb \in I$ , so the minimality of  $b$  gives  $r = 0$ . Therefore  $b$  divides  $a$ , so  $a \in (b)$ . It follows that  $I = (b)$  is principal.  $\square$

Let  $R$  be a non-trivial ring. Then there exists a unique ring homomorphism  $f: \mathbb{Z} \rightarrow R$ . We define the **characteristic** of  $R$  to be  $\text{char}(R) := n$  where  $\text{Ker}(f) = (n)$  and  $n \geq 0$ .

**Proposition A.9.** *Let  $K$  be a field. Then the polynomial ring  $K[X]$  is a principal ideal domain.*

*Proof.* The argument is entirely analogous to that of the previous proposition. Let  $I \triangleleft K[X]$  be a non-zero ideal, and let  $g \in I$  be chosen such that  $\deg(g) \geq 0$  is minimal. Let  $f \in I$ . By the division algorithm, there exist polynomials  $q, r$  such that  $f = qg + r$  and  $\deg(g) > \deg(r)$ . Now,  $r = f - qg \in I$ , so the minimality of  $g$  gives  $\deg(r) = -\infty$ ; i.e.  $r = 0$ . Therefore  $g$  divides  $f$ , so  $f \in (g)$ . It follows that  $I = (g)$  is principal.  $\square$

Let  $R$  be an integral domain and  $a \in R$  a non-zero non-unit. We call  $a$

**prime** if  $a|xy$  implies  $a|x$  or  $a|y$ .  
**irreducible** if  $a = xy$  implies  $x$  is a unit or  $y$  is a unit.

**Proposition A.10.** *Let  $R$  be an integral domain and  $x \in R$  a non-zero non-unit.*

1.  $x$  is prime if and only if  $(x)$  is a prime ideal.
2.  $x$  prime implies  $x$  irreducible.
3. If  $R$  is a principal ideal domain, then  $x$  irreducible implies  $x$  prime. Moreover,  $(x)$  is maximal.

*Proof.* (1) Let  $x$  be prime and suppose that  $ab \in (x)$ . Then  $x|ab$ , whence  $x|a$  or  $x|b$ . In other words,  $a \in (x)$  or  $b \in (x)$ , so that  $(x)$  is a prime ideal. The converse is similar.

(2) Let  $x$  be prime and suppose that  $x = ab$ . Without loss of generality  $x|a$ , so that  $a = xy$  for some  $y$ . Now  $x = ab = xyb$ , whence  $1 = yb$  and  $b$  is a unit. Thus  $x$  is irreducible.

(3) Let  $R$  be a principal ideal domain and let  $x$  be irreducible. Suppose that  $ab \in (x)$ , say  $ab = xy$ . We need to show that  $a \in (x)$  or  $b \in (x)$ . The ideal  $(a, x) = (d)$  is principal, say  $d = ar + xs$ . Since  $d|x$  we have  $x = de$  for some  $e$ . Thus either  $e$  is a unit, in which case  $a \in (d) = (x)$  and we are done, or else  $d$  is a unit and we may assume that  $d = 1$ . Then  $ab = xy$  and  $1 = ar + xs$ , so

$$b = b(ar + xs) = abr + xbs = xyr + xbs = x(yr + bs).$$

Hence  $b \in (x)$  as required.

Suppose now that  $x$  is prime and consider  $(x) \subset (y) \subset R$ . Since  $y|x$ , we have  $x = ay$  for some  $a \in R$ . Since  $x$  is irreducible, either  $a$  is a unit, in which case  $(x) = (y)$ , or else  $y$  is a unit, in which case  $(y) = R$ . Thus  $(x)$  is maximal.  $\square$

An integral domain  $R$  is called a **unique factorisation domain** if

1. each non-zero non-unit  $a \in R$  can be written as a product of irreducibles  $a = x_1 \cdots x_m$ , and
2. this expression is essentially unique, so that if  $a = x_1 \cdots x_m$  and  $a = y_1 \cdots y_n$  with each  $x_i$  and  $y_j$  irreducible, then  $m = n$  and (after re-ordering)  $(x_i) = (y_i)$ . Equivalently, there exist units  $u_i \in R^\times$  such that  $y_i = u_i x_i$  for all  $i$ .

**Lemma A.11.** *Let  $R$  be a unique factorisation domain. Then  $x \in R$  is irreducible if and only if  $x$  is prime.*

*Proof.* We already know that prime implies irreducible, so let  $x$  be irreducible and suppose that  $ab \in (x)$ , hence  $ab = xy$  for some  $y \in R$ . Since  $x$  is irreducible and factorisations are unique,  $x$  must occur in the factorisation of either  $a$  or  $b$ , whence  $a \in (x)$  or  $b \in (x)$ .  $\square$

**Theorem A.12.** *Every principal ideal domain is a unique factorisation domain.*

*Proof.* Let  $R$  be a principal ideal domain. We first show that every non-zero non-unit can be expressed as a product of irreducible elements.

Suppose we have an increasing sequence of ideals  $I_1 \subset I_2 \subset \dots$ . Then the union  $I := \bigcup_i I_i$  is again an ideal. Now, each ideal in  $R$  is principal, so we can write  $I_i = (a_i)$  and  $I = (a)$ . Now,  $a \in \bigcup_i I_i$ , so  $a \in I_i$  for some  $i$ . Therefore  $I \subset I_i$ , so  $I = I_i = I_{i+1} = \dots$ . [This says that every increasing sequence of ideals stabilises, so that  $R$  is Noetherian.]

Now, suppose for contradiction that  $a_1 \in R$  cannot be written as a product of irreducibles. Since  $a_1$  is not irreducible, we can write  $a_1 = a_2 a'_2$  with both  $a_2$  and  $a'_2$  non-zero non-units. If both  $a_2$  and  $a'_2$  can be expressed as a product of irreducibles, then the same would be true of  $a_1$ , so we may assume that  $a_2$  cannot be written as a product of irreducibles. Repeating the argument yields an increasing sequence of ideals  $(a_1) \subset (a_2) \subset \dots$ . Also, by construction,  $(a_{i-1}) \neq (a_i)$ , since  $a_{i-1} = a_i a'_i$  and  $a'_i$  is not a unit. Therefore this sequence of ideals does not stabilise, contradicting the above result.

To see that this expression is unique, let  $a = x_1 \cdots x_m = y_1 \cdots y_n$  with each  $x_i$  and  $y_j$  irreducible. Since  $(x_1)$  is a prime ideal (in fact maximal),  $R/(x_1)$  is an integral domain (in fact a field) and  $\bar{y}_1 \cdots \bar{y}_n = \bar{a} = 0$  in  $R/(x_1)$ . Thus, after re-ordering,  $\bar{y}_1 = 0$ . Hence  $y_1 \in (x_1)$ , say  $y_1 = x_1 u_1$ . Since both  $x_1$  and  $y_1$  are irreducible,  $u_1$  must be a unit. Therefore  $(x_1) = (y_1)$  and  $x_2 \cdots x_m = u_1 y_2 \cdots y_n$ . Since  $y'_2 := u_1 y_2$  is irreducible and  $(y'_2) = (y_2)$ , the result follows by induction on  $m + n$ .  $\square$

[In fact, if  $R$  is a Noetherian integral domain, then  $R$  is a unique factorisation domain if and only if all irreducible elements are prime. The proof is the same, but using the Noetherian property to deduce that the ascending chain of ideals stabilises.]

**Lemma A.13.** *Let  $\alpha \in K$ . Then the kernel of the evaluation map  $\text{ev}_\alpha: K[X] \rightarrow K$  is the ideal  $(X - \alpha)$ . In particular,  $\alpha$  is a root of a polynomial  $f$  if and only if  $X - \alpha$  divides  $f$ , and  $f$  has at most  $\deg(f)$  distinct roots in  $K$ .*

*Proof.* Let  $I = \text{Ker}(\text{ev}_\alpha)$ . Then  $(X - \alpha) \subset I$ , and  $(X - \alpha)$  is a maximal ideal by Lemma A.10. Since  $I$  is a proper ideal, we must have  $I = (X - \alpha)$ .

Now,  $\alpha$  is a root of a polynomial  $f$  if and only if  $0 = f(\alpha) = \text{ev}_\alpha(f)$ , which is if and only if  $f \in \text{Ker}(\text{ev}_\alpha) = (X - \alpha)$ , which is if and only if  $X - \alpha$  divides  $f$ .

If  $\alpha_1, \dots, \alpha_n$  are distinct roots of  $f$ , then each  $X - \alpha_i$  divides  $f$ , and since  $K[X]$  is a unique factorisation domain, we must have that  $\prod_i (X - \alpha_i)$  divides  $f$ . Hence  $\deg(f) \geq n$ .  $\square$

Let  $R$  be a unique factorisation domain. We define a **greatest common divisor** of two elements  $a, b \in R$  to be an element  $d = \text{gcd}(a, b) \in R$  such that

1.  $d$  is a divisor of  $a$  and  $b$ , i.e.  $d|a$  and  $d|b$ , and
2. if  $e$  is another divisor of  $a$  and  $b$ , then  $e|d$ .

**Proposition A.14.** *Let  $R$  be a unique factorisation domain. For  $a, b \in R$ , the greatest common divisor  $\gcd(a, b)$  exists and is unique up to a unit of  $R$ .*

*Proof.* Write  $ab = up_1^{s_1} \cdots p_r^{s_r}$  with  $u$  a unit and the  $p_i$  distinct irreducible elements, so  $(p_i) \neq (p_j)$  for  $i \neq j$ . Then we can write  $a = u'p_1^{m_1} \cdots p_r^{m_r}$  and  $b = u''p_1^{n_1} \cdots p_r^{n_r}$  for some units  $u', u''$ . Observe that  $s_i = m_i + n_i$  and  $u = u'u''$ . Define  $d := p_1^{t_1} \cdots p_r^{t_r}$  where  $t_i := \min(m_i, n_i)$ . Clearly  $d$  is a divisor of  $a$  and  $b$ . Now let  $e$  be a divisor of  $a$  and  $b$ . Then  $e$  is a divisor of  $ab$ , so by unique factorisation is of the form  $vp_1^{t'_1} \cdots p_r^{t'_r}$  for some unit  $v$  and some  $t'_i$ . Since  $e$  divides  $a$  we have  $t'_i \leq m_i$ , and since  $e$  divides  $b$  we have  $t'_i \leq n_i$ . Thus  $t'_i \leq t_i$  for all  $i$ , whence  $e$  is a divisor of  $d$ .  $\square$

Let  $R$  be a unique factorisation domain and consider a non-zero polynomial  $f = a_n X^n + \cdots + a_0 \in R[X]$ . We define the **content**  $\text{cont}(f)$  of  $f$  to be the greatest common divisor of the coefficients  $a_i$ . We call  $f$  **primitive** if  $\text{cont}(f)$  is a unit. Note that, if  $0 \neq d \in R$ , then  $\text{cont}(df) = d \cdot \text{cont}(f)$ .

More generally, let  $K = \text{Quot}(R)$  and let  $0 \neq f \in K[X]$ . By clearing denominators, there exists  $0 \neq d \in R$  such that  $df \in R[X]$ . We therefore define  $\text{cont}(f) := \text{cont}(df)/d \in K$ . To see that this is well-defined (up to a unit of  $R$ ) let  $0 \neq d' \in R^\times$  also satisfy  $d'f \in R[X]$ . Then

$$d' \cdot \text{cont}(df) = \text{cont}(d'df) = d' \cdot \text{cont}(d'f),$$

so that  $\text{cont}(df)/d = \text{cont}(d'f)/d'$ . It follows as before that if  $d \in K^\times$  and  $f \in K[X]$ , then  $\text{cont}(df) = d \cdot \text{cont}(f)$ .

**Lemma A.15.** *Let  $R$  be a unique factorisation domain with quotient field  $K$ . Then for  $f \in K[X]$  we have*

1.  $f/\text{cont}(f) \in R[X]$  and is primitive. Conversely, if  $c \in K^\times$  is such that  $f/c \in R[X]$  is primitive, then  $c = \text{cont}(f)$  (up to a unit of  $R$ ).
2.  $\text{cont}(f) \in R$  if and only if  $f \in R[X]$ .

*Proof.* (1) If  $f \in R[X]$ , then it is clear from the definitions that  $f/\text{cont}(f) \in R[X]$  is primitive. If  $f \in K[X]$ , take  $0 \neq d \in R$  such that  $df \in R[X]$ . Then  $f/\text{cont}(f) = df/\text{cont}(df) \in R[X]$  is primitive. Finally, let  $c \in K^\times$  be such that  $f/c \in R[X]$  is primitive. Then  $1 = \text{cont}(f/c) = \text{cont}(f)/c$ , so that  $c = \text{cont}(f)$ . (2) If  $c := \text{cont}(f) \in R$ , then  $f = c \cdot f/c \in R[X]$ . The converse is clear.  $\square$

**Lemma A.16** (Gauss' Lemma). *Let  $R$  be a unique factorisation domain with quotient field  $K$ .*

1. If  $f, g \in K[X]$ , then  $\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$ .
2. If  $f \in R[X]$  is irreducible over  $R$ , then it is irreducible over  $K$ .
3. The converse holds provided that  $f$  is primitive.

*Proof.* (1) Write  $f = cf'$  and  $g = dg'$  with  $f', g' \in R[X]$  primitive and  $c, d \in K^\times$ . Then  $fg = cdf'g'$ , so if we can show that  $f'g'$  is primitive, then  $\text{cont}(fg) = cd = \text{cont}(f)\text{cont}(g)$  as required.

Let  $p \in R$  be prime and consider the factor ring  $R[X]/pR[X] \cong (R/pR)[X]$ . Since  $R/pR$  is an integral domain, so is  $(R/pR)[X]$ . If  $p|\text{cont}(f'g')$ , then  $\overline{f'g'} = 0$  in  $(R/pR)[X]$ . Since  $\overline{f'g'} = \overline{f'} \cdot \overline{g'}$ , we must have that either  $\overline{f'} = 0$  or  $\overline{g'} = 0$ , whence  $p|\text{cont}(f')$  or  $p|\text{cont}(g')$ . Since both  $f'$  and  $g'$  are primitive, this cannot happen. Therefore  $\text{cont}(f'g')$  is not divisible by any irreducible element of  $R$ , hence is a unit. Thus  $f'g'$  is primitive.

(2) We prove the contrapositive. Suppose  $f = gh \in K[X]$ . Since  $\text{cont}(f) = \text{cont}(gh) = \text{cont}(g)\text{cont}(h)$  by (1), we can factorise  $f$  over  $R$  as

$$f = \text{cont}(f) \cdot (g/\text{cont}(g)) \cdot (h/\text{cont}(h)).$$

(3) Let  $f \in R[X]$  be primitive and suppose that  $f$  is irreducible over  $K$ . Let  $f = gh$  be a factorisation over  $R$ . Since  $\text{cont}(f) = 1$ , we see that  $\text{cont}(g)$  and  $\text{cont}(h)$  are units in  $R$ , so  $g$  and  $h$  are primitive. Since  $f$  is irreducible over  $K$  we may assume without loss of generality that  $g$  is a unit in  $K[X]$ , so  $\deg(g) = 0$ . Therefore  $g = \text{cont}(g) \in R^\times$  is a unit, so  $f$  is irreducible over  $R$ .  $\square$

**Theorem A.17.** *Let  $R$  be a unique factorisation domain. Then the polynomial ring  $R[X]$  is again a unique factorisation domain. The units of  $R[X]$  are the units of  $R$ . The irreducible elements of  $R[X]$  are the irreducible elements of  $R$  together with the primitive irreducible polynomials.*

*Proof.* We have already observed that when  $R$  is an integral domain then so is  $R[X]$ , and the units of  $R[X]$  are just the units of  $R$ . By considering degrees it is clear that each irreducible in  $R$  remains irreducible in  $R[X]$ . Finally, by Gauss' Lemma, a primitive polynomial  $f \in R[X]$  is irreducible over  $R$  if and only if it is irreducible over  $K = \text{Quot}(R)$

Let  $f \in R[X]$ . Since  $K[X]$  is a principal ideal domain, it is a unique factorisation domain, so we can write  $f = g_1 \cdots g_r$  with each  $g_i$  irreducible in  $K[X]$ . Set  $c_i := \text{cont}(g_i)$  and  $f_i := g_i/c_i \in R[X]$ , so  $f_i$  is primitive and irreducible over  $R$ . Then  $f = cf_1 \cdots f_r$  where  $c = c_1 \cdots c_r = \text{cont}(f)$  by Gauss' Lemma. Since  $R$  is a unique factorisation domain, we can write  $c$  as a product of irreducibles in  $R$ . Thus each polynomial can be written as a product of irreducible elements.

To see that this expression is unique, suppose that  $f = cg_1 \cdots g_r$  and  $f = dh_1 \cdots h_s$  with  $c, d \in R \setminus \{0\}$  and  $g_i, h_j \in R[X]$  primitive irreducible polynomials. In the principal ideal domain  $K[X]$  we have that  $c, d \in K^\times$  and, after reordering,  $r = s$  and  $g_i = u_i h_i$  for some  $u_i \in K^\times$ . Since  $g_i$  and  $h_i$  are primitive,  $u_i = \text{cont}(g_i) \in R^\times$ . Setting  $u := u_1 \cdots u_r \in R^\times$ , we have that

$$dh_1 \cdots h_r = cg_1 \cdots g_r = cuh_1 \cdots h_r.$$

Since  $R[X]$  is an integral domain,  $d = cu$ . Since  $R$  is a unique factorisation domain, we are done.  $\square$

**Examples.**

1.  $\mathbb{Z}$ ,  $\mathbb{Z}[X]$ ,  $\mathbb{Z}[X, Y]$  are all unique factorisation domains, but only  $\mathbb{Z}$  is a principal ideal domain. For example, the ideal  $(2, X) \triangleleft \mathbb{Z}[X]$  is not principal.
2.  $K$ ,  $K[X]$ ,  $K[X, Y]$  for  $K$  a field are all unique factorisation domains, but only  $K$  and  $K[X]$  are principal ideal domains. For example,  $(X, Y) \triangleleft K[X, Y]$  is not principal.
3.  $\mathbb{Z}[\sqrt{-2}]$  is a principal ideal domain, in fact a Euclidean domain (there is a version of the Euclidean Algorithm). The units of  $\mathbb{Z}[\sqrt{-2}]$  are the elements  $a + b\sqrt{-2}$  such that  $a^2 + 2b^2 = 1$ , so just  $\pm 1$ .
4.  $\mathbb{Z}[\sqrt{-5}]$  is not a unique factorisation domain, since  $1 + \sqrt{-5}$  is irreducible but not prime.
5. Let  $R$  be a unique factorisation domain. A polynomial  $f \in R[X]$  is called monic if its leading coefficient is 1. All monic polynomials are primitive.

**Theorem A.18** (Eisenstein's Criterion). *Let  $R$  be a unique factorisation domain and let  $f = a_0X^d + \cdots + a_{d-1}X + a_d \in R[X]$  be primitive. Suppose that there exists a prime  $p \in R$  such that  $p|a_i$  for  $1 \leq i \leq d$ , but  $p \nmid a_0$  and  $p^2 \nmid a_d$ . Then  $f$  is irreducible.*

*Proof.* Suppose that  $f = gh$  for some  $g, h \in R[X]$  non-units. Write  $g = b_0X^r + \cdots + b_r$  and  $h = c_0X^s + \cdots + c_s$ , so that  $d = r + s$ ,  $a_0 = b_0c_0$  and  $a_d = b_rc_s$ . Moreover, since  $f$  is primitive,  $g$  and  $h$  must be non-constant, so  $r, s \geq 1$ . Consider  $\bar{g}\bar{h} = \bar{f} = \bar{a}_0X^d \in (R/pR)[X]$ . Since  $(R/pR)[X]$  is a unique factorisation domain, it follows that  $\bar{g} = \bar{b}_0X^r$  and  $\bar{h} = \bar{c}_0X^s$ , so  $p|b_i$  for all  $1 \leq i \leq r$  and  $p|c_j$  for all  $1 \leq j \leq s$ . In particular,  $p^2|b_rc_s = a_d$ , a contradiction.  $\square$

**Theorem A.19** (Rational Root Test). *Let  $R$  be a unique factorisation domain,  $K = \text{Quot}(R)$  and  $f = a_0X^d + \cdots + a_d \in R[X]$ . If  $\alpha = p/q \in K$  is a root of  $f$  such that  $\gcd(p, q) = 1$ , then  $q|a_0$  and  $p|a_d$ .*

*Proof.* We have the equality

$$0 = q^d f(p/q) = a_0p^d + a_1p^{d-1}q + \cdots + a_{d-1}pq^{d-1} + a_dq^d.$$

Thus  $p|a_dq^d$  and  $q|a_0p^d$ . By unique factorisation, using that  $\gcd(p, q) = 1$ , we deduce that  $p|a_d$  and  $q|a_0$ .  $\square$

This theorem is often used in the following form.

**Corollary A.20.** *Let  $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$  be a monic polynomial. Then any root  $\alpha \in K$  of  $f$  actually lies in  $R$  and is a divisor of  $a_0$ .*

## Appendix B

# Zorn's Lemma and Applications

This chapter is non-examinable.

A **partially ordered set**, or **poset**,  $(S, \leq)$  is a set with a relation  $\leq$  satisfying

<b>Reflexivity</b>	$a \leq a$ for all $a$ .
<b>Antisymmetry</b>	$a \leq b$ and $b \leq a$ imply $a = b$ .
<b>Transitivity</b>	$a \leq b$ and $b \leq c$ imply $a \leq c$ .

The poset  $(S, \leq)$  is **totally ordered** if, for all  $a, b \in S$ , either  $a \leq b$  or  $b \leq a$ . A **maximal element** of  $S$  is an element  $a \in S$  such that if  $a \leq b$ , then  $a = b$ .

If  $(S, \leq)$  is a poset, then a **chain** in  $S$  is a non-empty subset which is totally ordered by  $\leq$ . If  $C \subset S$  is a subset, then an **upper bound** for  $C$  is an element  $a \in S$  such that  $c \leq a$  for all  $c \in C$ .

**Zorn's Lemma.** Let  $(S, \leq)$  be a non-empty poset in which every chain has an upper bound. Then  $S$  has a maximal element.

Zorn's Lemma is logically equivalent in [Zermelo-Fraenkel Set Theory](#) to the **Axiom of Choice**, which says that if  $S_i$  are sets, then the product  $\prod_i S_i$  is non-empty. In other words, we can make an infinite number of arbitrary choices. We often use Zorn's Lemma when proving statements for infinite sets when we would have used induction for finite sets.

Typical examples are the following three results, the first of which uses the Axiom of Choice; the latter two, Zorn's Lemma.

**Theorem B.1.** *Every surjective map between sets has a right inverse.*

*Proof.* Let  $f: X \rightarrow Y$  be a surjective map between two sets. A right inverse  $g$  of  $f$  is a map  $g: Y \rightarrow X$  such that  $fg = \text{id}_Y$ . Therefore, to construct  $g$ , we need to choose an element in the fibre  $f^{-1}(y) \subset X$  for each element  $y \in Y$ . Thus,

if  $Y$  is infinite, we need to make an infinite number of arbitrary choices, hence require the Axiom of Choice.  $\square$

**Theorem B.2.** *Every vector space has a basis.*

*Proof.* Let  $S$  be the collection of linearly independent subsets of a non-zero vector space  $V$  over a field  $K$ . This is non-empty, since each non-zero vector is linearly independent. We endow  $S$  with the partial order  $\subset$  coming from inclusion.

Let  $C = \{B_i\}$  be a chain in  $S$ . Then  $C$  has an upper bound, namely the union  $B = \bigcup_i B_i$ . For, consider a finite linear relation  $\sum_j \lambda_j b_j = 0$  with  $\lambda_j \in K$  and  $b_j \in B$ . Since there are only finitely many  $b_j$  in this relation, they all lie in some  $B_i$ , so are linearly independent. Thus  $\lambda_j = 0$  for all  $j$  and  $B$  is linearly independent.

Zorn's Lemma implies that  $S$  has a maximal element  $B$ . We claim that  $B$  is a spanning set for  $V$ , and thus a basis. For, if not, then there exists some  $v \in V$  which cannot be written as a finite linear combination of elements of  $B$ . Thus  $B \cup \{v\}$  is a linearly independent set, which contradicts the maximality of  $B$ .  $\square$

**Theorem B.3.** *Every proper ideal of a ring is contained in a maximal ideal.*

*Proof.* Let  $R$  be a ring. Let  $S$  be the set of proper ideals of  $R$ , ordered by inclusion  $\subset$ . This is non-empty, since  $(0) \triangleleft R$ . Let  $C = \{I_i\}$  be a chain in  $S$ . Then  $I = \bigcup_i I_i$  is an upper bound for  $C$ . We need to check that  $I$  is a proper ideal. It is an ideal, since if  $x, y \in I$ , then  $x, y \in I_i$  for some  $i$ . Hence  $x + y$  and  $rx$  for  $r \in R$  are both contained in  $I_i \subset I$ . To see that  $I$  is proper, suppose otherwise. Then we can write  $1 = \sum_j r_j x_j$  as a finite linear combination with  $r_j \in R$  and  $x_j \in I$ . Since there are only finitely many  $x_j$  in this relation, they all lie in some  $I_i$ . Hence  $1 \in I_i$ , a contradiction since  $I_i$  was assumed to be proper. Hence  $I \triangleleft R$  is proper.

Zorn's Lemma implies that  $S$  has a maximal element  $I$ , which is necessarily a maximal ideal.  $\square$

One should remark that, although generally assumed to hold, Zorn's Lemma, or equivalently the Axiom of Choice, also yield several 'paradoxes', for example the [Banach-Tarski Paradox](#).

For some nice quotations on the Axiom of Choice, visit [here](#).

## Appendix C

# Algebraically Closed Fields

This chapter is non-examinable, and is included only for completeness.

A field  $L$  is called *algebraically closed* if every non-constant polynomial  $f$  has a root in  $L$ . In other words, the only irreducible polynomials are those of degree one.

**Proposition C.1** (Existence of Algebraically Closed Fields). *Let  $K$  be a field. Then there exists an extension  $L/K$  with  $L$  algebraically closed.*

*Proof.* Set  $K_0 := K$ . We define  $K_n$  inductively such that  $K_{n+1}/K_n$  is a field extension and every polynomial in  $K_n[X]$  has a root in  $K_{n+1}$ . We proceed as follows. For each non-constant polynomial  $f$  we take an indeterminate  $X_f$  (in fact it suffices to take monic irreducible polynomials). We form the polynomial ring  $R := K_n[\{X_f : f \in K_n[X] \setminus K_n\}]$  and consider the ideal  $I$  generated by  $f(X_f)$ .

We claim that  $I$  is a proper ideal. If not, then there exists an expression  $g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1$  for some distinct polynomials  $f_i$ . The product  $g_1 \cdots g_n$  uses only finitely many variables, which we denote  $X_1, \dots, X_m$  with the convention that  $X_i = X_{f_i}$  for  $1 \leq i \leq n$ . Thus  $\sum_{i=1}^n g_i(X_1, \dots, X_m) f_i(X_i) = 1$ .

Let  $E/K_n$  be a finite extension in which each  $f_i$  has a root, say  $f_i(\alpha_i) = 0$ . Set  $\alpha_i = 0$  for  $n < i \leq m$ . Then, on substituting  $\alpha_i$  for  $X_i$  we obtain  $1 = \sum_i g_i(\alpha_1, \dots, \alpha_m) f_i(\alpha_i) = 0$  in  $E$ , a contradiction. Thus  $I$  is a proper ideal and the claim is proved.

By Zorn's Lemma (see Appendix B), every proper ideal is contained in a maximal ideal, so we can take  $I \subset M$  with  $M \triangleleft R_n$  maximal. We define  $K_{n+1} := R/M$ . The composition  $K_n \rightarrow R \rightarrow K_{n+1}$  is non-zero, so  $K_{n+1}/K_n$  is a field extension. Moreover, by construction, every non-constant polynomial  $f \in K_n[X]$  has a root in  $K_{n+1}$ , namely the element  $X_f + M$ .

In this way we obtain a chain of fields

$$K_0 \subset K_1 \subset K_2 \subset \cdots$$

Let  $L$  be the union of the  $K_n$ . Then  $L$  is a field, since if  $\alpha, \beta \in L$ , then  $\alpha, \beta \in K_n$  for some  $n$ , hence  $\alpha \pm \beta$ ,  $\alpha\beta$  and  $\alpha/\beta$  for  $\beta \neq 0$  all lie in  $K_n$ , hence lie in  $L$ . The field axioms with respect to this addition and multiplication are easily checked. Finally, if  $f \in L[X]$  is a polynomial, then all the coefficients of  $f$  lie in some  $K_n$ , hence  $f$  has a root in  $K_{n+1}$ , hence has a root in  $L$ .  $\square$

In fact, every polynomial over  $K$  splits already over  $K_1$ . For, let  $f \in K[X]$  be irreducible, let  $M/K_1$  be its splitting field extension over  $K_1$ , and let  $L \subset M$  be the splitting field extension of  $f$  over  $K$ .

Suppose first that  $\text{char } K = 0$ . Then  $L/K$  is separable, so simple by the Primitive Element Theorem. Hence  $L = K(\alpha)$  for some  $\alpha$ . Let  $m$  be the minimal polynomial of  $\alpha$  over  $K$ . Then  $m$  has a root  $\alpha'$  in  $K_1$  by construction, and  $L = K(\alpha) = K(\alpha') \subset K_1$ . Since  $f$  splits over  $L$ , we see that  $f$  splits over  $K_1$ .

Now suppose that  $\text{char } K = p > 0$ . From our discussion on separability, we know that  $f(X) = g(X^{p^r})$  for some  $r$ , where  $p = \text{char } K$  and  $g \in K[X]$  is separable and irreducible. Let  $G$  be the Galois group of  $L/K$  and let  $E$  be the fixed field of  $G$ . We note that  $E = K$  if and only if  $L/K$  is separable, which is if and only if  $f = g$ , or equivalently  $r = 0$ . Then  $L/E$  is Galois, so simple by the Primitive Element Theorem, say with  $L = E(\alpha)$ . On the other hand, for each element  $\beta \in E$  we have  $\beta^{p^s} \in K$  for some  $s$ , so that  $\beta$  is *purely* inseparable over  $K$  with minimal polynomial  $X^{p^s} - \beta^{p^s}$ .

To prove this, let  $m_\beta$  be the minimal polynomial of  $\beta$  over  $K$ , and let  $\beta'$  be any other root of  $m_\beta$  in  $L$ . Thus one has a  $K$ -embedding  $K(\beta) \rightarrow L$  sending  $\beta \mapsto \beta'$ . Since  $L/K$  is normal, this extends to an automorphism of  $L$ , so lies in  $G$ . We know, however, that  $G$  fixes every element of  $E$ , so in particular fixes  $\beta$ . Thus  $\beta' = \beta$  and  $m_\beta$  has a unique root. By our discussion on separable polynomials,  $m_\beta(X) = n_\beta(X^{p^s})$  for some  $s$ , where  $n_\beta$  is separable and irreducible. Since  $m_\beta$  has the unique root  $\beta$ , we must have that  $n_\beta$  is linear, whence  $s = \deg m_\beta$  and  $m_\beta = X^{p^s} - \beta^{p^s}$  as required.

Let  $\beta_1, \dots, \beta_n$  be generators for  $E/K$ . Then  $L = K(\alpha, \beta_1, \dots, \beta_n)$ . Let  $m$  be the minimal polynomial of  $\alpha$  over  $K$ , and let  $m_i$  be the minimal polynomial of  $\beta_i$  over  $K$ . Now each  $m_i$  has a root in  $K_1$ , and since  $\beta_i$  is the only root of  $m_i$ , we have  $\beta_i \in K_1$ . In particular,  $E \subset K_1$ . Similarly,  $m$  has a root  $\alpha' \in K_1$ , and so  $L = E(\alpha) = E(\alpha') \subset K_1$ . Thus  $f$  splits over  $K_1$ .

Now, it is clear that  $K_1/K$  is algebraic, and similarly  $K_2/K_1$  is algebraic, so that  $K_2/K$  is also algebraic. Let  $f \in K_1[X]$  be an irreducible polynomial, and let  $\alpha \in K_2$  be a root of  $f$ . Since  $\alpha$  is algebraic over  $K$ , it has minimal polynomial  $m \in K[X]$ , which we have just shown splits over  $K_1$ . Thus  $\alpha \in K_1$ , so that  $K_2 = K_1$ . Therefore  $K_1$  is algebraically closed. Since  $K_1/K$  is algebraic, we deduce that  $K_1/K$  is an algebraic closure of  $K$ .

**Theorem C.2.** *Let  $L/K$  be algebraic and  $\iota: K \rightarrow M$  an embedding with  $M$  algebraically closed. Then we can extend  $\iota$  to an embedding  $\sigma: L \rightarrow M$ .*

*Proof.* We wish to extend  $\iota$  to an embedding  $\sigma: L \rightarrow M$ . We again appeal to

Zorn's Lemma.

Let  $S$  denote the set of all pairs  $(F, \tau)$  such that  $L/F/K$  and  $\tau: F \rightarrow M$  is an embedding extending  $\iota$ . We endow  $S$  with a partial order by setting  $(E, \rho) \leq (F, \tau)$  if  $F/E$  and  $\tau$  extends  $\rho$ . Clearly  $S$  is non-empty, since it contains  $(K, \iota)$ . Moreover, every chain has an upper bound. For, if  $\{(F_i, \tau_i)\}$  is a totally ordered subset, then  $F := \bigcup_i F_i$  is a subfield of  $L$  containing  $K$ , and we can define  $\tau: F \rightarrow M$  by setting  $\tau(\alpha) = \tau_i(\alpha)$  for any  $i$  such that  $\alpha \in F_i$ . Then  $(F, \tau)$  is an upper bound for the chain  $\{(F_i, \tau_i)\}$ .

By Zorn's Lemma,  $S$  contains a maximal element  $(F, \sigma)$ . We claim that  $F = L$ . Otherwise, let  $\alpha \in L \setminus F$ . Then  $\alpha$  is algebraic over  $F$ , say with minimal polynomial  $m$ . Now  $\sigma(m) \in \sigma(F)[X]$  has a root  $\alpha' \in M$  since  $M$  is algebraically closed. Therefore, by **Artin's Extension Theorem**, we can extend  $\sigma$  to an embedding  $\tau: F(\alpha) \rightarrow M$  via  $\alpha \mapsto \alpha'$ . Thus  $(F, \sigma) < (F(\alpha), \tau)$ , contradicting the maximality of  $(F, \sigma)$ . Therefore  $F = L$  and there exists an embedding  $\sigma: L \rightarrow M$  extending  $\iota$ .  $\square$

**Theorem C.3** (Existence and Uniqueness of Algebraic Closure). *Let  $K$  be a field. Then there exists a field extension  $L/K$  such that  $L/K$  is algebraic and  $L$  is algebraically closed. Moreover,  $L$  is unique up to isomorphism. We call  $L$  the algebraic closure of  $K$  and denote it by  $\overline{K}$ .*

*Proof.* Let  $M/K$  be a field extension with  $M$  algebraically closed. Let  $L = M^{\text{alg}/K}$  be the subfield of those elements algebraic over  $K$ . We already know that  $L/K$  is algebraic, and we claim that  $L$  is algebraically closed.

Let  $f \in L[X]$  be a non-constant polynomial. Since  $M$  is algebraically closed,  $f$  has a root  $\alpha \in M$ . Since  $\alpha$  satisfies a polynomial  $f \in L[X]$ , it is algebraic over  $L$ . Since  $L/K$  is algebraic, **Theorem 3.10** tells us that  $L(\alpha)/K$  is algebraic, whence  $\alpha$  is algebraic over  $K$ . Thus  $\alpha \in L$  and  $L$  is algebraically closed.

Suppose now that  $\iota: K \rightarrow K'$  is an isomorphism and that  $L/K$  and  $L'/K'$  are algebraic with both  $L$  and  $L'$  algebraically closed. We wish to show that we can extend  $\iota$  to an isomorphism  $\tilde{\iota}: L \rightarrow L'$ . By the theorem, we have an embedding  $\tilde{\iota}: L \rightarrow L'$  extending  $\iota$  and an embedding  $\sigma: L' \rightarrow L$  extending  $\iota^{-1}$ . Consider  $\sigma\tilde{\iota}: L \rightarrow L$ . This is an extension of  $\iota^{-1}\iota = \text{id}: K \rightarrow K$ , so by **Proposition 4.5** it is an automorphism. Similarly  $\tilde{\iota}\sigma: L' \rightarrow L'$  is an automorphism, so that  $\tilde{\iota}: L \rightarrow M$  is an isomorphism.  $\square$

We can apply this to the rational numbers to obtain the following result.

**Corollary C.4.** *The algebraic closure  $\overline{\mathbb{Q}}$  of  $\mathbb{Q}$  is isomorphic to the subfield  $\mathbb{C}^{\text{alg}/\mathbb{Q}}$  of  $\mathbb{C}$ .*

Still to be done: We similarly obtain the splitting field extension of any subset  $S \subset K[X]$ . For  $S$  finite this is in the main text. For  $S = K[X]$  this gives the algebraic closure. In this way, many results in the text extend from finite to algebraic.